

METHOD OF IMPLEMENTING NEAR FIELD COMMUNICATION (NFC) APPLICATIONS WITH NON-NFC MOBILE DEVICE AND SYSTEM THEREOF

Background

5 **Technical Field**

Embodiments of the present invention relate to Near Field Communication (NFC) system using mobile device and, secured authentication and storage, and more particularly to using existing non-NFC mobile devices as front end interaction with customised Wi-Fi readers.

10

Description of Related Art

Most current Near Field Communication applications are in the areas of access control, personal identification, payment, electronic ticketing, portable file, and product identification. These applications are used in diverse fields, e.g. public transport, parking, company badges, passports, university cards, car rental, driver licenses, loyalty cards, road toll, car wash, copy machines, vending machines, medical data storage, container identification, stock administration and many more.

At present, most of the payment applications use contact (ISO 7816), contactless (ISO 14443) smartcards or dual interface cards. These cards are robust, have extended lifetime, are built with high security against fraud and manipulation, have reduced maintenance costs and are user friendly.

Most contactless cards used in these applications are ISO 14443 microprocessor cards which have built-in anticollision feature which allows selection of one card out of two or more cards presented at a reader to ensure that later cards entering into the detection field will not interfere with the current communication. These cards generally support authentication techniques according to security standards specified by ISO 9798-2.

30

In 2004, the NFC Forum was formed and since then the NFC Forum has moved on to establish technologies for NFC applications. Successful trials have been performed using dedicated NFC phones with SWP (Single Wire Protocol) NFC Subscriber Identity modules (SIM). However, there are several issues which have delayed the adoption of this technology. One of the reasons is the delay in the mass availability of dedicated NFC handsets. Another reason is the need for additional system to manage the allocation of space in the SIM to different vendors, loading applications and related secured keys, etc, to manage the overall security.

In view of the above and other problems, an improved system and method for near field communication applications is highly desired.

Summary of the Invention

Embodiments of the invention allow existing non-NFC dedicated mobile devices to be appropriately configured for facilitating NFC applications and transactions. This is particularly advantageous in that the users do not have to replace their existing mobile devices in order to gain access to NFC applications. Further, the configuration steps disclosed by the invention are convenient and user-friendly.

According to one embodiment of the invention, a method of implementing near field communication (NFC) applications using non-NFC mobile device, comprises: installing a transport layer into a memory storage of a non-NFC mobile device; installing a selected transaction application into a secured memory which is electrically coupled to the mobile device, the selected transaction application is adapted to process a predefined transaction upon receiving a command from the mobile device or a Wi-Fi reader; detecting a presence of the Wi-Fi reader when the mobile device enters a detection zone of the Wi-Fi reader and establishing a connection between the mobile device and the Wi-Fi reader; using the transport layer, detecting a signal of at least a predetermined strength emitted from the reader, and upon successful detection, cross authenticating the mobile device and the Wi-Fi reader; and processing the predefined transaction according to the selected transaction application by passing transaction data between the mobile device and a transaction terminal through both the transport layer and the Wi-Fi reader which is electrically coupled with the transaction terminal.

According to another embodiment of the invention, a system of implementing near field communication (NFC) applications using non-NFC mobile device, comprises: a Wi-Fi reader which is electrically coupled with a transaction terminal; a non-NFC mobile device including: a secured memory having an application storage area for storing at least one transaction application which is adapted to process a predefined transaction upon receiving a command from the mobile device or the Wi-Fi reader; a memory storage installed with a transport layer application; a processor for operating the mobile device including operation of the transport layer application, wherein the transport layer application is adapted to detect a signal of at least a predetermined strength emitted from the Wi-Fi reader, and upon successful detection, the transport layer application is adapted to cross authenticate the mobile device and the Wi-Fi reader, and to process the predefined transaction by passing transaction data between the mobile device and the transaction terminal.

Brief Description of the Drawings

Embodiments of the present invention will be further described by way of non-limitative examples, with reference to the accompanying drawings in which:-

Figure 1 is an overview of a system of implementing NFC applications with non-NFC mobile devices according to one embodiment of the invention;

Figure 2 is a block diagram of a secured memory of a non-NFC mobile device;

Figure 3 is a flow sequence for configuring a non-NFC mobile device;

Figure 4 is a flow sequence for initialising the mobile device;

Figure 5 is a flow sequence for personalising transaction application-related secret and data keys; and

Figure 6 is a flow sequence of using the initialised and personalised mobile device to perform a transaction.

Detailed Description

In the following description, numerous specific details are set forth in order to provide a thorough understanding of various illustrative embodiments of the invention.

It will be understood, however, to one skilled in the art, that embodiments of the invention may be practiced without some or all of these specific details. In other instances, well known process operations have not been described in detail in order not to unnecessarily obscure pertinent aspects of embodiments being described. In the drawings, like reference numerals refer to same or similar functionalities or features throughout the several views.

Reference is made to Figure 1 which illustrates a system of implementing NFC applications with non-NFC mobile devices.

According to a first aspect of the invention, there is provided a Wi-Fi reader 14 which functions like a standard Wi-Fi router or access point. The Wi-Fi reader 14 complies with IEEE 802.11n/g/b, supports Wireless speed up to 150Mbps, and is compatible with 2.4GHz Wi-Fi devices. The Wi-Fi reader 14 also supports WEP, WPA/WPA2, WPA-PSK/WPA2-PSK encryptions, and TCP/IP protocol. The Wi-Fi reader 14 may have a signal range of up to about 100 cm, and other suitable signal ranges are possible.

According to a second aspect of the invention, there is an Application Programming Interface (API) for providing a communication interface between the Wi-Fi reader 14 and an industry standard terminal or transaction terminal 16 for processing a transaction, e.g. payment. In use, the API allows data transfer between the Wi-Fi reader 14 and terminal 16 for facilitating a transaction.

According to a third aspect of the invention, there is provided a secured memory 20 electrically coupled to a mobile device 12. The secured memory 20 may be provided as a Subscriber Identity Module (SIM) or any other data storage means adapted to store secured data and information.

According to a fourth aspect of the invention, there is provided an update application residing in the secured memory 20 adapted to update a respective part of the secured memory 20 to store or delete application or security information (e.g. keys and data) based on a command received from the mobile device 12 or Wi-Fi reader 14 and to return a result code to the mobile device 12 or Wi-Fi reader 14.

According to a fifth aspect of the invention, there is provided at least a transaction application residing in the secured memory 20. The transaction application is adapted to execute a predefined transaction, including updating and storing data in specific parts of the secured memory 20. The transaction application will be executed upon receiving an appropriate command from the mobile device 12 or Wi-Fi reader 14.

According to a sixth aspect of the invention, there is provided a transport layer application, provided as computer-executable instructions, for facilitating NFC applications. The transport layer application resides in a memory of the mobile device 12 and is adapted to ascertain or analyse signal strength from the Wi-Fi reader 14, connect to a predefined Service Set Identifier (SSID) residing in the secured memory 20. When a signal of a predefined strength is detected, a connection between the mobile device 12 and the Wi-Fi reader 14 is established; the transport layer application then cross authenticates the mobile device 12 with the Wi-Fi reader 14. The transport layer application is also adapted to communicate and transfer requests, responses and data between the mobile device 12 and Wi-Fi reader 14. The transport layer application is further adapted to transfer data in accordance with the fourth and fifth aspects of the invention as described above.

Reference is made to Figure 2 which is a block diagram of a secured memory 20 of a mobile device 12. The secured memory 20 may be provided as a SIM or any memory storage adapted to be used or integrated with the mobile device 12.

The secured memory 20 may include three separate areas, as follows:

- (a) Application storage area. This part of the memory may be reserved for storing transaction applications for processing a predefined transaction such as mandatory key update application and optional payment, electronic ticketing, identification, electronic-purse, etc. In the present disclosure, the term "transaction" is not restricted to payment-based transfers; it refers to transmission and processing of data and/or an act of obtaining and paying for an item or service.
- (b) Secured data storage area. This part of the memory may store mandatory transport and transaction application key as well as other mandatory and optional application data storage.

(c) Data update plug-in or module. This part of the memory is utilised when any transaction application needs to update any data. Mandatory and optional data can only be operated upon by this plug-in. The data update plug-in ensures the required security and access control for the actual data.

In addition to the secured memory, a mobile device 12 may also include a processor for operating the mobile device 12 including operation of the transport layer application, a display screen for displaying notification, a user interface with input means and output means, and other components as known in the art.

Reference is made to Figure 3 which illustrates a flow sequence 300 for configuring a mobile device 12 for NFC applications.

The flow sequence 300 is performed when a user wishes to use an existing, non-NFC mobile device 12 for NFC applications. The flow sequence 300 begins with loading/installing a transport layer for NFC applications into a memory storage of a non-NFC mobile device 12 (block 302). The transport layer may be made available on a public source, e.g. App StoreSM for iPhone® device, Android Market or Google Play for Android™ mobile devices 12. In use, the transport layer is adapted to connect the mobile device 12 to a Wi-Fi reader 14, detect whether the mobile device 12 is within a predefined connection zone 18b, e.g. 10 cm, of the reader 14 by analysing the strength of a signal from the Wi-Fi reader 14, and transport data between mobile device 12 and the Wi-Fi reader 14. Thereafter, the flow sequence 300 proceeds with formatting the secured memory 20 of the mobile device 12, and loading/installing of key update application and data update plug-in into the secured memory 20 (block 304). Also, the sequence proceeds with loading/installing required transport keys and any other data into a key storage area (in secured data storage area) of the secured memory 20 via key update application (block 306). The above-described sequence may be performed via Wi-Fi, over-the-air programming (OTA) (using ISO 11.14) or through the Wi-Fi reader 14.

Reference is made to Figure 4 which illustrates a flow sequence 400 for initialising the mobile device 12 after the flow sequence 300 of Figure 3 has taken place. The flow sequence 400 begins with selecting one or more preferred transaction applications from a database of transaction applications depending on the type of transactions required (block 402), and then loading/installing the associated transaction application modules into the application storage area of the secured memory 20 (block 404). This may be performed via Wi-Fi, OTA (using ISO 11.14) or through the Wi-Fi reader 14.

At this stage, the transaction application module is dormant and is not usable until personalisation of the transaction application is completed. Reference is made to Figure 5 which illustrates a flow sequence 500 for personalising the transaction application module by loading/installing the application's specific required keys, secrets and data via over-the-air programming (using ISO 11.14) or reader 14 using transport keys. Particularly, the flow sequence 500 begins with loading/installing a transaction application-related secret key, using transport keys, into the secured data storage area (block 502). Thereafter, the flow sequence 500 proceeds to load/install a transaction application-related data key, using the transaction application-related secret key, into the secured data storage area (block 504).

Reference is made to Figure 6 which illustrates a flow sequence 600 for using the initialised and personalised mobile device 12 to perform a transaction.

The flow sequence 600 begins with a user bringing his mobile device 12 into proximity of a Wi-Fi reader 14 which is electrically coupled to an industry terminal 16 for processing transactions, e.g. payment (block 602). The terminal 16 and/or Wi-Fi reader 14 may follow predefined anticollision rules which allow the terminal 16 and/or reader 14 to select one mobile device 12 out of two or more mobile devices present at a reader 14 and to ensure that later mobile devices entering the detection field will not interfere with the current communication with a mobile device 12.

When the mobile device 12 enters a predefined detection zone 18a, e.g. within a predefined short range of the Wi-Fi reader 14, the mobile device 12 detects the Wi-Fi reader 14 with predefined Service Set Identifier (SSID) stored in its secured data

storage (block 604). The mobile device 12 may then establish a connection with the Wi-Fi reader 14 (block 606) using the security option stored in the secured memory 20, according to standard IEEE 802.11n/g/b connection procedures. When the transport layer of the mobile device 12 detects a signal of at least a predefined strength, which is emitted from the Wi-Fi reader 14, cross authentication procedures, e.g. similar to ISO 9798-2 standards, are performed between the mobile device 12 and the terminal 16 via the reader 14 (block 608). Typically, a detected signal from the Wi-Fi reader reaches at least the predefined strength when mobile device 12 enters a predefined connection zone 18b, e.g. 10 cm from the Wi-Fi reader 14. After cross authentication is successfully performed, transaction procedures e.g. payment, identification, may be initiated by the terminal 16 and the predefined transaction is processed with the mobile device 12 (block 610). The stream cipher method or any other suitable methods may be used for data or information transfer between the mobile device 12 and Wi-Fi reader 14. Depending on the transaction nature, the user might be prompted to endorse certain actions, e.g. payment-type actions, before the predefined transaction is processed. During the transaction, if required, the mobile device 12 may provide transaction status, e.g. in code form, to the terminal 16. After completion of the transaction, the mobile device 12 may provide a completion code which indicates a successful or unsuccessful transaction, and any errors (block 612). Depending on the transaction application and on the completion code, an appropriate message may be displayed on the mobile device 12 by the transaction application. After the transaction is completed, the reader 14 may terminate the earlier-established connection with the mobile device 12 (block 614).

Example: Toll Payment Application

Embodiments of the invention may be applied to toll payment and one example is described below. In a Toll Payment application, standard industry toll payment terminals 16 are installed at toll stations along certain locations on a motor highway. A user with a non-NFC mobile device 12, e.g. Android phone, wants to use his phone to process toll payment at the toll stations. The Toll Operator should have a tie-up with the Telecommunication Operator of the user.

Preparation:

The user first obtains a specially-designated SIM card which will provide the secured memory 20. The SIM card may be loaded with a diversified transport key which is generated by diversifying a secret master key known to the Toll Operator and a unique number related to this SIM card such as but not limited to its unique serial number, i.e. Integrated Circuit Card Identifier (ICCID).

Initialisation:

The user logs on to a database hosting various transaction applications, e.g. Android Market or Google Play for Android™ mobile devices 12, to select an associated Toll Payment Application which is then downloaded and installed. During installation, the transport layer associated with the Toll Payment Application is installed in a memory storage of the mobile device 12 and the Toll Payment Application is installed in the secured memory 20, particularly in the applications storage area.

Personalisation:

The Toll Operator may now send the actual diversified operation keys and data encrypted with the diversified transport key applicable to this mobile device 12 using OTA service from the Telecommunication Operator. When the mobile device 12 receives these OTA 11.14 messages, it calls the Data update plug-in with the specific data. The Data update plug-in decrypts the message using the diversified transport key from key storage and stores the keys to specific locations in key storage. The Data update plug-in stores the Toll data, electronic-purse data, SSID, and the security key and type related to IEEE 802.11n/g/b in Toll data storage. The mobile device 12 is now ready to use with Toll Payment Application via NFC.

Separately, customised Wi-Fi readers 14 at the Toll Stations may be integrated with industry payment terminals 16 using API provided by the manufacturer of the readers 14.

Usage:

When a user reaches a Toll Station, he activates the Toll Payment Application in his mobile device 12 and brings his mobile device 12 into proximity with the reader 14. The mobile device 12 processor retrieves the SSID that was personalised for toll

operation from the secured memory 20. When the mobile device 12 is within a detection zone 18a of the reader 14, the mobile device 12 detects the reader 14 with the correct SSID and establishes a connection with the reader 14 using the security option stored in the secured memory 20. This is the standard IEEE 802.11n/g/b connection procedure.

The transport layer may now proceed to analyse signal strength from the Wi-Fi reader 14. When the mobile device 12 is within a connection zone 18b, e.g. 10 cm, of the reader 14, a signal from the Wi-Fi reader 14 which is at least of a predefined strength is detected by the transport layer. Upon detection of the reader 14 in proximity within the connection zone 18b, the Toll Payment Application is activated to commence cross-authentication. Meanwhile, data transfer between the Wi-Fi reader 14 and the mobile device 12 may be passed through the transport layer. During cross authentication, the Toll Payment Application performs cross authentication with the terminal 16 using the application keys from key storage area via transport layer. Once the cross authentication is completed, the terminal 16 sends the required debit command to the Toll Payment Application. The Toll Payment Application will check the current balance of the user's electronic purse and if the user's current balance allows for debit of the toll amount, a prompt may be presented on the mobile device 12 screen to request an authorisation from the user to proceed with debiting the Toll amount. After the user inputs his authorisation to proceed with the debit, the Toll Payment Application processes the debit command in the electronic purse and passes the required transaction details via the transport layer and the reader 14 to the terminal 16 at the Toll Station. Upon completion of the transaction, the Toll Payment Application informs the user the transaction outcome such as by an appropriate notification on the mobile device 12 screen. Also, upon completion of the transaction, the Toll Payment Application may be closed by the user and the connection between the reader 14 and the mobile device 12 will be terminated.

Embodiments of the invention allow existing non-NFC mobile devices, including mobile phones, smartphones, tablets, portable digital assistants, etc, to be used in NFC applications without the need for users to change to dedicated NFC-enabled mobile devices.

Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the invention. Furthermore, certain terminology has been used for the purposes of descriptive clarity, and not to limit the disclosed embodiments of the invention. The embodiments and features described above should be considered exemplary, with the invention being defined by the appended claims.

10

15

20

25

What is claimed is:

1. A method of implementing near field communication (NFC) applications using non-NFC mobile device, the method comprising:

installing a transport layer into a memory storage of a non-NFC mobile device;

installing a selected transaction application into a secured memory which is electrically coupled to the mobile device, the selected transaction application is adapted to process a predefined transaction upon receiving a command from the mobile device or a Wi-Fi reader;

detecting a presence of the Wi-Fi reader when the mobile device enters a detection zone of the Wi-Fi reader and establishing a connection between the mobile device and the Wi-Fi reader;

using the transport layer, detecting a signal of at least a predetermined strength emitted from the reader, and upon successful detection, cross authenticating the mobile device and the Wi-Fi reader; and

processing the predefined transaction according to the selected transaction application by passing transaction data between the mobile device and a transaction terminal through both the transport layer and the Wi-Fi reader which is electrically coupled with the transaction terminal.

2. The method of claim 1, wherein the detection zone is up to 100 cm.

3. The method of claim 1, wherein the detecting the signal of the predetermined strength takes place when the Wi-Fi reader is within 10 cm from the mobile device.

4. The method of claim 1, further comprising: after installing a transport layer into a memory storage of a non-NFC mobile device, installing a key update application and a data update plug-in into the secured memory.

5. The method of claim 4, further comprising: installing a transport key into the secured memory via the key update application.

6. A system of implementing near field communication (NFC) applications using non-NFC mobile device, the system comprising:

a Wi-Fi reader which is electrically coupled with a transaction terminal;

a non-NFC mobile device including:

- 5 a secured memory having an application storage area for storing at least one transaction application which is adapted to process a predefined transaction upon receiving a command from the mobile device or the Wi-Fi reader;

a memory storage installed with a transport layer;

- 10 a processor for operating the mobile device including operation of the transport layer,

wherein the transport layer is adapted to detect a signal of at least a predetermined strength emitted from the Wi-Fi reader, and upon successful detection, the transport layer is adapted to cross authenticate the mobile device and the Wi-Fi reader, and to process the predefined transaction by passing transaction data between the mobile device and the transaction terminal.

15

7. The system of claim 6, wherein the transport layer is adapted to detect a signal of at least a predetermined strength emitted from the Wi-Fi reader when the Wi-Fi reader is within 10 cm from the mobile device.

- 20 8. The system of claim 6, wherein the secured memory is installed with a key update application and a data update plug-in into the secured memory.

9. The system of claim 8, wherein the secured memory is installed with a transport key via the key update application.

25