Inside NFC: secure payment technology

Inside NFC: secure payment technology

NFC (near field communications) is based on RFID (radio frequency identification) technology. There are many ways to use this NFC technology. For example peer to peer mode where two devices can exchange data (business card sharing), reader and writer mode (reading NFC enable smart poster) and card emulation mode (phone act as our credit card).

In this article we are going to focus on card emulation mode to give a generic overview how this technology works and what are the components/units involved for the complete echo system.

Why contactless payment is necessary

The RF-based contactless payment devices are easy to use; consumers like the increased speed, control of transactions and using the devices instead of cash.

- Contactless payments replacing cash
- Contactless payments are fast and convenient
- Contactless payments are safe and secure

To realize and satisfy the above requirement we need to emulate our phone just like smart card. Multiple NFC applications must be supported with mobile devices. This includes, but are not limited to, credit/debit payment, public transport ticketing, and loyalty and service initiation (through tag reading). The focus of the document will be solely on those aspects of the handset that involves supporting mobile NFC services based on the use of the Universal Integrated Circuit Card (UICC) as the secure element (SE).

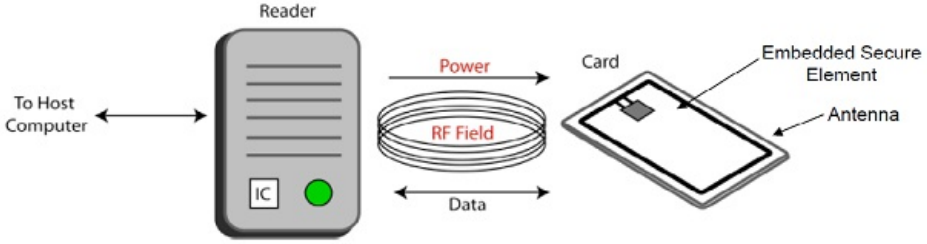
In Card Emulation mode, the NFC device appears to an external reader much the same as a traditional contactless smart card. Mobile users don't need to carry multiple cards. This card can be generalized to any kinds of cards where secured data is stored, for example personal identification number with social security code. That means it replaces usage of smart cards and our NFC enabled device act like smart cards. Contactless payments are thought to be the most important card payment innovation in the last decade. With investments by the card associations and early adoption on the part of major card issuers and top-branded merchants contactless payments are already in the hands of millions of consumers and in the checkout lane of thousands of merchants.
Following figure shows the important use case.

• A framework or echo system to build ticketing and payment services
o I swipe my phone to travel to a check point
o I swap my phone to pay at point of sales
o No cash, no paper receipts, electronic receipts, simple, quick and convenient

Existing contactless smart card

A contactless smart card is any pocket-sized card with embedded integrated circuits that can process and store data, and communicate with a terminal via radio waves. Contactless smart cards can be used for identification, authentication, and data storage. They also provide a means of effecting business transactions in a flexible, secure, standard way with minimal human intervention. Smart card has a microprocessor or memory chip embedded in it that and coupled with a reader it has the processing power to serve many different applications. Following figure shows a separate contactless smart card with reader. In NFC card emulation mode, mobile phone will work just like this card with the additional benefits that we don't need to carry extra cards.

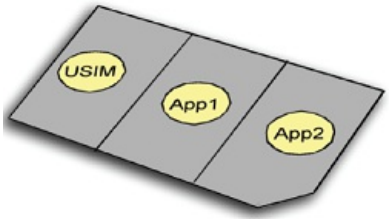
(C) Copyright Nokia 2014. All rights reserved.



• The contactless smart card is the driving element for embedded smart card solutions
• The existence of multi-application contactless smartcard is a precursor to multiple smartcard resident in mobile device on a single secure element
• Infrastructure is on the reader side, as well as the bridge to the OTA (over the air) manage a smartcard in a mobile will drive the use cases accordingly

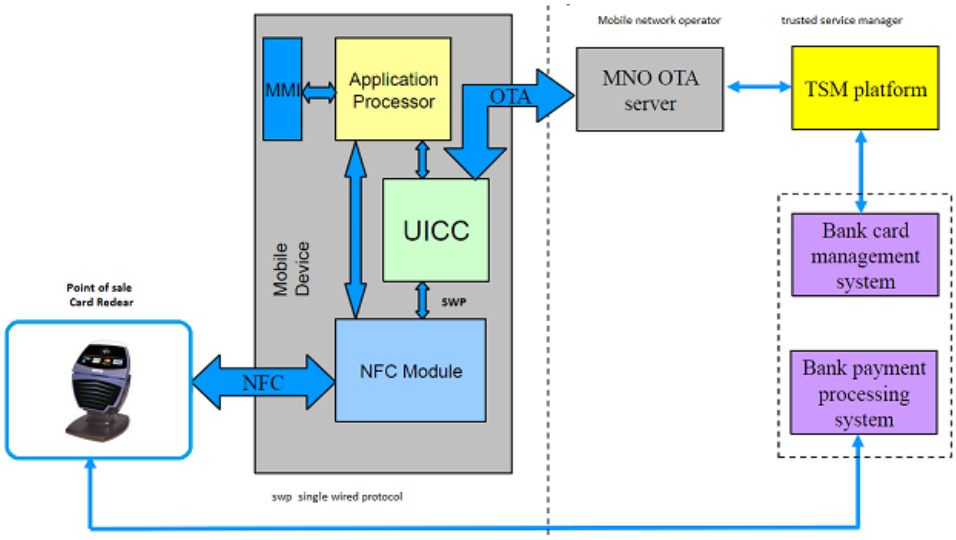
How NFC card emulation mode works

In general, MNO (mobile network operator) issues SIM (subscriber identification module) card to mobile user where personal identity and application (such as contact application) are stored. Multiple contactless application can be stored in this card (updated from conventional SIM) for each use cases. This card works as secured element that stores and execute the contactless applications. UICC (Universal Integrated Circuit Card) cards are the evolution of SIM cards. Like SIMs, they go in our phone, have an application that stores our contacts, let our network identify who we are, and work with any network in the world. However UICC cards can run more than one application.



Multiple applications run in single UICC (NFC SIM card) card.

Following diagram shows the complete echo system those are involved in end to end system.



More than one credit or debit card can be stored in the same UICC, increasing the convenience of PBM (Pay Buy Mobile) to the consumer. In use, data transferred by NFC from the handset (actually from the UICC) to the reader is communicated to financial organizations using the same secure process as used for conventional credit or debit card transactions. One of the hottest topic with regard to NFC are SWP (Single Wire Protocol) enabled UICCs. Whereas several handset manufacturers such as Nokia can equip its phones (some series 40, and some coming Symbian devices) those are capable to communicate with embedded secure element. The SWP connects the UICC to the NFC Modem through a single wire and thus adds contactless functionality to the UICC (SIM.

Security is a key consideration with NFC. Retail and transit payments with a mobile phone require wireless carriers, retailers, transport providers and banks to all work together. All of the transaction and payment card accounts information need to be kept secure and apart. For this reason, NFC requires the use of a "secure element." The UICC is the preferred technology for the secure element that stores subscriber details – such as credit card account numbers, transit accounts, and mobile phone details –

(C) Copyright Nokia 2014. All rights reserved.

and keeps these details separate and secure. To enable proximity payments, secure element capable of authenticating itself to a bank, and resistant to physical or logical attack. Contactless frontend interface standardized by ETSI to connect a UICC to a contactless frontend to pass data from UICC to card reader via NFC where the payment is processed by other echo system members. Data is communicated between UICC and NFC module with SWP which was developed to support the use of contactless payment applications running on UICCs – it enables the payment application on the UICC to communicate with contactless readers via the NFC interface of the handset. The standard is approved by ETSI November 2007.

Let's take an example of micro payment application "NFC Wallet" consists of several parts. The first one - and the only one that is actually recognized by the user – is the applications running on the device. This part provides the user with a GUI (graphical user interface) and allows him/her to recharge the wallet over the air and view the amount of money available on the handset. To recharge the wallet, the application is able to establish a GPRS connection to a transaction server located at the mobile network operator's supported bank for example. The transaction server accepts the incoming connection from the NFC handset. The authentication of the device is done thru a solution of the mobile network operator. The server checks the balance of the account of the customer and then sends the money (encrypted) back to the handset. There the money is directly stored in the secure element.

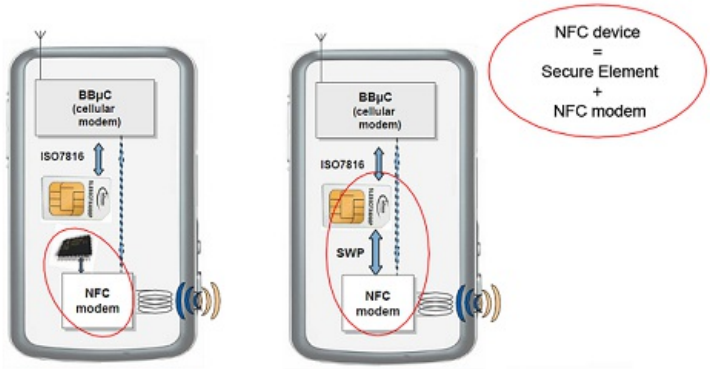
Another example could be using credit card application (see the previous figure). User select the application in device (may needs to give password), he/she touches the NFC reader (at point of sales), the reader gets the user's credit card details from the UICC via NFC and pass it to process with conventional ways and in return user get an electronic receipt that can be stored in device.

Different ways to realize secure element

There are several kinds of implementation of secure element implementation already in market.

- SIM Based (mobile network operator centric approach) where the secured application runs in UICC and UICC is connected with SWP. With this approaches operator can updates and controls device over the air services, see the following figure.
- Embedded in Mobile Phone (handset manufacturer centric approach),

following figure shows two kinds of devices SIM based secure element and device based secure element. Device manufactured are responsible for updating the firmware and MNO has little or no control over it.

- 

- Removable Secure Element (SD Card)

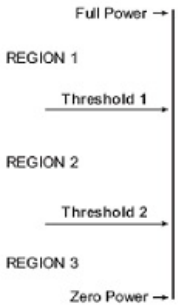
In this approaches the secured application is stored in SD card.

Power Management during secure transaction

When the device goes to low power mode that is handled by the power management specification. The regions are defined as follows:

- Region 1 (Full Power to Threshold 1): all functions are available in the mobile device;
- Region 2 (Threshold 1 to Threshold 2): all the functionalities of the mobile phone are shut down, except the clock module and a few other remaining functions, where NFC functionalities are still available.
- Region 3 (Threshold 2 to Zero Power): No functions are available in the mobile device.

(C) Copyright Nokia 2014. All rights reserved.



References

- http://www.nfc-forum.org/specs/
- http://www.gsmworld.com/our-work/mobile_lifestyle/mobile_money/pay_buy_mobile/
- 081028 nfc_standards_payments Narada.pdf
- Mobile_Contactless_Payments_Service_Management_Roles_Reqs_Specs_V2.pdf
- Mobile_MasterCard_PayPass_SWP_Handset_Approval_Guide_v1-0.pdf
- reqs_swp_nfc_handsets_v2.pdf
- SIM-OTA-Mobile-Operator-role-NFC.pdf
- GSM Association: Requirements for SWP NFC Handsets reqs_swp_nfc_handsets_v2.pdf
- http://www.gemalto.com/companyinfo/download/smartcardforum.pdf
- gsma_pbm_white_paper_11_2007.pdf
- 2008_09_11_Cardis.pdf
- fonseca.pdf
- http://www.nfc-research.at/index.php?id=10

Additional Information

This document summarizes technical overview about NFC secure element (SE) and payment system.

It has accumulated NFC payment related public information to a single document to give an overview of related technology and information. If reader wants to get more information related to this he/she could consult with the references documents that has been mentioned in the references section. Since these are collection of public information, it is independent of Nokia's current or future implementation and technology and it does not reflect Nokia.

(C) Copyright Nokia 2014. All rights reserved.