



The role of SIM OTA and the Mobile Operator in the NFC environment

NFC, Near Field Communication, is a standards based communication technology that makes possible a new, expanded role for the mobile handset. The mobile handset becomes the subscriber's key for authorizing payments, accessing services and getting information from their immediate environment. This white paper describes the role of SIM OTA as a key enabler for applications based upon NFC.

Table of Contents

Executive Summary.....	1
Introduction	2
The SIM as a secure environment.....	3
The role of OTA.....	4
Opening up to third parties.....	6
Conclusion.....	8
About the author.....	9
Glossary.....	10
Further reading.....	11

Executive Summary

NFC introduces a new role for the mobile handset: as a device for interacting with a subscriber's immediate environment. With close-range contactless technology, we will use our handsets as credit cards, to access public transportation, open doors and many more applications.

NFC is a close proximity (within a few inches or centimeters), standards-based wireless connectivity technology that enables simple and safe two-way interactions among electronic devices. A chip in the handset performs the wireless communication. The display, keyboard, and the mobile network capability of the handset enables the implementation of a wide range of powerful applications with real user benefit and business cases behind..

To bring value to the NFC chip, applications are required to take advantage of the NFC functionality. To protect the consumer these must be securely deployed and managed regardless of where the subscriber is and the time of day. The UICC (also referred to as USIM) is a true secure environment for deploying these applications.

The SIM OTA platform used to manage UICC cards plays a key role with its secure communication capability allowing NFC applications to be dynamically provisioned and personalized to the user on the basis of new business needs and the interest of consumers. Only the creativity of application and business developers puts a limit on what can be implemented on this new platform.

SmartTrust endeavors to ensure that the information in this document is correct and fairly stated, but does not accept liability for any error or omission. The development of SmartTrust products and services is continuous and published information may not be up to date. It is important to check the current position with SmartTrust. This document is not part of a contract or license save insofar as may be expressly agreed. SmartTrust is a trademark of SmartTrust AB. All other trademarks are the property of their respective owners.

© SmartTrust April 2009. All rights reserved.

For more information about SmartTrust, please visit our web site at www.smarttrust.com

Introduction

Near Field Communication (NFC) is a wireless technology allowing two devices to communicate over a short distance of less than 10 cm. NFC is standardized internationally and defined in ISO/IEC 18092 and ECMA-340. The ubiquitous nature of mobile phones makes these the ideal device to place NFC chip technology.

Integrating NFC chips in mobile phones opens up a wide range of contactless applications. These applications can be deployed in the handset, in the UICC (Universal Integrated Circuit Card also known as USIM) or both. It is generally believed that the first NFC services to be deployed will be payment and ticketing, but the potential is much larger.

The space on the UICC can be effectively leased to companies wishing to provide services via NFC to subscribers. One example is the concept of an “electronic wallet”. Today’s wallet contains an innumerable quantity of plastic cards of different types. These all can be represented by NFC applications on the UICC. As well, loyalty cards, tickets, door lock systems, membership cards; in short any magnetic stripe card, chip card or access token carried on the person of a subscriber can be represented and implemented as an NFC application on the UICC.

The advantages of using the UICC are its personal nature, portability between mobile phones, inherent security and perhaps most importantly that the UICC is controlled by the issuing party; the handset is not.

Applications on the UICC may be resident when these are delivered from the UICC manufacturer, but in the long run this will not be sufficient. As with any application environment, there will be a need for adding new applications, deleting old ones, upgrading with new versions and providing applications with up-to-date data. This management requires an OTA platform. The mobile operator plays a key part here as they have the infrastructure in place already today for OTA management.

NFC applications resident on UICC can be quite powerful, but there can arise the need to provide a user interface. Examples of applications that would require a user interface are showing a transaction receipt for a vending machine purchase, status of service, list of credit / debit cards available for use, ticket bar code for entrance to events and confirmation of a monthly transport ticket purchase. As well, owners of the services empowered by the NFC cardlets will want to present their branding and identity to the subscriber.

NFC Applications may as well utilize the Smartcard Web Server (SCWS) framework. SCWS would provide the integration of handset and SIM functionality for the user interface.

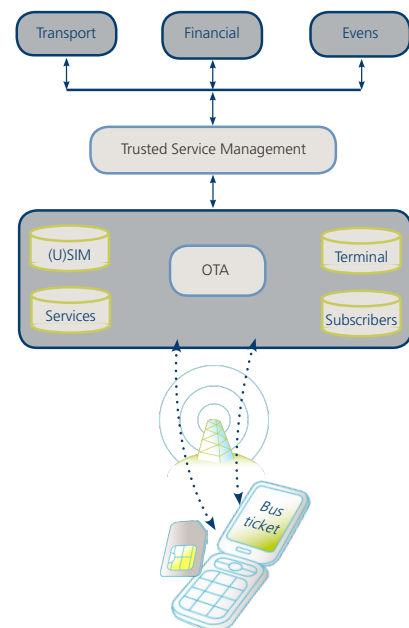
Downloading, upgrading and deleting NFC applications on a UICC card requires Remote Applet Management (RAM) functionality. However, an Applet may take many Short Messages (SMS) to download to the UICC. This becomes especially problematic for updating large batches of UICCs simultaneously. The use of a high-speed communications method such as BIP (Bearer Independent Protocol), that utilizes GPRS and UMTS data channels, is the preferred way of performing the card updates:

It is also possible to download NFC applications OTW (Over-The-Wire) via a point-of-sale terminal card reader in the shop where the subscription is sold. Ideally, a single SIM management system will be used for both OTW and OTA NFC application management.

Here follows a list of potential NFC applications that can be run on the UICC:

Potential NFC applications running on the UICC:

- Identity card for citizen services
- Transport card
- Payment Transaction authorization
- Micro-payments
- Credit / Debit card
- Loyalty card
- Service discovery
- Sending smart poster coupons to consumers
- Access control (Physical & Logical)
- Exchange of information M2M (Machine to Machine)
- Access digital content
- Electronic business card



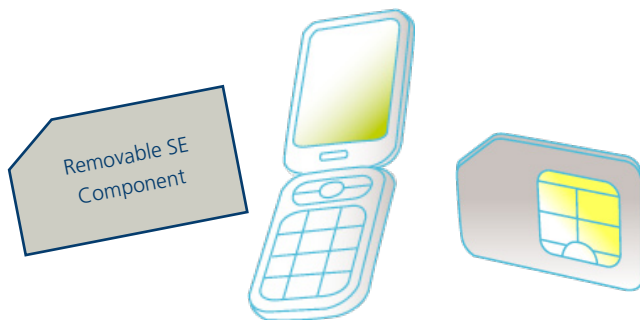
Overview of NFC environment with SIM OTA Management platform

The above diagram illustrates how the OTA platform makes possible management of the NFC applications for various service providers. The unique knowledge of the mobile operator about subscribers, the mobile devices (terminal & (U)SIM) makes possible personalized management and adaptation of the services to ensure the best possible fit to the individual. Mobile operators are well positioned to provide this service for NFC application service providers.

This white paper addresses the benefits of the UICC as a secure element, the advantages of OTA management for NFC and the advantages for third parties of mobile operator OTA management of their NFC applications.

The SIM as a secure environment

To be able to provide NFC based services that involve value for the subscriber and service provider both parties must be assured that the transaction takes place in a protected environment. This protection is achieved by use of a Secure Element (SE). The SE can be implemented in one of three methods: 1) on a separate removable SD (Secure Digital) card, 2) on a physically embedded (not removable) Smart Card in the terminal or 3) on the UICC. The UICC is the physical smart card that the Subscriber Identity Module (SIM or USIM) is implemented upon. The UICC is therefore commonly known as a SIM or USIM.



Three choices for the Secure Element (SE)

A removable SD card may seem to be an attractive option for the SE. Several factors complicate this choice. There is a lack of standardization for the management of removable SD cards making it difficult to effectively manage NFC applications deployed on the card. On top of this is the fact that no mass deployments of this method exist. A further degree of difficulty is added by a lack of an infrastructure for the distribution and management of this type of card. It would be quite impractical to have each NFC provider distribute their own removable card. The optimal solution for the consumer is to have one single SE uniquely tied to them.

Embedding the SE in the handset is good from the standpoint of standardized logistics. But as the SE should be personal, the consumer must have their new SE registered and personalized after they buy a new terminal. As well, it will be more than likely that they need to de-activate the SE of the old terminal.

Implementing the SE using the UICC gives the advantages of portability between mobile phones, a standard for communication between the UICC and NFC chipset, an existing logistics infrastructure and the support of the GSM Association. The GSM Association has stated that the UICC is the strategically best alternative as a Secure Element.

Still, the situation may very well arise where a mixture of UICC-based SEs and SEs embedded into the handset appear and co-exist in the market. In both cases the SE is a smartcard. As such, the OTA management use cases and low-level protocols as specified in Global Platform specifications are similar in many ways. As well, the application data, such as credit card application user data, is the same.

However, the transport protocol differs. For a UICC, the transport is based on ETSI and 3GPP standards. For embedded SEs, the transport is proprietary: often done through GPRS or a 3G data

channel and a midlet proxy in the handset. These midlet proxies are not standardized and are dependent upon the specific handset model of the mobile phone vendor. For trials, an embedded SE may be acceptable, but for mass market deployment using the UICC is the preferred method.

This means that mobile operators that choose handset embedded SEs initially in their NFC solutions should ensure that UICC Secure Elements can be handled in the future.

In an NFC ecosystem where multiple actors co-exist, a common party should manage the SEs. The mobile operator is in an ideal position with its existing card logistics infrastructure to manage the SEs. In a situation where independent Trusted Service Managers (TSMs) handle Secure Elements, it is important to clearly define the mobile operator's role towards the TSM.

The mobile operator's SIM OTA platform is key here, it is a way for the mobile operator to provide essential management functionality to TSMs and Application Service Providers. While not necessary for the mobile network, they may choose to assume the role of the TSM as well. This will help accelerate the build-out of the NFC infrastructure.

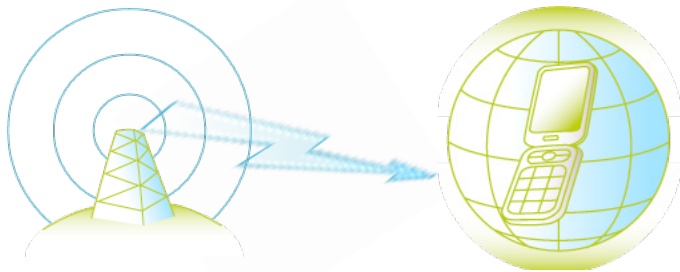
The UICC provides an ideal environment for the NFC application. It is personal, secure, portable and easily managed remotely with OTA technology. The subscriber can rest assured that transactions are executed with protection of their personal information. Providers of services delivered via NFC technology do not risk losing customers when subscribers change handsets. Best of all, the applications are kept up to date using well proven industry standard SIM OTA technology.

The next chapter of this white paper will describe in more detail the role of SIM OTA in the NFC ecosystem.

The role of OTA

The NFC environment will be dynamic. Applications will be continually created, updated and become eventually end of life. The only effective way to reach the users of mobile phone based NFC applications is with Over-The-Air (OTA) technology. OTA technology reaches users regardless of time and place. Users of NFC applications managed by OTA technology will always have the right NFC applications available for use.

With OTA technology, new NFC applications are delivered to the UICC. This ensures that an NFC based system is dynamic and able to adapt to a changing environment. New entrants can have their application launched seamlessly and existing participants can update and manage their applications as these evolve. Because the management is performed OTA, the consumer does not need to go to a physical shop or connect their handset to a docking station to update the NFC applications available.



Always on-line - Always manageable

In NFC ecosystems where the UICC has been chosen as the SE, members of the ecosystem have the advantage of an existing infrastructure for SIM management. Mobile network operators have the logistics in place for UICC procurement, distribution, management and updating.

For instance, after the UICC has been issued to the subscriber, it will sometimes be necessary to deploy a new NFC application. Using OTA, the mobile network operator creates a secure space, a "Security Domain" for the new NFC application service provider on the UICC and assigns unique security keys to it. This is all done securely with the mobile network operator's SIM OTA platform. The application and required data are thereafter either downloaded OTA to this newly defined space or copied from a pre-loaded instance of the application on the UICC. The NFC application owner will have securely and quickly opened their business on the subscriber's UICC.

As an example, a subscriber applies for a credit card service. This particular NFC application service provider was not known or selected when the card was ordered from the UICC manufacturer. The service provider requests the mobile network operator (in its capacity as the card issuer) to allocate space on the UICC and downloads the application with related data. The application is then personalized and made ready to use. The subscriber, without needing to perform any action and via a highly secure procedure, has the credit card service available to them in their mobile phone.

Via the OTA platform, it is possible to lock and / or delete UICC services, or the entire contents of the UICC, when it has been lost or stolen. This is vital functionality especially for credit card applications. The mobile network operator can lock and / or delete the all the services on the behalf of the NFC service providers. This

means customers call one number if their mobile is lost or stolen to block usage of the NFC services.

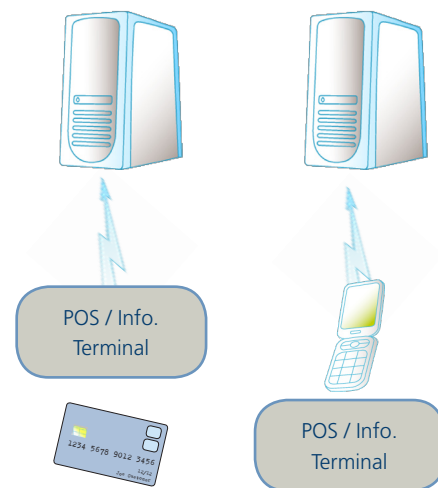
The mobile network operator's SIM OTA system has an extensive database. This allows NFC applications to be easily re-installed on the UICC. The mobile network operator re-allocates the space required by the applications and the NFC service provider can re-issue, personalize and activate the services. This applies to the restoration of services to a UICC when it is recovered or installation of the services to a replacement UICC card.

As well, for credit card applications, the capability to issue and execute EMV (Europay, MasterCard & VISA) scripts on the SE via OTA will likely become a vital part of the business process. For example, the ability to reset the EMV counter for off-line transactions or change the EMV PIN.

The OTA platform plays a key role when implementing the related use cases SIM swap, MSISDN change and new handset acquisition. For these use cases there is a need to run the business logic for activation and download NFC applications to the new UICC and / or handset. For many applications, this means initiating a provisioning flow involving multiple third party NFC actors such as banks, transport and ticketing authorities.

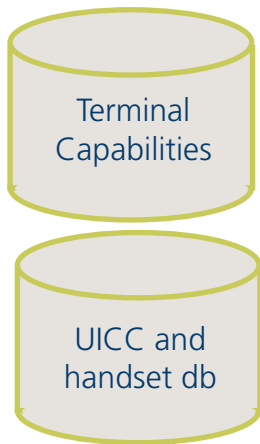
After the download, personalization and activation of the NFC applications, the OTA platform continues to play a part in the NFC ecosystem. OTA enables providing on-line transaction data, detailed service information and direct marketing offers to the subscriber.

Traditional payment and information networks rely upon the service provider's card terminal being on-line. The customer token, for instance credit card, is not on-line. The customer receives paper print outs and receipts of their transaction. These are generally not personalized and difficult to manage for the customer.



On-line: Traditional vs NFC based payment / information system

With the NFC systems utilizing mobile technology, it is the customer who can be on-line. This opens up many new possibilities. For example, the ability to send personalized messages to the subscriber over the air in conjunction with a transaction. This makes possible sending back transaction receipts to the user, maps to where an event takes place, rebate coupons from NFC enabled posters and keeping an always updated account balance in the UICC or handset. Co-marketing is also possible. A record shop purchase could result in a promotional message sent to the user with a coupon giving a 10% discount on a concert.



The MNO has unique knowledge about SIM, Subscriber & Terminal

The mobile operator is in a unique position to provide the best possible conditions for successful OTA management of the NFC applications. The mobile operator will always know where the subscriber is, what connectivity is available for them and in nearly all cases what type of handset they have in their possession.

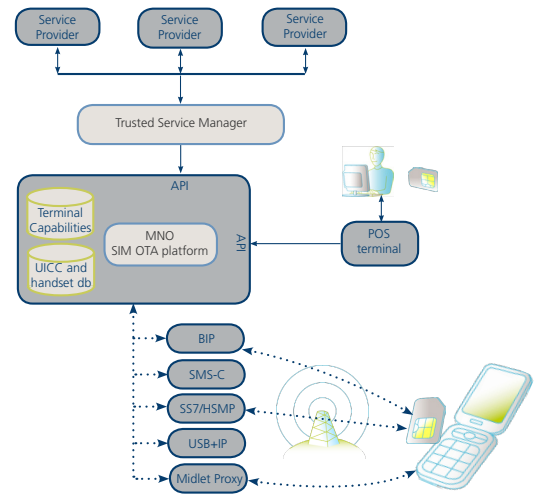
Applications in the form of Java cardlets on the UICC may be pre-loaded by the UICC vendor before delivery to the mobile network operator. But in some cases it may be more convenient to download these OTA to the UICC, after the cards have been issued to the subscriber. This is especially relevant in cases where it is not known at card issuance what applications or service providers shall be used by the subscriber.

NFC applications already present on the UICC card may require certain operations to be performed that need to wait until a specific event has occurred. For instance, service activation will in most cases require that the card's subscription has been sold and / or the UICC card has been distributed to the subscriber.

One example is a transport ticketing application that requires initial configuration with user credentials, and / or top-up with credit after the subscriber has bought a new travel ticket. The credentials are distributed to the UICC with the information about the travel ticket status of the subscriber. Because the credentials and ticket information have been downloaded OTA to the UICC card, the NFC card reader used by the transport company does not require a server network connection to validate the ticket. This means fast validation and a positive customer experience.

The OTA platform provides OTA message encryption. The encryption is double with both NFC service provider and the mobile network operator encrypting the message with their respective encryption keys. This provides the security required for remote application management and for customer acceptance of NFC. This is described in more detail in the next section of this white paper.

High-capacity bearers when using OTA technology are invaluable to managing an NFC solution. Several kilobytes of data may on occasion need to be downloaded to the UICC when downloading activation data or an NFC applet. Providers of services using NFC will not want to disrupt the service access and will want to make new services available as quickly as possible. Using GPRS/UMTS and the BIP (Bearer Independent Protocol) protocol, Java cardlets are rapidly deployed OTA to the UICC card.



OTA Channels supported by information about UICC and Handset

To increase the probability of a positive customer experience the OTA platform should support a selection of bearers: SMS via connection to an SMS-C, midlet proxy, BIP via GPRS, EDGE and UMTS, direct connection to the SS7 network (HSMP) and even via Point of Sale terminals where downloads are made via a card reader. The OTA platform is able to make a selection of what bearer to use, based on several parameters such as its knowledge of SIM and handset capabilities.

Bearer	Approx download time	Test Case
SMS	10 minutes	Java applet of 9kB (675MS)
HSMP	5 minutes	Java applet of 9kB (675MS)
BIP	25 seconds	Java applet of 9kB (675MS)

Comparison of download times for a Java Applet to the USIM

In an environment where multiple types of Secure Elements (embedded and UICC-based) exist, as well as multiple bearers based on handset and SIM capability (BIP, SMS, midlet proxy, point of sale terminals), it is important to have information about what capabilities are valid for the current subscriber. In order to select the best bearer for an OTA download, the SIM OTA platform needs to have this information available. One important facility is the Terminal Capabilities Repository, where the capabilities of different handsets are stored.

For an NFC service provider to manage their application and its related data they need secure access to the UICC and their application. The next section of this white paper will examine how third parties can manage their own NFC applications via the mobile network operator's SIM OTA platform.

Opening up to third parties

The success of NFC applications rests in the ability for the application owners to successfully manage their services securely and regardless of where the user is located. This means that the SIM OTA platform must allow third parties to directly manage their applications. The mobile network operator has the key responsibility of managing the allocation of space on the UICC. It must ensure that space is made available to third parties and that these third parties can manage their applications without interference and without effecting the other third parties present on the UICC card.

This is achieved by creating Supplementary Security Domains (SSDs) on the UICC. An SSD is the method used by the mobile network operator that allows an NFC service provider to use a specific area on the UICC for their NFC applications. The SSD is primarily intended to contain an application in the form of a Java cardlet and its associated data.

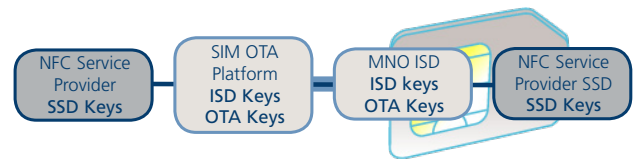
An NFC service provider can publish their NFC application to an own SSD on the UICC that they alone control. The SSD is protected with security keys that are a shared secret between the NFC service provider and the UICC. To ensure the security of each party's SSD, unique security keys are issued.

Allocating new SSDs is done over the air by the mobile network operator. Creating and downloading a new NFC application to the UICC for NFC service providers not already present on the UICC involves creating a new SSD securely via OTA, and assigning keys to it. This procedure has been standardized by Global Platform.

The mobile network operator creates and hands over an own SSD to the NFC service provider. The mobile operator dynamically assigns the management of the area on the UICC to the NFC service provider. They can then in turn install and manage their applications.

A key part of the overall UICC management is memory management. As the issuer of the UICC, the mobile network operator has the natural role to fulfill for the memory usage and memory quota allocation on the UICC.

The rapid advances in large memory SIM cards ensures that opposed to the real world where real estate on the high street is in scarce supply, mobile network operators can issue new cards allowing them to allocate more memory as the number of NFC service providers increases.



End to end security and double encryption

In the illustration above, the NFC service provider has a secure end-to-end communication link using the SSD keys pair. This traffic is in turn wrapped by the mobile network operator's SIM OTA platform. This is protected by the OTA key pair. In addition, the mobile network operator controls the ISD keys for effectively managing the SSD quota and memory allocation.

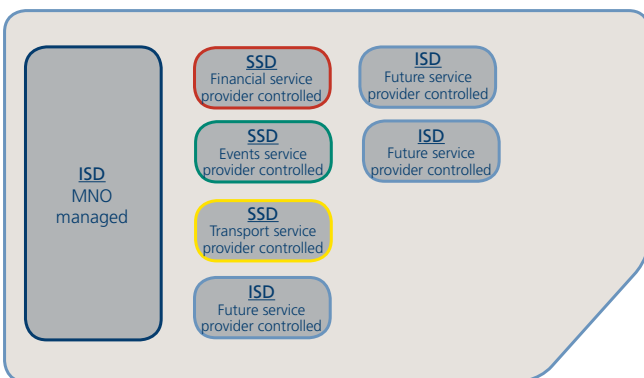
The NFC service provider OTA message that reaches the card is doubly encrypted. This means that it is encrypted both with the NFC service provider's key (SSD key) and the mobile operator's OTA keys. The NFC application on the UICC card can then verify and unwrap the message, first with the operator's OTA key and then with the SSD key, before processing the message.

There are OTA operations that can be delegated by the mobile operator to a third party such as a TSM. The prerequisite is that an SSD exists on the UICC, for which the management ownership has been transferred to the third party.

A Delegated Management (DM) token (delegated OTA key) is issued for the NFC service provider or a TSM executing the NFC application management on the UICC card. The mobile network operator's SIM OTA platform will have the capability to issue these tokens.

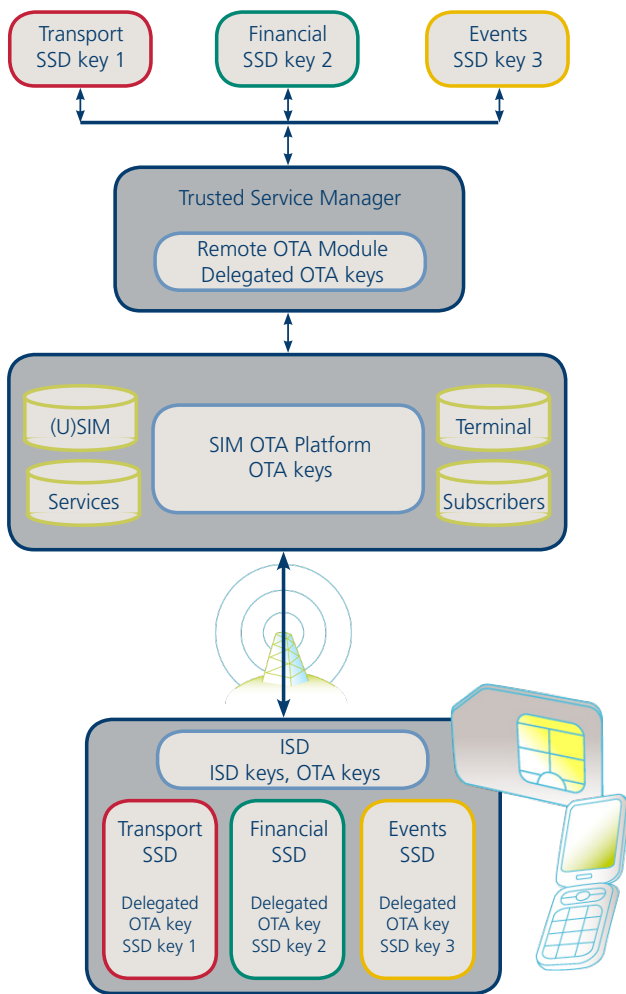
Whilst these OTA operations may be delegated, it is not absolutely necessary. These operations may also be run by the mobile operator, acting as a TSM on the behalf of the NFC service providers.

In practice this means that the mobile network operator operates the SIM OTA platform. They then provide a remote OTA module via which a third party is able to control a leased area (their SSD) on the UICC. The remote OTA module is deployed either at the NFC service provider's premises, the Trusted Service Manager (TSM) or at a separate, secured, location within the mobile operator. The communication of the remote OTA module to the UICC goes via the mobile network operator's SIM OTA platform.



Security Domain management responsibility

The mobile operator keeps the overall responsibility of the UICC. The Issuer Security Domain (ISD) remains the mobile operator's domain which ensures the orderly management of the UICC as a whole. This is one of the most important operations performed by the mobile in the NFC ecosystem.



Delegated OTA management example

For a payment application such as a credit card applet, the application needs to be provided with personalization data. The financial institution will want to directly manage their own application without any intermediaries. The personalization data contains information that is personal to the subscriber and includes PIN codes, keys and configuration data.

For a traditional plastic credit card issuance, this personalization data is sent to a personalization bureau. The plastic card is then distributed by normal postal channels or logistics fulfillment service. In many cases, this means that for security reasons, the customer must physically pick-up their new card at a post office, bank branch or distribution center. For an NFC-enabled UICC, the same personalization data is transmitted to the card by the financial institution using their delegated OTA authority and the mobile network operator's SIM OTA platform.

The ability to delegate management authority of space on the UICC securely via the use of Supplementary Security Domains and remote SIM OTA management modules ensures an open environment. This open environment is what makes it possible for third parties to deploy, launch and manage services providing value to subscribers.



Conclusion

Near Field Communication joined with mobile telephony has the potential to leverage the ubiquitous nature of the mobile phone in today's society. The mobile phone has graduated from a simple extension of voice communications to a powerful personal assistant. It keeps us in contact with the world, allows us to capture memories with its camera, be entertained with music, TV and video and now with the advent of NFC navigate everyday life.

We can move seamlessly from the newspaper kiosk with our daily news to the underground on our way to the match of the day pausing only to swipe our phone along the way. The mobile network with its existing SIM OTA infrastructure has the backbone in place to enable this new ecosystem.

The UICC, with its unique personal, portable, secure and controlled environment is ideal as the Secure Element for NFC. Using SIM OTA the NFC ecosystem stays dynamic allows for new market entrants and continual enhancements to the services launched. Flexible SIM OTA platforms will support delegation of management authority keeping NFC service providers in control of their applications.

Using an independent SIM OTA supplier that supports numerous SIM vendors means that interoperability issues between UICC implementations are removed as a problem. This is significant as many vendors often make own added value extensions to industry standards. A SIM OTA platform that can not adapt and evolve to the ever changing SIM market will result in inflated UICC costs in the long run.

The latest release of the SmartTrust SIM OTA platform, DP8, is built to meet the needs of the NFC ecosystem. The DP8 with its proven ultrahigh OTA capacity, extensive UICC card management functionality and over 10 years of experience in delivering mission critical OTA systems make it the ideal platform for supporting the NFC ecosystem.



About the author

Daniel Ericsson

Daniel works as a Business Development Director within the SIM OTA business unit of SmartTrust. Since joining SmartTrust in 1998, he has worked in numerous roles leading the development and standardization of the smart card in mobile telephony. He has worked as a Solution Architect, architecting and delivering customer solutions based on SmartTrust products to some of the world's largest mobile operators. Before starting at SmartTrust, Daniel worked in the defense industry with mission critical Air Defense Command & Control systems.



Daniel is a leading innovator and designer within new technology areas. His work has resulted in a number of new products. He was instrumental in the development of the first version of the SmartTrust WIBTM, the world's most widely deployed smart card application execution environment. He was a key player in the development of the patented SmartTrust SmartRoam dynamic roaming steering management product. He has been actively participating in ETSI and 3GPP standardisation for the SIM card in mobile telephony since end of 1999.

Outside of the office, Daniel enjoys spending time with his family, skiing, skating and photographing. He has a Masters of Science degree in Engineering Physics from the Uppsala University in Sweden.



Glossary

- 3G**
3rd Generation Network, i.e. UMTS
- 3GPP**
Third Generation Partnership Program, a group dedicated to driving 3rd generation mobile telephony standardization
- BIP**
Bearer Independent Protocol, a method for high-speed access to the SIM & USIM cards
- CA**
Certificate Authority, issues digital certificates to users within a Public Key Infrastructure (PKI) that binds their identity to the certificate and to a public key listed in the certificate
- Certificate**
A digital certificate is a digital document that confirms the identity and key ownership of an individual, a computer system (or a specific server running on that system), or an organization
- DP**
SmartTrust Delivery Platform, a SIM OTA platform.
- ECMA**
European Computer Manufacturers Association
- EDGE**
Enhanced Data rates for GSM Evolution, packet data technology for GSM
- EMV**
Europay, MasterCard & VISA, a standard for interoperation of IC cards and IC terminals for authenticating card payments
- ETSI**
European Telecommunications Standards Institute
- GlobalPlatform**
A non-profit industry association that focuses on establishing and maintaining interoperable specifications for single and multi-application smart cards, acceptance devices and systems infrastructure
- GPRS**
General Packet Radio Service, packet data technology for GSM
- GSM**
Global System for Mobile communications, the world's most widely used mobile telephony technology
- HSMP**
High Speed Messaging Package, a SmartTrust product for direct connection to the SS7 network
- IEC**
International Electrotechnical Commission
- IP**
Internet Protocol
- ISD**
Issuer Security Domain
- ISO**
International Organization for Standardization
- MNO**
Mobile Network Operator
- MSISDN**
Mobile Station Integrated Services Digital Network Number or Mobile Subscriber ISDN
- NFC**
Near Field Communication
- OMA**
Open Mobile Alliance – a standards body that develops open standards for the mobile telephony industry
- OTA**
Over-The-Air
- OTAP**
Over-The-Air-Provisioning
- OTW**
Over-The-Wire
- PIN**
Personal Identification Number, a shared secret between a user and a system used for authentication
- PKI**
Public-Key Infrastructure, in a PKI, public and private key pairs are used to securely exchange data on a basically insecure public network, such as the Internet. The private and public key pairs are obtained and shared through a CA (see CA)
- POS**
Point-of-Sale
- Private Key**
See PKI
- Public Key**
See PKI
- SD card**
Secure Digital Card, memory card format used in devices such as digital cameras and handheld computers
- SE**
Secure Element
- SIM**
Subscriber Identity Module
- SM**
Short Message
- SMS**
Short Message Service, a transmission service for short text messages to and from a mobile phone, fax machine, and/or IP address.
- SMS-C**
Short Message Service Centre (See SMS), which delivers an SMS to the appropriate mobile device



Glossary continued

SS7

Signaling System #7, a signaling protocol

SSD

Supplementary Security Domain

TSM

Trusted Service Manager

UICC

Universal Integrated Chip Card

UMTS

Universal Mobile Telecommunications System, a Third Generation mobile telephony network technology

USB Universal Serial Bus

USIM Universal Subscriber Identity Module, an application on the UICC for 3G networks

Further reading

GSMA Near Field Communications (NFC) technical guidelines white paper,

April 2007 (http://gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf)

GSMA Mobile NFC Technical Guidelines

November 2007 (http://www.gsmworld.com/documents/gsma_whitepaper_nfc_vs2.pdf)

GSMA Pay-Buy-Mobile Business Opportunity Analysis

November 2007 (http://www.gsmworld.com/documents/gsma_pbm_white_paper_11_2007.pdf)

Mobey Forum Best Practice for Mobile Financial Services

2008 (<http://www.mobeyforum.org/files/bestpractice/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf>)

Mobile NFC Services,

January 2007 (<http://gsmworld.com/documents/aa9310.pdf>)

Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications

October 2007 (http://www.nfc-forum.org/resources/white_papers/nfc_forum_marketing_white_paper.pdf)

Requirements for Single Wire Protocol NFC Handsets,

November 2008 (http://gsmworld.com/documents/reqs_swp_nfc_handsets_v2.pdf)



Headquarters:
Årstaängsvägen 19B, 2nd floor
Box 47152
SE-100 74 Stockholm
SWEDEN

Phone: +46 8 685 93 00
Fax: +46 8 685 65 30

www.smarttrust.com