Chair

Mario Maawad  CaixaBank

Contributors

Matias Seppovaara  Nordea
Alexander Luijt  UL
Zafar Kazmi  CaixaBank
Niall O’Donoghue  Trusted Computing Group
Natalí Melgarejo  GMV
Ira McDonald  Trusted Computing Group
Douglas Kinloch  Metaforic

Keywords

NFC, security, PAN, GlobalStandard, Service Provider, Trusted Service Manager, Mobile Network Operator, Payment, Key Management, Mobile Device, Secure Element, SE,

Related Documents


Copyright © 2014 Mobey Forum Part 2 in a Series of Whitepapers on NFC security
Table of Contents

1. Executive Summary ......................................................................................................................................... 6
2. Introduction .................................................................................................................................................... 8
3. NFC Payment Business Models .................................................................................................................. 8
4. Securing the Mobile Device Lifecycle ........................................................................................................ 9
   4.1. Mobile NFC Installation .......................................................................................................................... 10
   4.2. Changing Mobile NFC phone ............................................................................................................... 11
   4.3. Lost or Stolen Phone ............................................................................................................................. 12
5. Secure Delivery of Financial Data to the NFC Device .............................................................................. 12
   5.1. Cryptography ......................................................................................................................................... 12
   5.2. Key Management .................................................................................................................................... 14
   5.3. User Data Persistence ............................................................................................................................ 16
6. Securing User’s Financial Data .................................................................................................................... 16
   6.1. The Role of SE....................................................................................................................................... 16
   6.1.1. SE Security Requirements ............................................................................................................... 16
   6.1.2. Tamper Proof Technology .............................................................................................................. 17
   6.1.3. Implementations ............................................................................................................................... 18
   6.1.4. SE Elements ..................................................................................................................................... 19
   6.1.5. Multiple SE interoperability .............................................................................................................. 20
   6.2. From “Issuer Centric” to “Consumer Centric” Model ........................................................................ 20
7. Securing Mobile Payment Application ........................................................................................................ 22
   7.1. Design Guidelines .................................................................................................................................. 22
   7.2. Prevention of Software Attacks on Mobile Devices ............................................................................. 23
   7.3. Appropriate Controls to Consign Merchants ....................................................................................... 23
   7.4. Limiting the Exposure of Account Data Viable Fraud ......................................................................... 23
   7.5. Proper monitoring of Mobile Payment Acceptance Solutions .......................................................... 24
8. Communication between NFC Mobile Devices and POS Terminals ..................................................... 24
   8.1. Consumer Perception ............................................................................................................................ 24
   8.2. Managing Multiple Applications ......................................................................................................... 25
   8.3. Potential for MIDlet Use ....................................................................................................................... 25
   8.4. PIN Requirements ............................................................................................................................... 26
   8.5. Payment Transaction Security ............................................................................................................... 27
9. Conclusions ................................................................................................................................................... 28
10. Citations and References ............................................................................................................................ 29
11. Appendices .................................................................................................................................................. 31
Table of Figures

**FIG. 1** DIFFERENT BUSINESS MODELS FOR APPLICATION MANAGEMENT ACCORDING TO NFC FORUM. DAP: DATA AUTHENTICATION PATTERN (SOURCE: NFC FORUM) ........................................................................................................ 9

**FIG. 2** UICC SHOWING THE DIFFERENT SDs AND KEYS USED TO MANAGE THEM ........................................................................................................ 15

**TABLE 1.** THREE DIFFERENT NFC COMMUNICATION PROTOCOLS ........................................................................................................ 34
1. Executive Summary

The aim of the document is to provide guidelines and best practices we have found within the industry to help the NFC ecosystem to function in a secure and efficient manner.

In the NFC ecosystem, there are many model configurations regarding the responsibilities of the stakeholders. The current paper presents considerations for the following three models:

- Simple model: the MNO performs the Card Content Management with the supervision of a TSM.
- Delegated model: the Card Content Management is done by the TSM, but the MNO authorises all the operations.
- Authorised model: the Card Content Management is delegated to the TSM but only for the UICC part.

A mobile device has a lifecycle and the respective stages of the cycle need to be secured. The most relevant processes are discussed in the whitepaper, namely:

- Mobile NFC installation: The first stage for the UICC personalisation and installation depending on its initial state from a factory. The installation can be done in three ways: 1) UICC application loaded and installed in the factory, 2) UICC application loaded in the factory but installed OTA, and 3) UICC application fully loaded and installed OTA.
- Changing NFC phones: There are two methods to launch and install the UI for the UICC application. Firstly, the phone can automatically detect that the UICC application UI is missing. Or alternatively, the MNO automatically detects the missing application UI and starts a new installation.
- Lost or stolen phones: the Mobile Application can be deactivated the same way as the physical card. However, there is an issue with the implementation of the application, and thus, it is better to leave some features out to minimise the risks.

During the mobile device lifecycle, configuration commands will be sent depending on the NFC configuration model explained above: i.e. the simple, delegated model or authorised model.

The delivery of financial data to the mobile handset is yet another critical dimension in a NFC mobile service. The process can be divided into following parts:
• Cryptography: the delivery and storing of the financial data requires encryption. There are three communication layers within the data delivery to the mobile handset: the 1) physical, 2) transportation, and 3) application layers. Each of them has their own protocols and encryptions that make them more secure. Moreover, when the financial data is stored in the UICC, the encryption type is important regarding the cryptography infrastructure and the message authentication.

• Key Management: the GlobalPlatform standards require that a mandatory series of keys are used for the Secure Domains and Supplementary Secure Domains. An extended example of Key Management will be provided later in the paper.

• User data persistence: TSM needs user’s financial data during the personalisation process. The relationship of trust between the TSM and the merchant is important, and is based on a secure exchange of their keys.

When it comes to securing the financial data inside the Secure Element and mobile handset, there are, however, other issues to take into account. For example, the location of the financial data in the mobile handset depends on the location of the SE, whether it resides in the a) USIM, b) embedded SE or c) SD memory card.

Nevertheless, regardless of the SE location, it should provide the following elements:

• An OS to support secure application execution
• Communication interfaces for multiple SE interoperability
• A Manager application to maintain the different contactless applications on the SE

The SE interoperability actually becomes an issue when more than one SE is active. According to the Global Platform standards, there might be two models to tackle the issue:

• Non-aggregation model: the user selects a single SE at a time.
• Aggregation model: various SEs are active at the same time and the user can choose the applications without having to know where they actually reside.

The Mobile Payment Application is yet another critical asset to protect in the Mobile NFC services. Basic best practices for that protection are as follows:

• Develop mobile applications following the secure coding guidelines.
• Ensure trusted application deployment and avoid application code to be tampered or altered.
• Provide the ability to identify the transactions coming from a merchant.
• Only allow the installation of trusted sources.
• User keeps the firmware of the device regularly updated and installs updates whenever they become available.
• Enable encryption of all public transmission data as well as protect the stored PAN and other sensitive information.

The PIN, as most common authentication method, has only basic requirements to ensure its security in mobile payment applications. The GlobalPlatform standards recommend three types of PIN depending on the level of access to some OS files and the interfaces of the mobile device: the Universal PIN, the Application PIN and the Local PIN. There is also the Mobile Payment Application Pin which should follow the requirements proposed by the PCI DSS.

Finally, the end user must be aware of the mobile device as a payment method and treat it like his/her normal credit card.

2. Introduction

The objective of the document is to provide a list of guidelines and best practices to all stakeholders involved in the NFC based payments ecosystem in order to enhance the overall security of NFC mobile payment services.

The whitepaper considers some important elements in the mobile NFC environment: for example, the mobile device lifecycle, delivery of data, user’s financial data, mobile payment application, and communication between the NFC mobile device and the POS. Following the same order, the whitepaper thus develops a series of best practices to improve the NFC services security.

3. NFC Payment Business Models

This section describes the best practices that should be followed when developing and deploying NFC mobile payment solutions. According to the industry practices, there are three deployment types supported by the standards. The MNO must decide which of the deployment cases is more appropriate for the UICC configuration during the mobile lifecycle. The respective deployment models are:

• Simple model: the MNO performs the Card Content Management (CCM) with the supervision of a TSM. The MNO OTA platform has to be able to ask for Data Authentication Pattern (DAP) from the TSM or Service Provider (SP) prior to any installation of Applet in the SP SD - if so required by the SP.
• Delegated model: the Card Content Management is done by the TSM, but all operations must be authorised by the MNO.
• Authorised model: the Card Content Management is delegated to the TSM but only for the UICC part. MNOs do not usually prefer the Authorised Model unless there is a high trust relationship between a MNO and TSM.

The above-described models are so-called “Issuer centric” models and that the model chosen by the MNO can be a combination of the above described, which are all supported by the GlobalPlatform standards.

The following sections will be based in the above-three use cases to provide an example of generic deployments that can exist in a typical implementation of NFC services such as UICC initialisation, personalisation, provisioning and card content management.

4. Securing the Mobile Device Lifecycle

This section gives an overview of the instances that may occur during a mobile device lifecycle and recommends responsibilities for each of the stakeholders in the NFC ecosystem. The objective of the section is to provide security guidelines for the lifecycle of a device on a general level. List of instances that may occur during a mobile device lifecycle are as follows:

• Mobile UICC application installation
- UICC user interface installation
- Change of UICC
- Change of mobile phone number
- Change of mobile device
- Lost or stolen mobile device (end user contacts MNO)
- Lost or stolen mobile device (end user contacts service provider)
- Recovery of a mobile device after a loss or theft
- New mobile device after a loss of theft

4.1. Mobile NFC Installation

NFC installation in a mobile device is the first stage for the UICC personalisation and installation. The UICC can be loaded and installed in a factory or over the air (OTA).

The UICC application is composed of several packages or instances and personalisation data. The way the data is delivered to the UICC will depend on the chosen deployment model. In the Simple Model (outlined above), the MNO sends the Card Content Management (CCM) commands after they receive the Service Provider Request. In the Delegated Model, the SP (Service Provider) will send the CCM commands after they have been authorised by the MNO.

There are three scenarios to consider regarding preloaded content before the OTA installation. These scenarios represent the state of UICC contents installed before OTA operations: the 1) fully preloaded, 2) partially OTA loaded, and 3) fully OTA loaded.

This section explains how the domains are created and by which role according to the UICC initial state.

**UICC Application Preloaded**

When the UICC application is preloaded, both the Supplementary Security Domain (SSD) is created and the UICC application loaded in the factory. The Service Provider (SP) can also perform the personalisation in the factory.

Once the UICC application personalisation has been done, the application will be activated OTA, either by the MNO (upon the SP’s request in the Simple model) or by the SP (upon MNO authorisation in Delegated Management model).

**UICC Application Partially Loaded OTA**

In this scenario, the application is loaded in the factory, but the MNO needs to verify/authorise the UICC application and upload it to the security domain of the SP (in the Simple Mode).
In the Simple Model, the MNO authorises the UICC application in the Service Provider Security Domain. In the Delegated Model, authorisation is done by the SP. Then the UICC personalisation is done by the SP in both models. The UICC application activation on the other hand is done again by the MNO (Simple Model) or by the SP (Delegated Model).

**Fully OTA**

In the case of fully OTA transactions, the SSD may be created in factory or OTA, and then all the following operations are done OTA. In the Simple Model, the UICC application instantiation and the release to the SP Security Domain is done by the MNO while in the Delegated Mode this is done by the SP.

The GlobalPlatform standards strongly recommend a minimum level of cryptographic functionality. In order to achieve this, the configuration of the UICC should follow a similar structure to the Secure Channel Protocol (SCP) of the GlobalPlatform standards. An example of the SCP configuration is the EMV CPS specification developed by EMV.

The complete description of the UICC installation and configuration is unfortunately out of this document’s scope. For an overview of the process, please refer to an Appendix 5.3 and the respective flow diagrams describing the UICC personalisation and installation process for both the Simple and Delegated model.

### 4.2. Changing Mobile NFC phone

When a consumer decides to change his mobile device, the application user interface must be launched and installed again for all mobile NFC services that were installed in the previous device.

Once the new device is in use, two methods can be used to ensure that the UI is updated in the new device:

- The mobile device detects the missing UI, comparing the content on the device to the content on the UICC. This could be done with an application developed by the MNO, which would alert the user of the missing UI. The MNO would then contact the SP to download and install the UI onto the device.
- The MNO remotely detects that the mobile device has changed.

When the detection is done remotely, the MNO notifies all relevant Service Providers about the end user’s new handset so that each Service Provider can invite the end user to download the UI again and benefit from full capacity of his mobile NFC service.

---

4.3. Lost or Stolen Phone

If a user loses his phone, the protocol to deactivate the Mobile Payment Application will be exactly the same as if he lost his physical payment card. The user must report the loss to the bank and his account will reject any new financial transactions. Then the bank has to send a payment application deactivation or block request through the TSM. The implementation of the Mobile Payment Application determines the security of that application: for example, if the Mobile Payment Application requests a password for every payment, then the risk will be minimised. The only security issue will be then potential offline transactions configured for the user.

5. Secure Delivery of Financial Data to the NFC Device

The key stakeholder in this part of the process is the TSM. It acts as a trusted third party between the Service Providers, financial institutions and MNOs, the issuers of SIM cards. When a transaction is made, the financial data is issued by a bank and passed through a TSM to the SE in the mobile device. The data should be protected with cryptography throughout the financial data delivery process. The TSM is in charge of the security during all of the stages.

5.1. Cryptography

In the case of a TSM based mobile payment environment, the secure transfer of account data from an issuing bank to the TSM relies on public key infrastructure and encryption based on the SSL/TLS standard. The financial data is encrypted and stored by the TSM.

Three separate layers of encryption are established within a packet data connection when a mobile device needs personalization:

1. The first layer is the link between the MNO and the mobile device when the latter establishes a packet connection across the Radio Access Network. The connection is encrypted at OSI Layer 1 (physical layer) with protocols based in the CDMA and GSM standards. In this layer, the MNO is the one in charge of the data encryption assuring confidentiality throughout the Radio Access Network and to avoid security breaches such as radio sniffing.

2. The second layer passes the security responsibility to the MPA (for example, a mobile wallet), which then initiates a secure TLS connection to the TSM’s personalisation server at OSI layer 4 (transport layer) using credentials known by a Certificate Authority.
3. The third layer is the establishment of the TLS connection: the TSM initiates another secure connection to the mobile device’s SE at OSI layer 7 (application layer). The final layer of encryption is secured by keys of the issuing bank.

The data needs to be secured in all of the three layers of encryption, because the data is transmitted OTA.

It is important to decide whether the UICC has a public or symmetric key cryptography. There also the issue of time needed to process the cryptographic operations. It has been proved that optimised elliptic curve cryptography with enough bits would make an equivalent of 1024 bits RSA². In fact, the elliptic curve cryptography was found fast enough for real life operations, but at the moment there are no actual implementations yet. However, problem with the Elliptic curve cryptography is that GlobalPlatform standards only support Des, 3-Des and RSA keys.

GlobalPlatform dictates the mandatory use of encryption and message authentication when communicating with high level security parts such as security domains. The standard algorithms described in the GlobalPlatform Card Specification version 2.2 are listed below:

- 3-DES in CBC or ECB mode using keying option 2 defined in ISO/IEC 18033-3
- Full Triple DES MAC defined in ISO 9797-1 for message authentication
- Single DES Plus Final Triple DES MAC defined in ISO 9797-1 for message authentication
- Secure Hash Algorithm (SHA-1) defined in FIPS PUB 180-1
- MULTOS Asymmetric Hash Algorithm defined in MAO-DOC-REF
- RSA using SSA-PKCS1-v1_5 defined in PKCS#1
- AES-128 to AES-256 is supported in a recent document

GlobalPlatform regulates the encryption protocols into the following standards:

- SCP01 – deprecated
- SCP02 – using symmetric keys
- SCP10 – using public key cryptography
- SCP03 – supporting AES and TDEA
- SCP80 – identical to ETSI TS 102 226 encryption

---

³ Woodbury, A. D., Bailey, D. V., and Paar, C. 2001. Elliptic curve cryptography on Smart Cards without coprocessors, Proceedings of the fourth working conference on smart card research and advanced applications on Smart card research and advanced applications, pp. 71-92

Copyright © 2014 Mobey Forum | Part 2 in a Series of Whitepapers on NFC security
For a more specific view of the requirements on cryptography within the GlobalPlatform standards, please refer to the latest version of the Card UICC Configuration.

5.2. Key Management

One of the TSM’s primary tasks is to ensure the security of the keys all the time. A good key management process keeps the cryptographic keys secure in a logical and physical way. Physical security involves physical barriers and alarm systems, while the logical security includes processes, procedures and software used to protect the keys.

To give a better view of how the Key Management System works, the paper presents below an example of a simple implementation and the introduction of domains at each stage of the system management using the GlobalPlatform standards.

The MNO provides the user with a mobile device that has a UICC chip standardised according to GlobalPlatform’s functions. The UICC chip includes the Secure Channel Protocol, which allows the MNO to establish Secure Domains where the applications provided by third parties are installed. Typically the user will have a Contactless Payment Application (EMV based for example), a Two Factor token application (OTAH based) and another application provided by the MNO, let’s say a music application (DRM).

Initially, the UICC only has a single Security Domain, the “Issuer Security Domain” (ISD) and it’s created using the Initial Issuer Master Key (KMC). The Initial Supplier Key (ISK) is the first key to be used to personalise the UICC.

Then, the music application is personalised and uploaded to the ISD using the keys derived from Initial Application Provider Master Key (KMD, Key Management Device). After that the ISD is locked, allowing the Music application to be executed in the ISD. Then, a Supplementary Security Domains (SSD) can be created.

After the above-described steps, the issuer is able to install the Payment Application. The bank requests the MNO to create an SSD. The MNO generates the new SSD using commands protected by the keys derived from the Issuer Master Key (CMK, Card Management Key). In setting up the security domain, the MNO loads a new KMD (Initial Application Provider Master Key) or AMK (Application Provider Master Key), subject to the implementation plans.

Finally, the MNO derives the keys necessary for the secure channel, e.g. ADKDEK (used for encrypting application keys), ADKENC (application load commands) and ADKMAC

---

4 DES Master Key for Personalization Session Keys: This DES Key is used to generate the Message Authentication Codes and to encrypt and decrypt during personalization.
(sending Message Authentication Codes). It then passes these three derived keys to the bank. If the Application Provider Master Key (AMK) is not transferred, a secure channel agreed in advance between the two parties will be used. The keys will be transferred securely to the chip as well as the optionally inserted DAP (Data Authentication Pattern) key of the bank - a public key, which can be used to verify that the bank has signed the code intended to run on the chip. Now the bank is ready to finish the chip personalisation with the contactless payment application based on the AMK key derivate.

To install another application like the Two Factor Authentication, the MNO needs to create a new SSD and repeat the whole process establishing the Secure Channel between the SP and the MNO. See Fig. 2 below illustrating different Security Domains (SDs) and keys to manage them.

Fig. 2 UICC showing the different SDs and keys used to manage them
5.3. User Data Persistence

The TSM needs to access the user’s financial data during personalisation. This will depend on the mobile network quality or user expertise on mobile applications.

When the user is ready to begin the personalisation process, the bank delivers the financial data to the TSM. The user’s data can be stored before he starts the personalisation process.

The TSM might never access the user’s financial data; then the bank should have a supplemental security domain pre-established on the SE by the MNO or a supplemental security domain with a temporary key known to the bank. Thus, the bank would establish the secure connection with the bank keys and personalise the card through the TSM.

If the bank directly entrusts the TSM with its keys, then the TSM could generate a supplemental security domain specific to each bank and personalise it with the financial data provided by the bank. Once the personalisation would be successfully completed, the financial data would have no reason to reside at the TSM.

6. Securing User’s Financial Data

This section reviews how the financial data is stored in the mobile device and how the applications and the POS access it securely.

The location of the financial data inside the mobile handset depends on the location of the SE. It can be the USIM, the embedded SE or the SD memory card.

6.1. The Role of SE

A Secure Element (SE) is a tamper resistant device with an embedded microprocessor chip; a platform, in which applications can be installed, personalised and managed, usually OTA. It is a combination of hardware, software, interfaces and protocols that enable the secure storage and usage of credentials for payments, authentication and other services. Many of the potential mobile contactless services these days require one or more SE’s to store keys and applications.

6.1.1. SE Security Requirements

In order for a NFC-enabled mobile device to completely emulate the functionalities of and be equal to a physical smartcard, some specific security-related features need to be taken into account: namely, protection of an SE and authentication credentials. These are discussed below.
Protection of an SE

The requirements for a SE protection are the following:

1. Secure Element verifies the mobile device.
2. Secure Element provides tamper-evident mechanisms for any installed firmware and software.
3. Secure Element authenticates the download of firmware and software.

Protection of authentication credentials

The requirements for the SE to protect user authentication credentials are the following:

1. Secure Element authenticates the legitimate user.
2. Secure Element uses a different authentication credential than the mobile device.
3. Secure Element uses at least two-factor authentication. Usually these two factors presented by the user can be something the user knows (e.g. a password), something the user has (e.g. a token, a signature) or something the user possesses (e.g. biometrics/fingerprinting or similar).
4. Secure Element provides tamper-resistant and tamper-evident mechanisms for the storage of authentication credentials.

6.1.2. Tamper Proof Technology

Tampering means unauthorised manipulation of a device, including information retrieval and modification. The term tamper proof refers to a device with the ability to resist and/or protect itself from tampering. Such functionality can include mechanisms for prevention and detection of unauthorised access, as well as device self-destruction.

Tamper proof devices can be classified as:

- Tamper evident: tampering with the device leaves evidence of tampering (e.g. physical damage), which allows detection of the attack.
- Tamper resistant: tampering with the device is difficult or impossible, which is the typical referral in a specific attacker model.

In microprocessors, tamper resistance can usually be achieved through a combination of two methods, namely limiting access to information only through APIs and providing these APIs with appropriate security measures. Note that information must be protected both logically and physically, since attacks may include, in addition to software-based attacks, the following:

- Physical attacks (temperature variations, radiation, chemical manipulation)
- Electronic attacks (unusual voltages, unusual clock signals, and so on)
A hardware-implemented version of a tamper proof device is recommended so that it can include specific counter-measures against physical and electronic-based attacks. The same applies to SEs also; preferably they have to be physically independent from the elements they interact with.

### 6.1.3. Implementations

Currently, there are a number of different possibilities of implementing an SE. For the purpose of this study, the following four types of SE’s are considered:

**UICC (SIM card)**

In third generation networks (3G), the physical Smart Card component is called UICC and they use Java-based Operating Systems. UICCs can contain SIM, USIM and/or CSIM Applications. Increasingly, UICCs can include additional Applications such as information-on-demand menus, SIM-based browsers, m-banking Applications, EMV profile Applications or ID credentials for MFS, and hence these serve as SE’s. When the UICC acts as the SE, it communicates with other components of the mobile device through UICC wires and connections.

**Embedded SE**

The concept of an embedded SEs is very close to the UICC SE model as it requires a TSM and leverages the same core provisioning technology. Embedded SEs, though, cannot be removed from a mobile device, and they have specific wire connections to the remaining elements of the mobile architecture. The integration of SEs in NFC enabled mobile devices has also been greatly simplified by technology vendors with limited impact on the mobile device design in terms of hardware and software.

**Secure Memory Card**

The Secure Micro SD card can be a mere storage provider and also SE container. Moreover, and this is particularly interesting for NFC-based MFS, the Secure Micro SD Card can include an NFC antenna. In fact, there are three possible models of Secure Micro SD Cards, listed below:

- Full NFC - the Card includes the SE elements, NFC chip and antenna.
- Antenna on the mobile - the Card includes the SE elements and NFC chip, but the antenna is on the mobile device.
- Only SE - the Card includes the SE elements. The NFC modem and the antenna are on the mobile device.

Similarly to the UICC model, the Secure Micro SD card is installed in the SD card slot of the device and it uses SD wires as physical media for communication with other elements of the mobile device.
NFC Stickers

NFC stickers are electronic stickers used to add NFC features to existing mobile devices. In general terms, a sticker provides the NFC circuitry needed to establish an NFC channel, i.e. an NFC antenna and an NFC chip. Optionally, the sticker can also include a SE, battery and/or another antenna providing communication to the mobile device (typically a Bluetooth antenna).

Depending on the kind of transaction taking place and the SE in use, an NFC sticker can work in three different modes:

- **Passive mode**: the sticker acts as a passive NFC tag, like a Smart Card for instance. An external reader can be used to read and/or alter the contents of the NFC chip/internal SE. Then the sticker acts completely independent from the handset to which it is attached and works in passive mode powered by an external reader.

- **Active mode**: This allows a connection to be established between the sticker and the mobile phone in order for the mobile device to read or change the content of the internal SE/NFC chip. It also allows the sticker to use the device’s SEs instead of the internal one.

- **Reader mode**: In the third mode, the sticker acts as an NFC reader and interacts with an external NFC tag. This mode, however, is not considered relevant in the current paper.

Commercial NFC stickers may support one or more of the above modes. When the Active and/or Reader modes are available, the sticker needs to include a battery or to use power of the mobile device, to which it is attached. Moreover, a Bluetooth antenna must be present to interact with the mobile device.

6.1.4. SE Elements

Regardless of the form factor, an SE should contain the following:

- An OS, which supports the secure execution of applications and secure storage of application data. The operating system may also support secure loading of applications.

- Two communication interfaces:
  - A device or contact interface, which enables the exchange of commands and responses between the SE and authorised mobile applications in the mobile device.
  - An antenna interface or contactless interface, which enables the exchange of commands and responses between an application in the SE and a contactless Point of Interaction via the NFC Controller of the mobile device.
6.1.5. Multiple SE interoperability

The different potential SE implementations raise a further issue regarding interoperability. Since a mobile device can be compatible with many implementations, also many SEs can coexist in a single device. In February 2010 the GlobalPlatform Mobile Task Force released an analysis of the implications and requirements for managing multiple SE’s within the same handset. That document identifies two business models:

(a) Non-aggregation model, in which one single SE selected by the user is active at a time; i.e. the SE can access the NFC controller and perform NFC transactions, and

(b) Aggregation model, in which various SEs are active at the same time and the user chooses from a portfolio without specifying the device it resides in.

The latter model is the most appropriate for the purposes of the current Mobey Forum security analysis paper.

6.2. From “Issuer Centric” to “Consumer Centric” Model

Recently, according to the latest trends in mobile payments, the industry has decided to move from an “issuer centric” to a “consumer centric” model. Considering GlobalPlatform’s role as the standard for loading, installing and personalising applications on SEs or TEE, current section will describe how the new model affects their role.

The new model implies changes in the GlobalPlatform security architecture that haven’t been released yet but are supposed to allow the consumer to decide over the applications installed on his/her mobile device and also guarantee proper security of the critical data.

GlobalPlatform’s Consumer-Centric Model suggests new elements to the ecosystem:

- **Trusted Token**: a secure, chip-based object, owned by the end user and serves as a personal security container. The Trusted Token can be any type of device or service: a Secure Element chip, UICC, microSD, USB Token or even a device with a Trusted Execution Environment. The Trusted Token may also contain

---

5 “A New Model: The Consumer-Centric Model and How It Applies to the Mobile Ecosystem”
different levels of trust. Most likely consumers will acquire the one that adds more security to the mobile banking applications.

- **Trusted Token Provider**: the supplier of the Trusted Token.

When a SP wants to verify the security of a Trusted Token, they will communicate with it. Thus, user will have control over the applications installed in the device while at the same time the consumer and SPs will have a verifiable level of security for the most sensitive applications.

In fact, GlobalPlatform’s technology is compatible with the new “Consumer Centric” model and concepts that have already been defined as the “Security Domain” will further help the model to succeed. However, some considerations must be taken in account regarding the roles in the ecosystem and the Security Domains, such as:

- The end user is able to view and prioritise the list of applications located in the registry of the trusted token, including the contactless applications. S/he can also delete Security Domains, applications and application data.
- The Trusted Token Provider is able to create root Security Domains for the benefit of SPs.
- The SP or its TSM is able to create Security Domains within its own tree and protect the messages it exchanges with the Trusted Token via its own Secure Channel protocol\(^6\) keys.
- The Trusted Token Provider cannot delete any Security Domains or applications belonging to another Security Domain tree without a request from the SP or its TSM.
- Mutual authentication between the actors and SDs on the token is needed.
- Integrity of commands and data exchange with the token has to be guaranteed.
- Confidentiality of commands and data is important to protect application code and data.

The developments of the GlobalPlatform security architecture will allow the new model to suit today’s market as well as add to the security needs from a practical and realistic point of view. The level of security for each application installed on the device will be chosen by the end user, giving him/her the responsibility for critical data saved in the device.

\(^6\) The Secure Channel Protocol has been published as an amendment to the Card Specification v2.2. It defines a new set of cryptographic methods based on AES for the communication between a smart card and an external entity. This specification enables the GlobalPlatform to be compliant with requirements for AES-based security.
7. Securing Mobile Payment Application

The following recommendations aim to guide in designing, developing and deploying a mobile payment application safely and thus, avoiding risking the user data.

7.1. Design Guidelines

- Provide payment acceptance applications and any associated updates in a secure manner with a verifiable chain of trust; a vendor should be able to provide assurance the code within a payment application has not been tampered with or altered without valid authorisation.
- Develop mobile payment acceptance applications based on software secure coding guidelines. Poor security coding practices can introduce vulnerabilities and expose customers to the risk of account data compromise. A vendor should be able to demonstrate the following:
- Have in place and always use secure software development/maintenance measures.
- Maintain security guidelines describing how the update mechanism is to be used when deployed platforms can be updated.
- Protect encryption keys that secure account data against disclosure and abuse in accordance with industry-accepted standards.
- Enable the unique identification of a transaction coming from a merchant. The acquirer or payment service provider should be able to identify the consumer mobile device, mobile terminal and/or mobile acceptance application. Among other benefits, this will allow recognition of unique fraud patterns emerging from mobile payment acceptance solutions.
- Restrict manual PAN Key transactions on a consumer mobile device to a minimum. Key entered transactions should never be used as a primary means of capturing account data. In the event of chargebacks or refunds, the acquirer or payment service provider should provide a means to allow for the chargeback or refund to be processed without requiring the input/display of a full PAN.

---

7 Mobile Payment Acceptance Visa Security Best Practices
7.2. Prevention of Software Attacks on Mobile Devices

The following list of instructions briefly summarises the main actions of preventing software attacks on consumer mobile devices in connection with NFC mobile services.

- Install software only from trusted sources. Merchants must respect the security measures on the consumer mobile device. To avoid a new attack vector to the consumer mobile device, install only trusted software necessary to support business operations and facilitate payment.
- Establish sufficient security controls to protect the consumer mobile device from malware and other software threats. For example, install and regularly update the latest anti-malware software.
- Merchants should also regularly update the firmware of their POS device and install application updates whenever they become available.
- Merchants who deliberately choose to undermine the native security controls of the consumer mobile device by “jailbreaking” or “rooting” the device will usually increase the risk of malware infection.

7.3. Appropriate Controls to Consign Merchants

Ensure that appropriate due diligence takes place when consigning and monitoring merchants; include, for example, adequate Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures. Acquirer and Payment SP must be in compliance with all local laws and regulations regarding merchants.

The payment SP interfaces with the Acquirer on behalf of its sponsored merchants, and it must ensure that its sponsored merchants are contractually obligated to operate according to the best practice requirements of the payment service provider.

7.4. Limiting the Exposure of Account Data Viable Fraud

- Provide the ability to encrypt all public transmission of account data. To maintain confidentiality and integrity, account data must be encrypted during transmission over wireless, public and/or private networks. All account data originating from a Mobile Payment Acceptance Solution sent to any other termination point must be encrypted in accordance with industry accepted encryption standards using industry-accepted algorithms and appropriate key sizes.
7.5. Proper monitoring of Mobile Payment Acceptance Solutions

Where network connectivity is available, ensure that all authorizations are processed online. Online processing provides the ability to monitor transactions and detect fraud. It reduces the exposure that a business may have to fraudulent transactions through use of the most up-to-date fraud monitoring system and thereby reduces the possibility of fraudulent transactions. Also, online processing facilitates other value add services such as couponing.

8. Communication between NFC Mobile Devices and POS Terminals

To make proximity mobile payments possible the NFC-equipped mobile device must be loaded with a payment application and the merchant terminal must be configured to accept contactless transactions. The payment transaction is then performed equal to a standard contactless credit or debit card transaction. The mobile device is presented to the terminal at the point at which a contactless payment card would be presented. The terminal, not the mobile device, initiates the transaction and the terminal does not attempt to read the mobile device until the transaction is initiated. The transaction communication between the mobile device and the terminal is immediate and the terminal displays an indication when the transaction is processing and when the transaction is completed.

8.1. Consumer Perception

From a consumer perspective, an NFC-enabled mobile phone behaves exactly like a contactless payment card during a transaction. The amount of interaction between the
consumer and the phone depends largely on the implementation of the payment application on the phone, which in turn is defined by the issuer or the payment brand. There are no specific requirements for consumer interaction, just as there are no requirements for a cardholder to interact with a contactless card during a transaction. The consumer only interacts with the terminal.

The payment application that is loaded on the mobile device may be designed such that the consumer must enter a password or present a fingerprint to the mobile device to initiate or respond to the terminal’s transaction initiation or to validate the payment. Password entry is meant to provide the consumer with assurance of control over the transaction. If the consumer has multiple payment applications on the phone, each could have different user requirements for conducting a transaction.

The handset firmware can also determine accessibility to the payment application using the NFC modem. The configuration options available for the NFC modem in a handset vary by handset manufacturer. For example, one handset could have the following configuration options:

- • Always allow access to the application (card is always available)
- • Allow access to the application only after user confirmation
- • Only allow access to the application upon input of the correct password (set by the user)

### 8.2. Managing Multiple Applications

When more than one payment application is installed on a single handset, a mobile wallet can be loaded on the phone to manage the multiple application interfaces. The wallet enables the consumer to select a preferred payment or issuer brand for each transaction, analogous to a consumer opening a wallet or purse and selecting the card to use for a transaction. A mobile wallet can also enable the consumer to designate one brand as a default payment brand. For example, if a person primarily uses one specific credit or debit card that application can be set as the default payment brand. Then to use a different payment account in a retail outlet, the user would need to select a different payment brand.

### 8.3. Potential for MIDlet Use

A MIDlet is a Java 2-based mobile phone or pager application. Many types of MIDlet functions can be added to mobile handsets for marketing and handset navigation purposes. For example, the handset firmware can be set up to automatically open a
MIDlet that displays a particular logo when a certain application is selected. When a bank payment application is used, the logo of that bank would then be displayed on the handset during or immediately after the transaction.

8.4. PIN Requirements

The PIN is commonly the password used by the Contactless Payment Application to authenticate the cardholder of the application. Following the standard, ETSI 102 221 “Smart Cards UICC-Terminal interface Physical and logical characteristics”, there are three types of PIN according to the standard: The Universal, the Application and the Local PIN. Two of them should exist in every UICC, namely the Universal PIN and the Application PIN.

Current document wants to emphasise the importance of the three PINs for the implementation of the security architecture in the UICC by verification and by access to the rules files in the UICC. If you want more information on technical implementation, please refer to the ETSI TS 102 221 standard. An example of the security architecture based on the standard can be found at the 3GPP TS 31.101 document, under the chapter 9 “Security features”, which you can download at http://3gpp.org/ftp/tsg_t/tsg_t/TSGT_05/Docs/PDFs/TP-99185.pdf

In addition to the UICC security, it is necessary to secure the application level of the NFC services too, for that purpose there are other standards such as the PCI DSS. The following list below lists the most relevant recommendations from the PCI DSS standards related to the PIN security:

- PIN requirements regarding the point of sale to meet the PCI DSS standard “PIN Transaction Security (PTS) Point of Interaction (POI)”. 8
- Requirements for PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security - v3.x
- Encrypting PIN Pad (EPP) Security Requirements- v2.1
- POS PIN Entry Device Security Requirements- v2.1
- Hardware Security Module (HSM) Security Requirements, v1.0
- Unattended Payment Terminal (UPT) Security Requirements - v1.0

---

8 PIN Transaction Security (PTS) Point of Interaction (POI)
https://www.pcisecuritystandards.org/pdfs/pci_pts.poi_sr.pdf

Copyright © 2014 Mobey Forum Part 2 in a Series of Whitepapers on NFC security
8.5. Payment Transaction Security

Transaction security refers to data and information security in financial and telecommunication networks, as well as to securing messages and transactions that contain sensitive customer data. It is important that these networks safeguard thes information while in transit and when in storage.

Proximity mobile payments leverage ISO/IEC 14443 standard, which sets the communication between the contactless devices and terminal. Payment transactions invoke additional layers of security during transaction processing, regardless of the type of transaction: stripe, contactless or mobile.

In case of mobile payment transactions, the first layer of security is provided by the SE itself, which protects the mobile payment application by installing it in the restricted access memory.

The terminal initiates communication with the mobile handset. The terminal does not constantly scan nearby (two to four-inch range) areas for an active mobile handset; rather, it only attempts to locate the mobile handset or contactless payment card when it prompts the user to present it to the device. Once the device is located, communication between the terminal and handset takes place within 500 milliseconds.

The mobile payment application generates a dynamic cryptogram that is integrated into the transaction communication process with the terminal. The merchant system and terminal perform risk management checks. Then the host system completes the authorisation, which is in charge of verifying the limit available and card validity, among other things.

When a transaction ends, a final command is sent to the mobile device by the terminal. However, the terminal does not consider the communication to be complete until the mobile device is moved out of the field of communication. In other words, another transaction cannot take place until the mobile device that executed the previous transaction is moved completely away from the contactless reader field and the cashier initiates a new transaction.

As can be seen, all parts of the process collaborate together to perform the security checks. A single security check done by an isolated part of the process is not considered secure enough.
9. Conclusions

The following conclusions summarise the guidelines presented in the whitepaper for the best practices in the NFC mobile payment environment involving all mobile service providers and other stakeholders:

- The industry standards provide many guidelines for better NFC mobile services deployment, but further studies may still be required to match future market trends. For example, the creation of a new business model such as the “consumer centric” model will bring new challenges in terms of new roles and features.
- The NFC services tend to be multiple SE operable in the aggregation model. Best practices need to be followed and the standards that support the model.
- It seems the MNO plays the most important role in the mobile device lifecycle. There are, however, models to decrease the responsibilities of the MNO if they authorises another stakeholder such as a SP or TSM to manage main tasks.
- The UICC cryptography recommended by the standards improves the confidentiality and integrity of the UICC financial data. Thus, the general recommendation will most likely be to use public key cryptography.
- The key management is based in keys interchanged between the stakeholders depending on a relationship of trust. As in any mobile service ecosystem, the procedures should be formalised and documented to make sure they are followed correctly.
- The development of a mobile payment application should follow the coding guidelines stemming from the best practices. A mobile payment application should be signed as well as continuously tested and updated.
- The secure management of an NFC mobile payment ecosystem depends on the strength of the bondage between the parties concerned and their motivation to follow the best practices in the most effective way possible.
10. Citations and References


GlobalPlatform Messaging Specification for Mobile NFC Services v1.0.pdf
http://www.globalplatform.org/specificationssystems.asp

GlobalPlatform Specifications in the UICC Configuration v1.0
http://www.globalplatform.org/specificationscard.asp

Chip and PIN is Broken 2010 IEEE Symposium on Security and Privacy at

“Chip and Pin is Broken” Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond, University of Cambridge 2010

Chip and Skim: cloning EMV cards with the pre-play attack at
http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf

“Eavesdropping Near Field Communication”. Norwegian Information Security Conference 2009 Henning, Siitonen, Kortvedt and Stig F. Mjølsnes Department of Telematics NTNU

Elliptic curve cryptography on Smart Cards without coprocessors”. Woodbury, A. D., Bailey, D. V., and Paar, C. 2001. Proceedings of the fourth working conference on smart card research and advanced applications on Smart card research and advanced applications, pp. 71-92


“Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks”. Saar Drimer and Steven J. Murdoch Computer Laboratory, University of Cambridge at http://static.usenix.org/events/sec07/tech/drimer/drimer.pdf

Mifare Classic analysis in Czech Republic / Slovakia

Mobile Devices Security on Practical Risks of NFC Payments at


11. Appendices

Appendix 1: Mobile Features

Application Activation User Interface (AAUI)

This is the element with which the user interacts to perform the application selection. There may be more than one AAUI on a mobile device, however only one is active at once. Whilst the payment applications are hosted on a secure element, the location of the AAUI may vary. For example, the AAUI could be implemented as an application running in the application environment of the mobile device (for example, a Java MIDlet), or it could be implemented on a secure element (for example, a UICC with the AAUI implemented as a smartcard web server (SCWS) application). The Proximity Payment System Environment could be implemented on a secure element, in the application environment of the mobile device, or even in the contactless module.

Application Execution Environment (AEE)

The mobile device functionalities may be expanded to realize NFC mobile services such as voice calling, packet communication, phonebook, browser, mailer, and so on. It also provides a user interface to execute phone services interactively. All these functionalities are used and expanded to realize NFC mobile services, and as a group are termed an Application Execution Environment (AEE). AEE supports data storage and processor capabilities and executes mobile phone services in a relatively secure manner, but this level of security may not be sufficient to meet the needs of all NFC service providers.

Trusted Execution Environment (TEE)

Some categories of NFC services, such as payment, require highly trusted environments, which are not necessarily realised by the AEE. The Trusted Execution Environment (TEE) executes security-relevant NFC applications in a trusted and secured environment. The TEE can have various form factors, some of which can be removable (or replaceable), but the most important characteristic from an interactive services point of view is that the TEE has an interface to the AEE.

A TEE provides secure data storage, secure management functionalities, secure execution environment and so on. The secure management functionality is used for realising OTA downloading of applications and remote issuing/personalisation of NFC mobile services. Some of these functionalities may be shared tasks with the AEE, but the TEE enhances security to satisfy the requirements for trusted NFC services. On the other hand, the TEE can disclose a specific interface to the AEE and give permission to access...
the TEE through the interface. For example, a mobile phone browser may access data stored in the TEE.

An NFC mobile phone may potentially have more than one TEE. There are various reasons to provide these, including user control, different service providers requiring separate TEEs for their applications, different levels of security policies, etc.

Appendix 2: Roles of Stakeholders in the NFC Ecosystem

This appendix outlines the roles of major stakeholders within the NFC ecosystem (considered relevant to this NFC security analysis study).

Application Developer (AD)

The Application Developer is an organisation that architects, designs or builds an application code. ADs can be solution providers or merchants who modify or create software.

Application Provider (AP)

The Application Provider has a direct business relationship with the customers and holds the responsibility for the mobile NFC service management in the Secure Element and mobile phone, but does not perform operational tasks; these tasks are delegated to the SDM. The AP procures the necessary components to load a complete application (i.e. application code, application data, application keys and/or certificates and data belonging to a specific cardholder) onto a card.

Mobile Network Operator (MNO)

The MNO is the actual mobile network for the mobile communications. The MNO maintains the mobile communication infrastructure and provisions wireless settings to the phones provided to consumers. It also determines both the required handset features and functions and service options to be provided with mobile phones sold by the operator. Finally, the MNO also ensures the OTA connectivity between the consumer and the NFC application Service Provider.

Security Domain Manager (SDM)

The Security Domain Manager is responsible for a set of security domains in a SE. Depending on the privileges associated to its Security Domains, the SDM may have the capability to directly load, install, extradite or personalise applications on behalf of an Application Provider. If it does not have sufficient privileges or it does not have an OTA capability, it may request the help of another SDM to perform individual card content management operations or OTA dialog.
Also, the SDM may be responsible for the global SE and mobile device NFC service management operations on behalf of the Application Provider. In this case, the SDM may need the knowledge of the global SE and mobile NFC service breakdown structure.

**Secure Element Issuer (SEI)**

The Secure Element Issuer is the entity that sources the SE, controls the SE’s secure domain keys, brands the SE and provides it to the end-users. The SEI can also open the SE to additional Application Issuers (AI). For instance, the SEIs can be MNOs, financial institutions, transport authorities, customer loyalty schemes owners, or even the TSM, which provides the service to the SP. Alternatively, an SEI can also be an independent organisation who wishes to empower the mobile financial service and claim a position in the new and constantly developing Mobile Financial Services Ecosystem.

Some of its main responsibilities include developing the card product profile and choosing the appropriate platform and application technologies. The SEI creates an Issuer Security Domain (ISD) inside of the secure element. The SDM performs card management operations with the ISD.\(^9\)

**Controlling Authority (CA)**

The Controlling Authority manages exchanges with an optional third party entity when it is required by the deployment model. The Controlling Authority enforces the security policy in an environment with multiple stakeholders accessing to the SE. Specifically, it may be used for secure Security Domain creation in a SE. The Controlling Authority entity is mandatory when using confidential application loading and personalisation.\(^10\)

The CA keys and certificate are loaded into the controlling authority secure domain by the card manufacturer during the UICC manufacturing.

The “Confidential Setup of Initial Secure Channel Keys” require that the CA entity must be a trusted third party to the Link Platform Operator (an entity operating an OTA platform, i.e. the MNO or TSM) and the entity in charge of the application personalisation (i.e. either the TSM or SP). The controlling authority may be a Certificate Authority or the SIM vendor itself.\(^11\)

**Trusted Service Manager (TSM)**

The Trusted Service Manager (TSM) is a trusted third party between SPs and NFC mobile phones. The SPs can deliver NFC Mobile Phones with remote management functionality

---

9 GlobalPlatform Messaging Specification for Mobile NFC Services v1.0.pdf
10 Chapter 11 “Confidential Setup of Initial Secure Channel Keys” of the UICC Configuration
11 GlobalPlatform Specifications in the UICC Configuration v1.0

Copyright © 2014 Mobey Forum Part 2 in a Series of Whitepapers on NFC security
through the TSM. Depending on the deployment, the TSM may have the following key functionalities:

- Issuing and managing the trusted execution environment
- Assigning trusted areas within the trusted execution environment to a specific service
- Managing keys for the trusted execution environment
- Securely downloading applications to NFC Mobile Phones
- Personalising applications
- Locking, unlocking and deleting applications according to requests from a user or a service provider

Above-described functionalities can be performed by MNOs, SPs or third parties and all or part of them can be delegated by one party to another.

Even though the TSM uses the word “trusted” in its name, this role is not necessarily associated with the key management functions. In most cases TMS will not be managing keys neither for the MNO nor the service provider.

Appendix 3: NFC communication protocols

Between the POS and the contactless card various protocols are involved in each of the layers of the OSI model. The following table lists them:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO7816-4</td>
<td>The protocol defined by the ISO7816 defines the communication between a smartcard and a partner. The ISO7816-1 to 3 defines the card physical characteristics and communication (these parts do not apply in a contactless environment, instead it is used the ISO14443-A) and part 4 defines the organization of information in the smartcard requests and responses.</td>
</tr>
<tr>
<td>ISO14443A-NFC</td>
<td>The protocol defined by specific ISO14443 RFID communication standard at a frequency of 13.56 Mhz, defines two sub standards A and B which differ from one another in the signal modulation methods. Variant A is commonly used in communications using NFC technology.</td>
</tr>
</tbody>
</table>
EMV

EMV (Europay Mastercard and Visa) is a standard for interoperability between POS and payment cards that integrate smartcard. The standard is currently managed by EMVCo entity and can incorporate controls to authenticate the card and prevent fraud.

There are three security modes some of which may operate offline and online:

- SDA (Static Data Authentication): The card does not implement any kind of cryptography and simply authenticate using a certificate that can be verified by a CA. This mode of operation is vulnerable to replay attacks.

- DDS (Dynamic Data Authentication): The card implements RSA encryption and private key used to encrypt a "nonce" produced by the POS. Advertise with the signed public key certificate for this to be verified by a CA.

- CDA (Combined Data Authentication): The card implements RSA encryption and private key used to generate a cryptogram with various data from the POS. It publics the signed public key with the certificate for this can be verified by a CA.

It should be noted that at the moment none of the aforementioned layers of communications encryption are implemented because:

- ISO7816-4 standard defines only the operations.

- ISO14443A standard defines only the physical communication and security delegated to higher layers.

- EMV was originally designed for communications in touch and no measures were implemented to encrypt communications.

Appendix 4: Standards and Certification Organisations

EMVCo

EMVCo LLC was formed in February 1999 by Europay International, MasterCard International and Visa International to manage, maintain, and enhance the EMV™ Integrated Circuit Card Specifications for Payment Systems. Europay was acquired by MasterCard in 2002. Japan Credit Bureau (JCB) joined the organization in 2004 and American Express joined in 2008. EMVCo is currently operated by American Express, JCB International, MasterCard Worldwide, and Visa, Inc EMVCo's primary role is to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications to ensure interoperability and acceptance of payment system integrated circuit cards Worldwide.
With regards to mobile payments, EMVCo intends to define clearly the role and scope of EMVCo in the development of a standardised platform for mobile EMV payments. The platform standardisation will enable that type of payment method to be deployed to a mass market. EMVCo envisions its role as a mobile payments industry standardisation coordinator. It aims to make the organisation recognized as the common voice of the payments industry on contactless proximity mobile payments standardisation. EMVCo’s role in this respect is two-fold, involving the organisation in both technical development issues and industry coordination.

**GlobalPlatform**

GlobalPlatform is a consortium that intends to maintain and drive adoption of its technical specifications, which provide an open and interoperable infrastructure for smart cards, devices, and systems. The GlobalPlatform smart card infrastructure is intended to simplify and accelerate the development, deployment, and management of applications across industries and geographies.

GlobalPlatform abides by the following guiding principles:

- Maintain the stability of specifications and changing them to meet market needs rather than for technical elegance
- Preserve backwards compatibility when updating technical specifications
- Support security architecture with a range of options to meet the different market needs
- Remain form-factor independent and allow implementation on a wide range of devices

To address the needs of the growing mobile payments market, GlobalPlatform launched the Mobile Task Force in April 2007 to actively contribute to the development of mobile telecommunications standards worldwide. In excess of 20 GlobalPlatform member companies currently participate in task force activity. The task force provides input to the technical committees concerning the specific and emerging requirements of the mobile sector so that the GlobalPlatform card, device and systems specifications can be expanded and updated to suit the mobile market’s needs.

**Smart Card Alliance**

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Alliance invests heavily in the education of appropriate uses of technology for identification, payment and other applications and strongly advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity. Through specific projects such as education programs, market research,
advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart card technology, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.
Table 2: List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEE</td>
<td>Application Execution Environment</td>
</tr>
<tr>
<td>AI</td>
<td>Application Issuer</td>
</tr>
<tr>
<td>AMK</td>
<td>Application Provider Master Key</td>
</tr>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CDA</td>
<td>Combined Data Authentication</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CVC</td>
<td>Card Verification Value</td>
</tr>
<tr>
<td>CMK</td>
<td>Card Management Key</td>
</tr>
<tr>
<td>DDS</td>
<td>Dynamic Data authentication</td>
</tr>
<tr>
<td>EMV</td>
<td>Europay MasterCard and Visa</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>ISD</td>
<td>Issuer Security Domain</td>
</tr>
<tr>
<td>KMD</td>
<td>Initial Application Provider Master Key</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OTA</td>
<td>Over The Air</td>
</tr>
<tr>
<td>PAN</td>
<td>Primary Account Number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>SD</td>
<td>Secure Digital</td>
</tr>
<tr>
<td>SDA</td>
<td>Static Data Authentication</td>
</tr>
<tr>
<td>SE</td>
<td>Secure Element</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SSD</td>
<td>Supplemental Security Domain</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TEE</td>
<td>Trusted Execution Environment</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TSM</td>
<td>Trusted Service Manager</td>
</tr>
</tbody>
</table>
USIM  Universal Subscriber Identity Module