Security of Proximity Mobile Payments

A Smart Card Alliance Contactless and Mobile Payments Council White Paper

Publication Date: May 2009

Publication Number: CPMC-09001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

TABLE OF CONTENTS

1 Introduction: Proximity Mobile Payments

The ability to pay for transit fares, groceries, and other products by simply waving a mobile phone near a point-of-sale (POS) device represents a new payment frontier in the United States and Canada although the technology has been in place in Japan for five years. Such payments, called proximity mobile payments, are defined as payments to a merchant that are initiated from a mobile phone that uses Near Field Communication (NFC) technology and that is held close to the merchant's POS equipment. Proximity mobile payments offer new business and revenue opportunities to banks, mobile network operators (MNOs),[1] merchants, processors, and startups.

This white paper provides an overview of the proximity mobile payments ecosystem. It describes both the end-to-end security requirements and an implementation model for using proximity mobile payments in North America. While a number of business models can be used to implement mobile payments,[2] this white paper focuses on a "collaboration model," where financial institutions, MNOs, trusted third parties and other stakeholders in the mobile payments ecosystem cooperate in the management and deployment of mobile applications. The white paper introduces the players, their roles, and their responsibilities in assuring the security of sensitive data. It explains how the payment application, consumer credentials, and consumer account information (such as a credit card number) are securely delivered to, loaded on, and stored in a mobile device. It also identifies risks present during the lifecycle of the payment information stored on the mobile device and suggests appropriate countermeasures.

This white paper focuses on the use of proximity mobile payments by consumers for credit and debit payment transactions only. Other approaches, such as those that involve stored value or closed loop transactions, are not addressed.

1.1 Technology Overview

NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. Using NFC technology as the basis for proximity mobile payments leverages the infrastructure currently being deployed to support contactless credit and debit card payments made using ExpressPay™ from American Express, Discover® Network Zip℠, MasterCard® *PayPass*™, and Visa payWave™. Implementations around the world, including small-scale trials in Atlanta, New York, and San Francisco, have produced unanimous feedback that proximity mobile payment is easy and convenient. [3]

NFC-enabled mobile phones incorporate smart chips that allow the phones to securely store the payment application and consumer account information and to use the information as a "virtual payment card." While these smart chips can be present in many forms, this paper addresses three options: smart card based subscriber identity module (SIM) cards, embedded secure elements in the phone, and secure digital (SD) memory cards. NFC payment transactions between a mobile phone and a POS terminal use the standard contactless communication protocols currently used by contactless credit and debit cards.

NFC will soon be available as standard functionality in many mobile phones. NFC will allow consumers to perform safe contactless transactions, access digital content, and connect electronic devices simply.[4] An NFC chip in a mobile device can act as a card or a reader or both, enabling consumer devices to share information and to make secure payments quickly.

For virtual payment cards to function on an NFC-enabled phone, a variety of entities must work together. Financial institutions, merchants, third-party systems providers, MNOs, mobile handset manufacturers, standards bodies, and industry associations all have roles and responsibilities in such an ecosystem.

---

1 Mobile network operators are also referred to as carriers.

2 Smart Card Alliance, *Proximity Mobile Payments Business Scenarios: Research Report on Stakeholder Perspectives*, July 2008.

3 *The New York Times*, "Phones as Credit Cards? Americans Must Wait," January 25, 2009.

4 NFC Forum, "One Year after Launch, NFC Forum Membership hits 70 Organizations Worldwide," press release, February 22, 2006.

1.2 Collaboration Model Overview

Figure 1 illustrates the entities involved in the collaboration model and shows the flow of information for the issuing financial institution to provision the consumer's payment account information to the phone and for the consumer to use the phone to make a proximity mobile payment. This model posits collaboration among financial institutions, the MNO, and other stakeholders in the mobile payments ecosystem, including (potentially) a trusted third party who manages the deployment of mobile applications (the trusted service manager, or TSM). In this figure, solid arrows are used to indicate payment related transactions, while outline arrows are used to indicate actions related to the personalization of the application.

Financial institutions prepare the account data, and send the payment account information to a TSM. The TSM delivers the consumer's payment account information over the air (OTA) through the mobile network to the secure element in the mobile phone. Once the payment account is in the phone, the consumer can use the phone as a virtual payment card at merchants who accept contactless credit and debit payments. Payments are processed over the current financial networks with credits and debits to the appropriate accounts.

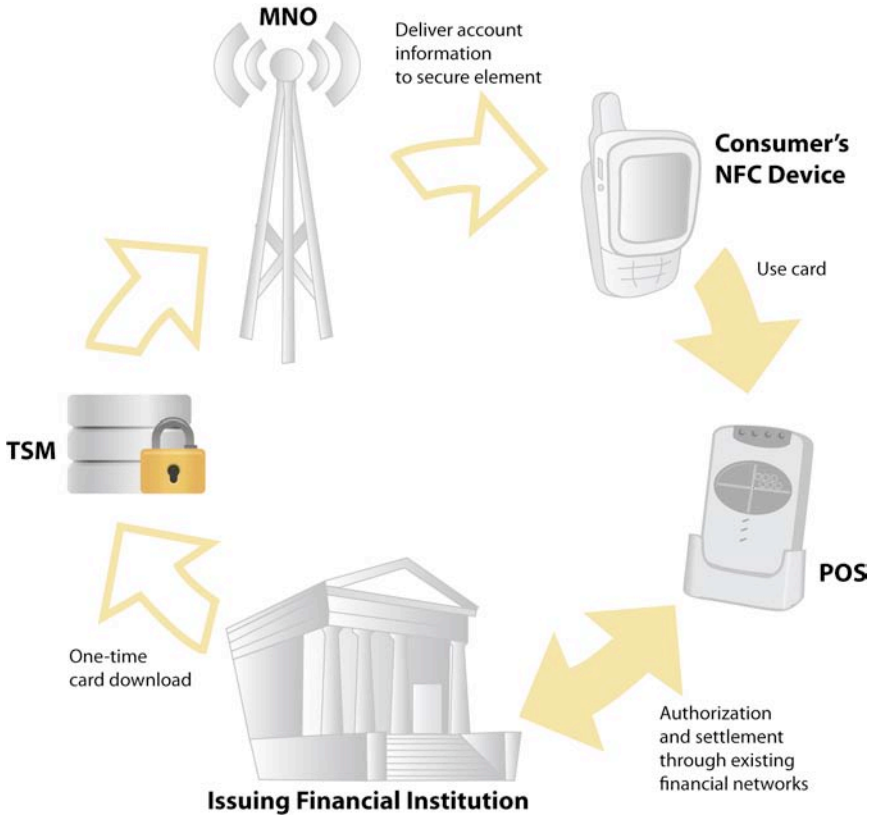

Figure 1. Collaboration Model Stakeholders

Figure 2 illustrates the security mechanisms that protect the processes used in the collaboration model.[5] Payment information personalization and lifecycle management from the issuer to the TSM are secured by standard Internet technologies such as secure sockets layer (SSL) or virtual private networks (VPNs). GlobalPlatform's secure channel protocol provides for the communication and storage of sensitive account data between the TSM and the secure element in the mobile device. Account data is further kept secure from OTA sniffing by encryption provided by the MNO.

[5] Details of this model may differ for Canadian implementations.

When the consumer uses the NFC device for payment, the transaction is protected using the same security mechanisms in place for contactless credit and debit cards. Account data is easy to secure because the chain of custody is clear and the information is never converted to a form in which it can be easily compromised.

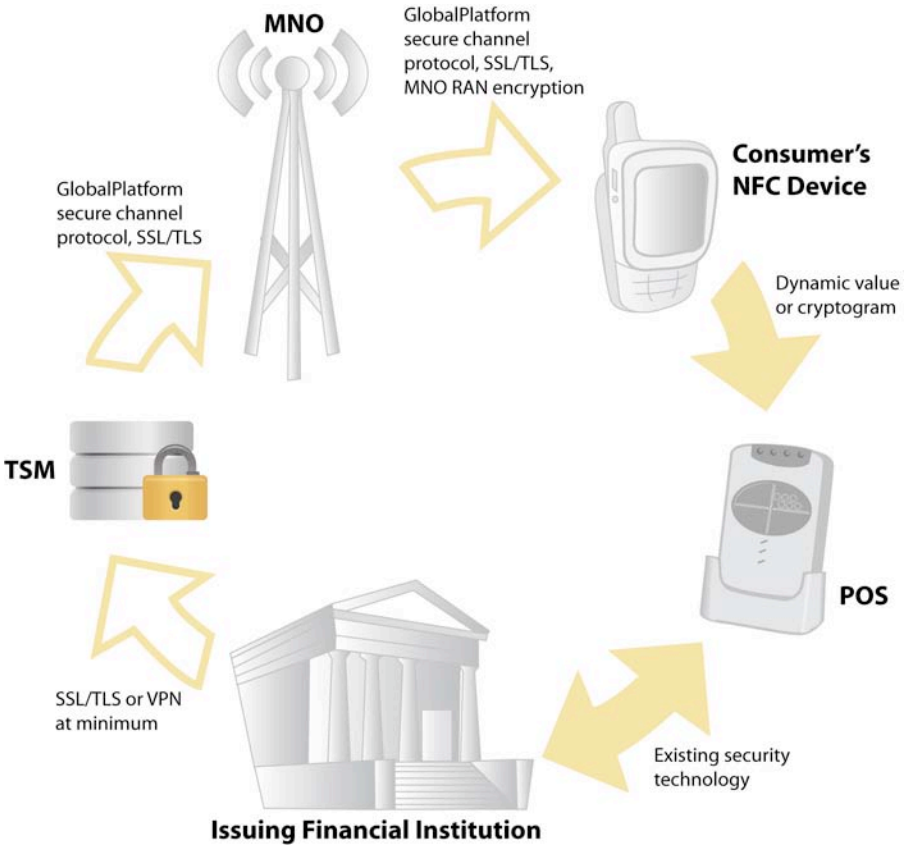

Figure 2. Collaboration Model with Security Mechanisms

1.3 Collaboration Model Stakeholder Roles and Benefits

1.3.1 Financial Institutions/Banks

Proximity mobile payments allow financial service providers to offer new, differentiated payment services to their customers, increase their credit and debit card transaction volumes, and extend their brands. In fact, institutions that traditionally lead with innovative new payment products are already piloting such services. Payment brands are also teaming with mobile device suppliers to incorporate their brands into emerging products.

By leveraging the contactless merchant infrastructure currently being deployed and adding contactless payment to mobile phones, financial institutions can provide their cardholders with the same trusted payment services in a new form factor, the mobile phone. This functionality allows customers to pay more quickly and conveniently thereby increasing customer loyalty. In addition, mobile payment allows financial institutions to further penetrate cash-and check-heavy merchant segments and open new acceptance channels.

1.3.2 Merchants/Retailers

Proximity mobile payment implementations capitalize on the existing contactless payment infrastructure and offer immediate value to merchants. Merchants who accept contactless payments have everything ready to accept proximity mobile payments. Transactions using contactless cards and proximity mobile payment devices are processed through a single, contactless-enabled POS system and the current financial networks, encouraging merchant adoption of both contactless and proximity mobile payments.

Numerous implementations worldwide have demonstrated that contactless payment offers immediate merchant benefits in the form of faster payment transactions, increased spending and improved customer convenience. Mobile payment can also help merchants establish stronger customer relationships and customer loyalty.

Merchants benefit from the operational efficiencies generated by faster transactions and fewer requirements to handle cash, which lower costs and enhance customer convenience. Merchants, like financial institutions, can offer their customers purchase-related and loyalty services, such as paperless receipts. Merchants can also make their gift card and loyalty programs more effective; customers' "payment cards" are always available in their mobile phones.

Merchants will also be able to deliver advanced mobile marketing and promotion programs that leverage the mobile device and proximity technology to deliver context-sensitive messages to customers, influencing their behavior inside and outside of the store. Mobile promotions and couponing were prominent features of multiple NFC mobile payment pilots and were proven to have positive influence on consumer behavior and great acceptance by consumers.

1.3.3 Trusted Service Managers

TSMs offer a single point of contact with mobile operators for financial institutions, transit authorities, and retailers who want to provide a payment, ticketing, or loyalty application to customers with NFC-enabled mobile phones. TSMs provide services to send and load the NFC application over the air to the mobile phone and to aggregate, send, and load personal consumer data over the air. This role parallels the role of card personalization service providers for credit and debit payment cards. In a large NFC ecosystem, use of a neutral third-party TSM can be the most desirable scenario. However, financial institutions or MNOs can also function as TSMs.

The TSM manages the mobile NFC applications, providing secure download and lifecycle management services. Because the TSM does not participate in processing the payment transaction, existing payment processing business models can be maintained.

Both MasterCard and Visa have strict requirements for entities that wish to act as TSMs. All TSMs are subject to security audits before being authorized to process the delivery of payment card data to a mobile device. An important TSM responsibility is to manage the cryptographic keys and system used to securely communicate the payment information from the financial institution to the consumer's mobile device. Without proper key management and security, the entire system could be exposed to attack and systemic fraud. TSMs will also need to be acceptable to the MNO, whose product will have to manage the consumer interface between the POS and the NFC application stored on the mobile phone.

Proximity mobile payments offer new business opportunities for service providers including existing third-party personalization service providers, to become TSMs and offer services to MNOs and financial institutions. The role of a TSM is critical in the proximity mobile payments ecosystem since it can enable interaction among many service providers and multiple MNOs.

1.3.4 Mobile Network Operators

The MNO's main function in the proximity mobile payments ecosystem is to offer NFC-enabled phones to their subscribers and to deliver sensitive account data and payment applications to mobile devices. When the account data is provisioned to the secure element of the device, the MNO's function is complete.

At a very minimum, the MNO is responsible for maintaining the integrity of the cryptographic keys that protect the secure elements on the mobile devices it provides to end consumers. The MNO is also responsible for the integrity of the keys and certificates that protect communication across its radio and core networks. If the MNO has chosen to fulfill the role of the TSM, it must also implement TSM functions.

According to a Deloitte & Touche report,[6] mobile operators could see significant economic benefits from offering mobile payments. Potential benefits include new customers, reduced customer churn, and revenues from new, payment- and NFC-related services (such as text message ads and coupons).

One of the challenges mobile phone operators face today is the high churn rate of their subscriber base. Operators seek applications that allow them to provide long-term services for customers and recognize that offering additional services can attract new customers and stabilize their subscriber base.

1.3.5 Payment Brands

Tens of millions of American Express, MasterCard and Visa branded contactless credit and debit payment cards and devices have been issued worldwide, proving the value of contactless payments to both merchants and consumers. The ISO/IEC 14443-based contactless merchant POS infrastructure that is now in place to support contactless credit and debit payment can also accept NFC-enabled proximity mobile payments, providing a head-start for broad acceptance and use.

The payment brands are continuing to extend their efforts to proximity mobile payments, participating in numerous pilots and working with industry groups to define the standards, specifications and processes for the new payment approach. Benefits to payment brand organizations include the ability to appear innovative and attractive to early adopter consumers. In addition to increasing the use of their branded products, proximity mobile payments offer the opportunity to continue to push broader merchant acceptance of contactless credit and debit payments.

1.3.6 Mobile Handset Manufacturers

The proximity mobile payments ecosystem is dependent on consumers having NFC-enabled mobile phones with the secure element that stores the payment application and account information.

Mobile handset manufacturers can gain a competitive advantage by offering mobile phones that support payment and other mobile applications. Just as the first camera phones captured consumer market share, so can the first mobile phones that support additional applications. Innovative mobile applications represent an opportunity for handset manufacturers to attract new customers and create additional business partnerships.

[6] Deloitte & Touche, "The Case for Using Mobile Phones for Payments," report, August 2004.

2 Standards and Certification Organizations

A mobile transaction depends on an ecosystem that includes a number of different elements: the mobile device, the contactless communications modem, a secure element hosting the payment application, a subscriber identity module (SIM) card, the payment application, and a user interface application running on the mobile device. The requirement for so many different elements presents a challenge: the entities involved must all acquire approvals from an assortment of governing bodies, each of which is responsible for the security and interoperability of a different element.

To ensure that the payment and mobile device technologies are interoperable, the technologies must comply with applicable standards and specifications. Several standards organizations define how the technology should be enabled. Other organizations define specifications that ensure the security of the payment transactions. The challenges that need to be to be addressed by the involved entities include determining an appropriate method for testing individual mobile phone handsets, secure elements, and resolving lifecycle issues.

All standards organizations are interested in increasing ease of access, global interoperability, and security of mobile payment technology to consumers. Table 1 summarizes the responsibilities of each individual standardization and specification organization that has a role to play in proximity mobile payments implementations. Appendix A describes the organizations in more detail.

Table 1. Summary of Standards and Certification Organizations

Organization	Standards or Activities Governed within the Mobile Payment Ecosystem			Responsibility
	Mobile Handset Only	Other Ecosystem Functions	Payment Applications	
PCI SSC		✓	✓	Maintains, evolves, and promotes standards for payment account security.
EMVCo			✓	Establishes specifications to ensure interoperability of smart card-based payment systems worldwide. For mobile payments, seeks industry collaboration and coordination in mobile payment standards.
Payment Brands			✓	Requires that a mobile payments application submit to a security and functionality qualification process for the application to be branded for their network (American Express, Discover, MasterCard, Visa).
GlobalPlatform			✓	Drives adoption of its technical standards, which provide an open and interoperable infrastructure for transactions performed on smart cards, systems, and devices.
ETSI	✓			Produces globally applicable standards for information and communication technologies including fixed, mobile, radio, converged, broadcast, and Internet technologies.
GSMA	✓	✓		Engages in technical, commercial, and public policy initiatives to ensure that mobile services are interoperable worldwide.
OMA	✓	✓		Develops mobile service enabler specifications to promote interoperability.

Organization	Standards or Activities Governed within the Mobile Payment Ecosystem			Responsibility
	Mobile Handset Only	Other Ecosystem Functions	Payment Applications	
NFC Forum	✓	✓	✓	Develops specifications for NFC devices that are based on the ISO/IEC 18092 contactless interface, ensuring interoperability among devices and services.
3GPP	✓	✓		Produces globally applicable technical specifications for third generation GSM.
3GPP2	✓	✓		Establishes standards for CDMA 2000.
CDG	✓	✓		Ensures interoperability among systems while expediting the availability of 3G CDMA technology to consumers.

3 Delivering Financial Data Securely to the Mobile Device

Using a TSM for proximity mobile payments allows issuing banks or other service providers to abstract themselves from the complexities of the mobile landscape while enabling consumers to achieve the maximum benefit from a broad-service ecosystem.

Proximity mobile payments do not require account data to be stored on a physical card. The data originates at an issuing bank and is passed securely through a TSM to the secure element in the mobile handset. The data is protected by cryptography throughout the process and the TSM has a critical role in managing the security of the process.

3.1 Cryptography

Cryptography is the primary mechanism used to keep sensitive payment applications and account data secure in the mobile payment ecosystem. Figure 3 shows an example of one implementation of a TSM-based mobile payment ecosystem.[7] As shown in this figure, the secure transfer of account data from an issuing bank to the TSM relies on public key infrastructure (PKI) and encryption based on the secure sockets layer (SSL)/transport layer security (TLS) standard.

The TSM stores the account information in an encrypted database. When a mobile device requests personalization, three separate layers of encryption are established with a packet data connection.

1. The mobile device establishes a packet connection across the MNO's radio access network (RAN). This OTA communication is encrypted at OSI[8] layer 1, based on protocols established by both the CDMA and GSM standards bodies. Security at this point is controlled by the MNO, because it manages the keys used to encrypt the data traffic. Data encryption on the RAN ensures privacy and confidentiality for data traffic between the MNO's core network and the consumer's mobile device. The OTA encryption layer adds another barrier to the potential for custody breach of account data due to radio sniffing.
2. Once the packet connection is established, the personalization service agent application running on the handset (for example, a mobile wallet application) establishes a TLS secure communication session to the TSM's personalization server at OSI layer 4, using credentials issued by a known certificate authority.
3. When this connection is established, the TSM initiates another secure connection to the mobile device's secure element using GlobalPlatform's Secure Channel Protocol, which executes at OSI layer 7. This final layer of encryption is secured by keys that belong to the issuing bank.

The use of application layer security leverages multiple protection levels. After this last connection is established, at least one logical layer of encryption, secured by the issuing bank's keys, always protects the data between the TSM's most sensitive process and the secure element in the handset. This layer is established by GlobalPlatform's Secure Channel Protocol. Most of the time two layers of encryption protect the data. While the data is traveling over the air, it is secured by three layers of encryption.

[7] Other ecosystem options include a distributed TSM model in which responsibilities for issuance and administration are controlled by different entities.

[8] Open Systems Interconnection (OSI) model, which posits an abstract description for layered communications and computer network protocol design. It divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers.

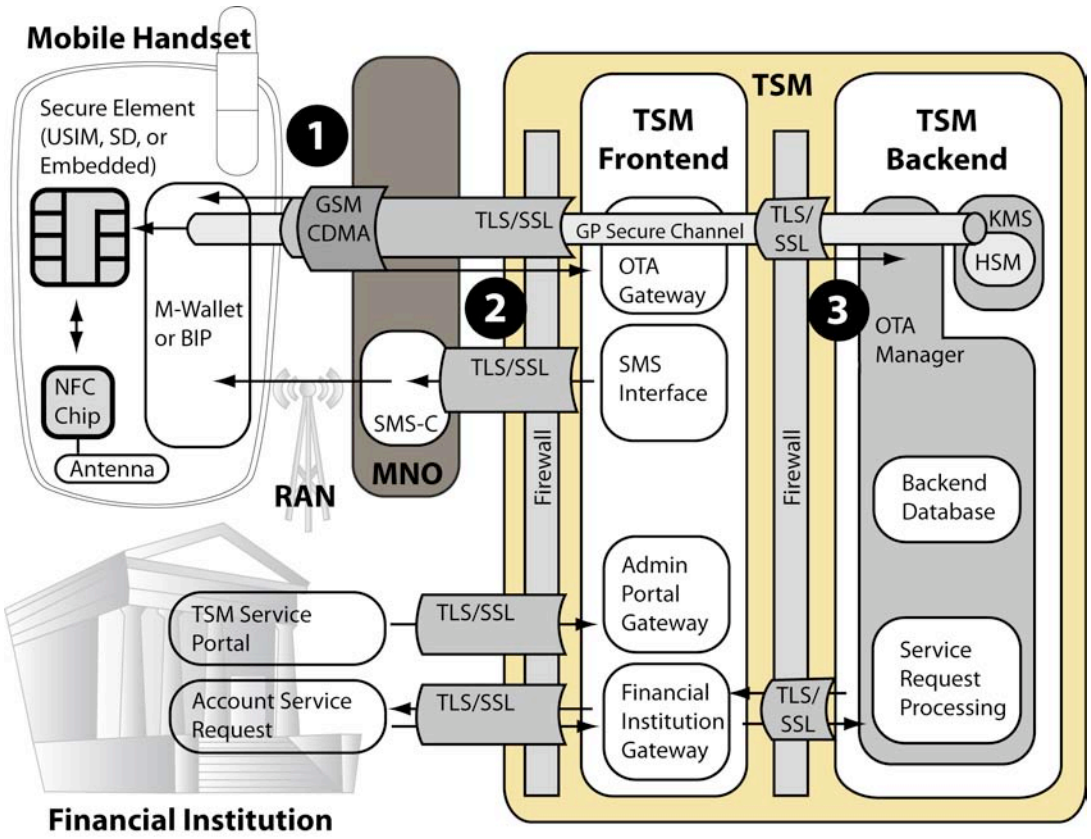

Figure 3. Example of TSM security architecture leveraging three separate layers of encryption

3.2 Key Management

Proper key management and security are essential to protect the system from attack and fraud. The key management process keeps the cryptographic keys secure. One of a TSM's primary functions is to ensure the security of the keys at all times.

Keeping the keys secure entails ensuring both physical security and logical security. Physical security prevents physical access to the key management server (KMS) and its related hardware security module (HSM). Physical security includes the use of man traps, physical barriers, and alarm systems. Logical security involves processes, procedures, and software used to safeguard the keys. Examples of logical security include password requirements, key import requirements and procedures, firewall rules, and the use of proxy systems for communications.

3.3 Data Persistence

A TSM needs custody of a consumer's account data for only the amount of time required to complete the mobile handset's personalization process. The process could take from 30 seconds to hours, depending on factors such as quality of network coverage or user expertise.

The bank transmits the account data to the TSM only after the consumer is ready to begin the personalization process on the mobile device. If the issuing bank transmits the data to the TSM before the consumer indicates readiness, the data is stored until the consumer initiates the personalization. This scenario might involve the consumer entering an activation code into the handset that initiates the personalization process.

Depending on the feature set agreed to between the parties in the value chain, the TSM may never have access to account information, because the data would remain encrypted by a bank's encryption key. This scenario could exist if the bank had a supplemental security domain (SSD) pre-established on the secure element by the MNO or if the TSM established an SSD with a temporary key that the bank knew. In this case the bank would generate the needed secure application protocol data units (APDUs) to establish a permanent SSD with the bank's keys and later personalize a card via a TSM pass-through.

If the bank directly entrusted the TSM with its keys, the TSM would generate a bank-specific SSD and personalize it with account data provided by the bank. In this scenario, once the personalization completed successfully, there would be no reason for any account data to persist with the TSM. In any case, the data need not persist at the TSM beyond the successful personalization of the mobile device.

4 Securing the Stored Payment Application and Account Information

Multiple layers of security apply to each stage of the proximity mobile payments process. Within the mobile phone, both the payment application and consumer account information must be protected and different NFC applications must be able to work securely and independently of each other. This section reviews how data is securely stored in the mobile handset, how data and applications are securely accessed and used, and how the mobile phone communicates with the POS reader.

Currently, there are three options for storing applications and data securely in the mobile handset: universal subscriber identity module (USIM) cards, embedded secure elements, or SD (memory) cards. All three options rely on the presence of a secure element in the mobile device.

4.1 Function of the Secure Element

The secure element (secure memory and execution environment) is a dynamic environment in which application code and application data can be securely stored and administered and in which secure execution of applications occur. The element resides in highly secure crypto chips[9] (usually a smart card chip). The element provides delimited memory for each application and functions that encrypt, decrypt, and sign the data packet. The secure element present in mobile devices is GlobalPlatform compliant to provide better interoperability.

Figure 4 illustrates alternatives for where the secure element can reside in a GSM or CDMA mobile phone. The first approach embeds a separate secure element directly in the handset (either mounted on the motherboard directly or connected in some way to the motherboard). A second approach is to embed the secure element into an SD card. A third approach is to embed the secure element in the USIM/SIM card. The industry is still evaluating the pros and cons of including multiple secure elements in a single mobile handset.

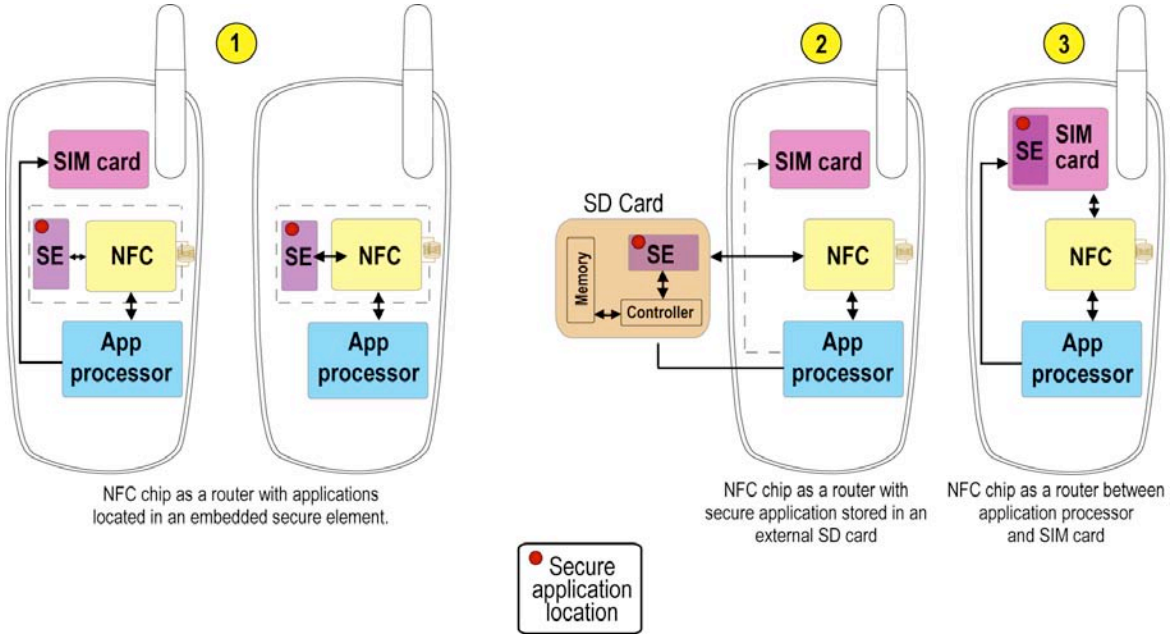

Figure 4. ① Embedded, ② SD Card-Based and ③ USIM Secure Element Solutions

[9] A crypto chip is a powerful, high-speed, programmable cryptographic engine for operating private and public key-based encryption systems.

4.2 Security Domains and Hierarchy

The GlobalPlatform specification (Version 2.2) defines multiple security domains that use authorized and delegated management to allow an application to be loaded into the secure element. The collaboration model establishes the hierarchy for security domains shown in Figure 5.

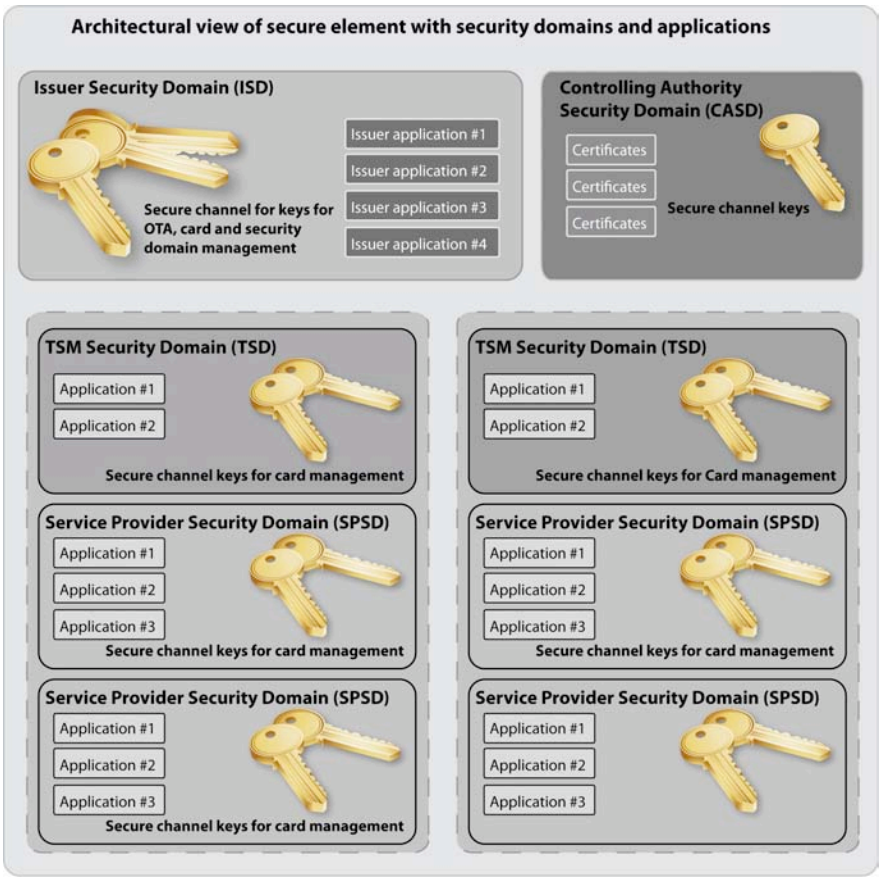

Figure 5. Architecture of the Secure Element, Security Domains, and Applications

Any GlobalPlatform-compliant secure element comes with one issuer security domain (ISD) and the option for multiple supplemental security domains (SSDs). As shown in Figure 5, the SSDs can be TSM security domains or domains belonging to service providers (such as credit card, ticket, prepaid/loyalty card, or transit card issuers). In addition, each secure element can have only one controlling authority security domain (CASD). This security domain architecture enables the service provider and trusted service manager to perform key management and application verification during load and installation processes.

The ISD is the portion of the secure element in which the MNO can store the keys for the following:

- OTA provisioning
- Card content management
- Security domain management

The ISD has privileges for global management, authorized management, and security domain management for the secure element. The ISD must be created during manufacturing and the key for card content management securely transferred from the manufacturer to the MNO. The ISD must authorize the creation of any SSDs. Only the ISD has the privileges to create an SSD and assign authorized or delegated management privileges.

An SSD can have its own card manager key for loading applications. The ISD can assign different sets of privileges (based, for example, on different business relationships) to the SSD designated as the TSM security domain and the SSD designated as the service provider security domain.

4.3 Chip-Level Security

The Smart Card Alliance white paper, *What Makes a Smart Card Secure?*[10] describes the multi-layer security architecture of a smart card chip. Security features manufactured into the secure microcontrollers used in smart card chips can prevent attackers from accessing sensitive information stored on the card.

The SIMs and USIMs in mobile phones are smart card chips, and have built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis.

With contact and contactless interfaces, increasingly powerful processors, a wide range of memory options, and flexible implementation of both symmetric and asymmetric cryptographic algorithms, smart card technology is a critical component of a secure system design.

4.4 API Interface to the Secure Element

An API between applications on the phone and the secure element is needed to enable over-the-air and local card management services. For phones that implement Java, two Java interfaces to the secure element are defined: JSR 177, to access SIM cards, and JSR 257, to access the NFC chip.

For phones that do not support Java, the handset and/or operating system vendor need to provide equivalent APIs to access the secure element and NFC chip.

A good practice is to require all phone applications that need to communicate to the secure element to be authenticated by a trusted entity (e.g., the carrier or handset vendor). The phone's operating system will then prevent access to the secure element APIs by any non-trusted applications,

4.5 Communication between the NFC chip and the Contactless Reader

Communication between the application on the secure element and the contactless reader (via the NFC chip) is based on two standards: ISO/IEC 7816 and ISO/IEC 14443. ISO/IEC 14443 helps the reader and NFC chip establish the device parameters for NFC communication. The NFC chip and the contactless reader exchange data using an application protocol data unit (APDU). The structure of an APDU is defined by ISO/IEC 7816-4.

While the reader and the secure element are in communication, the NFC chip is in card emulation mode. The contactless reader communicates with the NFC chip to identify which card is being emulated. The contactless reader then sends commands appropriate for that card type (Visa payWave, MasterCard PayPass, American Express, Discover Zip or other branded card) to start communication with a specific applet.

[10] Smart Card Alliance, *What Makes a Smart Card Secure?* October 2008, Publication Number CPMC-08002.

5 Interaction between NFC Mobile Devices and POS Terminals

For a proximity mobile payment transaction to be 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 much like 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 initiates the transaction, not the mobile device, 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 instantaneous and the terminal displays an indication that the transaction is processing and complete.

Figure 6 shows the transaction flow.

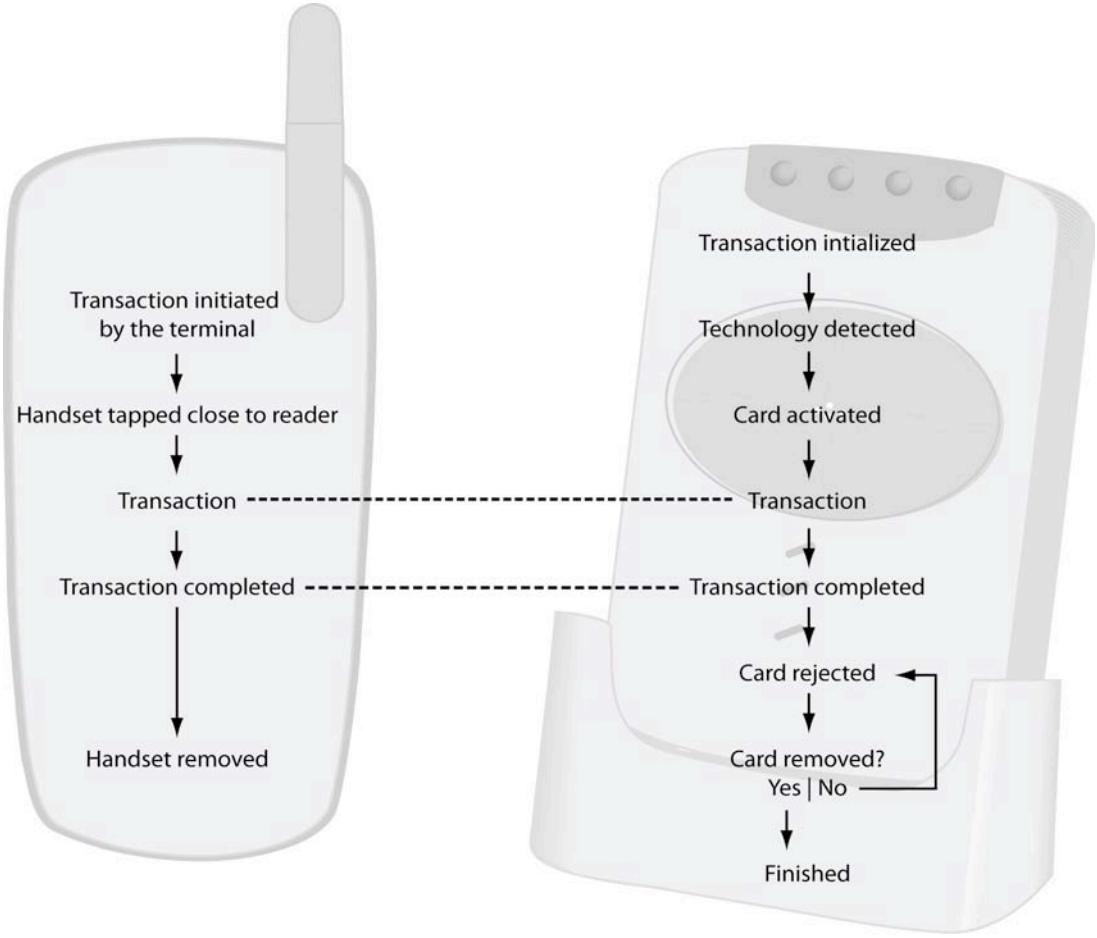

Figure 6. Mobile Contactless Transaction Flows

5.1 Consumer Perception

From the perspective of the consumer, 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 is defined by the issuer or the payment brand. There is no specific requirement for consumer interaction, just as there is no requirement 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 to the mobile device may be designed such that the consumer must enter a passcode or present a fingerprint to the mobile device to initiate or respond to the terminal's transaction initiation or to validate the transaction. Passcode entry is meant to provide the consumer with comfort or a sense of control over the transaction. If the consumer has multiple payment applications on the phone, each could feasibly 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 passcode (set by the user)

5.2 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 a specific credit or debit card, that application can be set as the default payment brand. To use a different payment account in a retail outlet, the user would need to select a different payment brand.

5.3 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.

5.4 Online PIN Requirements

A PIN is not inherently required to use a proximity mobile payment application. However, an issuer can choose to require it in appropriate circumstances. The use of an online PIN entered at the point-of-sale is issuer-dependent and out of scope of this white paper.

5.5 Transaction Initiation and Completion

The terminal initiates communication with the mobile handset. The terminal does not constantly scan the nearby (two to four-inch range) area 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 the device. Once the device is located, communication between the terminal and the handset takes place within 500 ms.

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. That is, 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.

5.6 Payment Transaction Security

Proximity mobile payments leverage ISO/IEC 14443, the standard that governs communication between a contactless credit or debit payment device and terminal. Payment transactions invoke additional layers of security during transaction processing, regardless of whether the transaction is a magnetic stripe transaction or a contactless or mobile transaction.

In the case of a proximity mobile payment transaction, the first layer of security is provided by the secure element itself, which protects the payment application by storing it in restricted access memory. The payment application generates a dynamic cryptogram that is integrated into the transaction messaging/communication process with the terminal. The terminal and the merchant system perform risk management checks; the host system then completes an authorization function, which checks the authorization limit available and card validity, among other things. The security provided by an isolated component in the process does not accurately represent transaction security as a whole.

6 Mobile Device Lifecycle Considerations

The mobile phone industry is highly competitive and driven as much by fashion as by features and functionality. People often see a mobile phone as a fashion statement and change their phone style based on trends in the fashion industry. The twin influences of fashion and functionality have resulted in a continuing compression of the handset life span and pressure on the handset manufacturers to shorten the handset development and release cycle.

In addition, for all practical purposes, there is no connection between the MNO's service contract and the phone used to fulfill the contract. It is common for consumers to change phones one or more times over the life of a service contract. When they do, the old phone ends up in a scrap drawer or the garbage. In the United States, the consumer generally has no need to do anything with the old phone when they discard it.

6.1 Mobile NFC Activation

The mobile payment application can be activated at the same time as the account-specific information is loaded onto the secure element, independent of the secure element form factor. Inactive mobile payment applications can be preloaded on a handset and delivered to consumers, who have the choice of whether and when to activate them. In the mobile NFC market, the payment application will be loaded in the secure element.

Once the handset manufacturer has released a mobile handset, an MNO purchases and inventories the phone. If the handset has an embedded secure element for the payment application, the application will already be on the phone but will need personalization and activation. It is also possible that the payment application could be loaded to the phone following release.

If the handsets are designed to be equipped with a USIM or SD device as the secure element, the handset will receive the payment application when the USIM or SD card is inserted into it. The MNO or handset vendor acting on behalf of the MNO (i.e., the retailer) adds the secure element when the phone is set up for the consumer. It is also possible that the retailer will have these secure elements prepackaged in the handset and inventory.

Since the payment application is not initially linked to the consumer, the consumer will be given instructions on how to personalize and activate their payment application. It is possible that the activation and personalization of the payment application can be performed at the retail outlet where the phone is sold.

6.2 Changing Mobile NFC Phones

The process of changing mobile NFC phones has different implications for managing the security of consumer data and payment applications resident on the secure element based on the model or type of secure element. Consumers will need to be educated to ensure that their personalized data and payment applications are securely transferred from one mobile NFC phone to a new phone.

As noted earlier, in the U.S., consumers have the habit of discarding "old" mobile phones when taking advantage of new handset functionality or fashion features. For 3G networks, the USIM card links the user's service contract to the phone and is the location of the secure element for mobile payment applications. Accordingly, the subscriber's identity and mobile payment applications will move with it as the USIM card is transferred from the old phone to the new NFC phone

For handsets with SD cards or USIM cards, when a consumer buys a new phone, the consumer will need to remove the USIM card or SD card from the old phone and place it in the new phone. Once the card is removed, the old phone is no longer connected to the person in any way. All personalized data and applications have been moved to the new phone. Use of a removable USIM or SD card allows the consumer to control the payment application. If not switching issuing banks or mobile network providers, there is no need to contact the bank or the MNO when changing phones other than to confirm that the new handset is payment enabled.

On the other hand, if the secure element is integrated into the phone, changing phones will require that the payment application on the phone be de-activated, if not removed. This may be possible through a user interface on the phone, or via a set of instructions for the consumer to follow.

6.3 Lost or Stolen Phones

If a phone used for proximity mobile payments is lost or stolen, the security of the payment application is determined by the payment application's implementation. In other words, if the handset is configured to require passcode activation of the payment application each time, the lost or stolen phone represents a minimal financial risk. The consumer would have to report the lost device to their bank, and the bank would have to send a payment application deactivation or block request through the TSM. However, the primary de-activation security will rely upon the host system as it does today with credit cards. If a card is lost or stolen, the consumer must report that fact to the issuer, who closes the account on the host system. When the account is closed on the host system, the card or phone will not be able to receive an authorization because the host system would also have been programmed to reject any new transaction requests. The only risk exposure would be linked to offline transaction limits that may have been configured for that consumer.

7 Countermeasures to Fraud

Whenever the payment industry develops a new way to make a payment, someone will try to exploit it for his or her gain. From the 1960s launch of the plastic card, up to the introduction of EMV-based transactions, fraudsters have worked tirelessly to find holes that they can exploit in the system.

The advent of proximity mobile payments will be a new challenge, but for the first time robustness can be built into all critical aspects of the system. Careful planning that considers all of the stakeholders, processes, and technologies involved, can result in a robust security model. And it can be a model that makes sense in the context of the transaction risk and does not represent an impediment to adoption.

7.1 Responsibility for Protection

One of the requirements of a robust security model for proximity mobile payments is to determine who is responsible vs. liable when the system fails. To identify responsibility, it is necessary to understand what entities are involved in system operations.

The industry has yet to establish an industry-wide operational model for proximity mobile payments. However, as described in Section 1, it is clear that, at the very least, the process will involve a consumer using a mobile handset, a mobile network operator enabling the loading of the payment account information and application, a merchant accepting the transaction with a POS terminal, a TSM aggregating the account information and transmitting it securely to the handset, and a processing service provider for settlement and clearing banking functions. Each of these stakeholders has a role to play in ensuring the integrity of the payment, and each should expect to bear some level of liability if they fail to fulfill their obligations.

For credit and debit payment transactions, comprehensive rules that were developed over time identify each stakeholder's obligations in the transaction and identify where the liability for fraud lies in different circumstances. The principles underlying these rules should be adopted by the mobile payments industry and expanded to ensure that all stakeholder obligations in the new operational model are covered.

7.2 Countermeasures

As with any new payment vehicle, fraudsters are likely to target proximity mobile payments; therefore upfront analysis and planning are essential to mitigate any risks.

Mobile payments should be deployed in a pragmatic fashion, to locations where speed and convenience make sense, and should be used to augment well-established payment mechanisms. A technically secure infrastructure should be designed based on industry best practices, such as PCI DSS, dynamic cryptograms, and multi-factor authentication. Separation and/or protection by encryption of credentials (account information, expiration date, and account holder name) throughout the mobile payment ecosystem are key factors in minimizing the impact of any breach.

It is also important to ensure that the transaction being undertaken is most likely being carried out by the person authorized or registered to carry it out, and that it is not out of character with that person's usual behavior. The payment application may be designed to require a consumer passcode or biometric (e.g., a fingerprint) to initiate or validate a transaction, providing the consumer with control over the transaction and adding a second authentication factor. Pilot studies have also introduced techniques that enable merchants to perform a rudimentary second tier validation that the purchaser is indeed the authorized user. These techniques include photo identification linked to the mobile account and verification of a physical token associated with the mobile account. Though far from ideal, these techniques can be enhanced as proximity mobile payment transactions are used for higher value and more risky transactions.

In addition, the control mechanisms developed by the banks over many years should be leveraged. A holistic view of transaction profiles across payment channels can result in greater confidence that a transaction is not fraudulent. Transactions also should be segmented by purchase amount, location, and merchant category and risk should be managed accordingly.

The location-based information available from the telephone companies should be monitored constantly for signs of a breach. To ensure that damage is contained when a breach occurs, the amount of reusable information managed, used, and stored at any one step in the lifecycle of issuance and payment should be limited.

Above all, the security measures must be appropriate to the level of risk and must not present a barrier to proper use. In addition, they must communicate to both the consumer and the merchant community that proximity mobile payments are a safe way to make a payment quickly.

8 Best Practices for Security

This section describes a practical approach to applying best practices to limiting the vulnerability of mobile payments systems and infrastructure. Many articles and textbooks identify the establishment of a security policy as the first step in the development of security provisions for computer-based information systems. In addition, the payment card industry has established specifications and standards that merchants and processors are required to meet.

To determine the level of security required for a mobile payment system, Figure 7 illustrates a best practices approach to assessing security threats and the associated cost of mitigation. This approach applies to both over the air provisioning of the payment application memory, and the card based payment application on the handset.

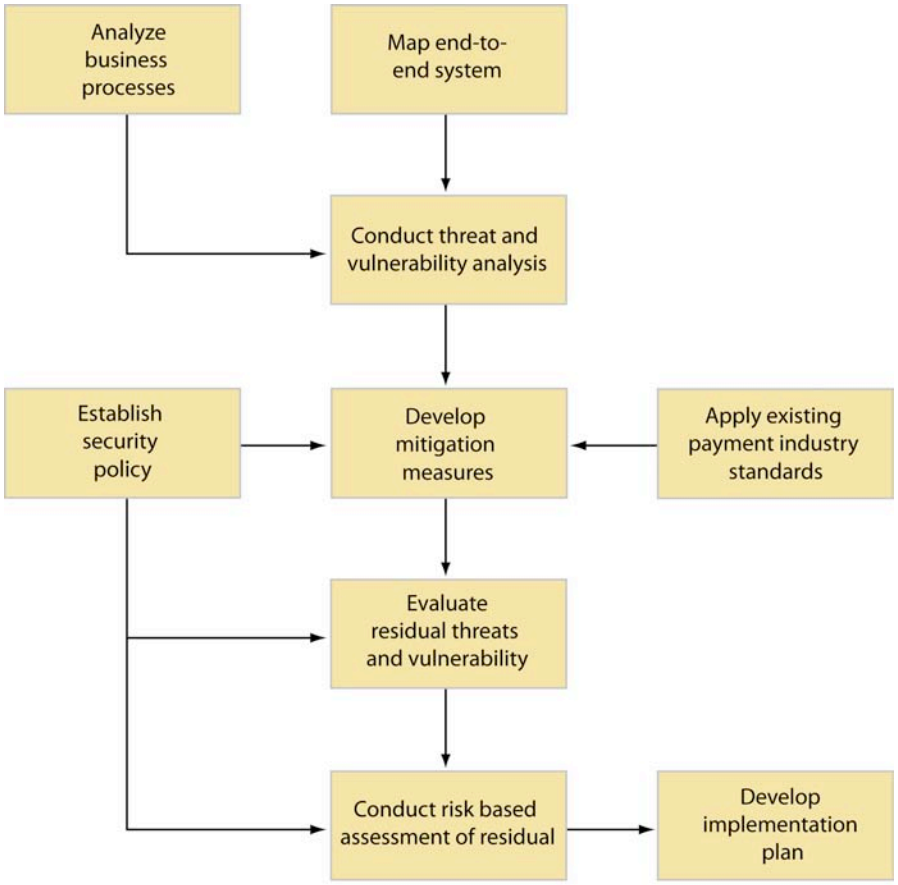

Figure 7. Best Practices Approach to Assessing Security Threats

8.1 Developing a Best Practices Framework

As illustrated in Figure 7, developing a best practices framework requires a number of key activities. This includes analyzing the business process and mapping the system from end to end.

The first step is to analyze the business processes. This analysis identifies weak links and pinpoints vulnerabilities to fraud and exploitation. The business processes critical to mobile payments consist of the following activities (illustrated in Figure 8).

- Device management, the activity that manages consumer devices and merchant POS terminals

- Credentialing, the activity associated with managing the lifecycle of the consumer's mobile payment identity
- Payment information access (storage), the process that collects and protects payment-related data
- Authentication, the process used to verify and validate a device based on a set of attributes from the device's mobile payment identity
- Authorization, the process used to verify and validate an entity's right to conduct a payment based on a set of attributes from the consumer's mobile payment identity

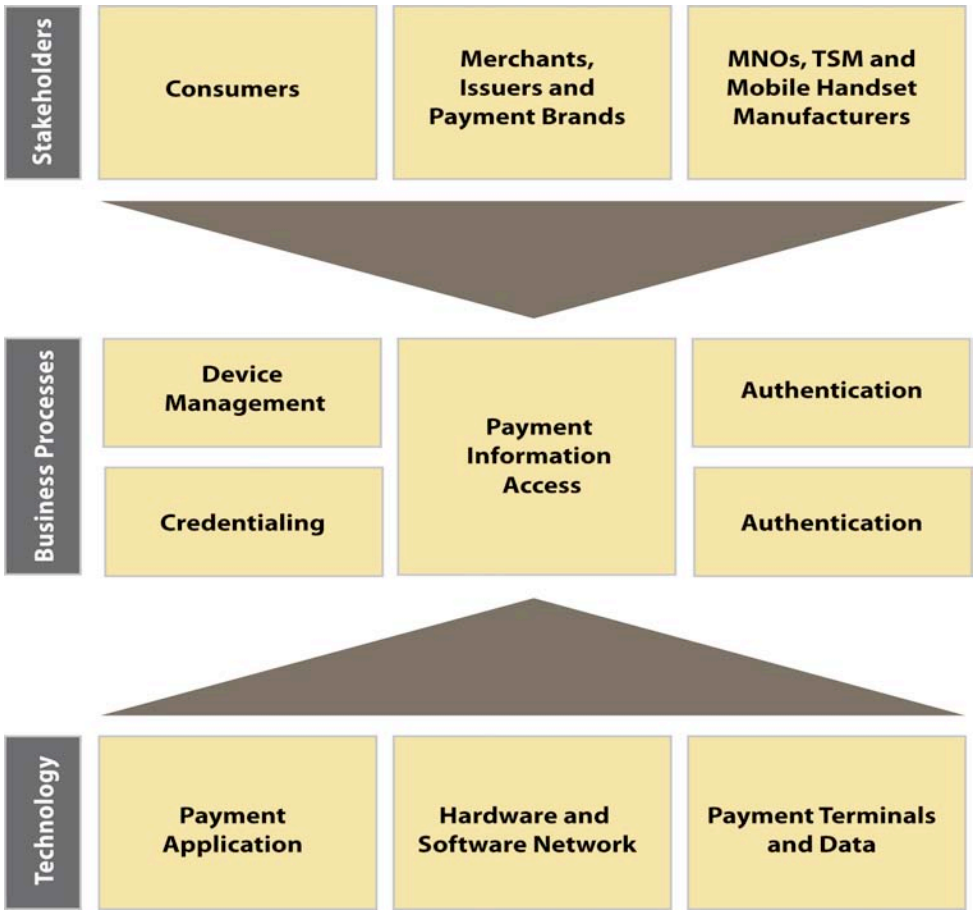

Figure 8. Critical Business Processes Associated with Mobile Payment

As shown in Figure 8, business processes are influenced by the technology required to support the delivery of mobile payments services, and the stakeholders in the mobile payment ecosystem (which are defined in greater detail in section 1.3 of this paper).

8.2 Mapping System from End to End

Another key to identifying where the system may be vulnerable to threats is to map the system end to end. Mapping entails the determination of data and process flows throughout the system. The mapping begins with the mobile device and ends with the permanent storage of the transaction record for a specific transaction.

Each component must be mapped at a level of detail that allows the verification of compliance with applicable standards and specifications.

8.3 Threat and Vulnerability Analysis

The next logical step after mapping the system from end to end is to use that map as a reference to conduct a threat and vulnerability analysis. The objective of this analysis is to identify how the mobile payment system may be misused. The most common threats in a card-based model include:

- Counterfeiting, which means the creation of duplicate payment card information in the handset memory
- Misrepresentation, or using someone else's access authorization or payment card
- Alteration, the unauthorized modification of data
- Collusion, in which procedures and technology are circumvented through illegal arrangements

The objective of this activity is to identify inherent vulnerabilities across the mobile payment system and to quantify the associated risk at each level in the system. Vulnerabilities are defined as events that cause disruption to normal operations or entail transfer of funds to an unauthorized party, resulting in financial exposure to legitimate stakeholders in the mobile payments system. Common vulnerabilities that need to be identified and quantified include: unauthorized data modification, data corruption and data exposure, and unavailability of the mobile payment system when required to conduct a payment transaction.

8.4 Addressing the Gaps – Mitigation Measures

As previously discussed in section 2 of this white paper, the payments industry has adopted extensive specifications and standards that address open payment system security. Any stakeholder participating in open payments is required to adhere to these standards and specifications. In situations where there are security gaps between an organizational security policy and payment industry specifications and standards, these gaps need to be identified, and measures defined to address the gaps. The foundation for a risk-based assessment is established by applying both the security policy and any required payments industry standards and specifications to any and all measures identified for mitigating the payment system vulnerabilities.

8.5 Residual Risk-Based Assessment

The next step is to conduct a risk-based assessment and to develop options to serve as the basis for conducting a cost/benefit analysis of the residual vulnerabilities that are not addressed by complying with required standards and specifications. The objective of this activity is to develop a set of logically sequenced metrics that identify the following:

- Threat vulnerability and countermeasures
- Security versus risk and mitigation measures

The final step is to conduct a risk-based cost/benefit analysis to determine the most cost-effective solution to mitigate the perceived risks and satisfy the established security policy.

9 Conclusions

With implementations already in place in Europe and Japan, strong consumer interest, and the ability to leverage the contactless POS infrastructure already in place, NFC-enabled proximity mobile payments show much promise.

This white paper examines the security of such payments when deployed as part of a collaboration model, in which mobile operators, banks, and TSMs cooperate to deliver an end-to-end payment system. This model requires a complex supporting ecosystem, incorporating security mechanisms designed to protect the consumer's payment account information and the payment application throughout the entire process. This includes the initial sending of account information from an issuing bank to a TSM, the provisioning of information onto the mobile phone, storing the information on the secure element in the phone, and using it at the merchant POS.

Both the financial and mobile industries have made much progress in defining how NFC-enabled mobile payments will take place and how financial information will be secured.

Security is bolstered by the use of industry standards and by the technology supporting proximity mobile payments. Industry organizations have defined standards-based approaches to ensuring that payment account information is delivered securely to the mobile phone and stored securely in the phone's secure element. From the consumer's perspective, the proximity mobile payment looks just like a contactless credit or debit card transaction. The NFC-enabled mobile phone leverages the existing ISO/IEC 14443 standard for communicating payment information from the phone to the merchant's POS terminal. Payments are processed over the current secure financial networks, with all of the layers of robust security used with traditional financial payment transactions.

The rich functionality built into mobile phones can support additional mechanisms to secure the payment application and information. Requiring a passcode or a fingerprint to initiate or respond to the terminal's attempt to initiate or validate a transaction can provide the consumer with additional comfort and a sense of control over a transaction. Appropriate risk analysis of an operational model for proximity mobile payments can identify where there is potential for fraud and misuse and assign responsibility, providing further confidence to the consumer that transactions using the phone are as safe and secure as transactions that use a contactless credit or debit card.

While implementations may vary, industry players are moving in a consistent direction. Industry organizations have made excellent progress in defining standards and specifications to ensure interoperability. Pilot studies in the United States and implementations worldwide have tested both the technology and the mobile payments process. Proximity mobile payments technology is solid. The largest remaining piece of the puzzle is the definition of a business model that accounts for the responsibilities and risks assumed by each stakeholder and defines how all stakeholders are rewarded.

With a proven technology, a merchant infrastructure that is ready to go, and features and capabilities that excite consumers, it is only a matter of time before industry first-movers in North America will come together and take advantage of consumers' ever-growing love of mobile technology to launch proximity mobile payments.

10 Publication Acknowledgements

This report was developed by the Smart Card Alliance Contactless and Mobile Payments Council to provide an overview of the security approaches being implemented for proximity mobile payments that use a collaboration model. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Contactless and Mobile Payments Council members for their contributions. Participants involved in the development of this report included: Booz Allen Hamilton, Capital One, Collis America, Cubic, Discover Financial Services, Giesecke & Devrient (G&D), IBM, IfD Consulting, Infineon Technologies, Keycorp, MasterCard Worldwide, Venyon, VeriFone, Visa, ViVOtech, and USA Technologies.

Special thanks go to the following individuals who contributed to the development of this white paper:

- **Deborah Baxley**, Independent Payments Consultant
- **Guy Berg**, Collis America
- **Graeme Bradford**, Keycorp
- **Joe DeFilippo**, Capital One
- **Sunil Dewan**, Mobile Commerce Consultant
- **Gwen Dido**, IBM
- **Willy Dommen**, Booz Allen Hamilton
- **Ian Duthie**, IfD Consulting
- **Ron Fridman**, USA Technologies
- **Micheal Gargiulo**, Mobile Consultant
- **Simon Hurry**, Visa
- **Ryan Julian**, Discover Financial Services
- **Mohammed Khan**, ViVOtech
- **Linnaea Knisely**, Smart Card Alliance
- **Pradeep Kumar**, ViVOtech
- **Mike Kutsch**, Cubic
- **Paul Legacki**, Infineon Technologies
- **Dan Loomis**, VeriFone
- **Cathy Medich**, Smart Card Alliance
- **Ken Moy**, MasterCard Worldwide
- **JC Raynon**, ViVOtech
- **Neil Ringwood**, IBM
- **Brian Stein**, G&D

About the Smart Card Alliance Contactless and Mobile Payments Council

The Contactless and Mobile Payments Council is one of several Smart Card Alliance technology and industry councils. The Council was formed to focus on facilitating the adoption of contactless and mobile payments in the U.S. through education programs for consumers, merchants and issuers. The group is bringing together financial payments industry leaders, merchants and suppliers. The Council's primary goal is to inform and educate the market about the value of contactless and mobile payment and work to address misconceptions about the capabilities and security of contactless technology. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

Trademark Notice

11 Appendix A: Standards and Certification Organizations

11.1 Payment Application Standards Organizations

11.1.1 Payment Card Industry Security Standards Council[11]

The Payment Card Industry Security Standards Council (PCI SSC) is a global open body formed to develop, enhance, disseminate, and assist with the understanding of standards for payment account security. The Council maintains, evolves, and promotes payment card industry security standards. It also provides tools needed to implement the standards, such as assessment and scanning guidelines, a self-assessment questionnaire, training, education, and product certification programs.

The Council's founding members, American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., have agreed to incorporate the PCI Data Security Standard as part of the technical requirement for each of their data security compliance programs. These companies have developed the Payment Application Data Security Standard (PA-DSS). The PA-DSS is intended to cover testing and certification requirements for payment applications. Each founding member also recognizes the Qualified Security Assessors and Approved Scanning Vendors qualified by the PCI SSC to assess compliance with the PCI DSS. The PCI SSC's founding member card brands share equally in the Council's governance and operations. Other industry stakeholders, including merchants, payment card issuing banks, processors, hardware and software developers, and other vendors all participate in reviewing proposed additions or modifications to the standards.

11.1.2 EMVCo[12]

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 standardized platform for mobile EMV payments. This platform standardization will enable this type of payment method to be deployed to a mass market.

EMVCo envisions its role as a mobile payments industry standardization coordinator. It intends the organization to become recognized as the common voice of the payments industry on contactless proximity mobile payments standardization. EMVCo's role in this respect is twofold, involving the organization in both technical development issues and industry coordination.

11.1.2.1 Technical Development Issues

As the mobile payments sector grows, there is an increasing need for EMVCo to address and resolve a number of technical infrastructure issues associated with enabling contactless proximity mobile payments. This technical development responsibility is in line with EMVCo's traditional role within the payments industry as a technology standards body. This technical focus will be an adjunct to the organization's work towards the development of specifications related to contactless payment and associated common Type Approval process for cards and terminals.

[11] Source: http://www.pcisecuritystandards.org
[12] Source: http://www.emvco.com

Its proposed role in this area encompasses the following:

- Define chip data security requirements
- Define a framework for Type Approval process
- Define global interoperability from a technical perspective
- Identify user interface issues

11.1.2.2 Standardization Issues

There is a need for the payments industry to adopt a collaborative approach to standardization. EMVCo will coordinate the payments industry's efforts in standardization work with other industry groups and market forces so that an interoperable contactless proximity mobile payments model for EMV transactions can be defined and created. Its proposed role in this area encompasses the following:

- Standardize the requirements for contactless proximity mobile payments infrastructure
- Augment the standardization of OTA card and application management (both secure element and user interface)
- Shape the development of and refer to chip interface requirements

11.1.3 Payment Industry Service Providers

In addition to EMVCo, the major industry payment brands (Visa, MasterCard, American Express, Discover, and JCB) require that payment applications be submitted to their respective labs for evaluation and certification before being deployed in their networks.

11.1.4 GlobalPlatform[13]

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, changing them to meet market needs, rather than for technical elegance
- Preserve backwards compatibility when updating technical specifications
- Support a security architecture with a range of options to meet 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.

The group's primary objectives are to facilitate new business opportunities between the mobile sector and other industries.

Although the Mobile Task Force formalizes GlobalPlatform's activity within the sector, GlobalPlatform has worked with the European Telecommunications Standards Institute (ETSI) since 1999 to standardize OTA application download and management of applications. The result is that as of October 2008, two billion midrange USIM/SIM cards worldwide are estimated to use GlobalPlatform card technology to enable OTA application downloads for 3G and GSM mobile networks.

[13] Source: http://www.globalplatform.org/

.

11.2 Mobile Devices

11.2.1 European Telecommunications Standards Institute[14]

The European Telecommunications Standards Institute (ETSI) produces globally applicable standards for information and communications technologies, including fixed, mobile, radio, converged, broadcast, and Internet technologies. Through its standards, ETSI provides business and industry with efficient solutions for accessing and developing new and established world markets. Standards and technical specifications such as GSM™ DECT™, TETRA, and DVB are prime examples of the influence ETSI has on the international markets.

ETSI is officially recognized by the European Commission as a European Standards Organization. The quality of its work and its commitment to an open approach to standardization has earned this organization the reputation for technical excellence.

ETSI has almost 700 member organizations drawn from 60 countries worldwide. The Association's worldwide members represent more than three billion GSM and 3GSM connections.

11.2.2 Global System for Mobile Communications Association[15]

The Global System for Mobile Communications Association (GSMA) is the global trade association representing the interests of over 750 GSM mobile phone operators and over 200 manufacturers and suppliers worldwide.

GSMA's mission is to create value for operators and the mobile industry in the provision of services for the benefit of end users. This allows users to easily and affordably connect to and use the services they desire, anywhere, anytime. GSMA's role encompasses technical, commercial, and public policy initiatives. GSMA focuses on ensuring that wireless services work globally, enhancing the value of mobile services to individual users and national economies while creating new business opportunities for operators and their supplier partners.

GSMA has the following strategic objectives:

- To support the evolution and broadest deployment of the GSM family of technologies, thereby enabling economies of scale and global interoperability
- To stimulate and support the development, launch, and promotion of new services and products
- To ensure that mobile services are made interoperable both nationally and internationally as rapidly as possible
- To provide services such as conferencing to operators and the mobile industry that promote and serve the goals of GSMA
- To support initiatives that stimulate social and economic development and help bridge the digital divide
- To develop environmentally sound and socially responsible policies for the mobile industry, its products, and services
- To advocate appropriate government policies and regulations on a local, regional, and global basis to ensure the continued development of the mobile industry to the benefit of everyone
- To communicate on behalf of the GSM operator community and ensure that its views are clearly communicated and understood

GSMA plays a pivotal role in the development of public policy relating to the mobile industry and its customers. The public policy team proactively leads the policy debate, representing the mobile industry

[14] Source: http://www.etsi.org
[15] Source: http://www.gsmworld.com

to governments and regulators, and delivering a regulatory environment that maximizes development opportunities for mobile operators and long-term benefit for mobile users.

11.2.3 CDMA Development Group[16]

The CDMA Development Group (CDG) is comprised of CDMA service providers and manufacturers, application developers, and content providers. By working together, members help ensure interoperability among systems while expediting the availability of 3G CDMA technology to consumers.

CDG's mission is to lead the rapid evolution and deployment of 3G CDMA-based systems, based on open standards and encompassing all core architectures, to meet the needs of markets around the world. The CDG and its members work together to accomplish the following:

- Accelerate the definition of requirements for new CDMA features, services, and applications
- Promote industry and public awareness of CDMA capabilities and developments through marketing and public relations activities
- Foster collaboration and the development of consensus among carriers on critical issues to provide direction and leadership for the industry
- Define the evolution path for current and next-generation CDMA systems
- Establish strategic relationships with government ministries, regulatory bodies, and worldwide standards and industry organizations to promote cooperation and consensus on issues facing the CDMA community
- Serve as the worldwide resource for CDMA-related information
- Minimize the time to market for new CDMA-based products and services
- Enable global compatibility and interoperability among CDMA systems worldwide
- Create global economies of scale to make CDMA the preferred choice of operators and end users

11.3 Other Ecosystem Elements

11.3.1 Open Mobile Alliance (OMA)[17]

Open Mobile Alliance (OMA) was formed in June 2002 by nearly 200 companies, including the world's leading mobile operators, device and network suppliers, information technology companies, and content and service providers.

OMA is a focal point for the development of mobile service enabler specifications, which support the creation of interoperable end-to-end mobile services. OMA drives service enabler architectures and open enabler interfaces that are independent of the underlying wireless networks and platforms. OMA creates interoperable mobile data service enablers that work across devices, service providers, operators, networks, and geographies. Toward that end, OMA develops test specifications, encourages third party tool development, and conducts test activities that allow vendors to test their implementations.

OMA has pioneered significant consolidation of mobile service enabler organizations. This consolidation promotes end-to-end interoperability across different devices, geographies, service providers, operators, and networks, and further supports OMA's focus on market and user requirements to guide specification work.

Significant new efforts by OMA are leading to the development of mobile service enablers in areas such as device management, push-to-talk over cellular, mobile broadcast, and more.

OMA has the following goals:

[16] Source: http://www.cdg.org
[17] Source: http://www.openmobilealliance.org

- Deliver high quality, open technical specifications based upon market requirements that drive modularity, extensibility, and consistency among enablers to reduce industry implementation efforts.
- Ensure OMA service-enabler specifications provide interoperability across different devices, geographies, service providers, operators, and networks; facilitate interoperability of the resulting product implementations.
- Be the catalyst for the consolidation of standards activity within the mobile data service industry; work in conjunction with other existing standards organizations and industry forums to improve interoperability and decrease operational costs for all involved.
- Provide enough value and benefits to all members of OMA, including content and service providers, information technology providers, mobile operators, and wireless vendors, so that they elect to participate actively in the organization.

According to OMA, the organization represents the entire value chain and marks a change in the way specifications for mobile services are developed. OMA is trying to consolidate all specification activities in the service enabler space in one organization.

11.3.2 Near Field Communication Forum[18]

The Near Field Communication (NFC) Forum was formed to advance the use of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. The Forum was formed in 2004 and now has 150 members, consisting of manufacturers, applications developers, financial services institutions, and companies representing other elements of the value chain, all working together to promote the use of NFC technology in consumer electronics, mobile devices, and personal computers.

The goals of the NFC Forum are:

- Develop standards-based NFC specifications that define a modular architecture and interoperability parameters for NFC devices and protocols.
- Encourage the development of products using NFC Forum specifications.
- Work to ensure that products claiming NFC capabilities comply with NFC Forum specifications.
- Educate consumers and enterprises globally about NFC.

The NFC Forum provides a highly stable framework for extensive application development, seamless interoperable solutions, and security for NFC-enabled transactions. The NFC Forum has organized the efforts of dozens of member organizations by creating committees and working groups that address different aspects of this technology.

In June 2006, only 18 months after its founding, the Forum formally outlined the architecture for NFC technology. As of December 2008, the Forum has released 11 specifications. The specifications provide a road map that enables all interested parties to create powerful new consumer-driven products.

11.3.3 3rd Generation Partnership Project[19]

The 3rd Generation Partnership Project (3GPP™) is an agreement that was established in December 1998. The agreement brings together a number of telecommunications standards bodies, which are known as the Organizational Partners. The current Organizational Partners are the European Telecommunications Standards Institute (ETSI), Association of Radio Industries and Businesses/Telecommunications Telecommunications Committee (ARIB/TTC) (Japan), Alliance for Telecommunications Industry Solutions (ATIS) (North America), and Telecommunications Technology Association (TTC) (South Korea). These partners represent the major global telecommunication organizations.

[18] Source: http://www.nfc-forum.org/aboutus/
[19] Source: http://www.3gpp.org

The original goal of 3GPP was to produce globally applicable technical specifications and technical reports for a third generation mobile system based on the evolved GSM core networks and the radio access technologies they support (i.e., universal terrestrial radio access, or UTRA, in both frequency division duplex [FDD] and time division duplex [TDD] modes). This goal was subsequently amended to include the maintenance and development of the Global System for Mobile Communication (GSM™) technical specifications and technical reports, including evolved radio access technologies such as General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE). Although the Partnership project description has not been maintained, the principles of operation of the project still remain valid.

A permanent project support group called the Mobile Competence Centre (MCC) has been established to ensure efficient day-to-day operation of 3GPP.

11.3.4 3rd Generation Partnership Project 2[20]

The 3rd Generation Partnership Project 2 (3GPP2) is a collaboration among telecommunications associations to develop a globally applicable third-generation mobile phone system specification within the scope of the ITU's IMT-2000 project. In practice, 3GPP2 is the standardization group for CDMA 2000, the set of 3G standards based on earlier 2G CDMA technology.

The participating associations are ARIB/TTC (Japan), China Communications Standards Association, Telecommunications Industry Association (North America), and Telecommunications Technology Association (South Korea).

[20] Source: http://www.3gpp2.org

12 Appendix B: Glossary of Terms

Acquirer bank
The merchant's banking partner that approves and settles the card transactions.

Application Protocol Data Unit (APDU)[21]
The communication unit between a reader and a card. The structure of an APDU is defined by the ISO/IEC 7816 standards. There are two categories of APDUs: command APDUs and response APDUs. As the name implies, the former is sent by the reader to the card; it contains a mandatory 5-byte header and from 0 to up to 255 bytes of data. The latter is sent by the card to the reader; it contains a mandatory 2-byte status word and from 0 to up to 256 bytes of data.

Applet
A Java Card-based application that runs in the secure element of a mobile device**.**

Asymmetric cryptography
Cryptography that uses two related operations: a public operation defined by public numbers or by a public key and a private operation defined by private numbers or by a private key. (The two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation.)

Attacks
Techniques implemented to compromise the security of a smart card IC by discovering what information it holds.

Authentication
The process of electronically validating the identity and/or attribute of a person or other entity.

Certificate authority (CA)
A trusted third party that is responsible for issuing and revoking digital certificates within the public key infrastructure.

Chain of trust
An attribute of a secure ID system that encompasses all of the system's components and processes and assures that the system as a whole is worthy of trust. A chain of trust should guarantee the authenticity of the people, issuing organizations, devices, equipment, networks, and other components of a secure ID system. The chain of trust must also ensure that information within the system is verified, authenticated, protected, and used appropriately.

Chip
Electronic component that performs logic, processing and/or memory functions.

Contact smart card
A smart card that connects to the reading device through direct physical contact between the smart card chip and the smart card reader. (See ISO/IEC 7816.)

Contactless payments
Payment transactions that require no physical contact between the consumer payment device and the physical point-of-sale (POS) terminal. In a contactless payment transaction, the consumer holds the contactless card, device or mobile phone in close proximity (less than 2-4 inches) to the merchant POS terminal and the payment account information is communicated wirelessly (via radio frequency (RF)).

Contactless smart card
A smart card that communicates with a reader through a radio frequency interface.

Cryptographic keys
In encryption and digital signatures, a value used in combination with a cryptographic algorithm to encrypt or decrypt data.

[21] Source: http://www.jguru.com

Card Verification Value (CVV) 3 / Card Verification Code (CVC) 3
Security codes used by the financial payment brands for credit and debit transactions to protect against credit card fraud.

Embedded secure elements
An embedded, fixed and therefore non-removable separate secure chip in the mobile phone.

EMV
Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

EMVCo
The organization 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. EMVCo is currently owned by American Express, JCB, MasterCard Worldwide, and Visa, Inc.

Encryption
The process of translating information into a code that can only be read if the reader has access to the key that was used to encrypt it. There are two main types of encryption – asymmetric (or public key) and symmetric (or secret key).

GSM
Global system for mobile communications.

GSMA
GSM Association: Association of about 700 mobile network operators (MNOs) in 218 countries around the world.

GPRS or (**G**eneral **P**acket **R**adio **S**ervice)
The first high-speed digital data service provided by cellular carriers that used the GSM technology. GPRS added a packet-switched channel to GSM, which uses dedicated, circuit-switched channels for voice conversations.

HSM, or Hardware Security Module[22]
Hardware-based modules that provide encryption processing and protection for the keys and applications that underlie critical security processes.

IC
Integrated circuit.

ISO
International Organization for Standardization. An agency of the United Nations concerned with international standardization, including stored value and other bank cards. Some of the pertinent standards for contactless payment cards are ISO/IEC 7810, 7811, 7816, 9992, 10202, and 14443.

ISO/IEC 7816
International standard for integrated circuit cards (i.e., smart cards) with contacts, as well as the command set for all smart cards.

ISO/IEC 14443
ISO/IEC standard "Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards." The international standard for contactless smart chips and cards that operate (i.e., can be read from or written to) at a distance of less than 10 centimeters (4 inches). This standard operates at 13.56 MHz.

Issuing bank
The bank that provided the credit card to the cardholder.

Java Card OS
A Java-based operating system for smart cards.

[22] Source: http://www.ncipher.com

JSR 177[23]
Java Specification Request 177, specifying the security and trust service APIs (Application Programming Interface) for J2ME (Java 2 Micro Edition) enabled mobile devices.

JSR257[24]
Java Specification Request 257. Specification defining J2ME Optional Packages for contactless communication, one package for bi-directional communication and the other for accessing read-only information.

Java Mobile Information Device Profile (MIDP) 2.0[25]
A programming interface (API) for mobile phones and pagers for the Java 2 Platform, Micro Edition (J2ME). It provides support for a graphical interface, networking and storage of persistent data for "MID Profile" applications, also known as "midlets."

Key
In encryption and digital signatures, a value used in combination with a cryptographic algorithm to encrypt or decrypt data.

KMS, or Key Management Server[26]
A server that hosts one or more HSMs.

MIDlet[27]
A mobile phone or pager application written in the Java 2 Platform, Micro Edition version (J2ME).

Mobile network operator (MNO)
The mobile telecommunications company that has the relationship with the end user.

Mobile wallet
A software application that is loaded onto a mobile phone for the purpose of managing payments made from the mobile phone. A mobile wallet application can also be used to hold and control a number of other applications (for example, payment and loyalty), in much the same way as a physical wallet holds a collection of physical cards.

Multi-factor authentication
The use of multiple techniques to authenticate an individual's identity. This usually involves combining two or more of the following: something the individual has (e.g., a card or token); something the individual knows (e.g., a password or personal identification number); something the individual is (e.g., a fingerprint or other biometric measurement).

Multi-application card
A smart card that runs multiple applications – for example, physical access, logical access, data storage and electronic purse – using a single card.

NFC – Near Field Communication
A short-range wireless standard (ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they are brought close together (within a few centimeters). NFC technology is compatible with ISO/IEC 14443-based technology.

OSI Model[28]
Open Systems Interconnection Reference Model (OSI Reference Model or OSI Model). An abstract description for layered communications and computer network protocol design. In its most basic form, it divides network architecture into seven layers that, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the OSI Seven Layer Model.

---

[23] Source: http://jcp.org
[24] Source: http://jcp.org
[25] Source: http://dictionary.zdnet.com
[26] Source: Windows Server Blog by Kurt Roggen: http://trycatch.be/blogs/roggenk/archive/2008/01/13/windows-server-2008-volume-activation-2-0-and-kms-key-management-server.aspx
[27] Source: PC Magazine Definitions http://www.pcmag.com/encyclopedia_term.
[28] Source: Wikipedia http://www.wikipedia.org

OTA
Over the air. The possibility to send and receive data to/from a device in distributed environment. In GSM networks, data connection or SMS could be used to do so.

Payment Card Industry Data Security Standard (PCI DSS)[29]
A widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit card companies: Visa, MasterCard, Discover and American Express**.**

Payment Card Industry Security Standards Council (PCI SSC)
An open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements. The PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

Personalization
The process of transforming a generic device/card into one that incorporates the unique and personal data of the user.

PIN
Personal identification number. A numeric code that is associated with a payment account or card and that adds a second factor of authentication to the identity verification process.

POS
Point–of-sale. This term is also used to describe the equipment used by the merchant to complete the payment transaction.

Proximity mobile payments
A payment to a physical merchant that is initiated from an NFC-enabled mobile phone held in close proximity (within a few centimeters) to the merchant's point-of-sale equipment.

QSR
Quick Sale Retail. A QSR merchant is pre-set up through their merchant services provider to accept credit and debit card transactions up to a certain dollar amount, without requiring the customer to sign a receipt, in order to move customers along more quickly.

RAN
Radio Access Network

RAN encryption
Radio Access Network encryption. The use of cryptographic techniques to protect data on the mobile network.

RF interface
The mode of radio frequency communication between the reader and the handset.

Reader
Any device that communicates information or assists in communications from a card, token, or other device and transmits the information to a host such as a control panel/processor or database for further action.

ROM
Read-only memory.

Sniffing
The act of auditing or watching computer network traffic. Hackers may use sniffing programs to capture data that is being communicated on a network (e.g., usernames and passwords).

[29] Source: http://www.financialsecurity.com/definitions

Smart card
A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, subscriber identification modules (SIMs) used in GSM mobile phones, and USB-based tokens.

SD card[30]
Secure digital memory Card. A flash memory card that provides storage for digital cameras, mobile phones and PDAs. Although SD cards support encryption and content protection (the "secure" in SD), they have been mostly used for regular storage due to their small size and fast transfer rate.

Secure element
A dedicated microprocessor system that contains an operating system, memory, application environment and security protocols intended to be used to store and execute sensitive applications on a mobile device. A secure element may reside on a (U)SIM, dedicated chip on a phone's motherboard, or as an external plug in memory card.

SIM
Subscriber Identification Module. A SIM is the smart card that is included in GSM (Global System for Mobile Communications) mobile phones. SIMs are configured with information essential to authenticating a GSM mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network.

SSL/TLS
Secure Sockets Layer/Transport Layer Security. Cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet. TLS and SSL encrypt the segments of network connections at the transport layer end-to-end to ensure that the transmitted information is only accessible by the server that was intended to receive the information.

Symmetric cryptography
Cryptography using the same secret key for both the originator's and the recipient's operation. (Without the secret key, it is computationally infeasible to compute either operation.)

Symmetric keys
Keys that are used for symmetric (secret) key cryptography. In a symmetric cryptographic system, the same secret key is used to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code).

Trusted service manager (TSM)
A neutral third party that provides a single integration point to mobile operators for financial institutions, transit authorities and retailers that want to provide a payment, ticketing or loyalty application to their customers with NFC-enabled phones.

USIM-based cards
The equivalent of a SIM card, but for WCDMA / UMTS (3G) phones.

3G CDMA
Third generation (3G) code division multiple access (CDMA) standards. CDMA is a method for transmitting simultaneous digital signals over a shared portion of the spectrum. Although used in various radio communications systems, the most widely known application of CDMA is for mobile systems that operate in the 800 MHz and 1.9 GHz PCS bands. Compared to GSM cellular systems, CDMA requires fewer cell towers and provides up to five times the calling capacity. Providing more than 10 times the voice traffic of earlier analog system (AMPS), CDMA is also the basis for 3G data transmission

[30] Source: http://www.pcmag.com/encyclopedia_term/