SMART PAYMENT ASSOCIATION

shaping the future of payment technology

Security for Mobile Payments

The SPA Position

June 2012 – V1.0

Table of contents

1. Introduction

Offering guidance on the most pressing issues in the payments world, this report from the Smart Payment Association (SPA) offers a detailed analysis of the mobile payments market; based on current live and trial deployments.

Focusing on security and fraud protection, it outlines the position of the SPA in this most crucial of areas, and delivers a series of **ten recommendations (Chapter 11)** aimed at helping member organizations, and the wider community, understand and address security concerns to deliver compliant services and solutions.

Inevitably in such as dynamic market, the analysis and conclusions contained in this document need to be continually reviewed in the light of expected technical, regulatory and operational innovations.

The SPA would welcome any feedback from the mobile payments community that addresses the content of this document.

2. Editorial summary

The following section offers an editorial summary of the detailed report.

The ubiquity of card payments across the developed world is based on two interconnected principles; security and standardization. Without the first the lack of consumer (and merchant) confidence would have stifled adoption, while the absence of the second would have prevented the kind of transaction volumes required for retail card payments to be considered successful.

It is the same for mobile payments.

Therefore, the SPA believes, the first step is to recognize the security issues the industry faces. We must develop a common understanding in terms of the vulnerabilities of proposed mobile payments systems, and recognize the central risks that must be overcome.

This is easier said than done, partly because of the number of commercial, regulatory and governmental actors at play, but also because the security policy adopted by a mobile payments scheme will largely be dependent on the nature and risks of the payment instruments offered.

A level of standardization is necessary, yet the competitive nature of the mobile environment has led to a profusion of payment products, services, rules and technologies. The existence of differing and often proprietary solutions based on incompatible devices, applications and operating systems – and indeed the use of non-transparent security specifications - means this dynamic market will not easily lend itself to blanket agreement on the way forward.

Working to resolve these issues is a community of organizations committed to delivering standard solutions for the interoperability of certain interfaces (Global Platform, EMVCo, European Payments Council, Mobey Forum, NFC-Forum), as well as promoting security mechanisms (ISO TC68, ISO JTC1 SC27).

This is a good sign, yet now the challenge is to provide a security framework that is flexible enough to accommodate different interests; one that will enable liability allocation settings, comply with regulatory constraints, scale to the needs of each particular mobile payments service and, to as great a degree as possible, be based on existing, proven infrastructures.

The SPA considers the process is best achieved at a regional level first. As an example, the European Payments Council is already working to create a Single European Payments Area (or SEPA) for all payments instruments. Once ratified the aim is to extend this harmonization worldwide; creating the appropriate international security standards, and crucially, monitoring their adoption through the development of roadmaps that take into account local market and legal peculiarities.

The logic, the SPA believes, of such an approach is irrefutable. It is crucial to maximize the synergies between interoperability and security. The former is necessary in order to optimize the network effect of existing systems, while the overall integrity of payments services can only be assured by the adoption of security protocols at each interface used to initiate and confirm a payment order.

Secondly, the security mechanisms being implemented by different payment processing devices should be certified using harmonized methodologies against transparent, formal and standard security requirements. Here, the SPA encourages the convergence of local initiatives as SEPA and EMVCo and PCI international certification practices.

In support of this, and because mobile payments security relies heavily on the device involved in the transaction, the SPA is also driving the development of a formal, standardized requirement for mobile phones, smartphones and tablets. Indeed, the computing power of today's smart devices lends itself to the deployment of advanced user authentication technologies, including biometrics.

Of course, the presence of the Secure Element (SE) within the device – be that the SIM, embedded Secure Element or MicroSD card – offers assurance today. Crucially, the development of Open APIs enabling applications to access the SE also offers an opportunity to create a common interface and over-the-air management capability for multiple services. In doing so this assures a more seamless user experience while creating a catalyst for banks, mobile telecommunications operators and Trusted Service Managers (TSM) to come together to develop key enabling agreements.

These recommendations form the basis of the ten more specific recommendations detailed in this paper. Accepting these, the SPA believes, will contribute significantly to the development of a seamlessly interoperable and secure ecosystem able to drive consumer and industry confidence.

3. Terminology

NOTE: *The following terms proposed are not standardized at present. They correspond to an SPA effort to provide a conceptual basis for the ideas and suggestions of this document. This common understanding may be subject to future revision, and as with the whole document, feedback will be welcomed.*

1. **Mobile Payment Scheme**: Legal business agreement to offer to the market a mobile payment instrument.

2. **Mobile Payment System**: Technical infrastructure required for the operation of a mobile payment instrument, run under the responsibility of the mobile payment scheme. It includes:

   - The mobile payment instrument and associated embedded mobile contactless payment applications
   - Authorization, acceptance and acquiring infrastructures for mobile payment transactions
   - A process for the functional and security certification of the mobile payment instrument and its applications
   - A process for the enrollment of new users of the system
   - An infrastructure for the management of mobile contactless payment applications
   - A mobile payment transaction clearing and settlement facility
   - Any other technical facility that might be required to comply with legal constraints (Know Your Customer rules, or a PKI).

3. **Mobile Payments Platform**: Part of the mobile payment system which:

   - Interacts with the mobile payment instrument during the mobile payment transaction
   - Provides a proof of the transaction
   - Generates the information required for the clearing and settlement of the mobile payment transaction
   - Possibly offers mobile contactless payment application management services, also referred to in this document as the "platform"

4. **Mobile Payment Application**: Set of logical data stored in a mobile payment instrument, which is:
   - Selectable using a unique identifier
   - Under control of the legitimate user and able to initiate and conclude a mobile payment transaction.

5. **Mobile Payment Instrument:** Set of one or more mobile contactless payment applications and of an execution and management environment owned by a mobile payment scheme.

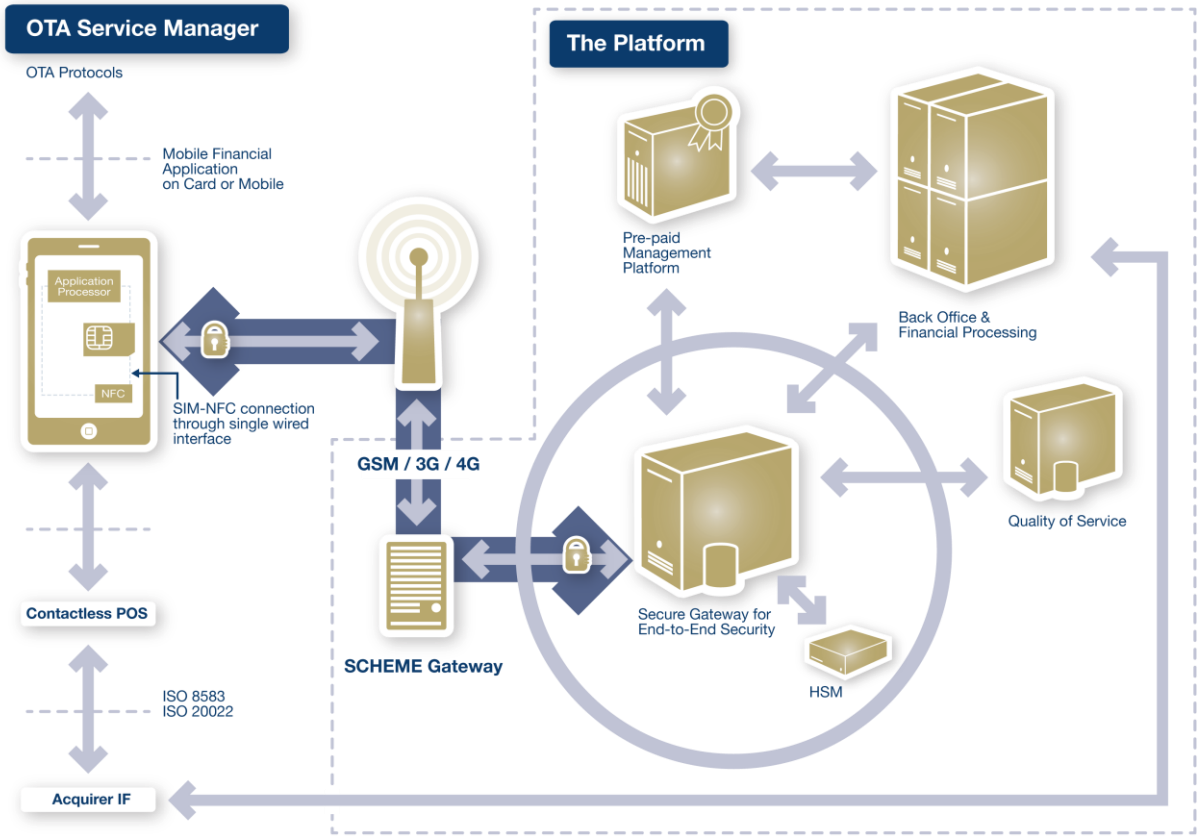
6. **Mobile Wallet:** Set of mobile payment instruments and associated computing resources available for mobile payments in a mobile payment device. This may include both contactless proximity and remote mobile payment instruments.

7. **Mobile Payment Device:** Personal mobile device storing at least one mobile payment Instrument.

8. **Proximity Contactless Payment:** Mobile payment emulating a contactless payment using an NFC channel compliant with ISO/IEC 14443.

9. **Mobile Remote Payment:** Payment transaction in which the mobile device is not establishing a direct communication channel with the payment accepting device.

Diagram 1: Standard Architecture For Mobile Payment Systems



4. Is security a driver for payments innovation?

The history of payment instruments is one in which the means used to pay have evolved as banking services have been made available to the world's population. Simultaneously, throughout the past century we reached a progressive understanding of the core functions of money, the way the money circulation impacted on economical development, and why the uncontrolled issuance of money represented a risk. Thus, banks progressively played a central role in payments intermediation, providing trusted payment instruments to payers, and facilitating the acceptance of such instruments by creditors.

The substitution of physical cash by electronic alternatives provided scope for substantial efficiency gains and increased convenience. Thus, banking payment intermediation has resulted in the progressive dematerialization of the money, and the subsequent replacement of physical cash by an equivalent electronic transfer. Payment electronification has taken many forms, but in the end any electronic payment results in the exchange of digital information between the bank of the payer and the bank of the payee. Well aware of the vulnerability of digital information during transmission, the financial industry developed and operated its own secured private networks and deployed cryptographic technology from early on.

Therefore, any new form of money or new electronic payment instrument raises genuine concerns about the risks linked to the innovation itself and the potential implications for monetary policy, user protection (retailers and consumers), fraud, and the stability of payment systems. Before approving a new form of money an in-depth analysis of the security measures available to counter the inherent risks is needed. In addition, a new regulatory framework intended to protect user interests and set liabilities may be necessary. The extent to which these concerns may be judged to be significant depends on the level of use of the new payment means as well as socio-economical conditions of the geographical region where the innovation is experienced.

In this respect, a key fact to be considered is that consumers adopt a conservative behavior when paying. Thus, in both the US and SEPA area mobile payment landscapes, consumer demand for mobile payments is low. In developed regions, payers have different payment instruments at their disposal. As a rule of thumb, in order to succeed, any new payment mechanism must be perceived by users as being at least as secure and convenient as the legacy ones. In an apparent paradox, the introduction and acceptance of a new means of payment can be more difficult, despite the highly technologically-educated user population, simply because differing means of payment are in competition. For instance, the growth of the debit card in US in recent years made payments for small value purchases quicker and more convenient, meaning that mobile payments have to compete hard with existing solutions.

Not surprisingly any new instrument is therefore marketed as a continuity, and not a disruptive break with existing devices. Thus, the mobile payments area is being approached as the "next step forward" by emulating a contactless card. However, even in this non-disruptive route to market there is a need to change the behavior of the payers by making new means of payment more attractive. In addition, there is also a supply-side issue such as the need to convince mobile handset manufacturers to integrate Near Field Communication (NFC) interfaces into their next generation devices for mobile contactless payment applications. When these interfaces are made available on mobile phones (in Japan, Singapore and Korea for example), and an acceptance infrastructure is available, mobile payments flourish.

At present, retail card payments rely on the 3- or 4-part architectures. This well established standard architecture provides a baseline for proven business models, with a revenue sharing model which is jointly established between issuer and acquirer banks, and funded by the user sector, retailers and consumers. Differences in the way the revenue sharing is set is largely regional dependent. The card transaction fees for the financial sector tend to be regulated. That means that new sources of revenue are worked out by multiplying acceptance points for cards and providing payers with new instruments that build on their previous user experience.

Whatever the strategy adopted to expand the payment business, in the end the payment instrument is jointly chosen by the retailer and the consumer. A new means of payment has to capture the merchant's interest, offering him a real advantage in terms of perceived costs of implementation and protection against fraud. In the mobile payments context, rapid technological developments and the speed with which criminals are adapting to this new environment make the prevention of, and the fight against, payment fraud particularly challenging. Fraud refers to the misuse of a mobile payment instrument, or of the information generated during a mobile payment transaction, by a person or entity other that its owner and without his consent, to pay for goods or services.

Diagram 2: Context Factors For Mobile Payments

To conclude, the business model for card payments relies on, and is the consequence of, reducing fraudulent payments. Similarly, mass market use of smart cards is the consequence of increased user convenience, which in turn relies on the perceived level of security of the system. The guarantee to be paid by automatically crediting a merchant's bank account is a key condition for merchants in accepting the card and to partially finance the operational costs of the system. This business model holds because the system guarantees a marginal level of fraud. This condition must be preserved to enable the adoption of mobile payments. **Fraud, even if it affects a minority of users, undermines general confidence in mobile payments systems.** Thus, maintaining or enhancing user confidence requires the commitment of all parties involved to offer and supervise mobile payment systems.

5. Preventing fraud in mobile payments

Great business opportunities result from the universal adoption of mobile phones and other mobile personal devices, encouraging both banks and non-banks to offer new payment instruments. This trend is worldwide. However the perception of the value of mobile payments depends on the world region considered. A fundamental difference exists between users in developing countries where mobile payments often represent first time access to electronic payments, and users in developed countries for whom a mobile payment is an additional channel because they are already banked. Consumers in developed countries benefit from technologically advanced mobile phones in the context of highly concentrated banking markets (the US is an exception here) and/or the leadership of mobile network operators in partnering with banks, government and public transport and transit authorities.

The growth in mobile financial services not only depends on technological advances but also on consumer confidence in the provided services. Moreover, the outsourcing of certain payment activities to mobile operators deserves further attention from financial regulators. Legal aspects play a substantial role in enhancing user trust in the offered services, especially in developed countries where many trusted payment instruments are already available.

The first challenge when addressing fraud prevention and setting preventive security policies is the diversity of mobile payment services and the current lack of a standard taxonomy for mobile payments, and therefore of their inherent risks. Some of the security concerns are common, and include:

1. Authentication and fraud, especially cross-channel
2. Payer verification methods proportionate to the risk of the payment transaction
3. Lost/stolen mobile phones, dropped calls
4. Data protection
5. Secure access to bank accounts via unsecure mobile telecom /wireless networks
6. The business requirements to generate not forgeable messages proving evidence, for instance:
   - of payment authorization
   - of user consent or
   - of agreement in the terms of a transaction.
7. The need to identify participants in a cross-border payment suspicious transaction.

Weaknesses during the development, implementation and monitoring of mobile payment systems result in security data breaches and the risk of fraud or misuse of the system. **The position of the SPA is unambiguous: mobile payments should rely on the user experience for security of the payment smart card. Smart cards have proven their ability to reduce fraud. The security model we propose to mitigate risks is therefore the card-centric one.**

Having stated this, the SPA considers that the perceived risk by users of the system depends on the type of mobile payment and the world region to be considered. To start our analysis we'll identify some of the characteristics which differentiate mobile payments concerns in developed and developing countries.

6. Managing mobile payments risks and threats

6.1. Which threats are specific to mobile payments?

From the financial institution perspective, threats arise from the vulnerabilities of those parts of the mobile financial system that are not directly under their control:

1. **The mobile device** - where confidential user data is to be protected against unauthorized use. Security mechanisms here include cardholder authentication, secure storage of data needed to generate a mobile payment transaction (e.g. storage in an SE) and the use of a secure operating system for the execution of the mobile financial application

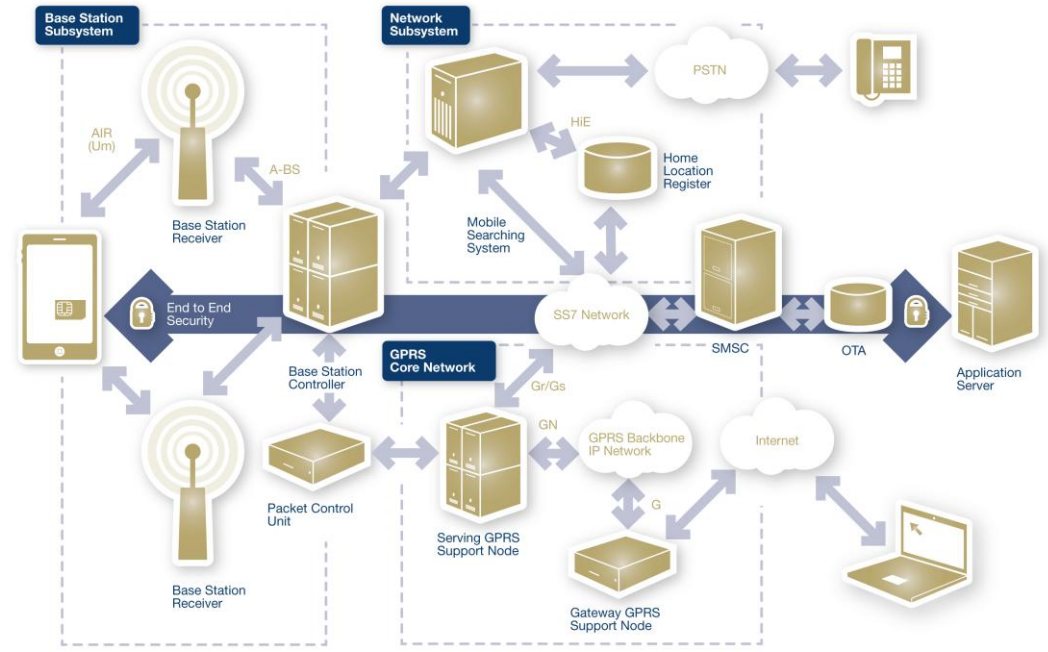
2. **The wireless interface** - the access to a telecom network or to a wireless infrastructure requires the protection of the transmitted data for: (1) any identity credential required for access to the mobile service and (2) upon authorization the mobile financial transaction related data. Wireless networks are, by their very nature, vulnerable to eavesdropping attacks. In addition, skimming attacks are possible.
3. **The mobile network infrastructure** - once the personal credentials and transaction data have been processed, the disclosure of this data is possible unless an end-to-end secure channel is established between the financial institution's back office and the mobile financial application.

Other than fraud and/or financial crime, the pervasive use of mobile devices also brings new privacy risks. People that make extensive use of mobile portable devices continuously leave traces of their physical location, identities and transactions, sometimes simply by carrying the devices around in their pockets. This privacy concern and individual tracking is independent from the use of the mobile to pay, and is the result of being powered-on when carrying it.

For widespread use and customer acceptance of m-payment services, both perceived and technical levels of security should be high and for end-users, privacy should not be compromised.

A system is only as secure as the weakest link in the security chain, which makes it essential to analyze every link leading to the execution of a mobile payment. These links include hardware and software executable environments including the SE, mobile operating system, the software development platform and the APIs it provides, and the user interface. All these elements participate in the generation and verification of the messages implementing a particular protocol for a given mobile financial service. These messages are then transported using wireless protocols and standards like GSM, 3G, 4G, Bluetooth and NFC for proximity contactless communications, depending on the capabilities of the mobile portable device. Each of these links introduces vulnerabilities because of the security threats posed by recent and future mobile worms and viruses, globally known as malicious software ("malware"). It follows that to ensure the security of the mobile payment system as a whole it is a requirement that every link is robust in relation to attacks.

Diagram 3: End-To-End Security



As we can see in the above figure, a formal secure mobile payment system analysis requires consideration of the internal mobile device subsystems, the wireless network components and interfaces, and a comprehensive understanding of their vulnerabilities in order to integrate the most appropriate security features.

6.2. Securing the mobile payment device

The mobile phone used as a mobile payment device:

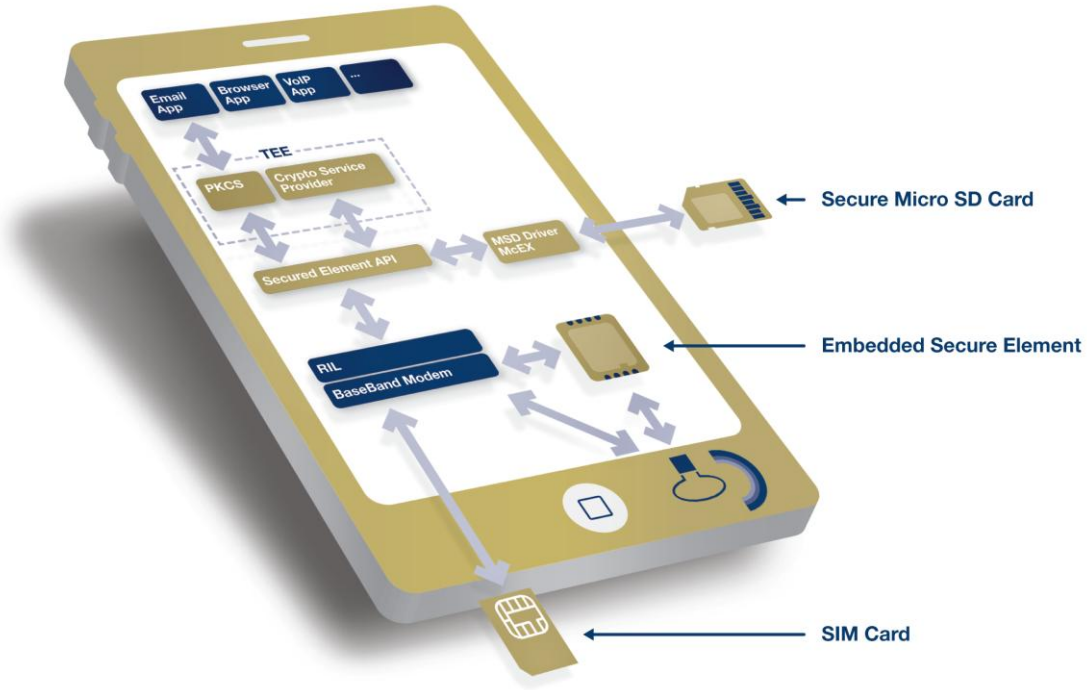
1. Ensures the secure execution of the mobile payment application. This application can be developed in Java (J2ME) for GSM mobile phones and in Binary Runtime Environment for Wireless (BREW) for CDMA mobile phones
2. Identifies and authenticates the legitimate user of the mobile payment application
3. Contains and provides with communication interfaces to the external world the Tamper Resistant Devices (e.g. an SE) storing the mobile payment application
4. Encrypts sensitive information
5. Provides the user with mechanisms for selection, monitoring and a list of available mobile payment applications and a secure selection mechanism
6. Provides with a request access authorization to an issuer financial institution and/or with the data needed to build this request authorization

7. May provide with services such as the generation and verification of mobile digital signatures
8. Supports distant lifecycle management of payment applications using OTA technology.

In order to cope with the intrinsic vulnerabilities of the mobile phone, an open computing platform with multiple communication interfaces and unsecure wireless networks, the SPA strongly recommends the personalization of mobile payment applications in a separate tamper-resistant device that may interact with the payer using a protected channel. The tamper-resistant device is the SE, with different standard form factors. To establish a secure channel between the user interface (e.g. for securely entering the PIN code) the SPA recommends the integration in the mobile phone of the Trusted Executing Environment (TEE). Both have the advantage of the availability of open APIs for the interoperable access to the services they provide.

These safeguards are compatible with additional security features that may control the access to the other communication interfaces of the mobile device (e.g. the modem).

Diagram 4: Client Security



The SE is a storage container embedded within the mobile device which provides confidentiality, privacy and integrity of authentication credentials, and may provide functionality for user authentication, cryptographic processes and key management protocols.

The opinion that a secure element is an integrated circuit chip (ICC) assumes that a hardware module is more secure than a software module. However, hardware modules often incorporate software to achieve functionality which may be deployed as software or firmware. Software executes on the general hardware relying on an operating system whereas firmware controls specific hardware components. Furthermore, the range of an ICC may be a read-only or read-write

module, or a complex micro-computer with an application programming interface (API) providing extensive functionality.

Malware exploits some vulnerabilities in the mobile device motherboard OS or acts as a man-in-the middle between the user interface and the SE storing the mobile financial applications. A typical security analysis involves identifying weak points in a system and indicating who might be in a position to fix them. An example of this is how PIN data is protected in a mobile portable environment - from the point of entry all the way to the SE containing the reference enrolled PIN.

The execution of some mobile financial services may require the creation of an electronic signature by the mobile portable device ("mobile signatures") with a legal value. In this context, it is important to implement the feature known as " What you see is what you sign". The term "You Sign" actually refers to "What the SE actually signs on your behalf". For non-repudiation purposes, the path leading from the display or the portable pin-pad and the SE should guarantee the integrity, the authenticity and possibly the confidentiality of the information entered and/or confirmed by the user using the mobile user interface.

The objective is to allow critical data and code to be isolated from threats in the mobile's open environment.

A standard solution to that problem could be provided by the Trusted User Interface (TUI) a functionality offered by the Trusted Executable Environment (TEE). The TEE is being standardized by organizations such as Open Mobile Terminal Platform (OMTP) and GlobalPlatform. Our approach is that the TUI could be tailored to the specific needs of the mobile financial market by properly combining with an SE using standard APIs.

Therefore, the SPA proposal is to develop a standard security model for mobile portable devices that relies on the following:

- One or more Secure Elements - of different form factors, accessible through a standard API of services, which enables access to the mobile financial applications
- One Trusted User Interface (TUI) - to secure the transmission of data between the SE and the user input/output devices. In particular the TUI may implement services such as:

Diagram 5: Finding The Right Balance Between Flexibility & Security

The TEE is intended to complement the SE in the mobile device, jointly implementing a TUI. This TUI provides a secure channel between the user interface in the mobile device and the SE, protecting against software attacks and creating a protected environment to handset's resources.

The TUI enables secure authentication and non-repudiation for sensitive transactions performed on smartphones. It controls the screen and keyboard and/or touchpad, isolating them from the operating system, therefore ensuring:

- **Secure authentication** - protected entry of user credentials, such as PINs and passwords, which can then be securely transferred through a private communication channel to a SE , or to a server for on-line verification. No malware can gain access to these credentials

- **Non-repudiation** - critical transaction information is displayed on screen in such a way that it cannot be tampered with. No malware can change the transaction information displayed on the user screen authentication credentials or other critical security parameters such as cryptographic keys. Access controls to authenticate the legitimate user requires the presence of a software module executing either on the mobile device or within the SE itself.

6.3. The wireless infrastructures

The mobile technology landscape provides various possibilities for implementing m-payments. Essentially, a GSM mobile phone may send or receive information (mobile data service) through three possible channels – SMS, USSD or WAP/GPRS. The choice of the channel influences the way m-payment schemes are implemented. Secondly, the m-payment client application may reside on the phone or else it may reside in the Subscriber Identification Module (SIM).

The SIM used in GSM/3G/4G mobile phones is a smart card i.e., a small chip with processing power (intelligence) and memory. The information in the SIM can be protected using cryptographic algorithms and keys. This makes SIM applications far more secure than client applications that reside in the mobile phone.

The mobile network infrastructure supports security services at transport and presentation layers for the voice and data transmission services provided by the telecom operator. The supportive protocols are standardized and enable (1) the telecom subscriber authentication, (2) the radio interface encryption, (3) the subscriber identity confidentiality, (4) a security layer between the SIM card or Universal Integrated Circuit Card (UICC) and the network processing back-office.

6.4. Security certification of mobile payment devices

The certification of mobile financial applications raised several interoperability issues with regards to the recognition of the security certificates for mobile financial services products. This means that the security evaluation and certification methodologies used for traditional payment cards has to be adapted to these multi-application platforms for mobile payments.

Several scenarios can be differentiated when certifying such platforms:

1. When both the platform and the application is owned by the financial institution, the certification process is similar to a mono or multi-applicative smart payment card
2. When the platform is owned by a third party and the application is owned by a financial institution, the certification of the configuration platform and the application is required.

One concrete example is the security evaluation and certification of an SE for mobile financial applications. Once a mobile application has been certified over a platform (SE) provided by vendor A using a security methodology of Laboratory A, it would be rational to reuse part of these evaluation results if the same application is to be executed over a platform (SE) made by vendor B.

This case leads to the need to harmonize the security and functional properties of those platforms that are suitable for the storage and execution of any given application. Therefore, the issuer of a SE will dispose of a series of mobile financial applications and will also have provisioned SEs from different certified hardware tamper resistant platforms offered by different vendors. The application vendor will not need to certify its application with any of the available platforms in the market.

7. Addressing security issues in developed countries

7.1. Fixing the context for mobile payments in developed countries

In developed countries, both the payer and the payee hold a bank account and share a common user experience for card payments. Because financial institutions have a long-term, well-established business relationship with their customers, they can propose new tailored financial services using the mobile device. Therefore mobile payment represents a new and convenient channel for existing payment instruments. In addition, customers of a mobile telecom operator usually have accounts in different banks which offer their own payment applications. The conditions are therefore met for a real multi-application payment environment which can be accessed through the mobile user interface.

In developed countries, legacy with existing card payment infrastructures is a central business requirement. In addition, users of the system may afford leading edge mobile phones (smart phones) with advanced security features. In particular, mobile handsets are able to support connectivity with multiple wireless network infrastructures, proximity (e.g., NFC), wireless (802.11-x) and with mobile networks of different generations.

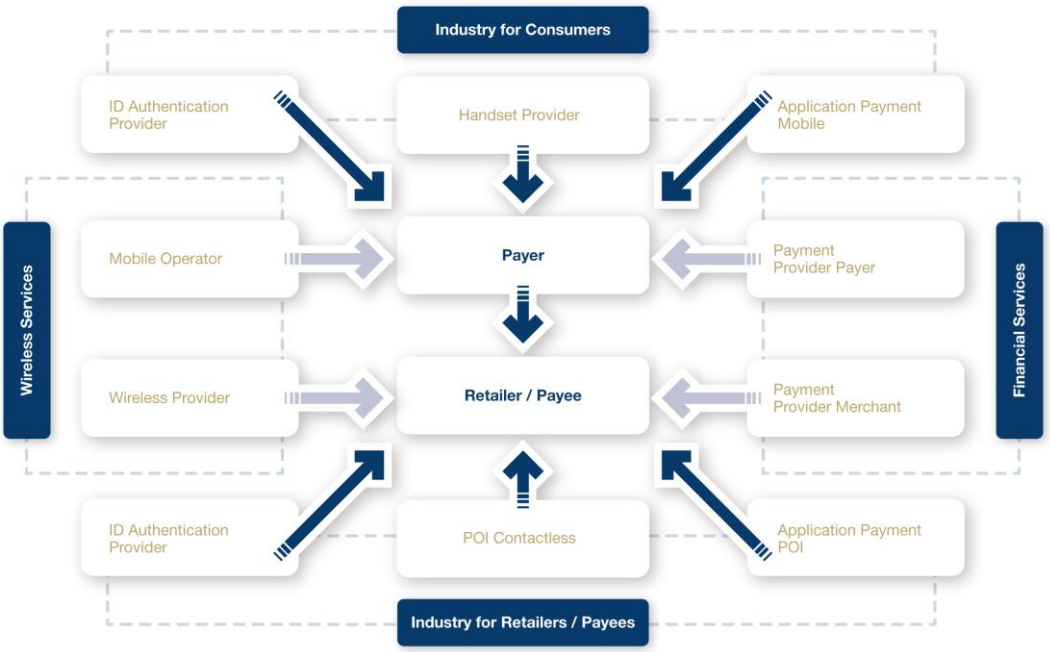
Mobile payments and the new European regulation such as the Payments Service Directive (PSD) introduce fresh challenges in terms of the impact of regulation on payments market structure, liability shifts, and the role of non-banking entities in the provision and operation of mobile payment systems. But whatever the new structure of the mobile payments market will be, the trust that users place on current financial intermediated payment systems should remain unchanged. Security countermeasures to prevent and detect fraud should start from existing practices, and be completed with specific mechanisms to mitigate the inherent risks of new mobile channels and payment devices.

7.2. Establishing a security policy

A clear understanding of the key issues and the multiple impacts of security policies on the business model and motivation of the stakeholders to enter the mobile payments market is needed. In order to establish security guidelines for mobile payments, the SPA proposes the following set of basic assumptions:

1. Implementing a mobile payment scheme requires a business agreement **between many stakeholders** - financial institutions, mobile telecom operators, payers and retailers/payees, debit/credit payment card networks, clearing/settlement organizations, software solution providers, mobile handset, secure element and chip vendors and third party payment processors. Whatever the contractual terms, the payment scheme issues a mobile payment instrument able to initiate a payment transaction

Diagram 6: Stakeholder In A Mobile Payment Scheme



2. Success is reliant on collaboration between industries that have never worked together before with a shared mobile payments infrastructure. We refer hereafter to this mobile payment infrastructure, made up of hardware and software components, with the generic term of "mobile payments platform" or simply "the platform". The mobile payments scheme offers the users of the system - retailers and consumers - a mobile payment instrument and agrees on a commercial strategy for adoption. In practice this will require contractual agreement on the security functions that the devices under the retailer's control have to support
3. The mobile payment scheme is launched to run monopolistically according to agreed governance rules – to include liability allocation and rules of fraud - between the platform and the merchants. While it is true that each party views its responsibilities and liabilities differently, a common roadmap is needed to sort out the infrastructure and functionality surrounding the mobile payment transaction. In particular, areas of liability in the event of a payment incident should also be given the technical means and processes to mitigate the identified risks
4. In some circumstances these industries might even compete in the mobile payments market. However in this context, the user of the system (payer or retailer/payee) is simultaneously the client of at least two entities, for example a financial institution and a mobile telecommuniations operator. Such entities may sign a business agreement with a third party (such as a payment network brand, TSM, or device vendor). However, the security for any payment transaction should be independent from the particular payment service provider and the particular mobile operator involved in any particular transaction
5. The success of a mobile payment scheme depends on the number of users - both retailers and payers. Retailers play a crucial role in the development of payment schemes, as their acceptance of mobile payment systems creates the market for such schemes. Providers face the so-called "chicken and egg" problem, as merchant acceptance equally depends on customer willingness to pay with a mobile device. In order to promote adoption of mobile payments, the

scheme should incentivize retailers to implement a fraud-prevention solution, according to the scheme security policy

6. From a security perspective, each player involved in the mobile payment scheme adds to the system risk and therefore must commit in cost terms when risk-mitigating policies are implemented. Platform rules may provide retailers with incentives to invest in fraud detection technology. However the prevention of some risks might require an investment effort by the platform owners – for example, the financing of security mechanisms in the mobile payment instrument and the platform itself

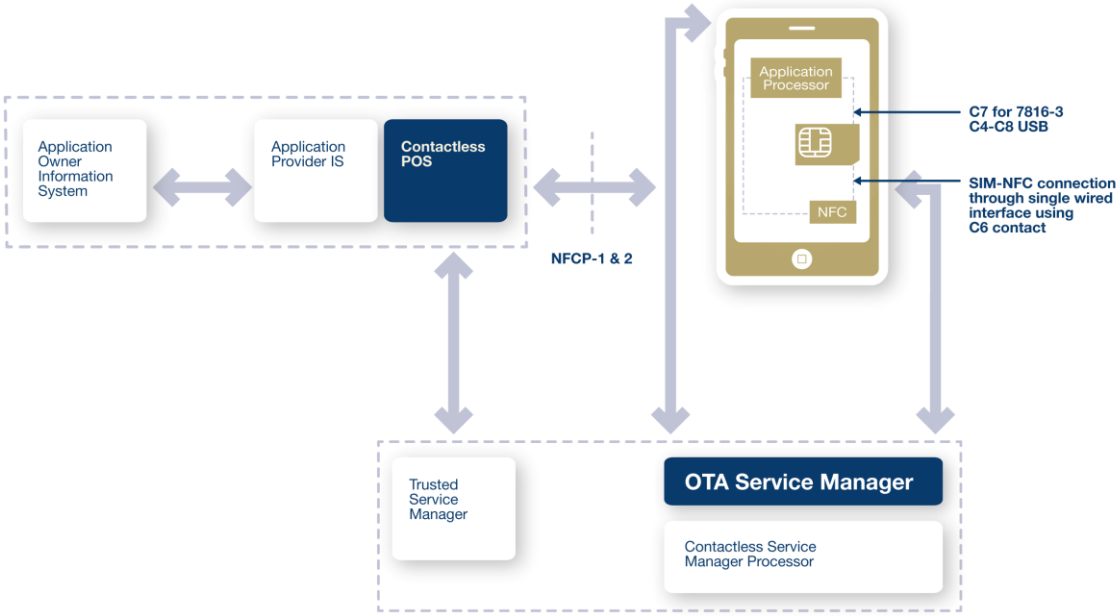
7. Developed countries will use mobile phones with NFC chips for retail purchase or transit applications, meaning proximity contactless payments. The vulnerabilities specific to the mobile phone combined with the NFC interface are to be addressed first. A number of valuable analyses have already been published, especially by the academic world. This document provides security guidelines and recommendations for practical implementation, based on the findings of these studies

8. The NFC circuitry, also known as the "analog interface", provides a common radio frequency interface to one or more SE. For consistency purposes the SPA suggests the adoption of EMV terminology, referring to applications supporting proximity payments as mobile contactless payment applications (MCPA). An MCPA is therefore any mobile payment application resident in the mobile device that is able to communicate with a contactless terminal, known in ISO as the PCD, using an NFC interface

9. The NFC mode of communication involves the conveyance of payment transaction messages using two different transport protocols:
   - One internal to the mobile device, between the SE containing the MCPA and the NFC module, which is wired
   - A second external, using a contactless protocol (e.g., EMVCo Contactless protocol) executed between the NFC module of the mobile device and the contactless terminal (the PCD). This second interface can be secured using for instance, the NFC–SEC protocol.

   However, this security layer is neither generated by the SE nor the MCPA and therefore does not protect the first path. It follows then that a secure channel common to both transmission paths, internal and external to the mobile device, is preferable

Diagram 7: Interfaces For Proximity Payments



10. The existence of the two interfaces, and the fact that the MCPA is controlled through a user interface that is not secured, constitute two major vulnerabilities intrinsic to the mobile device payment when compared with proximity payment using a contactless card, for example. If security countermeasures are implemented, these risks are minimized and then the mobile device and its user interface could be used for a local verification of the payer identity

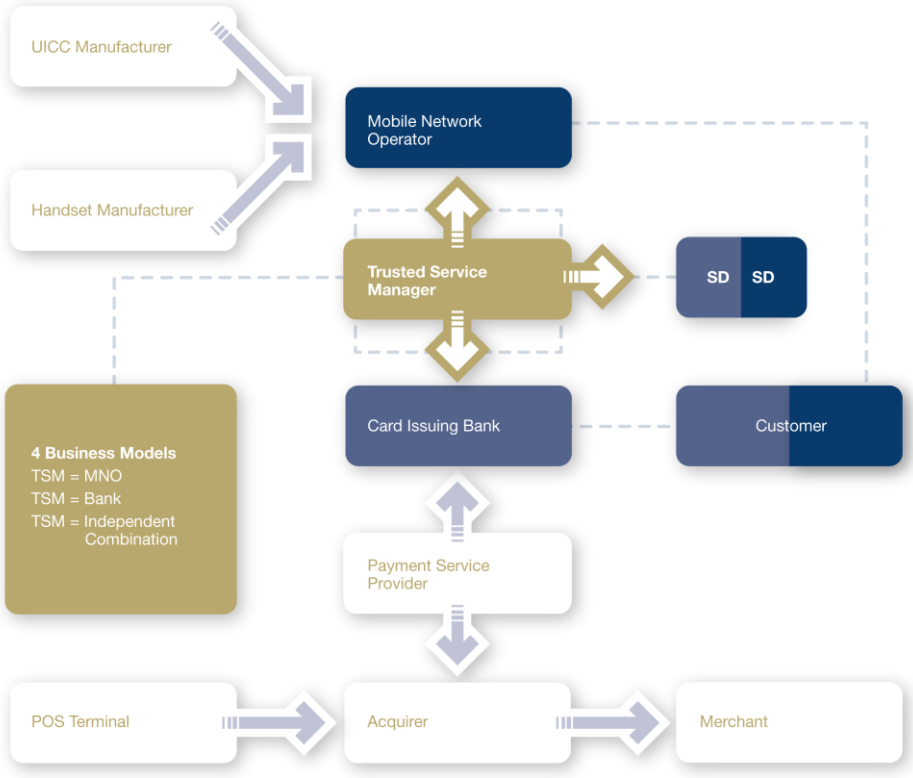
11. The MCPA can be selected by either a user interface on the mobile handset or in certain contexts where the speed of transaction is key (e.g., to avoid queuing in access applications) by the application resident in the PCD itself. This last option is recognized in the Volume Book of Requirements, published by the European Payments Council. In any case, upon successful selection, any MCPA resident in the mobile payment instrument has the ability to securely connect and authenticate to the platform

12. The MCPA can be owned by an entity external to the mobile payments scheme. However the security conditions for the life cycle management of the MCPA and its execution shall be set by the scheme itself, possibly after negotiation with the MCPA owner. A good design practice for the scheme is therefore provided with a flexible SE that may support different security arrangements for application downloading purposes. The scheme is expected to become liable in front of the users in relation to any malfunction due to any application offered by the platform, and in front of application providers in relation to any security incident as a result of a flawed application owned by a third party

13. One of the basic agreements that any mobile payment scheme has to achieve is the management of the mobile contactless applications in the mobile payment instrument. So whose entity, and under which conditions, is authorized to download/activate/deactivate/remove a MCPA into a device (e.g., a SE) owned by the scheme? In this respect, the Global Platform provides specifications offering different business arrangements. The SPA is in favor of supporting those options that facilitate the constituency of

mobile payments schemes taking into account the interests of both financial institutions and mobile telecom operators. In order to speed up the return on investment, options making use of existing personalization infrastructures (e.g., OTA server based) should be encouraged

Diagram 8: Roles For Mobile Payment System Operations



14. Other than proximity payments (also known as C2B payments) a new challenge relates to secure person-to-person (P2P) mobile payments. In this segment new players are already playing a central intermediation role. Therefore platform should be able to authenticate both communicating parts so they can agree on the payment terms. Upon confirmation (to be secured) of the payer, the platform will then transmit the corresponding payment order to the institutions holding the payment accounts of the payer and the payee

15. In the previous scenario, the mobile payment scheme is the mobile payment service provider who previously enrolled the payer and the payee. The legal background for the operation depends on the licensing conditions required to play this payment service provider role. Dependent on the regional legal framework, this payment service provider may or not be authorized to hold payment individual payment accounts for the users of the system. In such closed mobile payment schemes, the proprietary security policy should be consistent with the policies applied by other payment service providers, in case these applications share the same executing environment in the mobile device

16. From the above it follows that the same mobile wallet may host:

- A mobile payment instrument holding one or more mobile contactless payment applications, for proximity payments purposes, owned by a single mobile payments scheme
- A functionally independent mobile payment instrument owned by another payment service provider for P2P mobile payments
- A mobile payment instrument holding both proximity and P2P mobile payment applications
- A combination of any of the above.

Because the risks inherent to these payments differ, specific security mitigating features for each payment instrument constitutes a good policy

17. The mobile payments device contains different functional modules which are central for the security of the mobile payment transaction:
    - The User interface including a display and a physical or tactile keyboard
    - The NFC module and other radiofrequency interfaces with the external world, to the mobile operator network and possibly to other RF receivers as well
    - Power-up and clocking of the SE
    - Possibly a TEE
    - A middleware for access to internal operating system resources
    - Hardware security computing resources (e.g. one or more SE).

    The internal architecture of the mobile device is a proprietary design decision of the manufacturer

18. The multilevel functional approach illustrated above means that the security architecture for mobile payments is distributed. The security of any system operation (enrollment, application life cycle management, payment transaction) will rely on the ability of the communicating parts to authenticate and establish a secure channel to protect any further data exchange between the mobile payment instrument and the PCD, between the PCD and the system (e.g., the acquirer infrastructure), or directly between the mobile payment instrument (or any resident MCPA) and a layer on the platform executing the same protocol (end-to-end security). The platform operated by the scheme is assumed to be secure

19. In such architecture, part of the security of the system is supported by the mobile device, part by the SE and/or the TEE, part by the mobile wallet (if any), part by the mobile payment instrument, part by the MCPA, and part by the PCD. This means that access rules are set at any of the logical hierarchical components owned by the scheme. These logical levels will handle the security status of any external device (component of the system or an external entity with a delegated authorization provided by the scheme) trying to get access to the mobile payment instrument resources. The model is equivalent to the security architecture proposed by ISO/IEC 7816-4. The platform in the mobile payments system is assumed to be secure

20. To be secure, the system cannot contain weak links. However, the decision in the way to optimize global security for the transaction, the choice of the algorithms and crypto-protocols to be implemented and the interfaces/system components to be specially protected may not rely on technical considerations but specially in the liability allocation decided by the scheme and the business model(s) supported

21. In a scenario where the mobile payments scheme is not the owner of the SE and/or the mobile device TEE specific security conditions, contractually agreed between the scheme and the SE issuer may apply for access to the mobile payment instrument. Such conditions may apply for instance to the authentication methods and secure protocol to be executed by the scheme platform to load a new application in its own mobile payment instrument. This can be the case when several MPIs owned by different schemes coexist in the same SE owned by a third party

22. A particular case for P2P payments is domestic and/or international mobile remittances. This raises specific concerns due to its potential misuse to transfer funds for the purposes of finance crime or to facilitate money laundering. In this case, specific financial crime preventive security measures may be required by law. These requirements will impact the security functionalities of the payment instrument and specially the platform. In this case the platform might integrate or more likely interface with an identity management system

23. The core of the ID management system is a database with the identifiers and authenticators of the enrolled users of the system. This database must be highly protected. The first purpose of the ID system is to track suspicious mobile payment transactions that could be reported to the local regulator. However ID management systems also protects users by facilitating further authentication from claimed legitimate users

24. Other than tracking users, the ID management system may also protect the privacy of the mobile scheme users (see point 25 next), provided that certain conditions are met. For instance, if the scheme offers access to virtual merchants, the scheme ID system may enable a way of authenticating consumers to the virtual merchant association. The scheme may then intermediate the payment without having access to the details of the purchase, which would remain confidential between the merchant and the consumer. If properly secured, mobile commerce is a natural generator of mobile payments

25. The multiplicity of players in the mobile payment value chain may lead to unauthorized leaks of personal information related to, for example, details of the payment accounts of the users of the system, or the nature of the goods and services purchased that may be in conflict with personal data protection laws. In each case, specific privacy protocols should be executed along with the mobile payment application or be embedded within the mobile payment application itself.

The above statements in section 25 prepare the way for establishing key requirements that apply to a mobile payment transaction with "advanced" security properties. These properties are provided by the cryptographic services of the logical components in the security architecture of the system. From an analytical prospective these components make up a security chain.

7.3. Security for mobile proximity contactless payments

Recently a number of so called 'successful' attacks on NFC transactions have been published in specialized literature. Regardless of the degree of practical feasibility, it remains true that the intrinsic nature of a radiofrequency interface means attach vulnerabilities are a possibility.

Skimming refers to an active attack to start a transaction with a contactless device without the awareness of the legitimate owner. Skimming is perceived as a considerable threat by payers, and from a business perspective represents a key security concern for mobile payment contactless products.

A good security policy for contactless payments must therefore include an anti-skimming feature in the mobile device. The second concern relates to the protection of confidential data which can be guaranteed by the creation of a secure channel with a negotiated cryptographic session key having the sufficient entropy.

Some crypto-protocols do not implement anti-skimming features, which results in the uncontrolled disclosure of information by the mobile device at the beginning of any transaction, legitimate or not. Other than fraud risks, there is a concern in relation to privacy, due to the problem raised by the transmission over-the-air of the certificate stored in the SE at the beginning of the execution of the protocol. In theory this makes it possible to trace the cardholder. To ensure privacy design protocols should include a first stage so that this certificate can be encrypted.

Anti-skimming protocols (e.g., password based) ideally have the advantage of including a tamper resistant device (e.g., a SAM) in the contactless terminal, facilitating backwards compatibility with the existing infrastructures. In addition, password-based protocols would enable the generation and exchange of a session key to encrypt the certificate of the secure element. This certificate is then to be verified to proceed to a dynamic authentication protocol. The verification of this password will also be useful to authenticate the payer. Once this certification has been transmitted in its encrypted form, a second session key may be negotiated to protect against eavesdropping. While the solution can be envisioned, the problem of longer transaction times remains.

Eavesdropping is a wireless specific passive attack that requires the attacker with an antenna to access the wireless channel and record transaction details. Establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping and any kind of data modification attack. This secure channel, using a key exchange protocol, can be performed with or without executing a previous mutual authentication:

- With no authentication
- With SE/mobile financial application authentication
- With mutual authentication: symmetric solution.

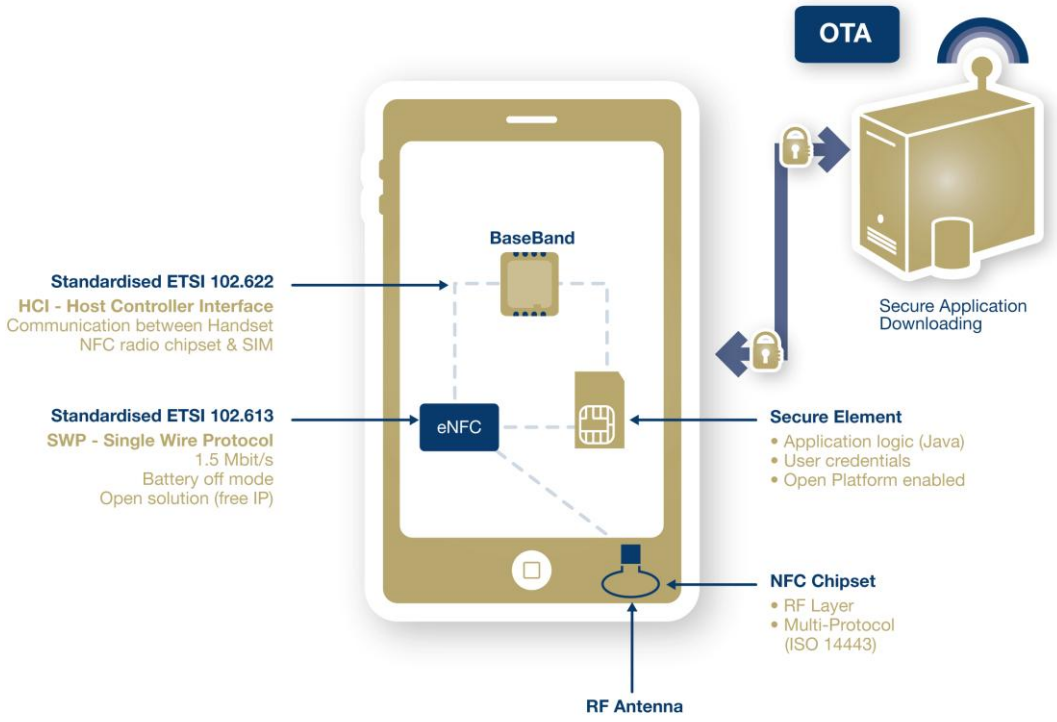
Relay Attacks - a NFC mobile device is used to pay to a legitimate PCD by using application-level data generated by a legitimate mobile payment application (resident in a contactless card or in a SE) that has been skimmed using a fake reader (e.g., a second NFC, see NOTE). Actually the contactless transaction takes place in two legitimate proximity applications, unaware of the attack. Relay attacks are not easy to circumvent because for the attack to work, the attacker doesn't need to get access to the data in-clear.

Transaction blocking is possible with an active attack by merely emitting spurious radio signals centered in the carrier frequency of 13.56 Mhz that saturate the receiver stage of the communicating devices. Other classical attacks, like man-in-the-middle are not considered to represent a significant risk in the NFC context.

The mobile contactless payment application (MCPA) makes use of its own set of keys to authenticate itself to an external entity and then to create a secure channel. In addition, the application may have at its disposal other keys and reference data for other services like mobile signatures and the verification of the payer by the application.

In this initial model, the mobile device itself emulates a contactless card, meaning the mobile handset is not part of the acceptance/acquisition part of the platform.

Diagram 9: Single Wire Protocol & NFC Mobile Architecture



7.4. Security for mobile remote payments

Compared with proximity contactless payments, remote mobile payments raise different issues in terms of risk. Whereas in NFC payments the main concerns are represented by skimming and eavesdropping, for mobile remote payments the main concerns are strong user authentication, the confidentiality and integrity of the exchanged messages, and the need to generate a strong proof of consent.

The security channel leading from the mobile application to the payment provider is longer and outside of the control of the issuer. Secondly, physical authentication of the payer is not possible and strong online authentication processes are required to verify a claimed identity and authorize the service. This means that authentication information is transmitted through unsecure networks.

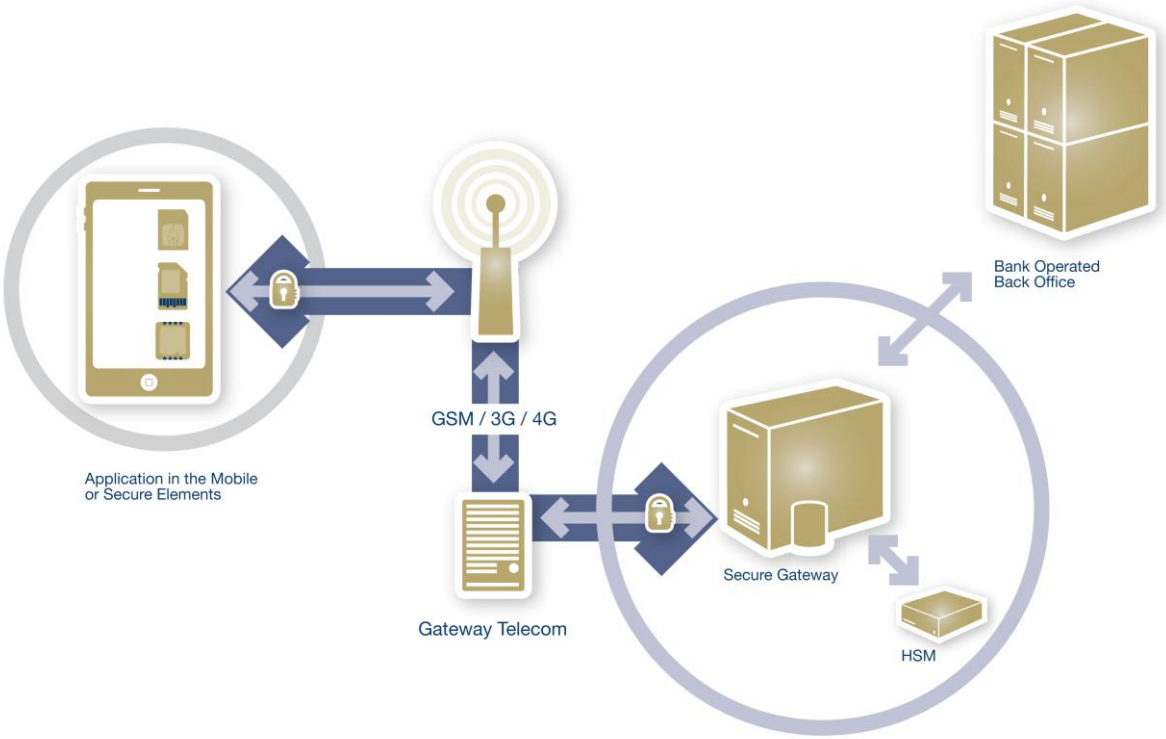
In addition, many in-field implementations are software based and make use of generic GSM or other standard short message services. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts.

In this context however, at least two different use cases are to be analyzed:

1. The payer connects directly with his/her financial institution and these considerations apply as well to mobile banking services

2. The payer is connected with a payment service provider during a mobile commerce transaction. In this case the payee is an online retailer.

Diagram 10: Generic Architecture For Remote Mobile Payments



7.5. Security countermeasures - cryptography

The SPA proposes that the following security objectives represent a commonality for any type of mobile payment.

1. Minimize the risk of capture or disclosure of the payer's personal data, when this data is:
   - At rest in the mobile device, and attacked by malicious software installed in the device or by the disclosure of data following a skimming attack
   - Being processed after application activation
   - Transmitted during a phishing attack
   - At rest in the financial institution, or in any computing resource across the security chain.
2. Minimize the risk of capture of PIN code when the PIN code is entered for verification purposes
3. Ensure the strict confidentiality, integrity and non-reusability of authentication information, and of any message proving the user consent to a given transaction
4. Ensure the integrity of the mobile financial application throughout its lifecycle - and especially during the personalization phase.

Many of the above safeguards are best implemented using cryptographic mechanisms.

For mobile payment schemes, strong customer authentication is key. And as per the general framework of any secure messaging system, confidentiality, integrity, non-repudiation and authentication should be guaranteed. The transport layer security offered by GSM/CDMA networks offers confidentiality (that messages cannot be read by anyone else) and message integrity (the assurance that the message has not been altered in transit) to some extent. Authentication (identifies the author of the transaction) and non-repudiation (makes sure that any of the users in the system cannot later deny the message they sent) can only be guaranteed with the help of wireless public key infrastructure (WPKI) and digital certificates.

Crypto Service	Use Case	Protects Against
Authentication	Prove Identity	Digital Impersonation
Confidentiality	Keep Secret	Eavesdropping
Message Integrity	Verify Information	Alteration during Transit
Non Repudiation	User Consent	Dishonest Behavior

ISO subcommittees JTC1 SC27 WG2 and TC68 SC2 collaborate in order to identify and select cryptographic mechanisms suitable for financial security purposes. These are:

1. Primitives (e.g., algorithms, symmetric and asymmetric ciphers, key lengths)
2. Schemes (e.g., modes of encryption, authentication)
3. Protocols (e.g., authentication, electronic signature).

Recently, standards on entity authentication, digital signatures, hash functions, message authentication codes, non-repudiation and key management have been published for the first time or revised by ISO. For mobile financial services only cryptographic schemes, which are provable in a strict mathematical sense, should be used.

8. Security issues in developing countries

8.1. The ecosystem for mobile payments in developing countries

The ecosystem for mobile payments in developing countries is very different. The lack of banking infrastructures, the existence of a large unbanked and low income population, and the limited volume of monetary exchange all requires a specific approach when setting security standards.

The 2.5 billion people in the world who today lack a formal banking relationship (or even access to banking infrastructure) but will soon become an emerging middle class presents an attractive target for all of the payments networks and issuing banks.

In an apparent paradox, the lack of legacy banking payment systems partially explains the success of mobile payment schemes in developing countries. In this separate segment of the market, systems deployed by mobile network operators succeeded to provide to the end-user with new payment instruments that offered real value and were massively adopted. Indeed, mobile payment devices enabled largely unbanked populations to benefit from services reserved in developed countries to the bank-served population. This success meant that the payment accounts initially intended to receive domestic remittances to be converted in cash evolved to provide most of the payment services offered by a bank account.

Mobile payments might well play an unprecedented role in social transformative by building on existing infrastructures, like telecommunication networks, not originally intended to sustain financial innovation. In countries lacking banking infrastructure to reach people located remotely mobile network operators have taken a lead role thanks to their extensive networks of local agents. Thus, mobile payments can replace 'risky' cash since not many payment alternatives exist.

In this context, when analyzing systemic security threats, other considerations should be taken into account: the fact that users are in general low income citizens and cannot afford top-of-the-range mobile equipment, and the fact that the opportunity for the financial inclusion of these populations should not be burdened by over-protective security policies. Yet this is a field for advanced cryptographic solutions, enabling the whole end-to-end payment chain to be secure even if a weak link exists in between. Other than a challenging technical problem for security engineers, there is clearly a need for specific local regulations in this area.

8.2. The case of mobile remittances: bridging payment systems from developing & development countries

International remittances bridge the above separate contexts: developed and developing areas payment systems. Developing countries are using mobile text messaging/SMS for remittances and money transfers between users. Remittances are a huge market in countries with high unbanked populations but also high mobile phone penetration, such as the Philippines, India, and Kenya.

A secure communication link should be created between the mobile payment application that, in the case of the payee, will be typically resident in the SE and the mobile device of the payee where some form of cardholder authentication (SIM card) is available.

Pre-paid accounts credited with an amount transferred using a remittance, mobile or not, is a solution that has been proved. The authentication provided by the SIM card may then enable the beneficiary to cash-put the credited amount in their account. Yet the lack of standards for interoperability means these systems remain at present closed. Future interoperability standards will dramatically increase the volume of mobile remittances and therefore this payment means will attract the attention of attackers. Security-specific standards will then need to be created; in particular these will have to address the challenge of creating a secure channel when one of the communicating end points is potentially unsafe.

9. Why standards are central to achieve security

At present there is a lack of adopted technology standards that provide a kind of universal mode of mobile payment. That is the consequence of being an innovative market with high growth expectations. Many market players have invested in proprietary technology which they then try to impose as the "de-facto" standard. The present scenario follows a classical curve for emergent technologies. In the mid-term, however, the myriad of non-interoperable solutions will result in market fragmentation. Indeed the lack of agreed standards will give rise to a lot of local and fragmented versions of m-payments being offered by different stakeholders (network operator centric models and bank centric models). Because mobile payments are a network-based technology, profitability of any payment scheme will depend on the number of transactions generated. This number will depend on the ability of the different components of different systems to communicate with each other. In other words, common gateways, bridging protocols and mechanisms for mutual recognition of devices; and a technical standard will be required. The consolidation of proprietary specifications in the mobile payments arena is critical and this will enable producers and consumers to make investments that deliver value.

The business requirement for interoperability – in other words, a high level of interconnectivity between heterogeneous system components – is driving the need to harmonize security requirements, reliable implementations and certification practices. As already mentioned, the mobile system is only as secure than its weakest link. Therefore the more complex the communication path between the local mobile payment application and the back-office processing platform (e.g., managed by a financial institution) the more likely it is that a mobile payment message is examined and/or processed by an unsecure component. This path is naturally complex when interoperable infrastructures enable a high level of connectivity.

Standards need to address security and privacy concerns of consumers as well as interoperability between various implementations. In the area of mobile payments, in the cross-roads of the telecom and banking industries, there is a rich legacy of specifications for interoperability. In order to inspire commonly agreed standards, the following examples might facilitate mutual understanding of the respective business needs:

Mobile Phones	Payment Card Networks
Any Secure Element (eg SIM/UICC) card works in any mobile phone	Any payment card could be read by any POI terminal
Any mobile phone can be used by any operator	Any terminal/merchant could send payment messages to any acquirer respecting the same standard
Any mobile phone can communicate with any other phone	Any card could be accepted by any merchant (e.g. both are EMVCo compliant)
Strong competition exists among OEMs and telecoms service providers	There could be visible price and service competition among payment card providers

10. The SPA in the evolving standards environment

As above, the existence of many proprietary mobile payment solutions may lead to excessive market fragmentation, and in the end could hamper market growth. SPA therefore considers that the existence of standards for mobile payments, flexible enough to accommodate different business models, address a key market need. In response, SPA members actively contribute to on-going standardization initiatives for mobile payments. As part of this wider discussion, the standards referred to here include documents published by formal international standardization body like ISO as well as specifications published by other bodies that act as "de-facto" standards bodies for the payments industry, such as EMVCo.

However, in order to describe the standards ecosystem, SPA differentiates those standardization bodies that issue specifications for the Single European Payments Area (SEPA), and those international standards targeting worldwide interoperability.

10.1. SEPA area mobile payments security standards

In the SEPA area the European Payments Council (EPC) has published a number of documents on mobile payments. They provide useful insights on security, as well as offering a considerable amount of relevant technical information. Unsurprisingly, part of this material is under consideration by ISO TC68 SC7 in the framework of the new standard ISO 12812 on mobile payments/mobile banking targeting the interoperability of mobile payment systems. SPA is actively collaborating with both the EPC and ISO; being involved in the relay of EPC requirements and principles being developed by international standardization bodies.

The EPC is collaborating with the other European payment stakeholders in the Cards Stakeholder Group (CSG), where SPA, along with Eurosmart, leads the vendor's sector.

The main objectives of the CSG are:

1. The maintenance of the "Volume Book of Requirements" specifying high-level functional and security requirements
2. The constituency of the SEPA Security Certification Management Body (SCCMB) for the certification of payment card products recognized as SEPA compliant.

In relation to mobile payments security, the CSG is specifying security requirements that apply to both proximity and remote mobile payments.

The Mobey Forum has produced a comprehensive analysis on the different SEs for deployment of Mobile Payment Applications. Documents published by the Mobey Forum, while cannot be considered as specifications, constitute useful material for other standardization bodies, including the EPC and ISO. SPA members are as heavily involved in different Mobey Forum Working Groups.

10.2. Encouraging international consistency

SPA has also been very active in promoting consistency between European and international payments standards. Along with our work with the SEPA - focused elements of payment - SPA has also been actively involved in international standardization initiatives from the very beginning.

For example, in a specific response aimed at addressing threats and vulnerabilities for the radiofrequency interface and the mobile handset, The Security WG of EMVCo is working in collaboration with SPA within the EMVCo Technical Associates Program framework.

In the area of security certification for mobile payment products, new security evaluation methodologies adapted to open multi-application platforms are being published. This so-called Composite Evaluation model is intended to facilitate the deployment of new mobile payment applications across additional platforms to the original in which the application was certified. SPA has been fully supportive of the standardization of these new methodologies in GlobalPlatform, and its endorsement by EMVCo.

For the secure design and certification of mobile payment handsets, the PCI Mobile Working Group has been launched in order to set forth security requirements for mobile handsets used as a payments access point. SPA has promoted the early collaboration between EMVCo and PCI, and between both bodies and the EPC to ensure a consistent reference document of security specifications, without gaps or overlaps, is available for the industry.

All the above initiatives target one of several core aspects for the standardization of mobile payments security infrastructures. However, there remains a lack of a single international standard covering all the mobile payment types with a significant market impact, and all the aspects related to implementation and regulatory concerns.

10.3. Moving towards a single standard

ISO TC68 SC7 aimed to fill this gap by launching the multi-part ISO 12812. This is the first international standard on mobile payments/mobile banking. The standard is supported by a significant number of banking players, both US and European, to enable the interoperability and end-to-end security of mobile payment schemes.

As a part of this new standard ISO 12812-2 specifically focuses on the security aspects of mobile payments and mobile banking, including:

1. A security model including an analysis of vulnerabilities, threats and countermeasures for the operation of mobile financial services
2. A proposal to secure mobile portable devices based on standard components, SEs and a TEE
3. Cryptographic protocols and mechanisms for mobile device authentication
4. Interoperability issues for the secure certification of mobile financial services
5. Recommendations for the data protection of sensitive data
6. Guidelines for the implementation of anti-money laundering rules

7. Mobile payment/banking security management system aspects

SPA members are ensuring the editorial work of ISO 12812-2 and promoting a large consensus within the banking industry on agreed security provisions suitable to generate user trust in this new payment channel.

11. The SPA's 10 proposals to secure mobile payments

1. The SPA considers that the perceived security by the users of mobile payments is the key condition for mass adoption. This perception will be the result of the lack of published attacks, an appropriate liability policy in order to reimburse disputed transactions, and the appropriate education of users of the system in particular in terms of (1) the investment efforts in security by the mobile payment scheme stakeholders and (2) clear direction in the way to proceed in case of payment incident or the mobile handset loss
2. The SPA considers that there is no single security solution optimized for all mobile payment services. Therefore the system's security properties must be carefully designed, so that they be proportionate to the risks inherent to the type of mobile payment instruments issued. The security policy decided by a mobile payment scheme should be the result of a risk analysis, considering the vulnerabilities of, and the threats to, the offered mobile payment instrument. A liability shift allocation should be put in place in order to incentivize the investment in security technology by the different stakeholders
3. The SPA is in favor of flexible standards that support different business models - whether financial-centric or telecom-centric. However, the risks linked to mobile payment transactions should be independent of the specific business model adopted. In practice that results in common security services being granted to the mobile payment application; in other words, the use of protocols based on security proven crypto-algorithms and common security certification practices
4. The SPA supports strongly the adoption by the mobile payments industry of the new security evaluation and certification methodologies such as the Composite Evaluation model. Widespread adoption of this model will result in the rational reuse of previous evaluation reports for applications, lowering the overall cost of certification, minimizing time-to-market and boosting the secure deployment of new mobile payment applications
5. The SPA can only be in favor of exporting the experience of payment smart cards to mobile payments. This means that SPA strongly recommends that all the mobile payment applications, and of course all security keys need to be in tamper-resistant environments which only execute security-proven cryptographic algorithms. In order to facilitate cross-industry arrangements the Secure Element (UICC, micro-SD embedded SE) appears to be the right choice to store mobile payment applications. The SPA does not provide specific recommendations in the SE form-factor to be adopted
6. With respect proximity contactless payments, SPA members recommend the worldwide adoption of the EMVCo functional and security specifications for mobile payments. The SPA commits to continue an active collaboration with EMVCo in the frame of the Technical Associates Program to optimize, in particular, cryptographic choices and security certification practices. The SPA considers that migration towards fast asymmetric elliptic-curve based cryptography is right, but

in the meantime, in order to find an optimized balance between security and performance, other options, such as lightweight cryptography, can also been envisioned

7. Mobile payment applications should only be stored and run in computing contexts that isolate the execution of the application from any existing malicious software resident in the mobile device. With this respect, the SPA is supportive of combining security technologies that jointly provides an optimized security environment for the execution of mobile payments. An example is the combination of the SE with a TEE, intended to deliver into the mobile handset an isolated environment for the interactions of the application and the user interface during its execution

8. The SPA recommends the early consideration of the applicable legal environment for the issuance and operation of mobile payments. This includes legal provisions for mobile payment application selection procedures, cardholder verification methodologies, data protection and "know-your-customer" identification requirements intended to prevent criminal misuse of the mobile payment system. In this respect, cross-border mobile remittances might raise legal concerns and require implementation of specific technical safeguards

9. The SPA strongly supports the use of mobile payment technology for financial inclusion purposes in both developed and emerging regions. The social transformational potential of mobile payments and other financial services will be leveraged with further integration of security requirements in existing and future mobile payments schemes in a way consistent with existing practices and state-of-the-art of the mobile handset park currently available.

10. The SPA encourages collaborative efforts to develop common security standards for mobile payments from the mobile operator community, the European Payments Council, and with worldwide standards-setting bodies such as EMVCo, PCI and ISO. SPA members will actively support and contribute with their technical expertise to facilitate early availability of a collection of security standards fitting the needs of the mobile payments industry.