THE HONG KONG ASSOCIATION OF BANKS
香港銀行公會

NFC Mobile Payment in Hong Kong

Best Practice

Version: 1.1

Date: 24-June-2016

Abbreviated version

Table of contents

1 Background

The Hong Kong Monetary Authority (HKMA) completed a consultancy study on Near Field Communication (NFC) mobile payment infrastructure development in Hong Kong and released the study result in March 2013. One of recommendations of the study was to establish a common set of standards and guidelines on the implementation of NFC mobile payment solutions in Hong Kong. In this context, an NFC task force was formed under the Hong Kong Association of Banks (HKAB) in March 2013 to develop such standards and guidelines.

The objective of this document is to provide both the minimum security requirements and some other recommended best practices to the member banks of HKAB and their business partners for the development of NFC mobile payment in Hong Kong. The document also includes the guiding principles and details of the NFC implementation framework for establishing an interoperable NFC mobile payment infrastructure. The implementation framework comprises three sections: the technical standards to facilitate the interoperability among different infrastructure components; the security requirements on payment transactions; and the operational processes between the banks and their business partners. The section on Security Requirements should be construed as the minimum security requirements which the HKMA expects banks and their partners to follow when implementing NFC mobile payment services.

2 Change History

This section keeps a change history for the benefit of the reader. As the standards and market infrastructure evolve, updates and changes to this document will be taken place from time to time.

Date (DD/MM/YYYY)	Description of changes	Version	Remark
25/11/2013	Document creation	1.0	
24/06/2016	Revision to 2nd paragraph of section 6.5.2	1.1	

3 Objectives and Principles

3.1 Development Objectives

The objective of the NFC mobile payment development is to provide a convenient, interoperable, safe and secure payment service to users. The service is aimed to benefit the users, the payment and retail industries in Hong Kong.

The following four development objectives are proposed by the HKMA and agreed by the banking industry:

1 Ability to download multiple payment services from different banks and payment service providers onto a single NFC-enabled phone

2 Payment service continuity despite switching from one mobile network operator to another operator

3 Payment service continuity despite changing one's NFC-enabled phone

4 High level of security in line with international standards and relevant regulatory requirements

3.2 Guiding Principles

To achieve the development objectives, the implementation framework for NFC mobile payment should include the following:

Open:

- allowing for different business models to coexist in the market
- allowing for different device form factors for users to choose from
- facilitating competition among market participants

Interoperable:

- based on widely adopted international and industry technical standards
- fostering the interoperability of the payment services across different mobile network operators, card schemes, trusted service managers, secure elements, etc.

Safe and secure:

- protecting the confidentiality, authenticity and integrity of payment information
- maintaining a high level of data privacy

3.3 Target Audience

The principles are applicable to member banks of HKAB and the stakeholders of mobile payment services, which include, but not limited to, mobile network operators (MNO), card schemes, phone manufacturers, secure element (SE) providers, trusted service manager (TSM) providers, card perso vendors, etc.

4 Standards and Guidelines

This section describes the best practices to implement the four development objectives.

1 Ability to download multiple payment services from different banks and payment service providers onto a single NFC-enabled phone

- Eligibility checking should be carried out to determine if the customer has a valid phone with a valid SE
- The existing stakeholder or service should not prevent the customers from getting another card onto the same SE
- The existing stakeholder or service should not prevent the customers from using a different SE on the same phone

2 Payment service continuity despite switching from one mobile network operator to another operator

- For SIM-based SE, it is subject to the availability of such service in the new MNO and the provisioning of the card credentials to the new SIM
- For embedded and external SE, it should be able to continue to use the service subject to additional customer verification procedures

3 Payment service continuity despite changing one's NFC-enabled phone

- For SIM-based SE, it should be able to continue to use the service subject to additional customer verification procedures
- For embedded SE, it is subject to the provisioning of the card credentials to the new phone
- For external SE, it should be able to continue to use the service subject to additional customer verification procedures

4 High level of security in line with international standards and relevant regulatory requirements

- To comply with the section Security Requirements

5 Technical standards

Standardization is crucial to the development of every new technology in the sense that openness and interoperability can be guaranteed. These factors facilitate the adoption of new technology and the development of new services using new technology. They allow greater flexibility and scalability for commercial deployment with respect to economies of scale, and fuel further growth by eliminating barriers to new entrants. Many industry players are actively involved with different standardization bodies and associations to define standards and guidelines surrounding the NFC ecosystem.

The initiative was started as far back as 2004, with the formation of the NFC Forum, and one of its main goals is to develop standards and specifications to ensure interoperability between mobile phones and NFC devices. Over the years, NFC technology has been maturing and progress is being made to address the market demand for innovative services. By the end of 2012, with the expansion of the NFC ecosystem, NFC-related standards and specifications spread across many organizations and associations such as ISO, ECMA, GSMA, NFC Forum, ETSI, GlobalPlatform, EMVCo, SIM Alliance, etc.

This section focuses on the following standards in the context of providing mobile contactless payment using NFC technology. These standards are widely adopted and deployed in various NFC services in global market. Due to the rapid evolution, the standards and recommendations expressed in this section may not by themselves be sufficient to meet the specific requirements of all the existing and future NFC payment services. New standards may be developed and released as the market evolves. It is a continuous effort to review the adequacy of this section.

- ISO standards
  - Contact and contactless smart cards
- ETSI standards
  - Remote APDU structure for UICC-based applications
  - Secure packet structure for UICC-based applications
  - SWP and HCI interfaces
- GlobalPlatform standards
  - TSM to TSM and PSP to TSM messaging specifications
  - SE-recommended architectures
- EMVCo standards
  - EMV Profiles of GlobalPlatform UICC configuration
  - ICC Specifications for payment systems (book 1 to 4)
  - Contactless entry point specifications
  - EMV card personalization specification
  - Application activation user interface, usage guidelines and PPSE requirements

6 Security Requirements

This section focuses on the security requirements in the implementation of NFC mobile payment products. The requirements cover the backend infrastructure, the frontend devices and the software applications installed in handsets. In addition, the Hong Kong Monetary Authority (HKMA) will take into account the security controls and measures set out in this section when reviewing the banks' NFC mobile payment products.

6.1 Management of Secure Elements

NFC payment credentials should be adequately segregated from each other within the secure element. This segregation is managed through the creation of the proper secure domain structure and hierarchy. Each PSP owns its security domain(s) where the NFC payment applications or credentials are stored.

GlobalPlatform System specifications define the framework for the security domain structure and hierarchy. EMVCo Contactless Mobile Payment specifications add some requirements for NFC mobile payment. They should be followed in the design of security domain structure.

6.2 Card Issuance and Provisioning

This section lists the main areas of consideration when it comes to security. It focuses in particular on the network security in relation to connections between an issuing PSP, a TSM and a secure element. With respect to data security, it also covers the way data are transmitted and how data are managed and stored within these components. Data here refer to payment applications, payment credentials and cryptographic keys.

For NFC mobile payment, the TSM security requirements should overall:

- adopt existing industry standards such as the Payment Card Industry (PCI) Data Security Standard (DSS), which is developed to enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally;
- adopt service bureau certification requirements, which is developed by the payment schemes to specifically address the EMV chip data preparation and card personalization processes;
- cover the specificity of over-the-air communication, focusing in particular on the secure provisioning of payment credentials to the mobile device and reciprocally on the protection of the TSM against intrusions or attacks from mobile devices.

The scope includes:

- securing the connections within the NFC ecosystem
  - Secure the interface between issuing PSP and TSM

- Secure the TSM interactive interfaces provided to the issuing PSP
- Secure the interface between the PSP TSM and the SE Issuer TSM
- Secure the communication between TSM and SE
- Secure the payment application provisioning and delivery

- Securing the data within the NFC ecosystem
  - Secure the data within the TSM
  - Secure the data within the logical data processing
  - Secure the key management within the TSM ecosystem

6.3 Mobile Payment Services Management

6.3.1 Mobile wallet

Mobile wallet is an application installed in a handset. It can be issued by banks, mobile network operators or other players. It provides an interface for end users to manage the NFC services residing in the SE.

An NFC wallet comprises the following key features and functionalities:

- New NFC services discovery –The available list of services may vary according to different parameters, including business agreements between stakeholders or technical capability of the mobile device.
- NFC services provisioning – End-users can securely and remotely download the NFC mobile payment application/credentials.
- NFC services management and administration – End-users can manage the NFC services residing in the handset. This includes activation and deactivation mechanisms, default selection, prioritization and any other preferences associated with the services being offered. The NFC services may belong to a single or several service providers.
- End-user authentication – This could be a username plus alphanumeric password, a numeric code or any other authentication pattern. There might be several types of authentication mechanisms embedded into a single wallet to cover the needs of different stakeholders offering services with different liabilities. Authentication could be required for provisioning, management or administration of NFC services, or entered as part of a payment transaction.
- End-user notification – Service providers can send offers and inform users about NFC services changes, NFC services misuse, malfunctions or fraudulent activities.

In addition, an NFC wallet may offer non-NFC services particular to a specific business context. For example, a financial institution may design a wallet to host several mobile financial services such as mobile banking, person-to-person payment and mobile commerce functions.

The safety and security of mobile wallets are of utmost importance as an end user accesses different NFC services through the wallet. An end-user should feel protected in every circumstance when a mobile wallet is accessed.

6.3.2 Management of multiple payment credentials

When multiple payment credentials from different issuers are installed in a SE, it is important to govern that only authorized mobile wallet application can access to the assigned payment credential stored in the SE. GlobalPlatform Device Technology – SE Access Control standard specifies the mechanism for a wallet to access a single payment credential or a set of credentials stored in a SE.

Secure element should implement adequate access controls and authentication to restrict access to the payment credentials by authorized mobile applications only.

6.3.3 Authentication Codes

Wallet PIN protection should be implemented to protect a mobile wallet. To provide flexibility on user preference, the implementation may provide a configuration setting menu for users to turn on and turn off the PIN protection. In this case, the default status of the protection should be on. Also, user education on the importance of security is necessary.

Wallet PIN and mobile PIN, if implemented, should be stored inside the secure element.

6.3.4 Access to sensitive information

Access to sensitive information such as NFC payment credential should only be allowed upon a PIN entry. When a wallet contains multiple NFC payment credentials provided by different issuers, the wallet should ensure that the sensitive information are adequately segregated and confined to the respective authorized issuer.

Access to and usage of transaction data should be restricted to either the authorized end-user or the business entity owning the data. Where a wallet contains information from multiple business sources, transmission or usage of the data should be subject to end-user authorization and business agreements between the entities involved.

6.4 Payment Transactions

6.4.1 Audit trail and Refund

Effective procedures and adequate audit trails should be in place to prevent and detect unconfirmed transactions, e.g. transactions are only updated on the chip but not the point-of-sale terminal, or vice versa.

Refund should be arranged promptly with proper customer notification upon detection of unconfirmed transactions.

6.4.2 Card-Not-Present transaction

NFC mobile credit card should be prohibited from conducting card-not-present (CNP) transactions unless the card information, e.g. card number, expiry date etc, are not readable by a contactless reader through electronic pick-pocketing.

Unnecessary information, such as cardholder name, card verification value (CVV) or card verification code (CVC), should not be accessible / readable via the contactless interface between the NFC mobile credit card and the contactless reader.

6.4.3 Transactions through contactless interface

Payment transactions should only be allowed through contactless interface (also known as external mode communication) unless there are effective security controls to guard against potential attacks, e.g. relay attack, through the contact interface (also known as internal mode communication).

6.4.4 Transaction limit

NFC mobile credit card payment should follow the current transaction limit implemented on contactless credit card payment. Transactions exceeding the limit should require a cardholder verification method (CVM) to authenticate the cardholder. The CVM should be chosen from the four options set out in the section Payment Operation or other alternatives developed by card schemes.

6.5 Cardholder authentication

6.5.1 Know your customer

Know your customer (KYC) is a mandatory due diligence process that financial institutions should perform to identify their customers. KYC policies are increasingly important around the world in order to prevent identity fraud, money laundering and terrorist financing. The requirements depend directly on type of product issued and indirectly on local regulation.

The existing KYC processes for traditional payment card products should be followed by payment service providers when launching NFC mobile payment services.

6.5.2 At service activation

After the installation of a wallet application in the handset, an NFC mobile payment service needs to be activated. The activation process includes the installation of an NFC mobile payment application in the SE and the insertion of the end-user's payment credentials into the SE application. To prevent an unauthorized third party from activating an NFC mobile payment service, cardholder authentication is required during the activation process.

If activation code approach is applied where an activation code is given to an end-user at subscription, it should be given to the end-user via the channel pre-registered or agreed by the customer. For example, where the service is going to be pulled by the end-user using OTA, the activation code should be sent through the authorized number the customer registered with the AI.

Cardholder authentication is mandatory in NFC mobile payment service activation.

6.5.3 Mobile PIN management

The value of the mobile PIN has to be injected into the NFC mobile payment service. There are two possible options:

- The issuing PSP manages the mobile PIN like a regular chip card PIN. The mobile PIN is thus part of the payment credentials, its initial value is defined by the issuing PSP and its value is injected during the activation of the NFC mobile payment service.
- The issuing PSP delegates the management of the mobile PIN to the cardholder. Indeed, it is possible to configure the payment application in such a way that the end-user is invited to change the mobile PIN just after the activation of the NFC mobile payment service. If the mobile PIN is lost by the cardholder, the issuing PSP needs to be able to reset it and allow the cardholder to redefine it.

Here is the list of functions involved in managing the mobile PIN:

- Unblock mobile PIN
    - It may be possible to unblock the mobile PIN through the wallet application, providing the PIN unblock key has been defined and is supported by the NFC mobile payment service.
    - The issuing PSP can also unblock the mobile PIN from the server side via a script command. At the same time, the issuing PSP has the option to provide a new mobile PIN to the user.

- Change mobile PIN
    - It may be possible to change the mobile PIN through the wallet application, providing that the end-user knows the current mobile PIN value.
    - The issuing PSP can also change the mobile PIN on the server side via a script command.

- Reset mobile PIN
    - The current PIN value is replaced by a default code ‘XXXX’ via a script command. In this case, the end-user is invited to choose a new mobile PIN.

If mobile PIN is chosen by the cardholder on first launch of the NFC mobile payment service, cardholder authentication has to be implemented at the beginning of the process.

7 Payment operation

This section focuses on the end-user payment experience. Such end-user payment experience includes the interaction between users and NFC-enabled handset as well as the payment experience at point of sales. Banks are suggested to draw reference from the recommended practices set out in this section when implementing the user procedures even though such practices are not mandatory requirements.

7.1 NFC mobile payment services selection and prioritization

If a user explicitly selects a specific payment credential for a transaction, the credential should have the highest priority over the other credentials in the SE and any payment credential with “always on” state should be automatically turned off by the handset in this scenario.

If a mechanism is deployed for setting up the preference on payment credentials, a user should have an interface to manage his preferred payment credentials. If a payment credential can operate on “always on” state, the payment credential issuer or the SE issuer should provide an interface allowing users to turn on and off the “always on” state of the credential.

Management of several wallets, each containing several payment credentials, involves complex procedures and is difficult to handle by most users. The introduction of a default NFC mobile payment credential across all wallets is normally adopted and recommended as it can enhance the user experience.

7.2 Cardholder verification methods (CVM)

High-value ticket transactions refer to payment transactions with the amount exceeding the current limit applied to contactless credit cards. When NFC mobile payment becomes popular, the market may demand for the support of high-value ticket transactions using handsets. These transactions should be authenticated by a cardholder verification method. Several cardholder verification methods are available below for consideration.

- User signature
- Over-The-Air PIN
- Online PIN
- Mobile PIN (Mobile passcode)

Among the four options set out above, it is recommended that mobile PIN be adopted as a CVM for high-value transactions based on NFC enabled handsets. It can also be used to secure the administration and management of NFC mobile payment credentials.

7.3 Considerations on different NFC mobile payment implementations

High-value transaction payment capability offers additional benefits compared to traditional low-value transaction payment capability using a contactless card and should be considered when further development is made to ensure a wide-scale adoption.

A common CVM to authenticate high-value payments and a common transaction limit to trigger the CVM are recommended.

Payment service providers, card scheme operators and merchant acquirers intending to launch NFC mobile payment services in Hong Kong should consider utilizing existing payment infrastructure to reduce cost and promote mass acceptance as the first priority.

7.4 Card Maintenance

PSP wallet application download

As users become increasingly accustomed to downloading mobile applications onto their handsets through online application stores, the preferred option is for users to install the wallet application from an online application store before the subscription.

Subscription channel

To facilitate adoption of the NFC mobile payment service, multiple subscription channels should be offered to a user. Among the channels, there should be one channel where the user is not obliged to go to the branch.

Eligibility of handset and SE

To ensure a smooth uptake of the NFC payment service, eligibility checks on the NFC capability of mobile handset and SE at the subscription stage are recommended.

Service activation by push/pull

To ensure efficiency and an enhanced user experience, user initiated NFC mobile payment service activation is recommended.

Service activation process

Given that most NFC infrastructures support the instant issuance of payment credentials, such arrangement is preferred as it enhances the user experience.

To facilitate the activation of the NFC mobile payment service, a solution using a pre-activation phase may be considered to simplify the activation flow.

Appendix A - Glossary

Term	Definition
Contactless payment	Contactless payment refers to payment made using a physical contactless payment card such as Visa's payWave card, a MasterCard PayPass card, UnionPay Quickpass or Octopus card.
NFC	Near field communication (NFC) is a short-range (over a few centimeters) wireless connection standard used by electronic devices for communication. Applications include contactless transactions, data exchange, tag reading and simplified setup of more complex connections such as Bluetooth or Wi-Fi.
NFC handset	An NFC-enabled handset or NFC device is a device that supports the NFC standard and is embedded with a minimum of an NFC chipset and antenna to communicate with the NFC external target. An NFC handset used for NFC mobile payment must be certified by the payment scheme.
NFC mobile payment applications	NFC mobile payment applications reside in the secure element. They interact with the point-of-sale (POS) terminal through the NFC chipset and antenna in a similar manner to a contactless card. The main payment networks have issued dedicated specifications for NFC mobile payment applications, with extended features to interact with wallets and with the issuer's back-office or payment networks using over-the-air (OTA) communication.
NFC mobile payment credentials	NFC mobile payment credentials reside in the secure element in an issuer-owned security domain. They consist of a set of personalized data that is unique to a given payment product. NFC mobile payment credentials are often referred as "mobile cards".
NFC services	NFC services are the term to describe those services that use NFC technology, including NFC handsets and secure elements.
Over the air	Over-the-air (OTA) is the general term used for wireless communication through the cellular network of mobile operators. OTA refers to wide range (over few kilometers) communication, while NFC refers to proximity (over a few centimeters) communication.

Term	Definition
Secure element	A secure element (SE) is a tamperproof smart card chip that can hold smart card-grade applications (for payment, transport, etc.) with the required level of security and features, which is connected to the handset NFC chipset. The SE can be integrated into various form factors such as a SIM card, MicroSD card, smart sleeve or it can be embedded in the handset. SEs used for NFC mobile payment must be certified by the payment scheme.
Trusted services manager	The TSM acts as a neutral broker who sets up business agreements and technical connections between service providers and mobile network operators, phone manufacturers or other entities controlling the secure element. The functionalities of the TSM are split: one set of functionality is designed for service providers to remotely provision and manage NFC services over the air. Another set of functionality is designed for secure element issuers to remotely manage secure element content.
Wallet applications	Wallet applications reside in the handset memory and make the mobile card visible to the end-user. Wallet applications can be issued by banks, mobile network operators or over-the-top (OTT) content players. Several wallets can coexist on a single NFC device, with segregated access to existing NFC mobile payment credentials.

Acronym	Description
Activation Code	A password used to authenticate the cardholder as part of over-the-air activation process
AFSCM	Association Française du Sans Contact Mobile, the French association for contactless mobile
AFI	Application family identifier
APDU	Application protocol data unit
API	Application programming interface
CAT	Card application Toolkit
CLF	Contactless front-end
CUP	China UnionPay
CVM	Cardholder verification method
ECMA	European association for standardizing information and communication systems
EMEI	Unique handset identifier – including brand, model and serial number
ETSI	European Telecommunications Standards Institute

Acronym	Description
eSE	Embedded secure element, a secure element embedded into mobile
FWI	Frame waiting time integer
GP	GlobalPlatform
GSM	Global system for mobile communications
GSMA	Global system for mobile communications
HCI	Host controller interface
HSM	Hardware security module
ICC	International Color Consortium
ISO	International Standardization Organization
KYC	Know your customer
MIDlet	A java handset application communicating with payment cardlet and acting as GUI or proxy or both
MNO	Mobile network operator
MSISDN	Mobile subscriber integrated services digital network number or end-user mobile phone number
µSD or MicroSD	Shortcut for µSD secure element, i.e. micro SD containing both flash memory and global platform secure element
NFC	Near field communication
OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
Online PIN	A CVM whereby the end-user enters his or her PIN on the point-of-sale. The online PIN is verified by the bank's authorization server during the online authorization
OS	Operating system
OTA	Over the air
Passcode	A new CVM in form of mobile PIN. The PIN is keyed from the handset keyboard and verified locally against the mobile payment application stored in the secure element – sometimes called mPIN or mobile PIN
PCD	Proximity coupling device
PED	PIN entry device
PICC	Proximity integrated circuit card
PPSE	Proximity payment system environment
POS	Point of sale (terminal)
PSP	Payment service provider

Acronym	Description
RF	Radio frequency
RFM	Remote file management
SIM	Subscriber identification module - a smart card for GSM systems holding the subscriber's ID number, security information and memory for a personal directory of numbers, thus allows them to call from any GSM device. It can also store and run applications and enable end-user services.
SE	Secure element – can be a UICC SIM, eSE or a µSD
SP	Service provider
STK	SIM toolkit
SWP	Single wire protocol
TEE	Trusted execution environment
TSM	Trusted services manager
UICC SIM	Also known as the SIM or USIM
UML	Universal markup language
USIM	Universal subscriber identification module
W3C	World Wide Web Consortium

END