Canadian NFC Mobile Payments

Reference Model

Version: 1.03

Date: 14-MAY-2012

Remarks: Initial Public Version

1 INTRODUCTION

The August 2011 Interim Report of the Canadian Federal Government's Task Force for the Payments System Review ("Payment Task Force") outlines the necessity of the Financial Services industry to work together to develop a framework for mobile payments. In this context, a Canadian Financial Institution ("FI") Industry Initiative was formed.

Canada's banks and credit unions have worked together to develop the standards in this document for the accelerated adoption of mobile payments in Canada that will benefit all Canadians. The development of mobile standards is a continuation of the work of the federally-appointed Payments Systems Task Force. The Task Force asked the Financial Institutions to develop mobile standards and the FIs involved in this work have worked hard from October of 2011 through January of 2012 to deliver on this request.

The Canadian Financial Institutions involved in this initiative ("Industry Initiative Participants") recognize that end users trust Canadian Financial Institutions to provide safe and secure services. Further, end users require and expect to be able to maintain control over which type of payment they use and how they access it. To that end, this mobile reference model ensures that the consumer has the ultimate say over whether their payments have pass code protection and which payment types are enabled on their mobile device. Merchants and consumer also expect transparency at point of sale. This document was prepared in furtherance of this expectation and to accelerate adoption of mobile payments.

The payment ecosystem takes the coordination of many parties to function effectively. It is hoped that providing early clarity on industry participation in the ecosystem will help stabilize and build efficiencies into the future deployment of mobile payments in Canada. Once functional, the mobile payments ecosystem will enable an end user to put a payment credential (i.e. card) on a mobile device and simply tap that mobile device to make a payment; a seamless user experience increasing convenience and security for the end user.

In this document, the Industry Initiative Participants establish a common reference model for NFC based mobile payments and offer a set of expectations for ecosystem participants. These expectations and the associated interactions create a common foundation, based on voluntary adherence, on which NFC mobile payment services in Canada may be built.

Although others have been consulted in the creation of this document, the final draft is at the discretion of the Industry Initiative Participants.

2 CHANGE LOG

This document may be periodically reviewed and updated as the ecosystem evolves. The purpose of this section is to list these changes for the benefit of the reader.

Date (D/M/Y)	Section(s)	Description of Change (s)	Version
14/05/2012		Initial Public Version	1.03

3 VISION AND GUIDING PRINCIPLES

The Canadian Mobile Payments Vision and Guiding Principles served as the foundation for this document and for the Industry Initiative Participants' outlook for NFC Mobile Payments in Canada.

At the core of the Vision Statement and Guiding Principles is a belief that consumers trust Canadian Financial Institutions to provide safe and secure services. In furtherance of this expectation, with the utmost focus on upholding this commitment between Financial Institutions and customers and to accelerate adoption of mobile payments, the Industry Initiative Participants developed the following Vision Statement and Guiding Principles for Mobile Payments in Canada.

3.1 VISION STATEMENT

The vision for mobile payments in Canada is a convenient, open, safe and secure ecosystem supported by standards based operating framework. This framework will increase user choice and accelerate the adoption of mobile payments.

3.2 GUIDING PRINCIPLES

The operating framework for mobile payments in Canada will be:

Open:

- Allows for different business models
- Fosters innovation
- Ensures competition among market participants

Safe & Secure:

- Protects confidential personal, financial, and transactional information within the mobile payments ecosystem
- Facilitates secure interactions between Financial Institutions and the mobile payments ecosystem

Responsive to End User & Merchant Needs:

- Provides for ease of use, speed, availability, security, transparency, choice and consistency for users

Standards Based:

- Establishes clearly defined standards essential for interactions between financial institutions and the mobile payments ecosystem
- Aligns with the Canadian regulatory environment and avoids overlap with existing standards
- Considers and respects international standards as a means of facilitating interoperability

Sustainable:

- Creates a path forward for standards to support the long term viability of mobile payments in Canada
- Encompasses activities between Financial Institutions and the mobile payments ecosystem
- Adapts over time as technology and the ecosystem evolve
- Allows for economically viable business models that accelerate mobile payments adoption for the mobile payments ecosystem

Focused on Mobile Technology Initiated Transactions:

- Focuses on payment transactions and enabling capabilities
- Considers pre-payment and post-payment services that enable transactions
- Considers multiple currencies and payment types
- Focuses on mobile NFC enabled devices and NFC enabling technologies

4 TABLE OF CONTENTS

5 GENERAL INFORMATION

5.1 PURPOSE

The purpose of the Canadian NFC Mobile Payments Reference Model (or "this document") is to establish guidelines for ecosystem participants. In so doing, the Industry Initiative Participants that came together to author this document sought to promote a vision for mobile payments in Canada. This vision is that of a convenient, open, safe and secure ecosystem supported by a standards-based operating framework.

The Industry Initiative Participants firmly believe that by defining and communicating processes, roles, responsibilities and expectations in the form of standards statements, the resulting ecosystem will be more effective at increasing user choice and accelerating the adoption of mobile payments.

5.2 COMPARISON BETWEEN CARD PAYMENTS AND MOBILE PAYMENTS

Traditionally, a customer wanting a credit card would apply to a Financial Institution which, upon acceptance of the application, would instruct its card fulfillment company to issue a plastic card to the customer. The customer would receive the card, activate the card and use the card at a merchant by swiping or inserting it into the reader.

In the mobile payments world, a customer (now called the end user) applies for the mobile payment service and requests a Financial Institution (now called the credential issuer) to enable the mobile payments service on a mobile device. The credential issuer instructs its Trusted Service Manager (TSM) (which has replaced the card fulfillment specialist) to transmit payment credentials to the end user's mobile. To do this, the credential issuer's TSM liaises with the mobile network operator. Once credentials are on the mobile device, the end user is validated in a process very similar to the card activation steps. Following verification, the end user may use the phone or other mobile device just as they would a contactless payment card.

Conceptually, the steps to setup and use a mobile payment service are similar to that of a traditional card transaction.

5.3 SCOPE

This document focuses on NFC based mobile payments including functional elements, roles, responsibilities and interaction models needed for the development of a NFC based mobile payments ecosystem.

NFC based mobile payments or contactless payments are transactions that require the mobile device to be in close proximity to the reader. Unlike other types of mobile payments such as barcodes or peer-to-peer payments, NFC mobile payments require integration of hardware and software on the mobile device.

This document discusses the elements needed to enable NFC mobile payments and process NFC mobile payment transactions. Installation or provisioning of payment credentials onto a mobile device is undoubtedly more complex but not entirely unlike provision payment credentials to a plastic card. Card provisioning served as one of many guides in the creation of this document. However, in this document, a significant amount of attention was given to SIM (i.e. UICC) and embedded NFC chips in the mobile device that enable contactless mobile payments.

Another area of similarity between NFC mobile payments and conventional card payments is at the Point of Sale (POS). This document assumes that once the contactless connection is made at the POS, all other transaction processing steps will use existing payment networks to process transactions. As such, this document does not redefine the role of payment networks.

5.3.1 DETERMINATION OF INSCOPE ITEMS

To determine the focus areas for this document, the Industry Initiative Participants considered the Vision & Guiding Principles (see the Vision & Guiding Principles section), interaction between ecosystem participants and areas that differ from existing payment offerings. From this, the following areas were identified for inclusion in this document: wallet and payment application Features & Functionality, provisioning, transaction processing, lifecycle management, loyalty and rewards and data & security.

5.3.2 DETERMINATION OF OUT OF SCOPE ITEMS

This document does not discuss mobile remote payments (i.e. those transactions that are initiated using a mobile device regardless of the location of the payee and the payer). This document also does not focus on other NFC technologies such as micro SD cards and contactless stickers.

Further, several items were intentionally excluded from the scope of this document. The following areas are not addressed in this document:

- **Non-Mobile NFC Payments:** Mobile payments types that have been excluded from this document are: barcode payments, Bluetooth payments, passive NFC and RFID payments (e.g. stickers and fobs), active NFC enablers (including Micro SD and NFC Cases), peer-to-peer payments and cloud based payments.
- **Non-Impacted Payment Processes:** This document assumes that NFC based mobile payments will leverage the existing payments infrastructure. As such, many areas of payment processing that are unaffected by mobile payments or those that are proprietary to individual institutions were not defined. These areas include end user acquisition, merchant acquisition, billing and settlement, collections and recoveries, POS deployment and certification, account management, reconciliation, and core payment processing.
- **Non-Traditional Currencies:** Emerging and virtual currencies such as those offered by social networks and loyalty programs have not yet gained common acceptance. Evaluation of these non-traditional currencies has not been included in this document.

5.4 IDENTIFICATION OF STANDARDS STATEMENTS

This document contains various types of information, including guidelines and standards. Standard statements are numbered, indicated in brackets "**[S1]**" and appear at the end of each section. Areas not labeled as standards in this document are intended to be informational.

5.5 STANDARD ADHERANCE

All standards statements will be followed by the Industry Initiative Participants and ecosystem participants with whom they partner. For this group, a claim of adherence to standards means that all standard statements in this document will be followed.

For other ecosystem participants, adherence to this document is optional. Once standards are publically released, other ecosystem participants may or may not choose to follow these standards. A formal review and certification process is not planned to evaluate claims of standards adherence.

5.6 GOVERNANCE AND DOCUMENT UPKEEP

This document was prepared by the Industry Initiative Participants. Publication and ownership of this document will be temporarily managed by the Canadian Bankers Association (CBA).

The owner of this document is responsible for hosting the document on a public website, conducting periodic reviews of the document to ensure its relevance and serving as the primary point of contact or inquiries related to this document and to the standards.

5.7 AUDIENCE

Finally, this document, the Canadian NFC Mobile Payments Reference Model, is intended for Canadian Mobile Payments service providers including but not limited to payment credential issuers, Trusted Service Managers (TSMs), Mobile Network Operators (MNOs), Original Equipment Manufacturers (OEMs), payment network operators (e.g. Interac, Visa, MasterCard), merchants, acquirers, loyalty service providers, wallet providers, regulators and all others interested in NFC base mobile payments. All readers however, will gain an early awareness of how the Industry Initiative Participants are approaching mobile payments and therefore benefit from increased certainty in determining their own approach to this new ecosystem.

This document provides broad, overall context for NFC based mobile payments. Consequently, readers of this document will find some sections more interesting than others depending on the role that they play. The following table provides role based recommendations for interpreting this document.

For role definitions, please see the Canadian Mobile Payments Solution Framework section or the glossary. All ecosystem participants in the following table appear in alphabetical order.

Ecosystem Participants	Suggested Sections
Acquirer	The Transaction Process and Data & Security sections review the steps of processing a mobile NFC payment including POS interaction with the handheld device. Data & Security provides an overview of data types available to each ecosystem participant.
Payment Credential Issuer	This document, in its entirety, will be of interested to organizations playing the role of the payment credential issuer.
End User (Also Consumer or Customer)	This document is not directly intended for the end user of NFC mobile payments services. Much of the lexicon, phraseology and concepts in this document may be foreign to the average payment card user or mobile payments user. However, if an end user does choose to review this document, they may find the Wallet and Payment Application Features & Functionality section of interest to understand what a wallet is and how it functions. The Transaction Processing section will inform the end user how NFC mobile payments will work at the Point of Sale (POS). Finally, the Data & Security sections will inform the end user as to the type of data involved in NFC mobile payments and which ecosystem participants will access each.
Loyalty Service	The Loyalty & Reward and the Data & Security sections will be of interest to loyalty service providers. The Loyalty & Rewards section provides an

Ecosystem Participants	Suggested Sections
Providers	overview of the type of Loyalty Programs expected to be offered on NFC mobile payments devices. This section does recognize that this is a rapidly evolving space and that there is great uncertainty about how the space will evolve. The Data & Security section will inform loyalty service providers of the type of information that will be available to them.
Merchant	The Transaction Processing and Data & Security sections will be of interest to merchants. In the Transaction Processing section, a merchant can find information on POS requirements and anticipated benefits to queue times. In the Data & Security section merchants can find information on data access and security.
Mobile Network Operator (MNO)	Much of this document will be of interest to a MNO. The Wallet & Payment Applications Features & Functionality section describes the storage and binding of payment credentials. The Enablement & Lifecycle Management section describes the MNOs involvement in the provisioning process and expectations around end user servicing. The Data & Security section describes the data elements that each ecosystem participant may access. The Transaction Processing section involves mostly the merchant, the end user and the payment networks; this section may not be of interest to a MNO.
Original Equipment Manufacturer (OEM)	Depending on the role they play, an OEM may or may not find this document of interest. If an OEM is directly involved in managing the secure element or UICC (see glossary or Solution Framework section for definitions), then they are likely to be interest in the same sections as a MNO. However, if the role of the OEM is limited to equipment manufacturing and if secure element or UICC administration activities are delegated to a MNO, then the OEM may only be interested in reviewing the highlighted GlobalPlatform specifications in this document.
Payment Network Operator	This document is designed to work in connection with and not separate from the services provided by payment networks such as Interac, Visa and MasterCard. While this document as a whole may be of interest to payment networks, they are likely to find the Enablement & Lifecycle Management section for provisioning, the Transaction Processing section for POS processes and the Data & Security sections to be the most relevant.
Regulators	Regulators will want to review this document in its entirety. While NFC mobile payments draw from many existing payment, banking and telecommunications capabilities, the future of mobile payments will call for these services to be combined in new ways. Regulators may want to keep a line of site into how the ecosystem is developing to ensure the overall safety and security of the Canadian Financial Services marketplace and the role of mobile payments.
Trusted Service	The Wallet & Payment Applications Features & Functionality, the Enablement & Lifecycle Management and the Data & Security sections will be of interest

Ecosystem Participants	Suggested Sections
Manager	to a TSM. The Wallet & Payment Applications Feature and Functionality describes the storage of payment credentials and the binding process between the wallet and the payment credentials. The Enablement & Lifecycle Management section describes the provisioning process to which a TSM is central. The Data & Security section describes the data elements to which each ecosystem participant will have access.
Wallet Providers	The Wallet & Payment Applications Features & Functionality and the Data & Security sections will be of interest to wallet providers. The first of these sections outlines general functions of and expectations for a wallet including security, features and interfaces. The Data & Security section describes the Data elements to which each ecosystem participant will have access.

5.8 REGULATIONS AND CONTRACTS

It is the responsibility of all ecosystem participants that adopt these standards to ensure that adherence to the standards in this document will not interfere with any legal, regulatory or contractual requirements.

5.9 TESTING AND APPROVAL REQUITEMENTS

Further, it is the responsibility of device manufacturers, software developers, integrators, banks, vendors, mobile network operators, third party processors and other ecosystem participants to perform full quality assurance testing on mobile payments products and services.

6 CANADIAN MOBILE PAYMENTS SOLUTION FRAMEWORK[1]

This section provides a general description of the framework on which the Canadian NFC Mobile Payments Reference Model is designed.

At the time this document was written, a global standard for mobile payments did not exist. There were, however, a series of regional standards and functional standards that focus on specific lifecycle events. Working from other standards as a base, this document was created with a mobile payments lifecycle view and the unique interest of Canadians in mind. Although this document is unique, it does borrow heavily from the work of other standards bodies including PayEz, AFSCM, GlobalPlatfom and EMVCo. References have been included in this document to give credit where appropriate.

6.1 BRAND ACCEPTANCE RULE

This document does not introduce any changes to brand acceptance rules. All branding rules must be followed according to branding guidelines **[S1]**.

- **MasterCard:** A mobile device's MasterCard application and payment credentials may only be accepted at a merchant's POS system that carries a MasterCard acceptance logo.
- **Visa:** A mobile device's Visa application and payment credentials may only be accepted at a merchant's POS system that carries a Visa acceptance logo.
- **Interac:** A mobile device's Interac application and payment credentials may only be accepted at a merchant's POS system that carries an Interac acceptance logo.

6.2 CONTACTLESS AND MOBILE PAYMENT SCHEME REQUIREMENTS

International and domestic card schemes such as MasterCard, Visa and Interac have developed a set of specifications for contactless mobile payment transactions. These specifications are primarily aimed at defining rules and requirements for the mobile form factor and at executing a purchase transaction with a contactless reader using ISO 14443 type A or B protocols [ISO-8][ISO-9] .

Compliance with MasterCard PayPass, Visa PayWave and Interac Flash contactless mobile specifications require mobile devices to support the "EMV mode" and the "MSD mode" (for Visa and MasterCard) to execute a contactless mobile payment transaction.

The Canadian Mobile Payments Reference Model support both MSD and EMV based technologies:

- For MasterCard PayPass transactions, mobile device and contactless reader specifications must support PayPass Mag Stripe profile as defined in PayPass Mag Stripe specifications and Pass M/Chip or Mobile M/chip profile as defined in PayPass M/Chip specifications **[S2]**.
- For Visa PayWave contactless transactions, mobile device and contactless reader specifications must support MSD and VMPA implementation as defined in Visa Mobile Specifications **[S3]**.
- For Interac Flash contactless transactions, mobile device and contactless reader specifications must support Interac Flash Mobile contactless specifications **[S4]**.

---

[1] This section was sourced from PayEz Mobile; Mobile Contactless Proximity Payment; Part 1: Product Definition; Release 3, April 2011; Page19

6.3 TRANSACTION PROCESSING REQUIREMENTS

Contactless mobile payment transactions, initiated with a mobile device, have been designed by MasterCard, Visa and Interac to introduce minimum impacts on the existing card payment infrastructure.

Processing of mobile proximity payments under a payment network brand must comply with brand requirements. Other applicable operating rules should use the same authorization network and clearing systems as for standard debit and credit card transactions **[S5]**. Examples of applicable operating rule include MasterCard, Visa and Interac guidelines as well as related Canadian Payments Association defined rules.

6.4 SEPA

SEPA working groups have published various documents that provide requirements and guidelines for payment transactions. The Canadian NFC Mobile Payments Reference Model complies with the following SEPA requirement documents:

- SEPA Card Framework [EPC-1]
- SEPA Cards Standardization "Volume" Book of Requirements [EPC-2]

6.5 GSMA/EPC

The Canadian NFC Mobile Payments Reference Model complies with guidelines and documents provided by GSMA and EPC.

- GSMA – EPX TSM Requirements [SPC-3]

6.6 EMVCO

The Canadian NFC Mobile Payments Reference Model complies with documents issued by EMVCo including:

- EMVCo Contactless Mobile Payment Architecture Overview [EMV-11]
- EMVCo Handset Requirements for Contactless Mobile Payments [EMV-12]
- EMVCo Application Activation User Interface Contactless Activation/Deactivation Scenarios, Overview, Usage Guidelines and PPSE Requirements [EMV-13]
- EMVCo EMV Profiles of GlobalPlatform UICC Configuration [EMV-14]

6.7 NFC

Near Field Communication (or "NFC") is a short-range wireless connectivity technology that enables safe communication between electronic devices that are within a short read range distance.

Three modes to exchange data between electronic devices are currently supported:

- NFC card emulation mode
- Peer to Peer Mode (out of scope)
- Read/Write mode (out of scope)

NFC card emulation mode must be used to execute a contactless mobile payment transaction between an end user's mobile device and a merchant's contactless reader using ISO 14443 Type A or ISO 14443 Type B radio frequency communication layer **[S6]**.

6.8 GLOBALPLATFORM MESSAGING[2]

For consistency and interoperability, the GlobalPlatform messaging standards have been adopted. GlobalPlatform defines three messaging constructs:

Mode	Description
Simple Mode	In a simple mode, the MNO or the SDM allows the credential issuer to use its secure domain for the payment application. The right to the secure domain remains with the MNO or SDM. Any updates or changes to the payment application must be managed through the Secure Domain Manager or MNO.
Delegated Mode	In a delegated mode, the MNO or SDM rents (or gives access) to a portion of the secure element to the credential issuer. The MNO or SDM still has ownership on the secure element and can control what applications are loaded in the secure element. Keys are exchanged between the MNO or SDM and the credential issuer (or the credential loader) to provide that access to the secure element.
Dual Mode	In a dual mode, the MNO or SDM has sold a portion of the secure element to the credential issuer. The credential issuer has full ownership and rights to that portion of the secure element. Keys are exchanged between the MNO or SDM and the credential issuer (or credential loader) as a part of the sale. The credential issuer can put any application on the secure element and does not need any permission from the MNO or SDM.

All messaging will be performed under the relevant guidelines. Refer to GPS_Messaging_ Specification_ for_Mobile_NFC_Services-v1.0.

While this document and GlobalPlatform recognize three constructs (Simple Mode, Delegated Mode and Dual Mode), those that adopt these standards must use only the Delegated Mode or the Dual Mode as defined by GlobalPlatform; TSMs must operate in Delegated or Dual Mode **[S7]**. The Delegated and Dual management modes will allow credential issuers to enforce the security of payment credentials and consequently support the safety and security of the ecosystem.

6.9 STANDARDS STATEMENTS

Number	Statement	Section

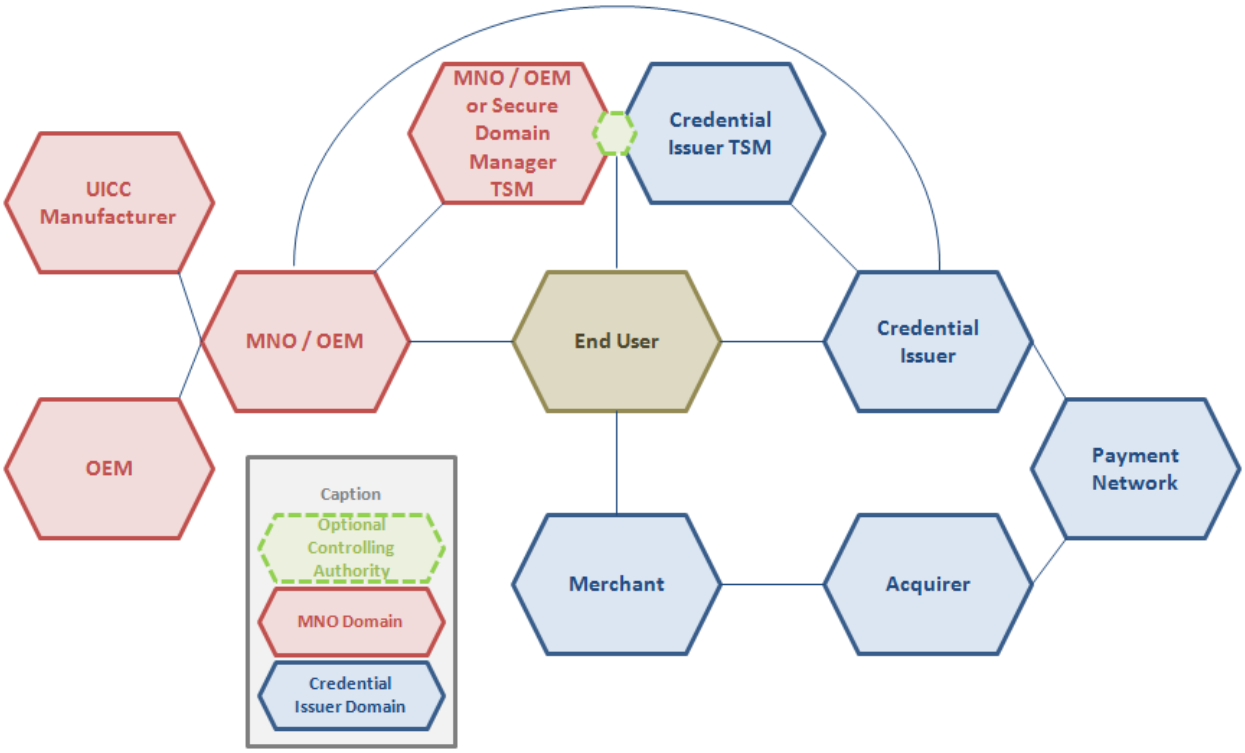
[2] GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0.

Number	Statement	Section
S1	All branding rules must be followed according to branding guidelines	6.1 Brand Acceptance Rule
S2	For MasterCard PayPass transactions, mobile device and contactless reader specifications must support PayPass Mag Stripe profile as defined in PayPass Mag Stripe specifications and Pass M/Chip or Mobile M/chip profile as defined in PayPass M/Chip specifications	6.2 Contactless And Mobile Payment Scheme Requirements
S3	For Visa PayWave contactless transactions, mobile device and contactless reader specifications must support MSD and VMPA implementation as defined in Visa Mobile Specifications	6.2 Contactless And Mobile Payment Scheme Requirements
S4	For Interac Flash contactless transactions, mobile device and contactless reader specifications must support Interac Flash Mobile contactless specifications	6.2 Contactless And Mobile Payment Scheme Requirements
S5	Other applicable operating rules should use the same authorization network and clearing systems as for standard debit and credit card transactions	6.3 Transaction Processing Requirements
S6	NFC card emulation mode must be used to execute a contactless mobile payment transaction between an end user's mobile device and a merchant's contactless reader using ISO 14443 Type A or ISO 14443 Type B radio frequency communication layer	6.7 NFC
S7	While this document and GlobalPlatform recognize three constructs (Simple Mode, Delegated Mode and Dual Mode), those that adopt these standards must use only the Delegated Mode or the Dual Mode as defined by GlobalPlatform; TSMs must operate in Delegated or Dual Mode	6.8 GlobalPlatform Messaging

7 NFC MOBILE PAYMENT ECOSYSTEM OVERVIEW[3]

This section provides an overview of the different components required by the Canadian NFC Mobile Payments Reference Model to enable a contactless mobile payment transaction.

7.1 ECOSYSTEM OVERVIEW



See the mobile payment roles and messaging section for additional details on ecosystem participants.

7.2 NFC MOBILE PAYMENTS REFERENCE MODEL – SOLUTION DESCRIPTION

The Canadian NFC Mobile Payments Reference Model enables NFC payment transactions via radio frequency. This document only considers NFC supported mobile payments.

To execute a NFC mobile payment, an end user must have the right hardware and software. Hardware in this context includes a NFC enabled mobile device. Software, in this context, includes a wallet application, payment application and payment credentials (see the Wallet & Payment Application Features & Functionality section for definitions). Hardware eligibility checks are not discussed at length in this document. This document assumes that the end user has the necessary hardware required for NFC mobile payments. For this reason, the Enablement & Lifecycle Management section of this document focuses primarily on software requirements.

[3] This section was sourced from PayEz Mobile; Mobile Contactless Proximity Payment; Part 1: Product Definition; Release 3, April 2011; Page19

Assuming the end user has the right hardware, an end user must first install the proper software on their device before they can engage in NFC mobile payments. This document examines wallet features and payment application installation and binding as the initial pre-payment setup steps in the Wallet & Payment Applications Features & Functionality section and the Enablement & Lifecycle Management section..

Once the initial setup is complete, a NFC based mobile payment transaction may be performed. The Transaction Processing section examines the steps required to perform a NFC mobile payment. The solution is designed to consider low value, high value and high risk transactions. The solution is characterized by a radio frequency short read range distance that requires the mobile device to be presented close to the contactless reader to enable a transaction.

In additional to core payment functionality, this document recognizes that loyalty and rewards services, including coupon and points redemption, will play a critical role in the adoption and utility of NFC mobile payment services. More than any other area, this space is still evolving. As a result, the Loyalty & Rewards section focuses mostly on rules and guidelines to influence the evolution of the ecosystem.

Data and security standards are critical for the development of a safe and secure mobile payments ecosystem and are themes throughout this document. The final section in this document is dedicated to these topics. The Data & Security section was designed around the general guideline that each ecosystem participant should only have access to the minimum information required to perform its primary role. That is to say, the default should be to protect end user and merchant data. Access to and usage of data beyond what is required for an ecosystem participant to perform its primary role must be disclosed to the end user and the end users' permission must be explicitly granted **[S8]**. For security and prevention of fraud, access to and usage of data beyond what is required for an ecosystem participant to perform its primary role must also be disclosed to the credential issuer and the credential issuer's permission must also be explicitly granted **[S9]**.

Drawing from the Vision & Guiding Principles, two themes had a significant impact on the definition of the NFC Mobile Payments Reference Model.

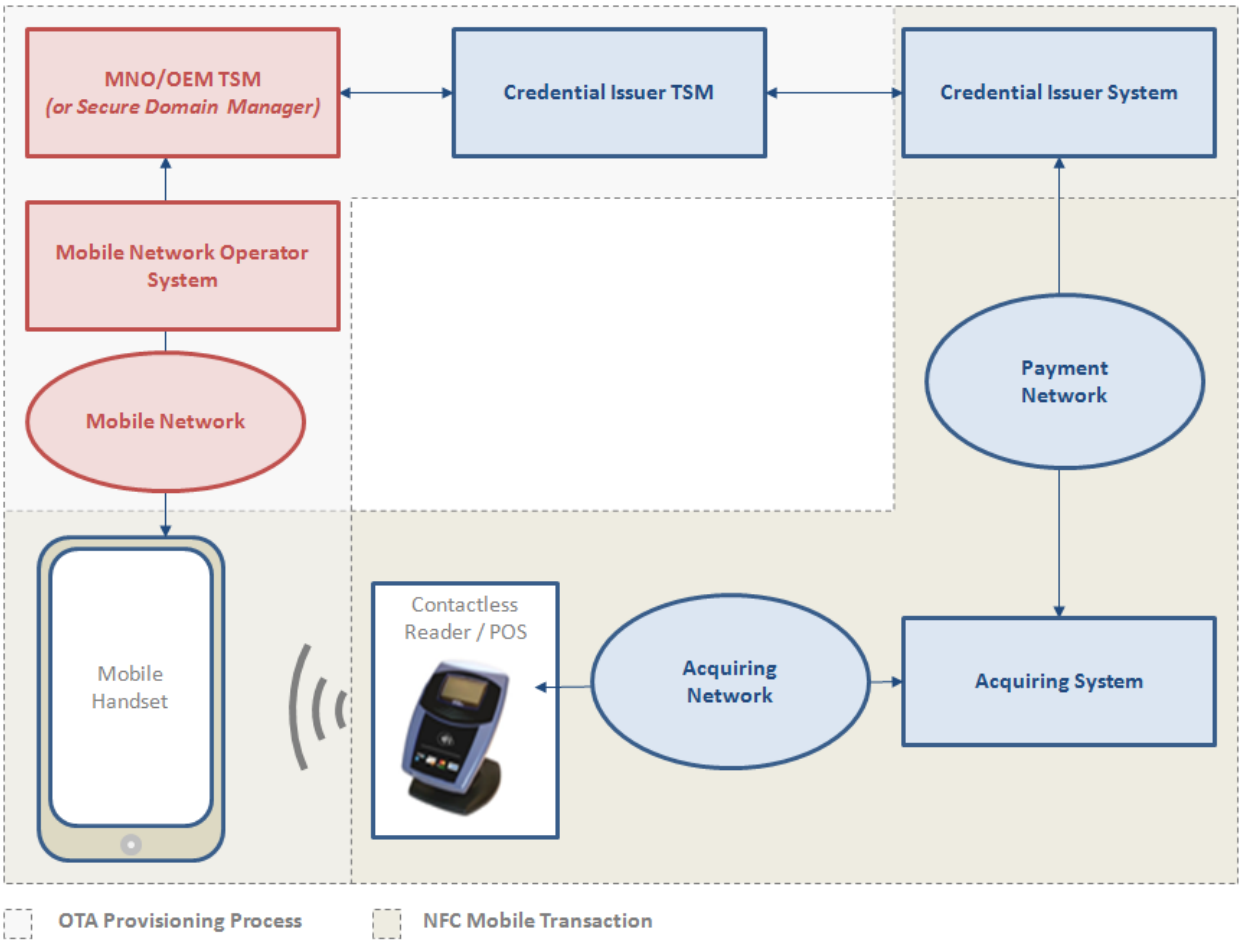
- First, both end user and merchant interests have been taken into consideration. Wherever possible, processes in this document start from the point of the end user.
- Second, interoperability with other emerging payment ecosystems is a goal for mobile payments in Canada. In support of this goal, this document makes reference to and draws from documents and decisions from other organizations interested in enabling mobile payments. Where appropriate, citations have been provided for existing standards used in this document.

A final note on the structure of this document, this document has been ordered based on anticipated end user familiarity to the content in each of the sections., For this reason, the main body of the document is order as follows: Wallet & Payment Applications Features & Functionality, Transaction Processing, Enablement & Lifecycle Management, Loyalty & Rewards and finally Data & Security.

7.3 ARCHITECTURE OVERVIEW

The figure below presents a high level overview of the main components required to:

- Configure a NFC mobile payments solution
- Execute and process a NFC mobile payments transaction



7.4 ROLES & ROLE DESCRIPTIONS

The table presents the roles in the Canadian mobile payments ecosystem. These roles are used throughout the document.

Role	Description
Acquirer	The acquirer is an institution that processes credit and/or debit card payments for a merchant.
Payment Credential Issuer or Credential Issuer (CI)	The CI is responsible for the encryption, safety and security of payment credentials. The relationship between the end user and the CI is based on financial services offerings and products. The CI may also play the role of the *Payment Application Owner*.
Controlling Authority (CA)	The CA may manage key exchanges in an 'Open Wallet.' This is a model that is recognized but not mandated in the NFC Mobile Payments Reference Model. This model is considered as an alternative to many-to-many relationships between a payment

Role	Description
	credential issuer's TSM and a Secure Domain Manager's TSMs.
End User	(*or the customer*) the end user is the consumer of mobile payment and mobile connectivity services.
Merchant	The merchant is the provider of goods or services for which the end user is providing payment.
Mobile Network Operator (MNO)	The MNO is the provider of mobile device connectivity services. For the purposes of this document, this role is sometimes used interchangeable with the OEM and Secure Domain Manager (SDM).
Original Equipment Manufacturer (OEM)	The OEM produces the mobile device hardware that is used by the end user. For the purposes of this document, this role is sometimes used interchangeable with the MNO and the Secure Domain Manager (SDM).
Payment Network	(*Or the Payment Application Creator*) creates the non user facing payment application software and manages the payment network *(e.g. Visa, MasterCard and Interac, etc.*
Secure Domain Manager (SDM)	The SDM manages access to the secure element; this role is often but not always combined with the role of the MNO. For the purposes of this document, this role is used interchangeably with the MNO and OEM.
Trusted Service Manager (TSM)	(*or Payment Application or Payment Credential Loader*) installs the payment credentials in the secure element. The TSM provides a secure link between multiple parties (e.g. Credential Issuer and MNO) to facilitate the installation of payment credentials.
Wallet Provider	The Wallet Provider provides the end user facing interface (e.g. Google Wallet, ISIS, Visa, MasterCard, Financial Institutions, or other 3rd Parties).

The role definitions were based on a combination of those provided by GlobalPlatform and those provided by PayEz.[4] Roles indicate actors that perform particular activities; the intent is not to specify which ecosystem participants will perform these roles.

[4] GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0 and PayEz Mobile; Mobile Contactless Proximity Payment; Part 1: Product Definition; Release 3, April 2011; Page22

7.5 SOFTWARE & DEVICES OVERVIEW[5]

The mobile device allows contactless communication by using NFC protocol (compliant with ISO 14443 Type A and ISO 14443 Type B) with the means of a dedicated NFC controller embedded in the mobile handset. The NFC controller is connected to the UICC or embedded secure element.

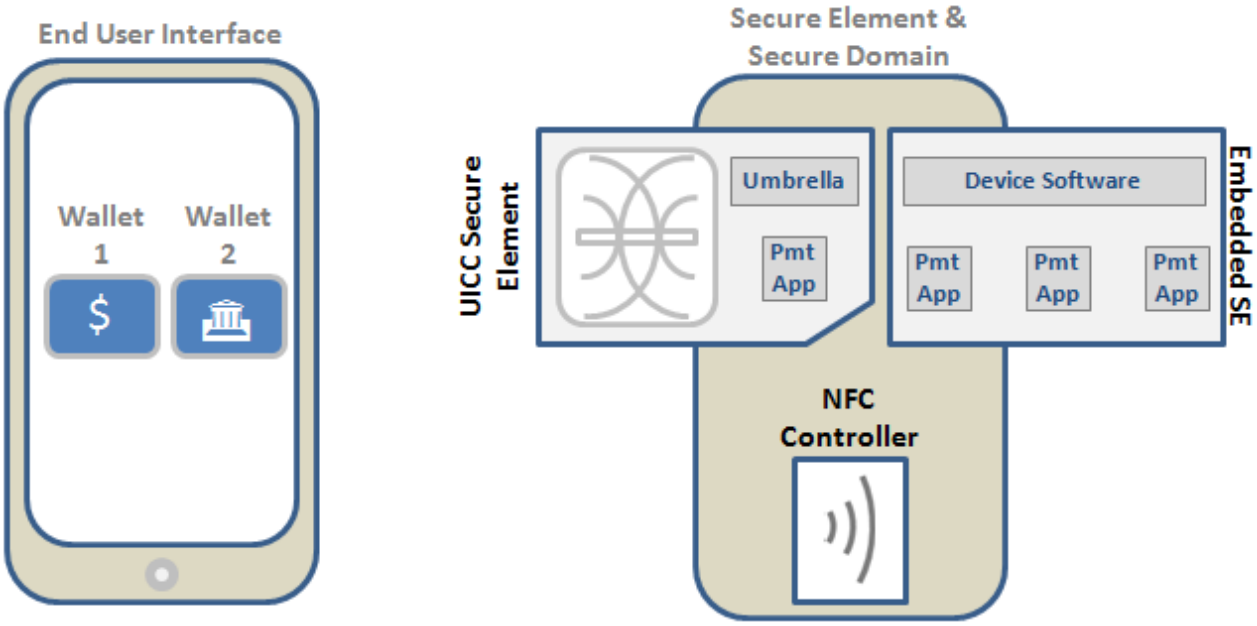
The NFC controller may be used in emulation mode to emulate a contactless card or, in reader mode, to read RFID tags.

The mobile device must be able to accept credential provisioning and maintenance activities via an OTA or "Over-the-air" process **[S10]**.

The UICC and the Embedded Secure Element are composed of separate Security Domains (SD) and Supplemental Security Domains (SSDs). SDs and SSDs may be dedicated to separate credential issuers.

Security domains hold cryptographic keys which are used to enable a secure channel between a credential issuer's TSM and its associated security domain.

This section explains elements of the mobile device related to NFC Mobile Payments.



Term	Definition
Companion Application	A companion application is associated with a payment

[5] PayEz Mobile Specifications; Page 5

Term	Definition
(not pictured)	application to increase functionality (by example: personal code management or transaction log). The companion application is provided at the discretion of the installer of the payment application.
Device Software	When a payment application and payment credentials are stored on the embedded secure element, device software plays the role of the umbrella application (see below) to locate payment credentials and connect these with the NFC controller.
NFC Controller	The hardware and software that, in combination, control the NFC radio signals transmitted to and from the mobile device.
Payment Application	A payment application provides the security requirements for making a payment and storing the payment credentials.
Secure Domain	A subdivision of the secure element.
Secure Element	Refers to the embedded secure area or secure area on the UICC where encrypted information is stored.
UICC	The UICC (Universal Integrated Circuit Card) is the smart card used in mobile terminals in GSM and UMTS networks as defined by ETSI Project Smart Card Platform (EP SCP).
Umbrella Application	The umbrella application is used only when a payment application is stored on the UICC. The umbrella enables the communication between a wallet and all payment applications related to this wallet. The relationship of the umbrella application to payment applications is a one-to-many relationship. For an embedded secure element, this role is played by the device software.
Wallet Application	The mobile wallet is the end user facing application which may be installed on the mobile device. The application allows users to enter and manage account specific information to be used in a NFC mobile transaction. It may be possible for one or more mobile wallets to reside on a mobile device at any given time.

7.6 CONTACTLESS READER/POS REQUIREMENTS[6]

POS contactless readers must comply with EMVCo contactless specifications [EMV-6] and MasterCard and/or Visa and/or Interac specifications **[S11]**.

A POS contactless reader has an antenna inducing an electromagnetic field enabling data exchange when an NFC enabled device is placed in proximity. The location of the electromagnetic field provided by the reader is known as the landing zone.

The landing zone is the area on the contactless reader where the radio frequency signal transmitted by the reader is the strongest. The strength of the radio frequency transmission is known as the operating volume. The landing zone is identified by the contactless symbol. The radio frequency reader automatically retrieves data from a NFC device which comes within a short read range.

A POS contactless reader can be fully integrated within a merchant acceptance terminal or can work as a standalone unit connected to a countertop merchant acceptance terminal or an electronic cash register.

A POS contactless reader may include 4 lights (e.g. LED type) to indicate that the reader is ready to exchange data with a mobile device and that the CMP transaction has been successfully completed. An audible beep will also confirm completion of a successful data exchange.

A distant beep (warning beep) may be used to notify the end user that the POS reader is standing-by for a mobile pass code. The mobile pass code is used for end user authorization of high value or high risk transactions.

7.7 INTEROPERABILITY[7]

Interoperability between the different components of a mobile payments ecosystem is a primary objective of the NFC mobile payments reference model. For the purposes of NFC based mobile payments, interoperability means that the multiple components of the ecosystem will evolve to be integrated with each other. In application, interoperability means that:

- The end user will have their choice of NFC mobile devices, credential issuers and MNOs
- Ecosystem participants and devices (e.g. POS terminal and devices) will work together
- Mobile devices will be able to communicate with any OTA platform
- An OTA platform will be able to communicate with any UICC or embedded SE
- A NFC mobile device will be able to communicate with any NFC contactless reader compliant to ISO 14443 Type A or ISO 1443 Type B
- A credential issuer will be able to connect to any OTA platform

[6] PayEz Mobile Specifications; Page 5
[7] PayEz Mobile Specifications; Page 5

7.8 STANDARDS STATEMENTS

Number	Statement	Section
S8	Access to and usage of data beyond what is required for an ecosystem participant to perform its primary role must be disclosed to the end user and the end users' permission must be explicitly granted	7.2 NFC Mobile Payments Reference Model – Solution Description
S9	For security and prevention of fraud, access to and usage of data beyond what is required for an ecosystem participant to perform its primary role must also be disclosed to the credential issuer and the credential issuer's permission must also be explicitly granted	7.2 NFC Mobile Payments Reference Model – Solution Description
S10	The mobile device must be able to accept credential provisioning and maintenance activities via an OTA or "Over-the-air" process	7.5 Software & Devices Overview

8 WALLET & PAYMENT APPLICATIONS FEATURES & FUNCTIONALITY

This section established the basic features and functionality for a wallet application and a payment application.

Some of the elements included in this section are standards and must be followed. Other statements are intended to be guidelines and to influence the evolution of NFC mobile payments in Canada.

This section builds on the basic definitions and architecture descriptions from the previous section.

8.1 TERMINOLOGY & SOLUTION CONSTRUCT

The mobile wallet is the application visible to the end user. This application may be used to:

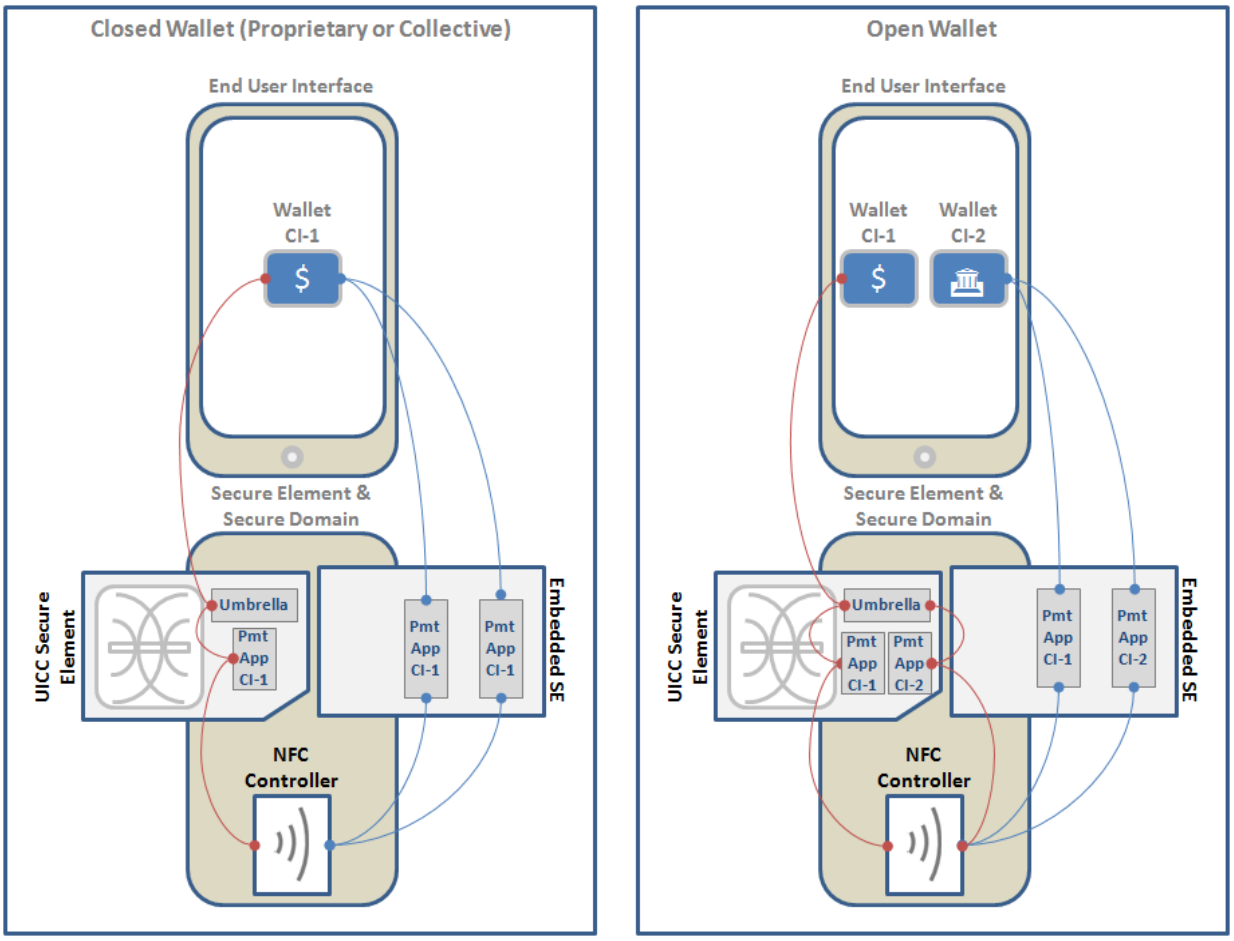
- Provision payment products / credentials
- Communicate with the end user
- Manage end user preferences
- Act as a mobile pass code entry device
- Manage payment products / credentials
- Manage loyalty and rewards information

Logic and business rules associated with the above functions may reside in the mobile wallet or in other, non user facing applications.

This document considers three types of wallet:

Wallet Type	Definition
Proprietary Wallet	A mobile wallet that is designed so that only the payment credentials from the wallet provider may be bound and used to make a NFC mobile payment.
Collective Wallet	A mobile wallet that is designed by a group of credential issuers so that payment credentials from only this group of credential issuers may be bound and used for payment.
Open Wallet	A mobile wallet that is designed so that payment credentials from multiple credential issuers can be bound and used for a payment. Although 'open,' this type of wallet still requires agreements and business relationships between credential issuers and wallet providers before a wallet may be bound to credentials.

On the left, a proprietary and collective wallet is issued by Credential Issuer 1 and connected to payment applications and credentials from Credential Issuer 1. On the right, one or more open wallets from Credential Issuers 1 and 2 are connected to payment applications and credentials from Credential Issuers 1 and 2.



This document acknowledges that, in the short term, proprietary and collective wallets will be the most likely go-to-market solution for ecosystem participants. Regardless of functionality in pilots or initial commercial launches, those that adopt these standards expect to implement an open wallet and migrate away from proprietary and collective wallets within 18 months of the first open wallet being launched in Canada **[S12]**.

8.2 OPENNESS AND INTEROPERABILITY

In furtherance of the goals of openness and interoperability, mobile wallets, mobile network operators, original equipment manufacturers, secure domain managers and credential issuers must not restrict access to payment applications from:

- Debit payment products from Interac and other networks
- Credit payment products from Visa, MasterCard and other networks
- Prepaid payment products
- Other payment products including transit and loyalty
- Payment products issued in a foreign currency (e.g. US Dollar denominated products)

This standards statement is subject to appropriate business relationships and technical capabilities being in place **[S13]**.

There are no restrictions as to the other payment application that a wallet may access. If the wallet owner, credentials issuer, and end user approve and have appropriate business relationship in place, the wallet may connect to any other credentials (payment or other). Payment applications or payment credentials must not be designed to prohibit a wallet from connecting with other payment applications or payment credentials, contingent on appropriate business relationships **[S14]**.

8.3 WALLET FEATURES & FUNCTIONALITY

The basic features and functionality of a mobile wallet are described in this section. The recommendations and standards statements provided here are intended to protect the end user.

Security, however, was not the only concern. In developing this section, consideration was given to balancing safety and security with the experience of the end user. For example, it would be most secure to require an end user to enter a pass code to enter their mobile device, another to access their wallet, another to authenticate a transaction and yet another to provide additional authentication for high value or high risk transactions. While secure, this model would have resulted in a negative user experience.

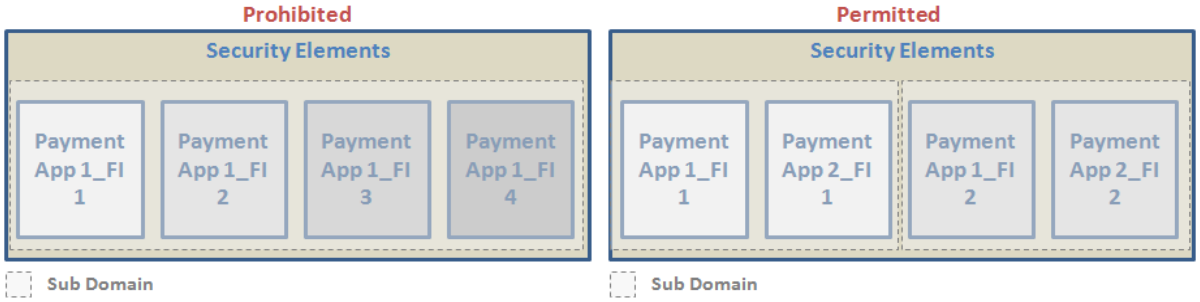
This section includes a series of standards statements that mandate a base level of security while still allowing the end user to enable additional security features if desired.

- **Credential Provisioning:** a mobile wallet may provide end users with the option to request provisioning of payment credentials, i.e. initiate the installation process.
- **Mobile Wallet Access:** for security, a mobile wallet must provide end users the option to lock the wallet and unlock the wallet using a user defined password **[S15]**. This standard does not require that a wallet password must be used, only that the end user must be given the option to set a password.
- **Default Credential Selection:** a mobile wallet must provide end users with the option to enable and disable a default payment credential **[S16]**. A default credential allows end users to initiate a payment without having to take the mobile device out of standby mode and without having to manually select a wallet. Wallets may also be designed to set global defaults, i.e. take into consideration the default options of other wallets and set one overall default payment credential for the device.
- **Manual Default Override:** a mobile wallet must provide end users with the option to override a default payment credential and manually select a payment credential to present **[S17].**
- **High Value & High Risk Payments:** a mobile wallet must have the ability to support entry of a pass code for end user verification of high value and high risk payments **[S18]**.
- **Transaction Data:** a mobile wallet may capture transaction data for all linked payment applications; however, if it does capture this data, access to and usage of this data must be restricted as per the standards in the Data & Security section of this document **[S19]**.
- **Electronic Receipts:** a mobile wallet may store, retrieve and transmit electronic receipts. If the wallet does store electronic receipts, receipts need only be maintained on the instance of the wallet used to make a payment.
- **Enabling a Return Transaction:** a mobile wallet and payment application must be able to facilitate return transactions **[S20]**. For return transactions, the end user will select the payment application to be used and will then tap the mobile device against the POS reader.
- **Loyalty & Reward:** a mobile device may be used to store and manage information on loyalty and rewards programs.

8.4 PAYMENT APPLICATION & PAYMENT CREDENTIALS

The payment application and payment credentials are essential for processing NFC mobile payments. The payment application is similar to the application installed in a contactless card (e.g. PayWave and PayPass). The payment credential is the personalized information within this application that is unique to a specific payment product. The payment application and the payment credential are non-end user facing applications that reside on the mobile NFC device. Unless specified, the terms payment application and payment credential are used synonymously in this document.

- **Payment Application Location:** all elements of the payment application and payment credential (including the pass code) must reside in a secure element within the UICC or in an embedded secure element area on the mobile device **[S21]**. Several options for storing the payment application were contemplated. However, for security reason, this document establishes only one approved method. Each credential issuer must store credential on separate supplemental security domains within the secure element **[S22]**. This standard does not prevent multiple payment applications from the same credential issuer or multiple payment credentials from the same credential issuer from residing in a single supplemental security domains. Each Supplemental Security Domain must hold unique cryptographic keys which are required to establish a secure channel between a credential issuer's TSM and its associated security domain[8] **[S23].**



- **Payment Application Sharing**: a payment application must only contain information from a single credential issuer **[S24].** Sharing of the payment application between credential issuers is not permitted.
- **Payment Application Openness:** a payment application must not prevent connection to multiple wallets assuming that appropriate business and contractual relationships are in place **[S25]**.
- **Credential Identification:** a payment application and payment credentials contain secure, encrypted information that must not be viewable by any other application **[S26]**. However, to allow the end user to identify and select a payment credential, it may be necessary to associate information with the payment credentials that is viewable by a mobile wallet or other application. To ensure a consistent user experience, this document recommends that only the following information is shared: the name of the credential issuing institution, the name of the payment network, card artwork, the type of payment product (e.g. debit or credit,) the masked account number and the expiration date (if applicable).
- **Payment Application Storage Protocols**: a payment application and associated payment credentials must be stored in accordance with appropriate EMVCo and payment network guidelines **[S27].**

[8] PayEz Mobile Specifications; Page 5

- **Turning a Payment Application On and Off:** Payment applications may need to be turned on to transmit payment credentials or turned off to prevent payment credentials from being transmitted. Turning a payment application on or off can be accomplished in several ways. One way is to block or disable the payment applications connection to the NFC radio. Another option is to restrict access to the payment credentials at the payment application level. (For information and standards regarding turning a payment application on and off, please see the Turning a Payment Application On and Off section – 8.4.1)
- **Companion Application**: additional services may be added to a payment application using a companion application. If a companion application is added, the credential issuer must approve of the addition of a companion application and the companion application must follow the same security protocols as a payment application **[S28].**
- **Umbrella Application or Device Software:** a payment application is connected to the wallet application (and sometime the NFC radio) via an umbrella application on the UICC and device software on the embedded secure element. The role of the umbrella application and the device software (used synonymously in this document) are to serve as a directory so that the payment application may be identified. The wallet application, umbrella application (if applicable) and payment application must go through a secure binding process **[S29].** Standards pertaining to the binding process appear in the "Linking a Wallet Application and a Payment Application" section – 8.4.2.

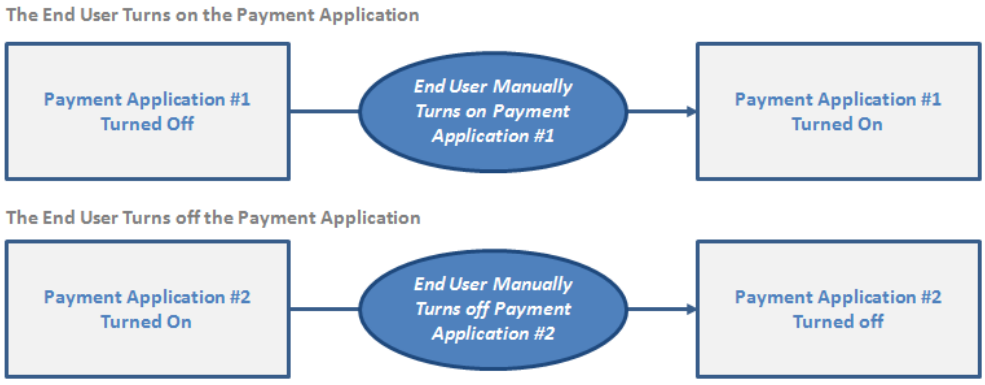
8.4.1 TURNING A PAYMENT ON AND OFF [9]

Turning a payment application on and off is one way of preventing a payment credential from being mistakenly presented for payment. NFC mobile payment solutions must ensure that only one payment application may be turned on, i.e. available for payment, at a time **[S30].** The payment application that is on will be used for all the payment transactions.

The payment application or payment credential that is turned on must be clearly identified in the list of the payment applications and payment credentials displayed in mobile wallet **[S31]**. To promote a consistent user experience, the enabled payment credentials may be bolded, highlighted or markets with a tick mark.

The end user may also have the option to set a default payment application or payment credential in the mobile wallet. If the end user has a default payment application, the default payment application will be turned on unless the user chooses to turn on another payment application. Once a wallet application is closed the default payment application will be turned on and the other payment applications will be turned off – i.e. only one application may be on at a time.

[9] PayEz Mobile Specifications 2.1



In the event that a default payment application has been setup, the default application must first be turned off before the selected payment application may be turned on **[S32]**.

If a payment application is blocked (i.e. use has been restricted at the device or the account level) by the credential issuer, it is not available to make a payment. The end user must not be able to select a blocked payment application to make a payment until approved steps are performed between the end user and the credential issuer to unblock the payment application **[S33].**

8.4.2 LINKING A WALLET APPLICATION AND A PAYMENT APPLICATION

Before a payment credential may be presented for a payment, a payment application and a wallet must be linked via a secure process that enables the wallet to access the payment application; this process is called binding **[S34].**

Prior to a connection being established between a wallet application and a payment application, there must be a valid business relationship between the credential issuer and the wallet provider **[S35]**. It is recommended that this business relationship is document in a contract that outlines security procedure, data privacy rules, liability, customer servicing and end user relationship management rules.

The mobile wallet and the payment application may be connected directly or via an umbrella application. The process for linking a wallet application and a payment application is described in the Enablement & Lifecycle Management section.

8.5 WALLET AND PAYMENT APPLICATION SECTION SUMMARY

The Wallet & Payment Applications Features & Functionality section established the basic Features & Functionality for a wallet application and a payment application. The standards established in this section were designed to protect the end user, promote safety and security of the ecosystem and ensure a consistent user experience.

The next section establishes standards to Transaction processing.

8.6 STANDARDS STATEMENTS

Number	Statement	Section
S11	POS contactless readers must comply with EMVCo contactless specifications [EMV-6] and MasterCard and/or Visa and/or Interac specifications	7.6 Contactless Reader/POS Requirements
S12	Regardless of functionality in pilots or initial commercial launches, those that adopt these standards expect to implement an open wallet and migrate away from proprietary and collective wallets within 18 months of the first open wallet being launched in Canada	8.1 Terminology & Solution Construct
S13	In furtherance of the goals of openness and interoperability, mobile wallets, mobile network operators, original equipment manufacturers, secure domain managers and credential issuers must not restrict access to payment applications from: • Debit payment products from Interac and other networks • Credit payment products from Visa, MasterCard and other networks • Prepaid payment products • Other payment products including transit and loyalty • Payment products issued in a foreign currency (e.g. US Dollar denominated products) This standards statement is subject to appropriate business relationships and technical capabilities being in place	8.2 Openness and Interoperability
S14	Payment applications or payment credentials must not be designed to prohibit a wallet from connecting with other payment applications or payment credentials, contingent on appropriate business relationships	8.2 Openness and Interoperability
S15	Mobile Wallet Access: for security, a mobile wallet must provide end users the option to lock the wallet and unlock the wallet using a user defined password	8.3 Wallet Features & Functionality
S16	Default Credential Selection: a mobile wallet must provide end users with the option to enable and disable a default payment credential	8.3 Wallet Features & Functionality

Number	Statement	Section
S17	Manual Default Override: a mobile wallet must provide end users with the option to override a default payment credential and manually select a payment credential to present	8.3 Wallet Features & Functionality
S18	High Value & High Risk Payments: a mobile wallet must have the ability to support entry of a pass code for end user verification of high value and high risk payments	8.3 Wallet Features & Functionality
S19	Transaction Data: a mobile wallet may capture transaction data for all linked payment applications; however, if it does capture this data, access to and usage of this data must be restricted as per the standards in the Data & Security section of this document	8.3 Wallet Features & Functionality
S20	Enabling a Return Transaction: a mobile wallet and payment application must be able to facilitate return transactions	8.3 Wallet Features & Functionality
S21	Payment Application Location: all elements of the payment application and payment credential (including the pass code) must reside in a secure element within the UICC or in an embedded secure element area on the mobile device [continued in S22]	8.4 Payment Application & Payment Credentials
S22	[continued from S21] However, for security reason, this document establishes only one approved method. Each credential issuer must store credential on separate supplemental security domains within the secure element	8.4 Payment Application & Payment Credentials
S23	Each Supplemental Security Domain must hold unique cryptographic keys which are required to establish a secure channel between a credential issuer's TSM and its associated security domain	8.4 Payment Application & Payment Credentials
S24	Payment Application Sharing: a payment application must only contain information from a single credential issuer	8.4 Payment Application & Payment Credentials

Number	Statement	Section
S25	Payment Application Openness: a payment application must not prevent connection to multiple wallets assuming that appropriate business and contractual relationships are in place	8.4 Payment Application & Payment Credentials
S26	Credential Identification: a payment application and payment credentials contain secure, encrypted information that must not be viewable by any other application	8.4 Payment Application & Payment Credentials
S27	Payment Application Storage Protocols: a payment application and associated payment credentials must be stored in accordance with appropriate EMVCo and payment network guidelines	8.4 Payment Application & Payment Credentials
S28	[Context: Companion Application: additional services may be added to a payment application using a companion application.] If a companion application is added, the credential issuer must approve of the addition of a companion application and the companion application must follow the same security protocols as a payment application	8.4 Payment Application & Payment Credentials
S29	The wallet application, umbrella application (if applicable) and payment application must go through a secure binding process	8.4 Payment Application & Payment Credentials
S30	NFC mobile payment solutions must ensure that only one payment application may be turned on, i.e. available for payment, at a time	8.4.1 Turning a Payment On and Off
S31	The payment application or payment credential that is turned on must be clearly identified in the list of the payment applications and payment credentials displayed in mobile wallet	8.4.1 Turning a Payment On and Off
S32	In the event that a default payment application has been setup, the default application must first be turned off before the selected payment application may be turned on	8.4.1 Turning a Payment On and Off

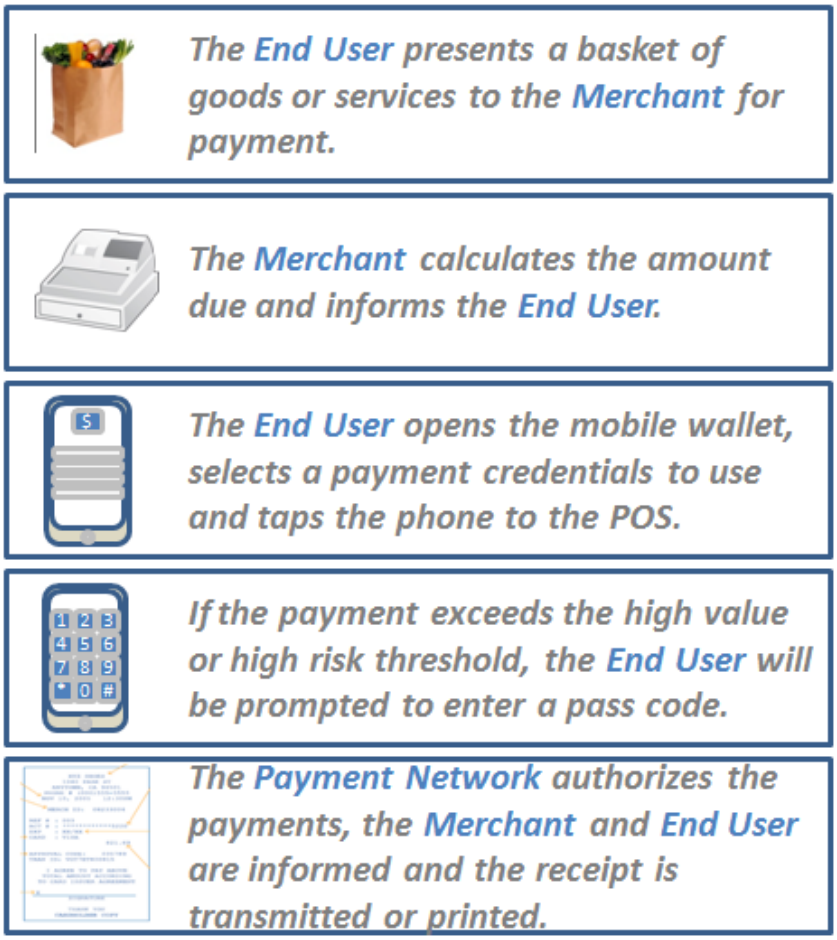
Number	Statement	Section
S33	The end user must not be able to select a blocked payment application to make a payment until approved steps are performed between the end user and the credential issuer to unblock the payment application	8.4.1 Turning a Payment On and Off
S34	Before a payment credential may be presented for a payment, a payment application and a wallet must be linked via a secure process that enables the wallet to access the payment application; this process is called binding	8.4.2 Linking a Wallet Application and a Payment Application
S35	Prior to a connection being established between a wallet application and a payment application, there must be a valid business relationship between the credential issuer and the wallet provider	8.4.2 Linking a Wallet Application and a Payment Application

9 TRANSACTION PROCESSING

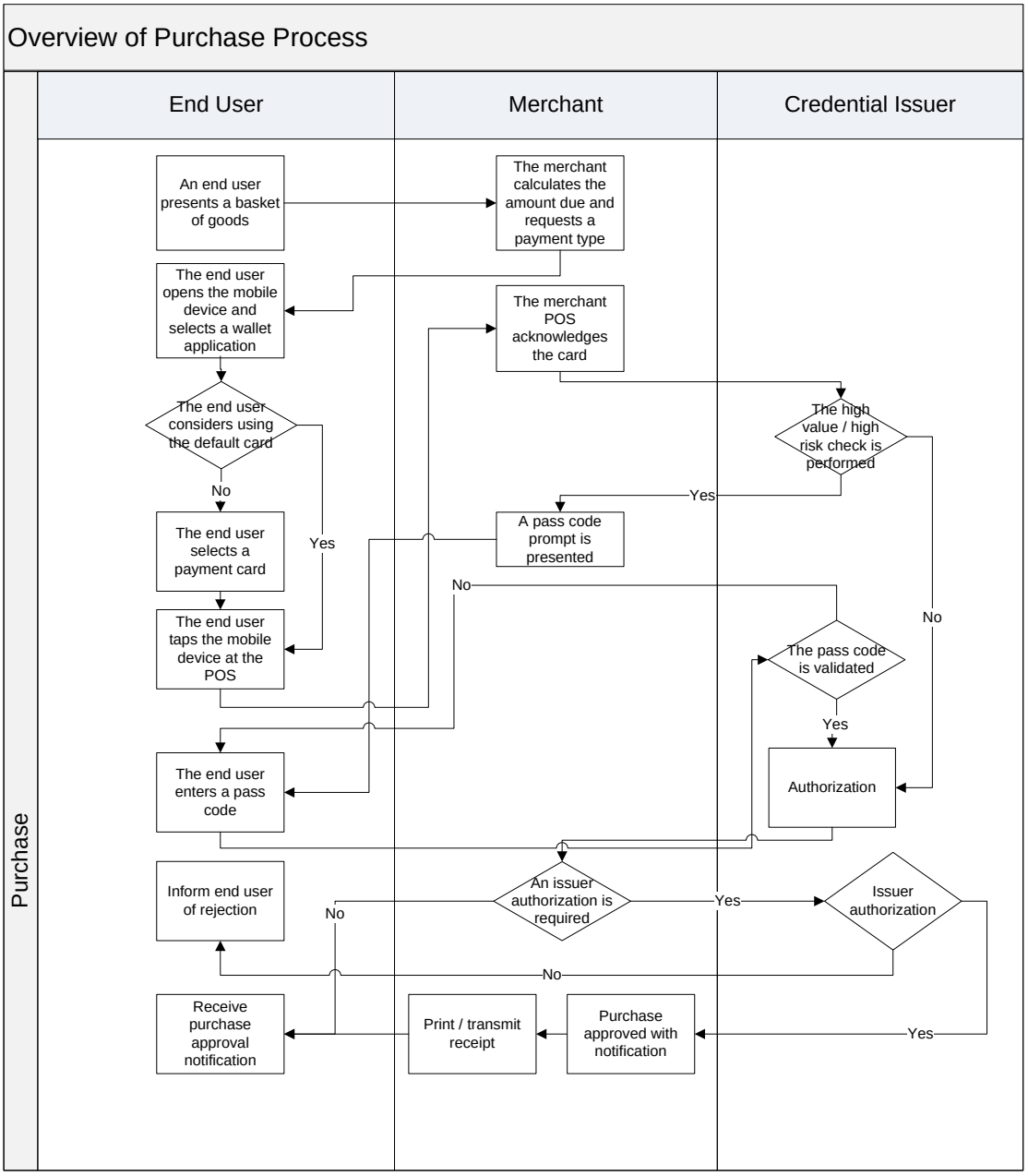
The Transaction Processing section focuses on aspects of a NFC based mobile payment transaction process that are new for mobile payments, i.e. those that differ from contactless card payments. This section establishes guidelines and standards that support the safety and security of the ecosystem, protect the end user and ensure a common user experience for NFC payment transactions.

This section was created under the assumption that NFC mobile payments will integrate with existing payment networks (e.g. Interac, Visa, and MasterCard). This model was specifically designed to minimize the impact to merchants, end users and other ecosystem participants. This section is based on the steps typically performed in a payment transaction and is intended to reduce the impact on the merchant by maintaining a consistent user experience.

Below is an overview of the purchase process for mobile payments:



A more detailed version of the transaction flow follows:



Note: while the CVM steps are included under the Credential Issuer, these steps are, in actuality, performed locally with the Payment Application.

Within the transaction flow, there are only a few areas that differ from contactless card transactions. These differences are evaluated in this section, including:

- Convenience Transaction
- High Value / High Risk Transactions
- Returns Transaction
- Electronic Invoicing

9.1 CONVENIENCE TRANSACTIONS USING MOBILE DEVICES

A convenience transaction is a transaction that meets certain dollar value and spend category criteria Convenience transactions are typically transaction that are performed frequently and quickly (e.g. purchasing a transit ticket or a coffee). Convenience transactions must not exceed high value or high risk transaction thresholds as defined by the payment networks **[S36]**. Further, a return transaction may not be a convenience transaction.

A convenience transaction must be performed as per existing payment network contactless guidelines; convenience transactions must not require more than a 'Tap and Go' to make a payment and must not require a Card Verification Method (CVM) **[S37]**.

9.2 HIGH VALUE / HIGH RISK TRANSACTIONS USING MOBILE DEVICES

9.2.1 OVERVIEW

High value and high risk transactions are defined by the credential issuer and/or the payment networks. High value and high risk transactions must be approved by the end user via a Card Verification Method (CVM) **[S38]**.

There are several different options that are available for conducting high value and high risk transactions verification via a mobile device. Although many different options were evaluated, only one approved method for end user authorization of high value and high risk transactions is approved. Once deemed acceptable by payment networks, high value and high risk transactions must be approved using the Tap and Confirm (i.e. also Tap-Enter and Verify Pass Code on Mobile – Tap) CVM **[S39]**. The appendix outlines other methods that were considered and rejected as the target CVM.

As the popularity and ubiquity of NFC mobile payments increases and as loyalty and rewards offers are integrated into mobile devices, it is anticipated that NFC mobile payments will be used for higher value purchases.

9.2.2 CVM OPTION OVERVIEW

There are seven commonly accepted CVM choices for high value and high risk transactions. After evaluating these methods, the Tap and Confirm CVM was selected as the target CVM for NFC mobile payments in Canada.

- **Tap and Go –** The end user taps the mobile device only once. No CVM process is performed; this is used for convenience transactions.
- **Pass code with OTA Verification –**The end user taps the mobile device as if for a convenience transaction, when prompted, the end user enters the pass code into the mobile device. The pass code is then transmitted over-the-air (OTA) using the mobile network and verified via the payment network.
- **PIN entered on Merchant POS –** The end user taps the mobile device as if for a convenience transaction, when prompted, the end user enters a PIN into the merchant POS device. The PIN is then verified via the payment network.
- **Tap and Confirm (the target method) –** The end user taps the mobile device as if for a convenience transaction, when prompted, the end user enters the pass code into the mobile device and taps the mobile device again. Pass code information is validated by the payment applications and approval or failure is transmitted to a third party. Tap and confirm is the only approved method,

all CVM must follow the tap and confirm process once deemed acceptable by payment networks **[S40]**.

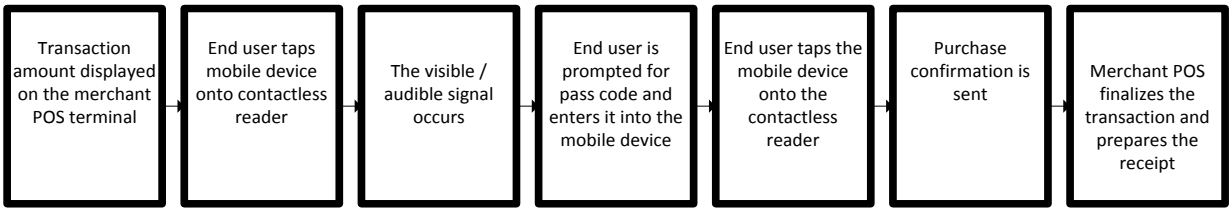
- **Tap, Confirm and Reconfirm –** The end user taps the mobile device as if for a convenience transaction, when prompted, the end use enters pass code information into the mobile device and then taps the mobile device to the POS. Finally, the end user is prompted to tap again to receive payment confirmation.
- **Tap and Connect –** The end user taps the mobile device. When prompted, the end user taps the device again, establishing a two way connection. Once the two way connection is established, the end user enters the pass code onto the mobile device. For this CVM, an open connection must be maintained for the entire CVM process.
- **Tap and Explore –** This is an extension of the tap and connects method. Here, the end user taps the mobile device and establishes a connection. The connection is used both for CVM and to pass loyalty information.

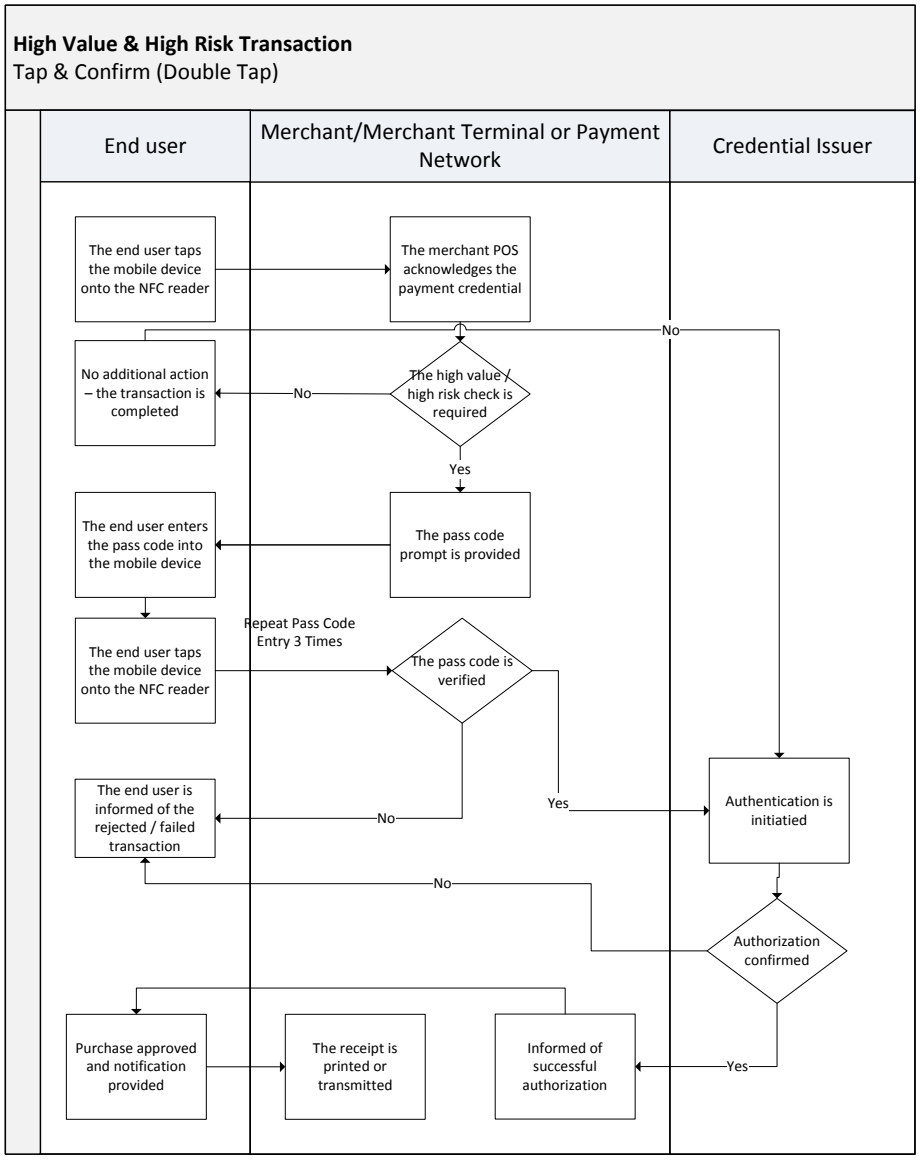
This section assumes that the end user has a preferred payment type selected. If the end user wants to select a different payment for the transaction, they can do so before tapping their mobile device to the POS. At the end of the interaction when the transaction is complete, the payment method will revert back to the default selection.

The standard CVM process in Canada for high value or high risk payments is **'Tap and Confirm' (i.e. double tap) [S41]**. Given current NFC POS device limitations and network roll out plans this standard will take time to be adopted. Other CVM process (like tap and sign, etc.) will be accepted until the credential issuers and payment networks agree that tap and confirm will be the only accepted CVM process. This standard is consistent with Visa, MasterCard, Interac and standards in Europe and will contribute to global interoperability.

9.2.3 TAP & CONFIRM – DOUBLE TAP

This is the standard for high value transactions that the European Payment Council has adopted. For a pure NFC based high value transaction to occur, two taps are required at a minimum. The end user requires one tap for low value transactions and two taps for high value transactions. Any updates to the payment application and confirmation happens OTA.





Note: while the CVM steps are included under the Credential Issuer, these steps are, in actuality, performed locally with the Payment Application.

See the appendix for other CVM process evaluated.

9.3 ELECTRONIC RECEIPTS

The final step in processing a mobile NFC transaction is receipt issuance. There are no unique mobile payment receipt issuance standards. Receipt issuance must be conducted as per existing guidelines **[S42].** Receipt issuance may be via paper, e-receipt or other means.

Some merchants offer end users the ability to receive electronic receipts. These receipts are typically sent from the merchant POS to the end user's email address. With the advent of the mobile wallet, end users may look for merchants to provide electronic receipts in lieu of paper receipts. Electronic receipts

are sent from the merchant to the end user's mobile wallet. Once received, electronic receipt may be securely stored in the wallet.

This section examines components of electronic receipts including enablement of electronic receipts, data transmission, storage and capture and mandatory information.

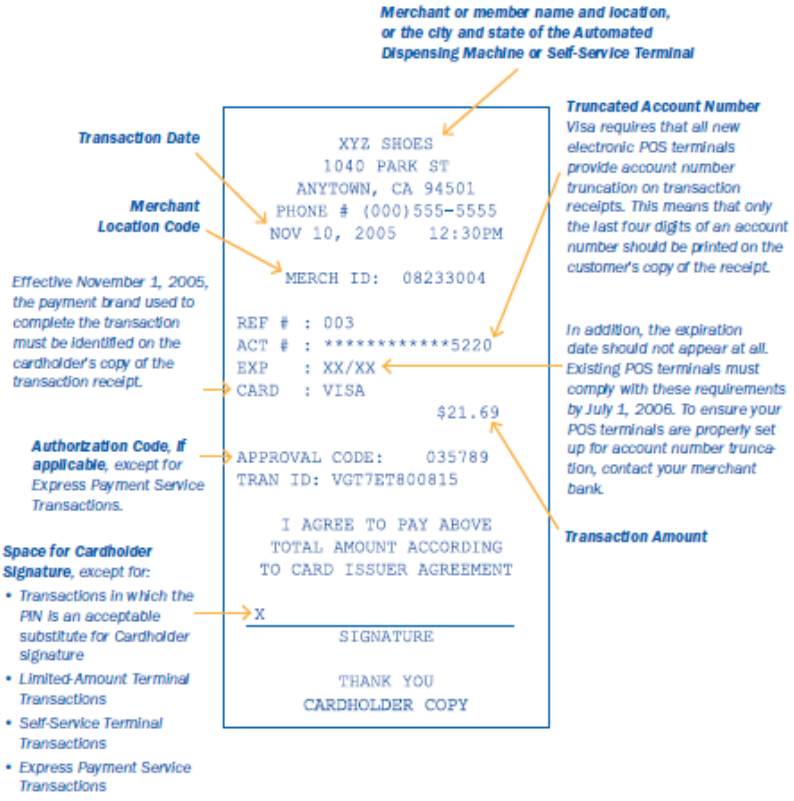
9.3.1 RECEIPT EXAMPLES

Electronic receipts will vary by merchant, credential issuer, payment network and even by wallet provider. This section examines the form and structure of electronic receipts.

9.3.2 CURRENT VISA STANDARDS FOR PAPER RECEIPTS

As an example of an electronic receipt, the following are the Visa requirements for all transaction receipts generated from electronic point-of-sale terminals are outlined below:

Electronic Point-of-sale Terminal Receipts



[10]

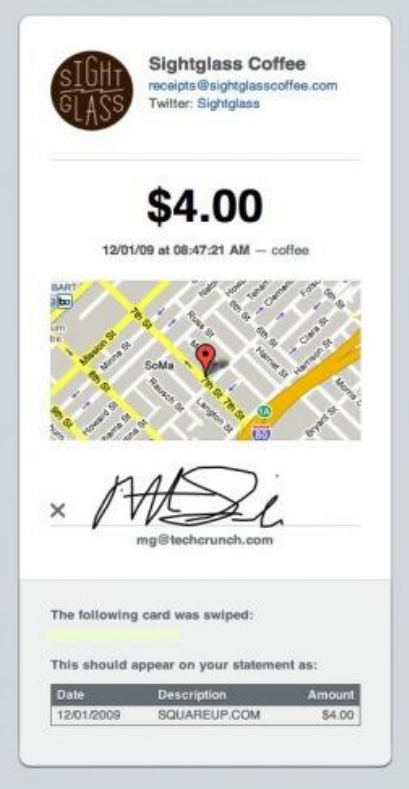
Visa has identified the following fields for inclusion in electronic receipts:

[10] Visa's website

- Merchant Name
- Merchant Location (Text)
- Merchant Location Code
- Truncated Account Number
- Transaction Amount
- Transaction Date
- Authorization Code (If Applicable)
- Space for the Account Holder's (end user's) Signature

9.3.3 CURRENT RECEIPT STANDARDS FOR SQUARE (PEER TO PEER ACCEPTANCE)

Another example of electronic receipts comes from square. Square's requirements for all transaction receipts generated from electronic point-of-sale terminals (including payment holder-activated terminals) follow:



Square has identified the following key fields:

- Merchant Name
- Merchant Location (Text)
- Merchant Location (Map)
- Merchant Email and Twitter
- Transaction Description
- Transaction Amount
- Transaction Date / Time

- Space for the Account Holder's (end user's) Signature
- Account Holder's (end user's) Email

9.3.4 ELECTRONIC RECEIPTS GUIDELINES

Advantages and Disadvantages of Electronic Receipts: There are advantages and disadvantages to offering electronic receipts. This document does not require electronic receipts, however, stakeholder should review their agreements to understand their own receipt requirements and must evaluate if electronic receipts are right for them.

Data Fields: Based on these examples and other research, if a merchant chooses to issue electronic receipts, it is suggested that the following fields are included:

9.3.4.1.1.1.1.1 Mandatory Fields	9.3.4.1.1.1.1.2 Description
9.3.4.1.1.1.1.3 Merchant Name	Name and contact information; allows the merchant to be identified
Merchant Location	Address information; allows the merchant to be identified
Reference # / Code	Transaction reference number; allows the transaction to be identified by the end user and for returns
Authorization # / Code	Bank authorization code; used for auditing an tracking purposes
Amount	The transaction amount; used to audit purposes, reconciliation with the statement and as a proof of purchase
Status	The summary of any actions required by the merchant
Date & Time	The date and time that the transaction occurred
Card Number (Truncated – last 4 digits)	The card number that has been truncated for security reasons but that is partially presented for tracking purposes
Mobile No.	The mobile number that has been truncated for security reasons but that is partially presented for tracking purposes
Loyalty #	The loyalty card reference number
Coupon #	The coupon reference number or barcode

Transmission Methods: Further, it is suggested that electronic receipts are transmitted by the following methods:

Method of Transmission	Description
Email	An email message formatted for review on the mobile device
SMS	Short Message Service (SMS) message sent to the mobile phone number attached to the account
Mobile OTA	Receipt sent OTA through mobile network to end user. The electronic receipt will have information that will allow it to be routed back to the merchant
NFC	The receipt is transmitted to the POS using NFC. The end user needs to tap their mobile device to transmit the electronic receipt.

Data Format: For receipts transmitted via SMS, Mobile OTA and NFC, it is recommended that receipts be sent in text format. For email based receipts, a text file or a PDF file should be considered:

Data Format	Description
Text Format (.txt) / (.csv)	Unformatted text
PDF (.Pdf)	Formatted text and images

9.4 RETURN TRANSACTIONS AND REVERSALS USING A MOBILE DEVICE

A return transaction covers the presentment and acceptance of payment credentials associated with the return of goods and services. Using a mobile wallet to reverse or process a return transaction will create a unique experience for the end user.

This section examines standards and guidelines for return or reversal transactions. This section includes user experience requirements for returns, CVM requirements for returns, presentment of electronic receipts for return transaction.

9.4.1 ELECTRONIC RECEIPTS AND RETURN TRANSACTIONS:

Conventional return processes are initiated by presenting the paper receipt to the merchant. The merchant then uses the transaction ID on the receipt identify the transaction in the POS system. As NFC mobile payments continue to develop, end users will increasingly choose to present the electronic receipt to initiate the returns process. The electronic receipt will likely be presented in one of three ways:

- **Visually:** The end user retrieves the receipt in the mobile wallet and presents it to the merchant. The merchant can either scan a bar code on the receipt or enter the transaction ID manually by reading the receipt
- **Electronically:** The end user transmits the receipt to the merchant electronically over-the-air using routing information provided by the merchant or coded into the receipt

- **NFC:** The receipt is transmitted back to the POS using NFC. The end user taps their mobile device to transmit the electronic receipt and start the returns process.

For returns, the proposed standard is for the end user and merchant to have a choice to accept electronic receipts both electronically and visually.

9.4.2 RETURNS PROCESS

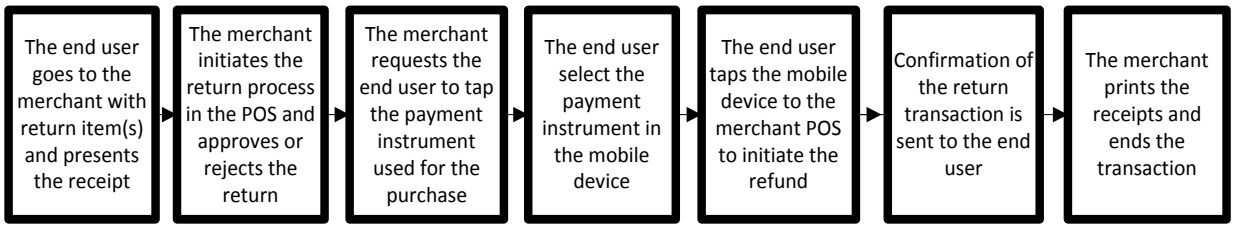
The "Offline" option, as defined by payment networks, must be followed for NFC mobile device return transactions in Canada **[S43]**. Accordingly, NFC mobile payment returns will not require a CVM such as a signature, pass code or PIN **[S44]**.

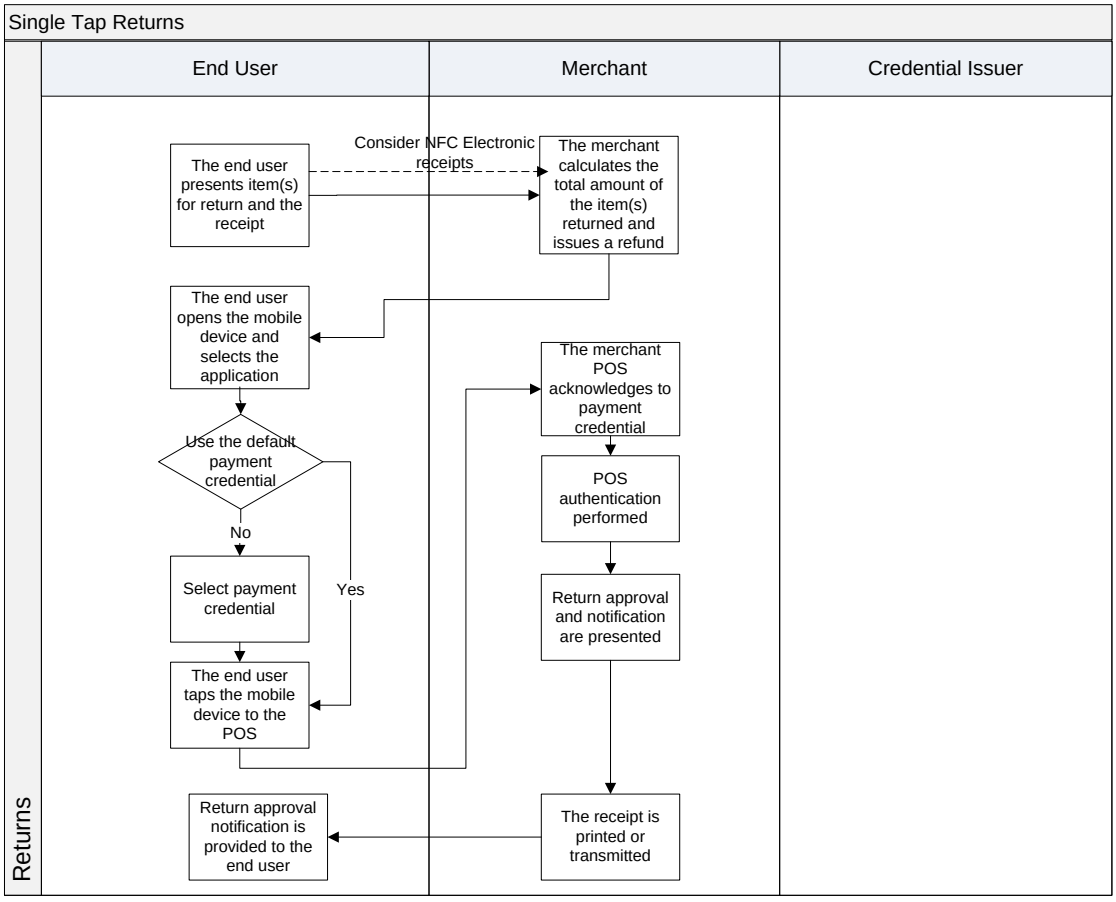
For information on the other ways evaluated of processing a return transaction, please see the appendix.

9.4.3 RETURNS PROCESS – OFFLINE RETURNS

This is the method adopted by the European Payment Council and the agreed approach for return, NFC mobile payment transactions in Canada by the industry participants

As an offline transaction, this type of return does not require back end authentication. As a result, this is a much faster process than some of the other options that were evaluated.





9.5 TRANSACTION PROCESSING SECTION SUMMARY

The Transaction Processing section summarizes the basic steps for processing NFC mobile payment transactions. This section includes basic payment processing, CVM process for high value and high risk payments, electronic receipt guidelines and returns using a mobile device. The standards in this section were designed to adhere to and integrate with existing rules and guidelines published by the payment networks. By integrating with the existing infrastructure, the impact to end users, merchants and the payment networks will be kept to a minimum.

9.6 STANDARDS STATEMENTS

Number	Statement	Section
S36	Convenience transactions must not exceed high value or high risk transaction thresholds as defined by the payment networks	9.1 Convenience Transaction Using a Mobile Device
S37	A convenience transaction must be performed as per existing payment network contactless guidelines; convenience transactions must not require more than a 'Tap and Go' to make a payment and must not require a Card Verification Method (CVM)	9.1 Convenience Transaction Using a Mobile Device

Number	Statement	Section
S38	High value and high risk transactions are defined by the credential issuer and/or the payment networks. High value and high risk transactions must be approved by the end user via a Card Verification Method (CVM)	9.2 High Value / High Risk Transactions Using a Mobile Device
S39	Once deemed acceptable by payment networks, high value and high risk transactions must be approved using the Tap and Confirm (i.e. also Tap-Enter and Verify Pass Code on Mobile – Tap) CVM	9.2 High Value / High Risk Transactions Using a Mobile Device
S40	Tap and confirm is the only approved method, all CVM must follow the tap and confirm process once deemed acceptable by payment networks	9.2.2 CVM Options Overview
S41	The standard CVM process in Canada for high value or high risk payments is 'Tap and Confirm' (i.e. double tap)	9.2.2 CVM Options Overview
S42	The final step in processing a mobile NFC transaction is receipt issuance. There are no unique mobile payment receipt issuance standards. Receipt issuance must be conducted as per existing guidelines	9.3 Electronic Receipts
S43	The “Offline” option, as defined by payment networks, must be followed for NFC mobile device return transactions in Canada	9.4.2 Returns Process
S44	Accordingly, NFC mobile payment returns will not require a CVM such as a signature, pass code or PIN	9.4.2 Returns Process

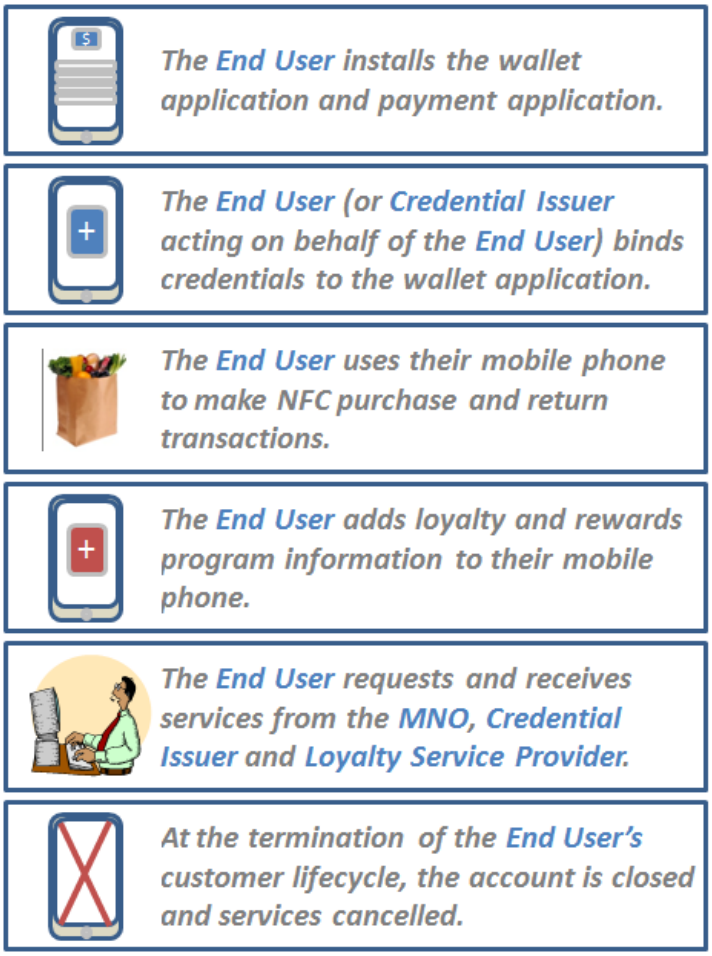
10 ENABLEMENT & LIFECYCLE MANAGEMENT

The Enablement & Lifecycle Management section establishes a common reference model for installing a wallet application and payment applications, loading end user payment credentials and maintaining those payment credentials while the end user is active. Enablement and lifecycle management activities in this section involve coordination between multiple ecosystem participants (e.g. credential issuer, MNO and TSM). The standards in this section consider both the user experience and the basic relationships that must be established to create a mobile payments ecosystem.

The Enablement & Lifecycle Management section includes the following sub sections:

- Business Relationships between Ecosystem Participants
- Key Management
- Installation of the Mobile Wallet
- Installation of the Payment Application & Payment Credentials
- End User Servicing
- Closure & Cancellation of Service

Enablement is a prerequisite to using a mobile device for NFC payments, the enablement activities must be performed before any transaction activities.



10.1 BUSINESS RELATIONSHIPS BETWEEN ECOSYSTEM PARTICIPANTS

A foundational concept in this section on enablement and lifecycle management activities is that interactions between ecosystem participants (including the wallet provider and credential issuer, the credential issuer and the TSM and the Credential Issuer and the MNO) must be preceded with steps to establish contractual business relationships **[S45]**.

Business relationship may be formed directly or through a central, hub organization such as a central controlling authority.

10.2 KEY MANAGEMENT MODE

At the foundation of this document and the provisioning process are the communication protocols and roles and responsibilities established by GlobalPlatform.

As indicated in section 6.8, all messaging must be performed under the relevant guidelines from GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0 **[S46]**.

Those that adhere to this document agree to use only the Delegated Mode or the Dual Mode as defined by GlobalPlatform for all enablement and lifecycle management activities **[S47]**. This standard is foundational to all enablement and lifecycle management activities because the Delegated and Dual management modes allow credential issuers to enforce the security of payment credentials and consequently support the safety and security of the ecosystem.

Additionally, before the provision process, a key management process must be established. The objective of the key management process is to determine protocols for managing secure data between the credential issuer's TSM and the SDM's TSM.

10.2.1 SECURE KEY MANAGEMENT

This section illustrates the exchange of keys between the credential issuer and the credential issuer's TSM. This process is required to facilitate the above payment application installation, credential loading, and binding steps.

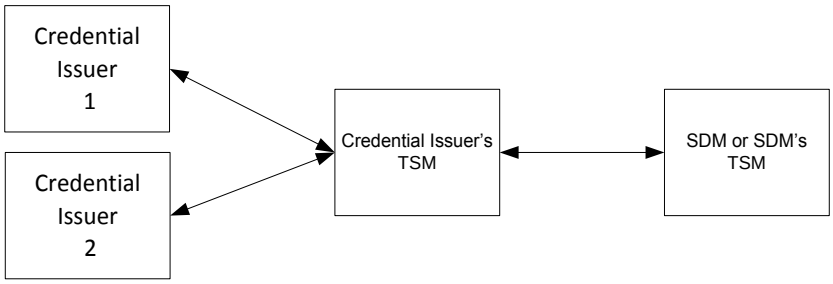
For proprietary wallets, secure key management processes must be established between a credential issuer, a credential issuer's TSM, a SDM's TSM and a SDM **[S48]**. For open wallets, protocols must be established to manage key between multiple parties **[S49]**. This can be accomplished by the addition of a third party TSM, hub TSM or Central Authority.

In this process, the credential issuer's TSM, the credential issuer, the SDM's TSM and the SDM must have an established business relationship, either directly or indirectly **[S50].**

Once this relationship is established, keys will be exchanged. Key exchange allows for the secure transmission of data needed to securely transmit credentials to the payment application. This interaction is exclusively between the credential issuer and the credential issuers TSM. The end user is not involved in this process.

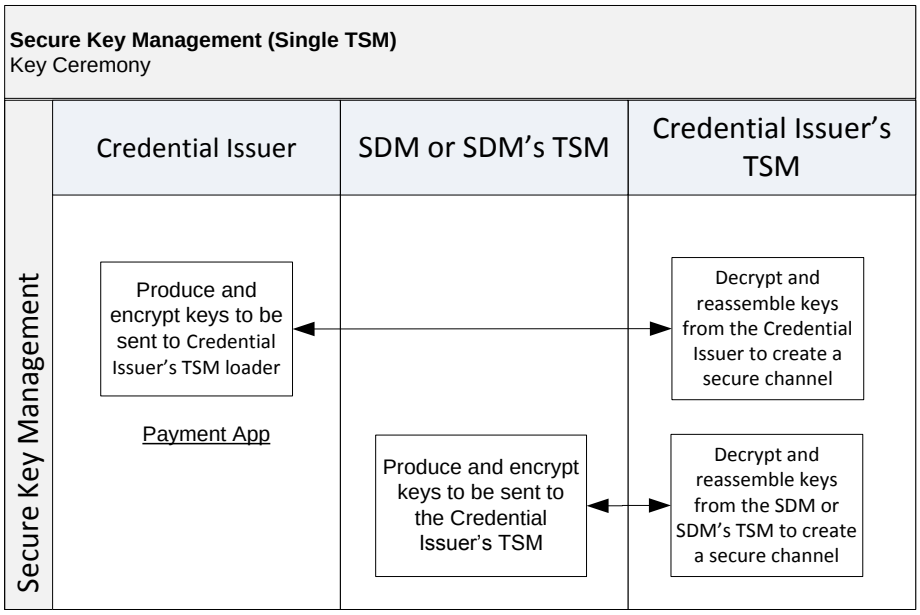
10.2.2 SINGLE CREDENTIAL LOADER

The following illustration depicts the relationships in a single TSM model. A single credential loader model would be used if each player in the NFC mobile payments ecosystem develops individual business relationships.



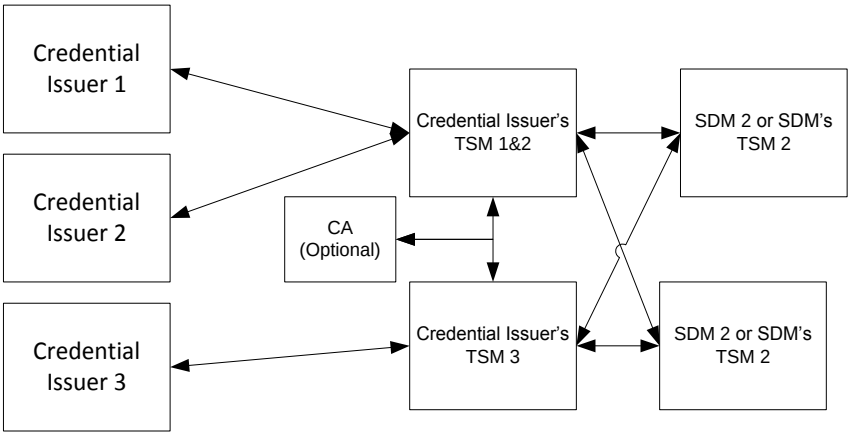
This credential loading process for a single credential issuer is initiated when the credential issuer establishes a new relationship with a TSM (this relationship facilitates initial provisioning and management of the secure keys). The credential issuer's TSM, will work with the credential issuer's payment processor (e.g.: TSYS), to produce an encrypted key set. This files containing the keys are transferred to the credential issuer's TSM as an encrypted data file package. This same process is established between the SDM and the SDM's TSM.

Key exchange must be performed under the guidelines set out by GlobalPlatform **[S51]**. When this process is complete, the key exchange will facilitate a secure data transmission channel between the credential issuer's TSM, the credential issuer and the SDM's TSM. This secure connection must exist for over-the-air provisioning to occur **[S52].**



10.2.3 MULTIPLE CREDENTIAL LOADER (HUB & SPOKE)

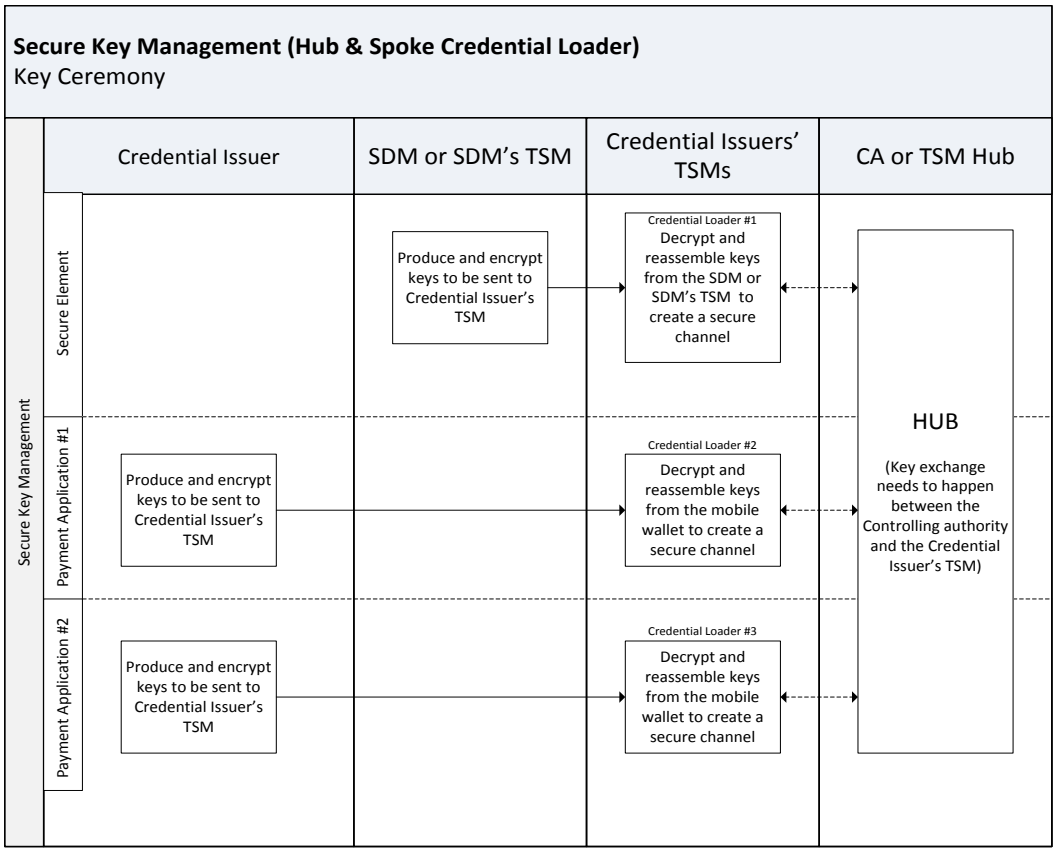
The more complicated scenario of multiple TSMs is presented below. This section depicts a scenario in which there is one or a few credential issuers' TSM functioning as a hub for the industry. This model could be used to facilitate multiple credential issuers launching in a single wallet application.



In this model, the credential issuer establishes a relationship with the credential issuer's TSM to exchange keys and to ensure that there is a secure way of transmitting information between ecosystem participants.

In the multiple credential loader model, a group of credential loaders will form a business agreement and relationship that enables transmission of information securely among the participants. The credential issuers' TSMs will then go through a process of exchanging keys among themselves to ensure that they can establish a secure connections – this exchange of keys must occur to facilitate the loading of credentials into an open or collective wallet **[S53].**

In this model, all parties must perform key exchanges under the guidelines set out by GlobalPlatform. The central authority or hub of credential issuers' TSMs must develop and make available protocols to facilitate these interactions **[S54].**

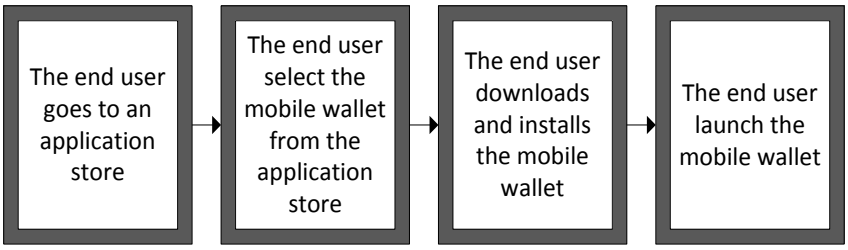


10.3 MOBILE WALLET INSTALLATION

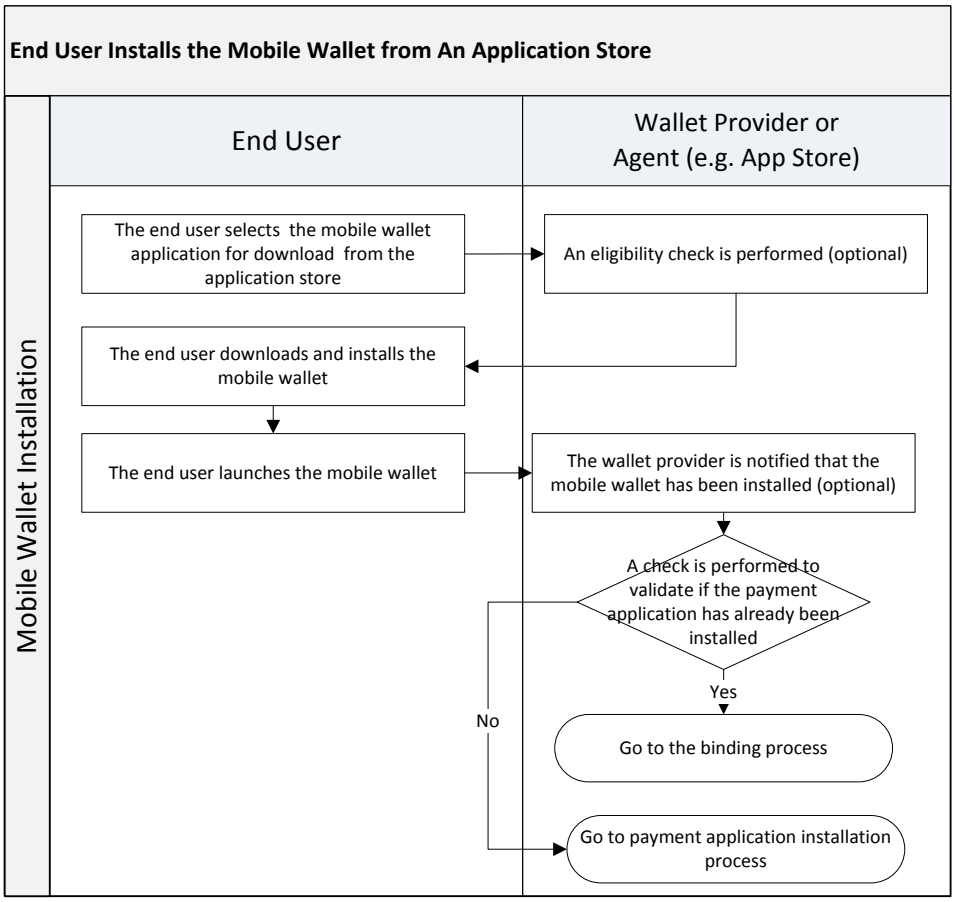
From the end user's perspective, enablement begins when the end user gains access to a wallet application. To begin the process of enabling mobile payments, the mobile wallet is installed on the end user's mobile device. This document considers two processes for installing the wallet application:

- **End User Initiated** – the end user installs the mobile wallet from an application store or website
- **Pre-Installed** – the credential issuer, MNO, wallet provider or other party pre-installs the mobile wallet on the mobile device prior to the end user accessing the mobile device

Pre-installation may also occur as an alternative to mobile wallet initiated installation. This document does not describe the pre-installation process. End user installation is described in this section starting with the end user accessing an application store or website. This step may be performed before or after the payment application and payment credentials are installed onto the mobile device.



This process illustrates the wallet installation being launched by the end user. Alternatives to this process may also occur. These alternatives include the credential issuing or MNO pushing the wallet to a mobile device.



10.3.1 PRE-INSTALLATION ELIGABILIITY CHECK

Some application stores, websites and service providers may require an eligibility check prior to downloading a mobile wallet. The purpose of such a check is to ensure that the end users' hardware can support NFC mobile payments, i.e. that the mobile device has an NFC radio.

While an eligibility check is not required, it is strongly encouraged. By including an eligibility check, end user confusion will be reduced, wallet installation troubleshooting costs will be minimized and potential security issue may be avoided (e.g. phishing).

10.4 PAYMENT APPLICATION AND PAYMENT CREDENTIAL INSTALLATION

Installation of the payment application is a separate, distinct process from the installation of the wallet application. The payment application and payment credentials are personalized by the credential issuer and contain highly sensitive, encrypted information.

This section examines several sub processes associated with the payment application and payment credential installation:

- End User Requests Access to Payment Application and Payment Credentials
- Validation and verification of the end user information
- Installation of the payment application
- Binding of the payment application to the mobile wallet (via the umbrella app)
- OTA provisioning of payment credentials

10.4.1 END USER REQUESTS ACCESS TO THE PAYMENT APPLICATION

The end user must be able to request the payment application installation process via a mobile wallet **[S55]**. In addition to requesting payment application installation via a mobile wallet, requests may also be initiated via other channels such as a website, branch, call center or mobile banking application. Whichever method of requesting the download of the payment application and payment credentials is used, the end user must give their consent prior to installation **[S56]**.

As indicated above, the actual request may come from several channels:

- End user requested via the wallet
- End user requested via another channel
- Credential issuer initiated

For mobile wallet initiated requests, the mobile wallet must display the names of credential issuer whose credentials can be loaded into that wallet **[S57].**

After requesting the payment application and payment credentials but prior to installation, the end user must first be verified (see next section for standards statements.)

10.4.2 END USER VALIDATION AND VERIFICATION

Prior to installing the payment application and payment credentials on the mobile device, the identity of the end user must first be validated **[S58]**.

The end user validation and verification process will differ by credential issuer. It is the responsibility of the credential issuer to define the process of end user validation and verification **[S59]**. This document does not establish requirements for this process. Some areas for consideration include mobile device ownership and client authorization to download credentials.

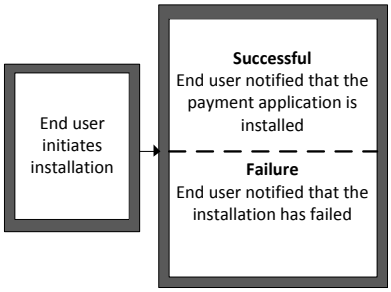
These standards allow for the initiation of the provisioning process via the wallet. The responsibility for validating will still remain with the credential issuer, as per the above standards statement.

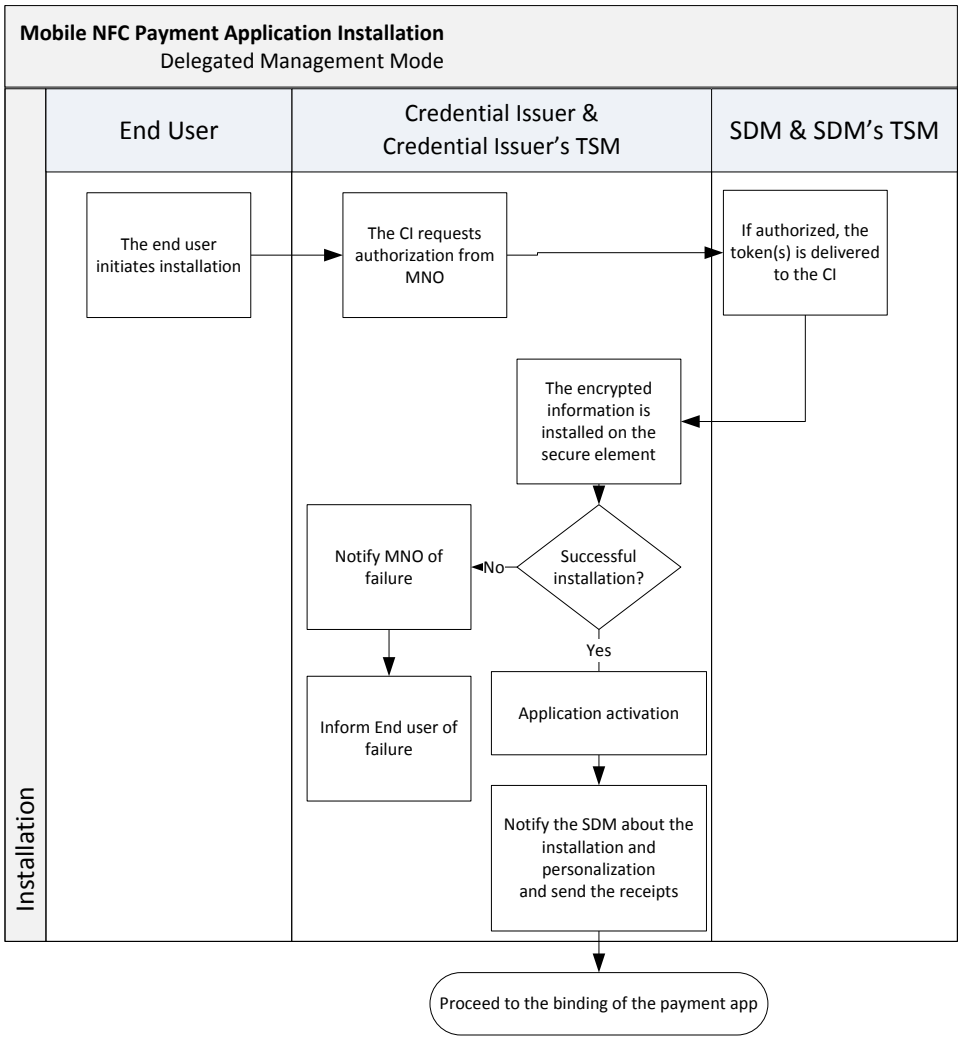
Following validation and verification, the credential issuer must prompt the end user with messaging confirming the next step **[S60]**. If the end user information is validated, the next step is the installation of the payment application.

10.4.3 MOBILE NFC PAYMENT APPLICATION INSTALLATION

Once the end user's identity has been verified and approved for mobile payment service, the next step is for the end user to have their mobile NFC service installed, personalized and activated. This document assumes that installation, personalization and activation occur at the same time. However, this step may also be performed before a wallet application is installed.

In this model, the role of installing and activating the mobile NFC service has been delegated to the credential issuer's TSM and SDM's TSM. All parties involved in this process must establish a secure communication link with the credential issuer and the SDM to effect installation of the payment application and payment credentials **[S61].** Once the secure connection is established, the TSM must handle all activities including installation and activation of the mobile NFC service **[S62].**





Following the installation of the payment application, the payment application must be bound to the mobile wallet and credentials downloaded before it can be used to make a payment (see the Mobile Wallet and Payment Application Binding section for standards statements).

10.4.4 MOBILE WALLET AND PAYMENT APPLICATION BINDING

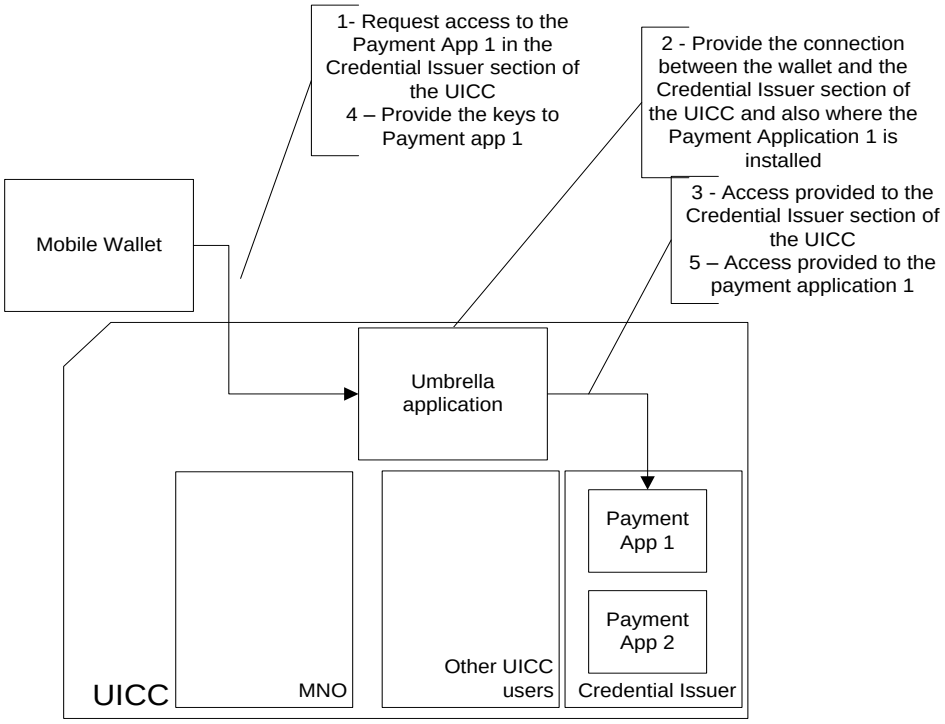
The binding process occurs between a mobile wallet and one or more payment applications. The purpose of binding is to provide a mobile wallet with information on the location of payment applications on the UICC and embedded secure element. Binding must occur for a mobile wallet to access a payment application **[S63].**

The binding process differs depending on where the payment application is stored.

10.4.5 SECURE ELEMENT ON THE UICC

For a payment application installed on the UICC to be used in a payment, a wallet and a payment application must go through a binding process**.** When a payment application resides on the UICC, the wallet will use the UICC's umbrella application to locate the payment application. The umbrella application serves as a directory for the UICC and must be provided by the SDM **[S64].**

During the binding process, the mobile wallet interfaces with umbrella application to determine where a payment application is stored. The umbrella application then informs the wallet application of where the payment application is stored and provides an identifier by which to locate the payment application. The construct of the identifier must be provided by the SDM **[S65]**.



Once the wallet application and the payment application have been through the binding process, the wallet application interfaces with the umbrella application to connect with and provide access to the payment credential for payment and maintenance activities.

10.4.6 EMBEDDED SECURE ELEMENT

Similarly, for payment applications installed on an embedded secure element to be used in a payment, the wallet and payment application must go through a binding process.

When the mobile wallet is involved in the credential provisioning process, the mobile wallet controls where the payment application is stored. When the payment application and payment credentials are downloaded before the wallet is installed or prior to integration with the wallet, the credential issuer or credential issuer's TSM determines where the payment application is stored.

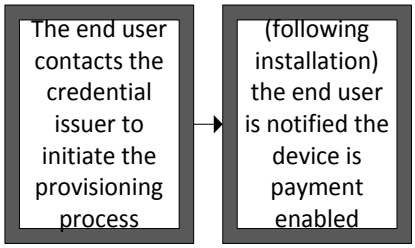
10.4.7 OTA PROVISIONING OF CREDENTIALS

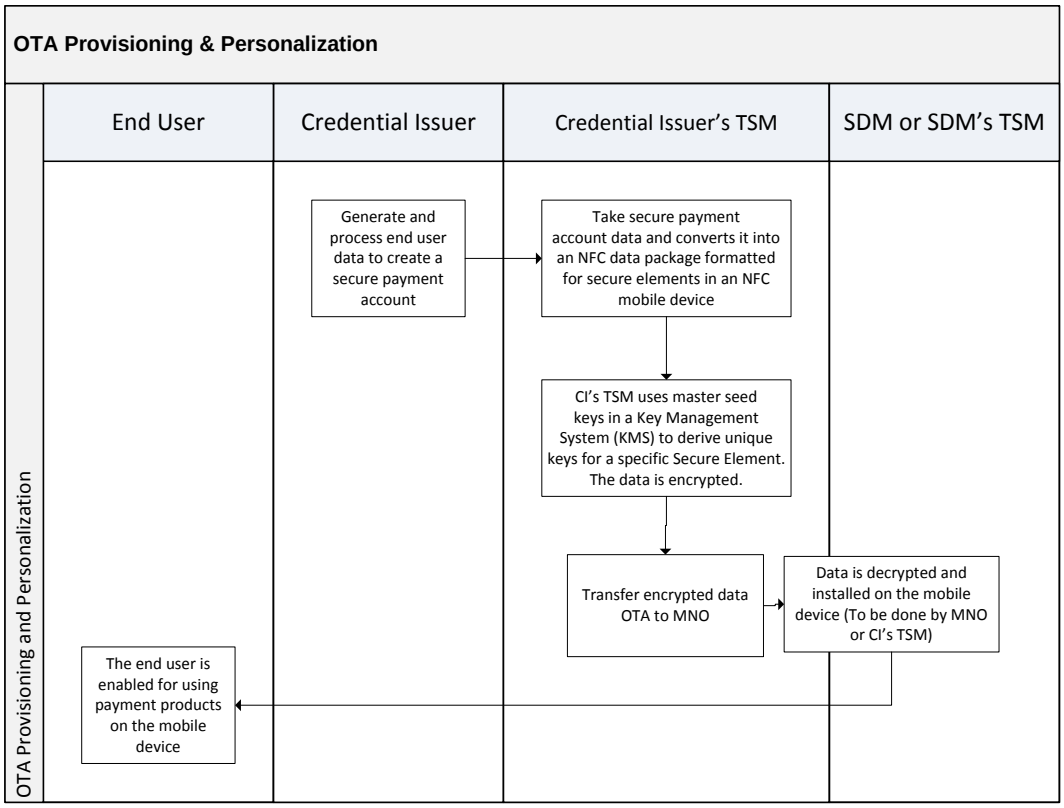
Although the payment credential may be installed with the payment application, these two steps may occur separately. This section illustrates OTA provisioning of the payment credentials into the payment application.

Credentials may also be pre-installed or sent to an existing mobile device OTA. The use case below illustrates the OTA provisioning and personalization process. Payment credentials are stored on the mobile device and must be able to be installed and updated over-the-air **[S66].**

In the OTA provisioning and personalization process:

- The credential issuer generates payment credentials
- The credential issuer's TSM is then responsible for the encrypted data package
- The data package is then installed on the supplemental security domain in the UICC of embedded secure element's





Once the wallet, payment application and credentials are downloaded and bound, the mobile device may be used to make a payment.

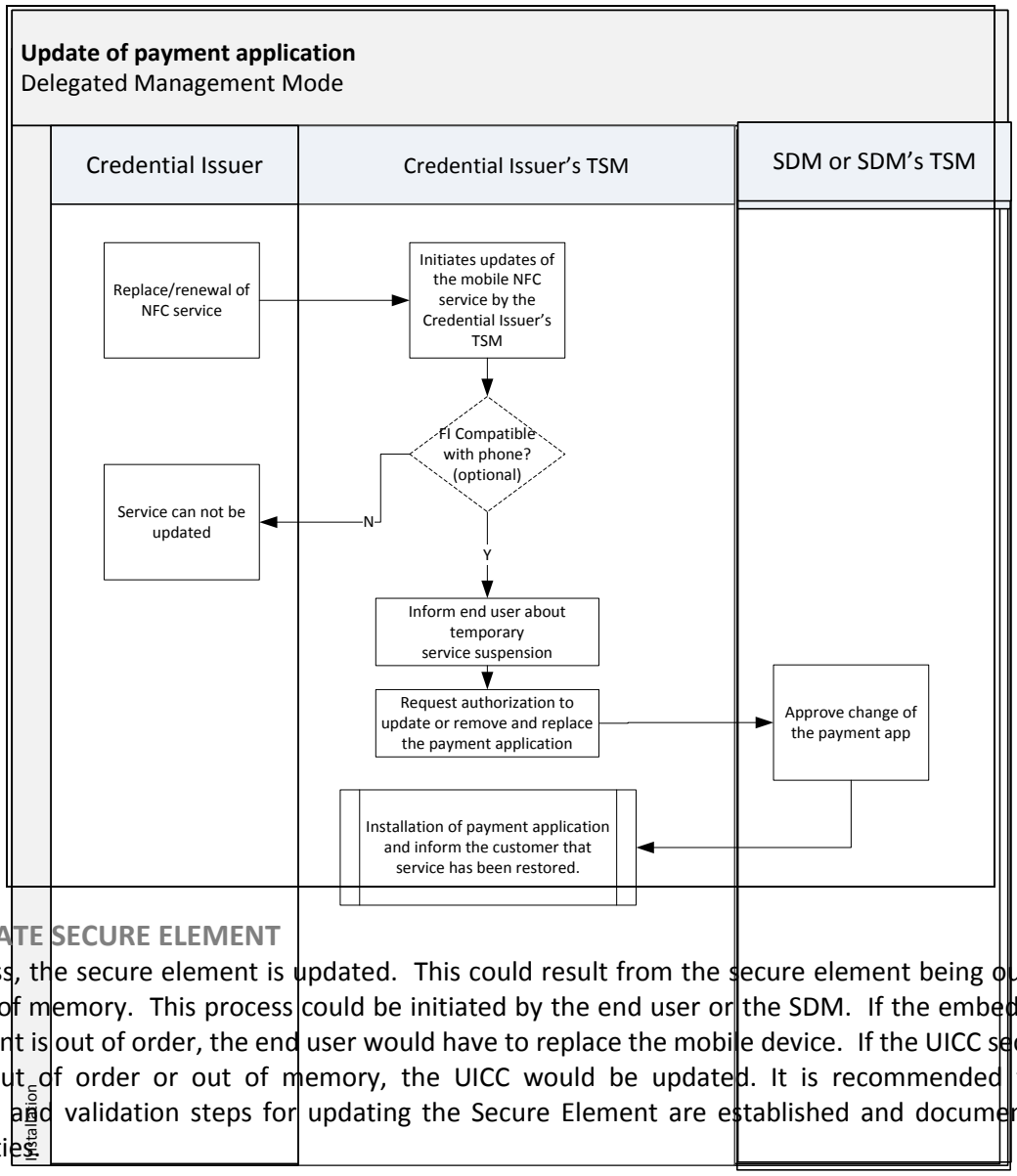
10.5 END USER SERVICING & MAINTENANCE

The End User Servicing & Maintenance section addresses significant events that could occur between when the end user enables NFC mobile payment services and when these services are disabled. This section included processes for maintenance and other lifecycle management activities. These activities will ensure that the end user is able to continue to use their mobile device for mobile NFC payments. The processes included in this section are:

- The payment application is updated
- The secure element is updated or changed
- The mobile device is changed or upgraded
- The mobile device is lost or stolen
- The mobile device is replaced

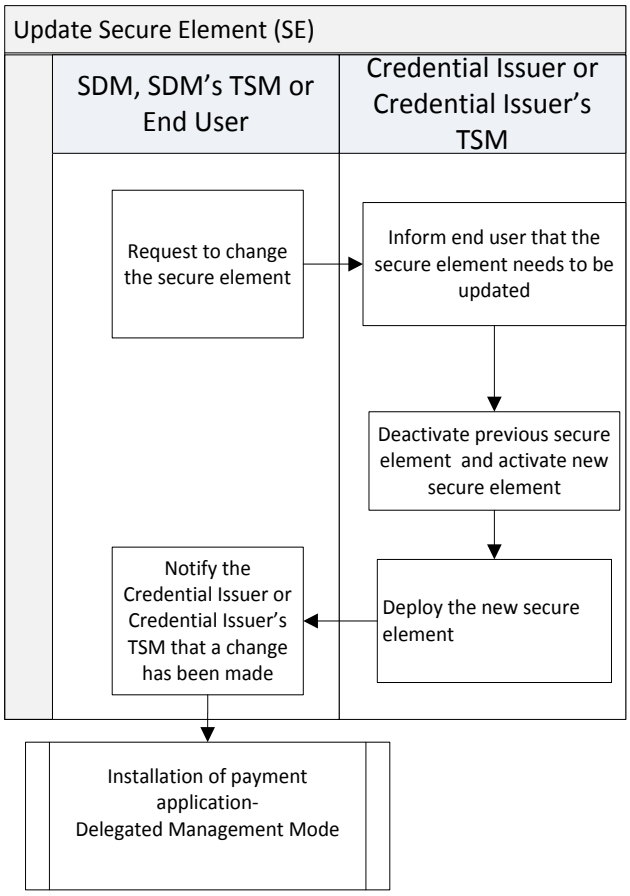
10.5.1 THE PAYMENT APPLICATION IS UPDATED

This process illustrates how a credential issuer would update the payment application for existing mobile payment users.



10.5.2 UPDATE SECURE ELEMENT

In this process, the secure element is updated. This could result from the secure element being out of order or out of memory. This process could be initiated by the end user or the SDM. If the embedded secure element is out of order, the end user would have to replace the mobile device. If the UICC secure element is out of order or out of memory, the UICC would be updated. It is recommended that responsibility and validation steps for updating the Secure Element are established and documented between parties.



Upon a secure element update requested by the SDM (or SDM's TSM), the party must contact the credential issuer's TSM to reinstall the payment application once the SE has been updated **[S67].** The payment application also needs to be personalized as part of the payment application installation process (see the above sections related to these steps).

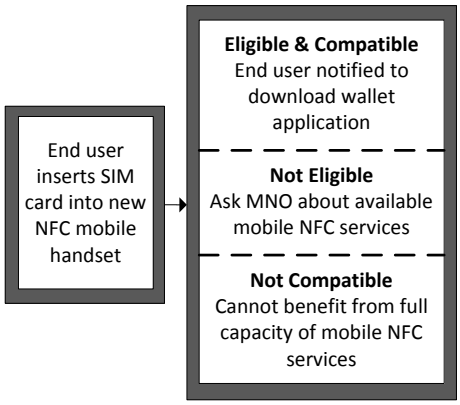
10.5.3 CHANGE MOBILE DEVICE

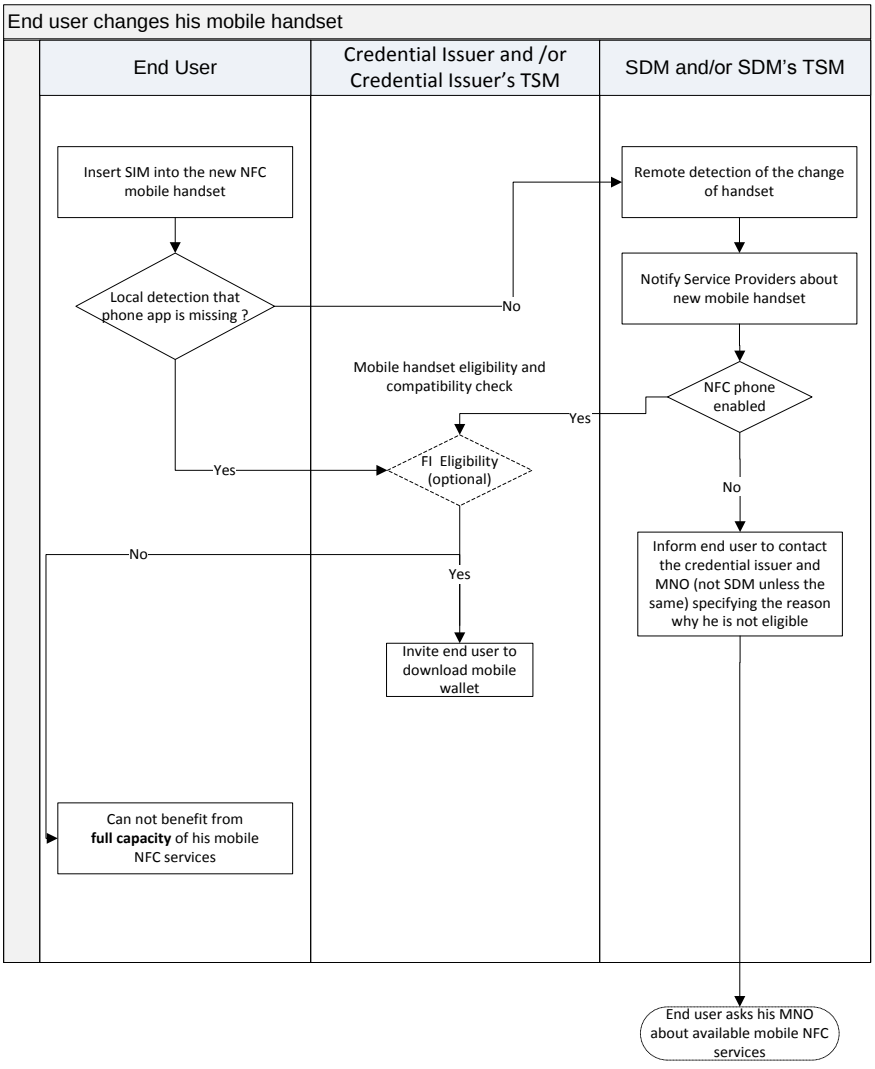
This process describes the steps that need to be followed when the end user changes their mobile device.

Change Mobile Device (Embedded SE): If the mobile payment application is stored in the embedded secure element, the end user must repeat the entire process of installing the mobile wallet and payment application (i.e. the end user, must setup a new device) **[S68].** However, if the mobile payment application is stored in the UICC, the end user needs to follow the steps below to change the mobile device:

- The UICC is transferred from the old mobile device to a new one.
- The wallet application is installed, the end user is verified and the payment application and the wallet go through the binding process.

Change Mobile Device (UICC SE): When the end user changes or adds a secondary mobile device, they must go through initial setup activities again, including end user verification and binding of the payment credential to the mobile wallet **[S69].**

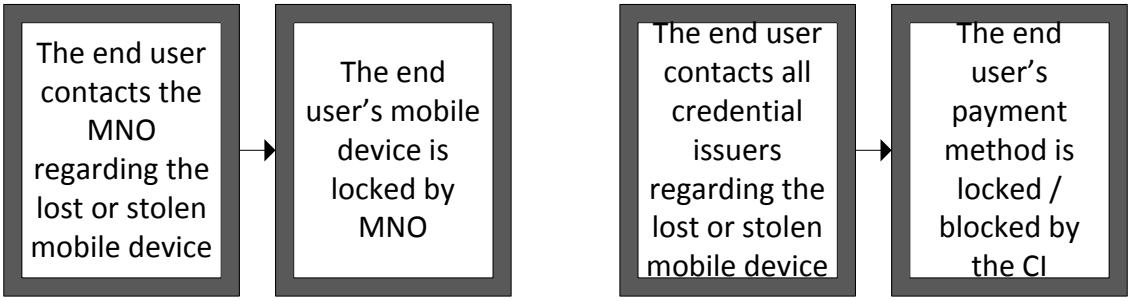


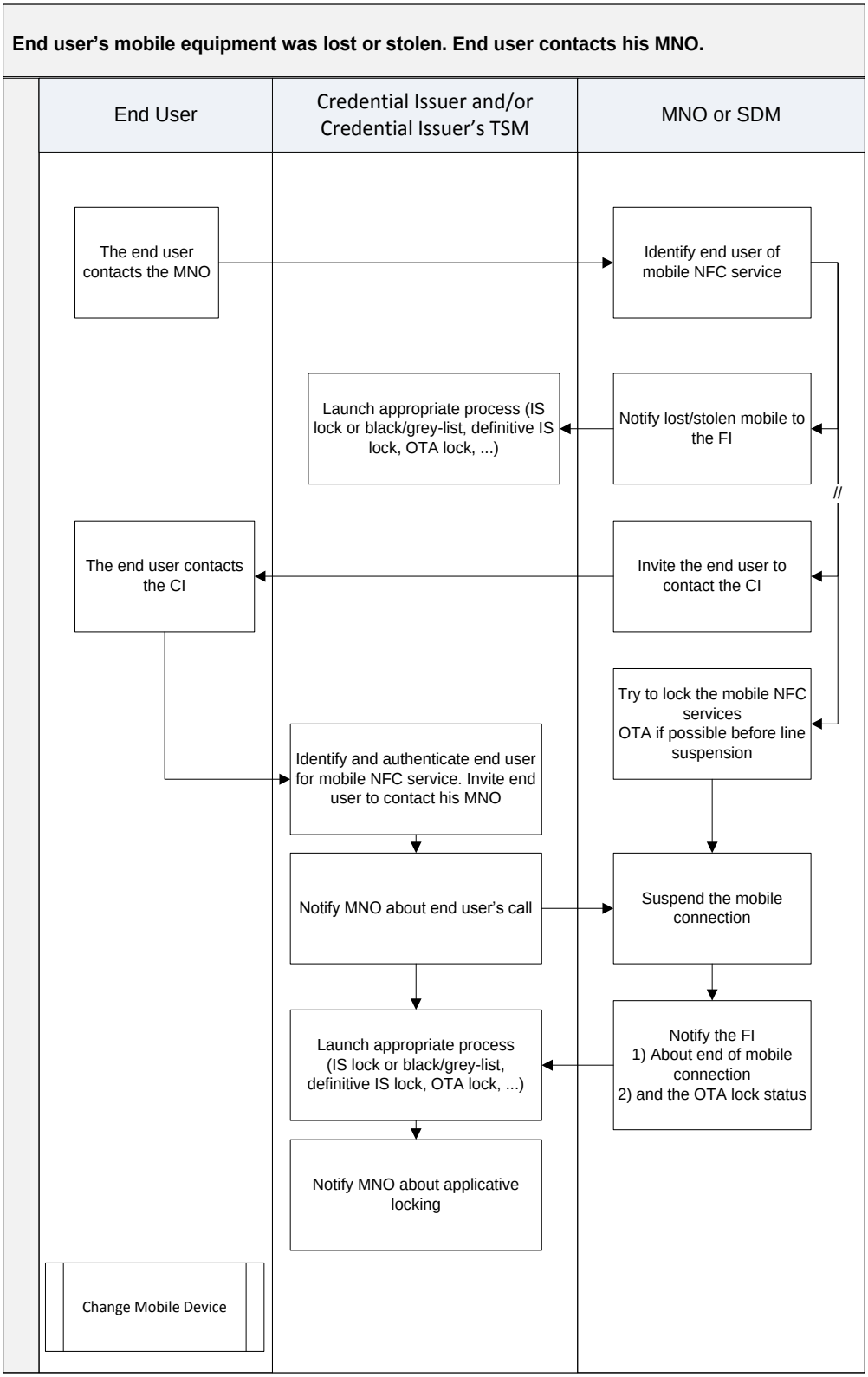


10.5.4 LOST OR STOLEN MOBILE DEVICE (USER CONTACTS MNO AND CREDENTIAL ISSUER)

This process defines the steps taken if an end user loses a mobile device with an active NFC mobile payment application.

- In the event of a lost or stolen mobile device, the end user must be instructed to contact both the MNO and the credential issuer **[S70]**.
- Once informed of a lost or stolen mobile device, the MNO or SDM (if different) must lock the mobile device – (including a SIM-lock for a SIM based mobile device or lock the secure area of the embedded element) **[S71]**.
- Once informed of a lost or stolen mobile device, the credential issuer must lock/block the payment method. (Additional internal steps may be followed which are similar to the current black listing of a card product) **[S72]**.
- Following the cancellation of service, the end user could begin the process to replace the mobile device and reinstall a wallet and payment credentials.



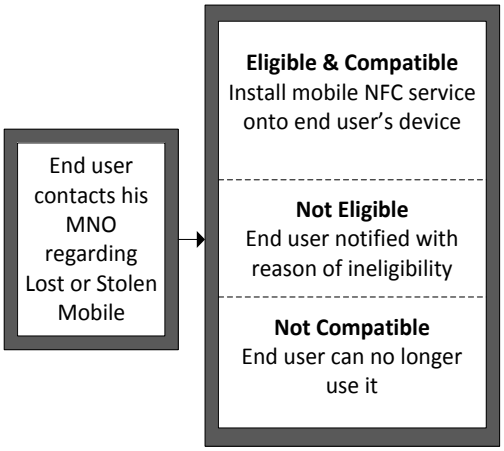

End user's mobile equipment was lost or stolen. End user contacts his MNO.
End User
Credential Issuer and/or Credential Issuer's TSM
MNO or SDM
The end user contacts the MNO
Identify end user of mobile NFC service
Launch appropriate process (IS lock or black/grey-list, definitive IS lock, OTA lock, ...)
Notify lost/stolen mobile to the FI
//
The end user contacts the CI
Invite the end user to contact the CI
Try to lock the mobile NFC services
OTA if possible before line suspension
Identify and authenticate end user for mobile NFC service. Invite end user to contact his MNO
Notify MNO about end user's call
Suspend the mobile connection
Launch appropriate process (IS lock or black/grey-list, definitive IS lock, OTA lock, ...)
Notify the FI
1) About end of mobile connection
2) and the OTA lock status
Notify MNO about applicative locking
Change Mobile Device

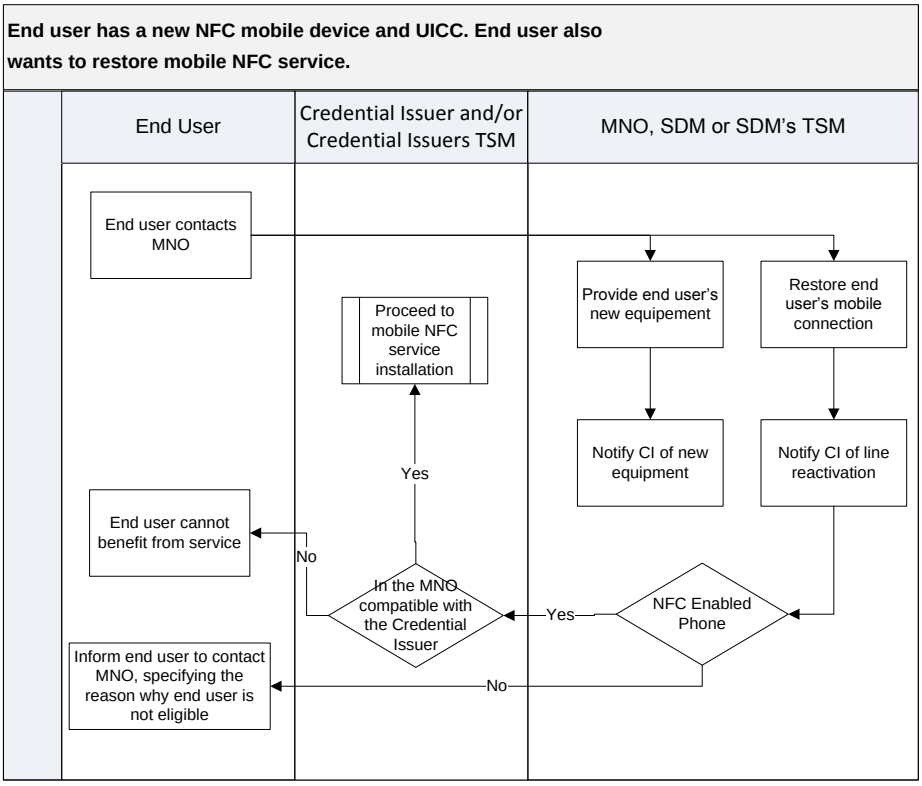
10.5.5 END USER REPLACES DEVICE (DUE TO UPGRADE OR AFTER LOSS OR THEFT)

This process defines how a new mobile device will be enabled. This upgrade could be driven by choice or by the theft or loss of a mobile device. Prior to a new mobile device being added and provisioned, the lost, stolen or old mobile device must have all payment credential information removed and positive confirmation of this action must be sent to the MNO, the SDM (if different) and the credential issuer **[S73]**.

In this process, the following will occur:

- A new mobile device is provided by the MNO or added to the MNO's network
- Mobile connectivity is provided by the MNO
- The end user requests mobile NFC payment services (following the same steps as in the initial setup process





10.6 END USER SERVICING

While active, the end user will require servicing of the payment application and support. NFC mobile payment service is complex due to the number of parties involved. In support of a positive end user servicing experience, the following responsibilities will be communicated to the end user:

10.6.1 MOBILE SERVICE AND MOBILE DEVICE

For mobile service and mobile device related issues, the end user will be instructed to contact their MNO **[S74]**. Even if service is disconnected, the payment application may continue to work for NFC payments. An agreement must be reached with the MNO or SDM to support OTA provisioning and maintenance activities even if the end users mobile service is blocked **[S75]**.

10.6.2 FAILED LOADING OF PAYMENT CREDENTIALS

For a failed loading of payment credentials, the end user will be instructed to contact the credential issuer **[S76].**

10.6.3 FAILED TRANSACTION

For a failed transaction, the end user will be instructed to contact the credential issuer of the payment instrument that is being used **[S77].**

10.6.4 ACCOUNT SERVICING

For all account servicing requests, end users will be instructed to contact the credential issuer **[S78].**

10.6.5 LOST OR STOLEN MOBILE DEVICE

For a lost or stolen mobile device, the end user must be instructed to contact both their MNO and their credential issuer(s) **[S79].**

10.6.6 BINDING ISSUES

For binding issues where the wallet is working properly but the payment application is not, the end user will be instructed to call the credential issuer **[S80].**

10.6.7 PAYMENT APPLICATION SERVICING

For issues with the payment application, the end user must contact the credential issuer **[S81].**

10.7 REMOVAL OF PAYMENT APPLICATION AND ASSOCIATED CREDENTIALS

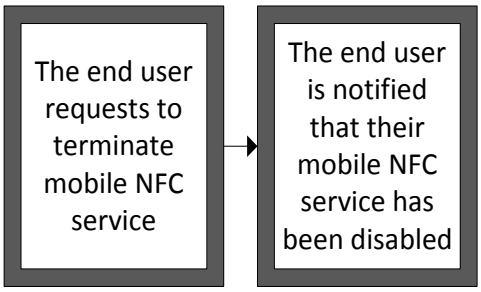
The final Enablement & Lifecycle Management area addresses closure and cancellation of service. This section describes the guidelines that are required to be followed when a mobile payment relationship is terminated. The mobile payment relationship can be terminated by the end user, the MNO or the credential issuer. This section does not distinguish differences in processes based on which ecosystem participant cancels NFC mobile services; all cancellation processes are assumed to be the same.

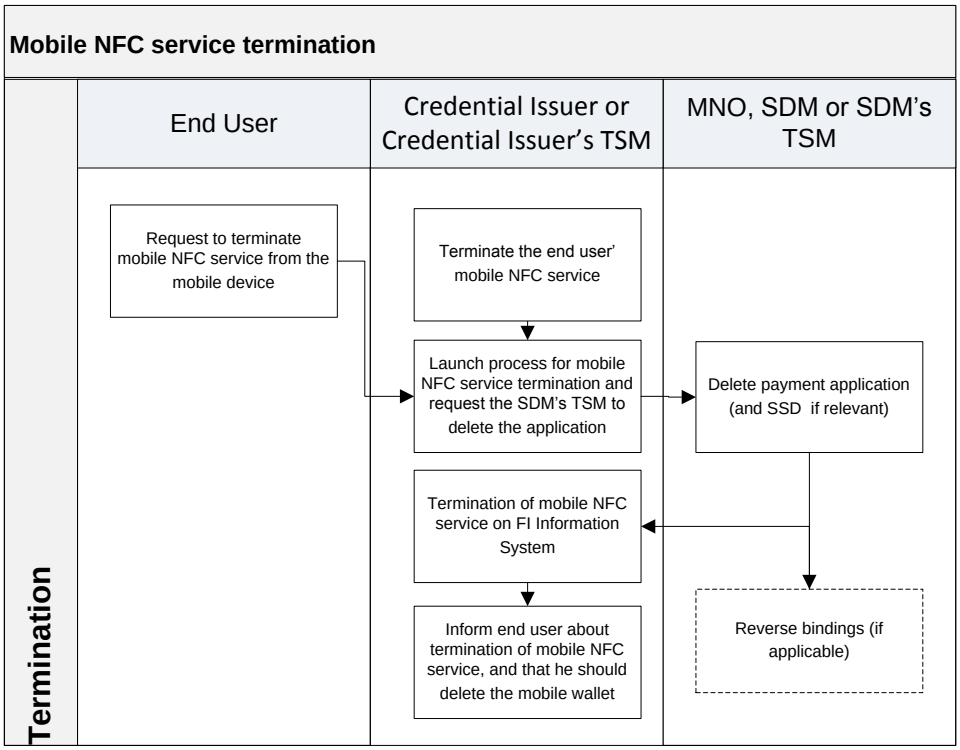
If the mobile service is terminated by the MNO, the payment application will still continue to work. Agreements must be establish between the MNO and the credential issuer establishing protocols in this situation **[S82].** While the mobile application will continue to function, it is recommended that the mobile NFC service be terminated when the MNO service is terminated and that the secure element is wiped clean by the MNO and the credential issuer is informed. Without this agreement in place, the end user could continue to use their mobile device as a payment instrument. However, the credential issuer or credential issuer's TSM would not be able to do OTA provisioning for a mobile device without an active cellular connection.

10.7.1 MOBILE NFC SERVICE TERMINATION BY CREDENTIAL ISSUER OR END USER

This scenario illustrates the termination of the mobile NFC payment service by the credential issuer or the end user.

- This process defines how the payment application and the associated credentials are securely removed from the mobile device. To terminate the business relationship, the end user would need to contact the credential issuer separately.
- This process can also be used by the credential issuer to remove the payment application and associated credentials from a mobile device for which an end user has already cancelled the payment product.





10.8 ENABLEMENT & LIFECYCLE MANAGEMENT SECTION

The Enablement & Lifecycle management section includes standards statements on downloading a mobile wallet application, procuring credentials to a mobile device and servicing those credentials throughout the end user's lifecycle.

10.9 STANDARDS STATEMENTS

Number	Statement	Section
S45	A foundational concept in this section on enablement and lifecycle management activities is that interactions between ecosystem participants (including the wallet provider and credential issuer, the credential issuer and the TSM and the Credential Issuer and the MNO) must be preceded with steps to establish contractual business relationships	10.1 Business Relationships Between Ecosystem Participants
S46	As indicated in section 6.8, all messaging must be performed under the relevant guidelines from GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0	10.2 Key Management Mode

Number	Statement	Section
S47	Those that adhere to this document agree to use only the Delegated Mode or the Dual Mode as defined by GlobalPlatform for all enablement and lifecycle management activities	10.2 Key Management Mode
S48	For proprietary wallets, secure key management processes must be established between a credential issuer, a credential issuer's TSM, a SDM's TSM and a SDM	10.2 Key Management Mode
S49	For open wallets, protocols must be established to manage key between multiple parties	10.2 Key Management Mode
S50	In this process [key management process],the credential issuer's TSM, the credential issuer, the SDM's TSM and the SDM must have an established business relationship, either directly or indirectly	10.2 Key Management Mode
S51	Key exchange must be performed under the guidelines set out by GlobalPlatform	10.2.2 Single Credential Loader
S52	[Context: When this process is complete, the key exchange will facilitate a secure data transmission channel between the credential issuer's TSM, the credential issuer and the SDM's TSM.] This secure connection must exist for over-the-air provisioning to occur	10.2.2 Single Credential Loader
S53	The credential issuers' TSMs will then go through a process of exchanging keys among themselves to ensure that they can establish a secure connections – this exchange of keys must occur to facilitate the loading of credentials into an open or collective wallet	10.2.3 Multiple Credential Loaders (Hub and Spoke)
S54	In this model, all parties must perform key exchanges under the guidelines set out by GlobalPlatform. The central authority or hub of credential issuers' TSMs must develop and make available protocols to facilitate these interactions	10.2.3 Multiple Credential Loaders (Hub and Spoke)

Number	Statement	Section
S55	The end user must be able to request the payment application installation process via a mobile wallet	10.4.1 The End User Requests Access to the Payment Application
S56	In addition to requesting payment application installation via a mobile wallet, requests may also be initiated via other channels such as a website, branch, call center or mobile banking application. Whichever method of requesting the download of the payment application and payment credentials is used, the end user must give their consent prior to installation	10.4.1 The End User Requests Access to the Payment Application
S57	For mobile wallet initiated requests, the mobile wallet must display the names of credential issuer whose credentials can be loaded into that wallet	10.4.1 The End User Requests Access to the Payment Application
S58	Prior to installing the payment application and payment credentials on the mobile device, the identity of the end user must first be validated	10.4.2 End User Validation and Verification
S59	The end user validation and verification process will differ by credential issuer. It is the responsibility of the credential issuer to define the process of end user validation and verification	10.4.2 End User Validation and Verification
S60	Following validation and verification, the credential issuer must prompt the end user with messaging confirming the next step	10.4.2 End User Validation and Verification
S61	All parties involved in this process must establish a secure communication link with the credential issuer and the SDM to effect installation of the payment application and payment credentials	10.4.3 Mobile NFC Payment Application Installation

Number	Statement	Section
S62	Once the secure connection is established, the TSM must handle all activities including installation and activation of the mobile NFC service	10.4.3 Mobile NFC Payment Application Installation
S63	Binding must occur for a mobile wallet to access a payment application	10.4.4 Mobile Wallet and Payment Application Binding
S64	The umbrella application serves as a directory for the UICC and must be provided by the SDM	10.4.5 Secure Element on the UICC
S65	[Context: The umbrella application then informs the wallet application of where the payment application is stored and provides an identifier by which to locate the payment application.] The construct of the identifier must be provided by the SDM	10.4.5 Secure Element on the UICC
S66	Payment credentials are stored on the mobile device and must be able to be installed and updated over-the-air	10.4.7 OTA Provisioning of Credentials
S67	Upon a secure element update requested by the SDM (or SDM's TSM), the party must contact the credential issuer's TSM to reinstall the payment application once the SE has been updated	10.5.2 Update the Secure Element
S68	Change Mobile Device (Embedded SE): If the mobile payment application is stored in the embedded secure element, the end user must repeat the entire process of installing the mobile wallet and payment application (i.e. the end user, must setup a new device)	10.5.3 Change Mobile Device

Number	Statement	Section
S69	Change Mobile Device (UICC SE): When the end user changes or adds a secondary mobile device, they must go through initial setup activities again, including end user verification and binding of the payment credential to the mobile wallet	10.5.3 Change Mobile Device
S70	In the event of a lost or stolen mobile device, the end user must be instructed to contact both the MNO and the credential issuer	10.5.4 Lost or Stolen Mobile Device
S71	Once informed of a lost or stolen mobile device, the MNO or SDM (if different) must lock the mobile device – (including a SIM-lock for a SIM based mobile device or lock the secure area of the embedded element)	10.5.4 Lost or Stolen Mobile Device
S72	Once informed of a lost or stolen mobile device, the credential issuer must lock/block the payment method. (Additional internal steps may be followed which are similar to the current black listing of a card product)	10.5.4 Lost or Stolen Mobile Device
S73	Prior to a new mobile device being added and provisioned, the lost, stolen or old mobile device must attempt to have all payment credential information removed and positive confirmation of this action must be sent to the MNO, the SDM (if different) and the credential issuer	10.5.5 End User Replaces Device
S74	For mobile service and mobile device related issues, the end user will be instructed to contact their MNO	10.6.1 Mobile Service and Mobile Device
S75	An agreement must be reached with the MNO or SDM to support OTA provisioning and maintenance activities even if the end users mobile service is blocked	10.6.2 Failed Loading of Payment Credentials
S76	For a failed loading of payment credentials, the end user will be instructed to contact the credential issuer	10.6.3 Failed Transaction

Number	Statement	Section
S77	For a failed transaction, the end user will be instructed to contact the credential issuer of the payment instrument that is being used	10.6.3 Failed Transaction
S78	For all account servicing requests, end users will be instructed to contact the credential issuer	10.6.4 Account Servicing
S79	For a lost or stolen mobile device, the end user must be instructed to contact both their MNO and their credential issuer(s)	10.6.5 Lost or Stolen Mobile Device
S80	For binding issues where the wallet is working properly but the payment application is not, the end user will be instructed to call the credential issuer	10.6.6 Binding Process
S81	For issues with the payment application, the end user must contact the credential issuer	10.6.7 Payment Application Servicing
S82	If the mobile service is terminated by the MNO, the payment application will still continue to work. Agreements must be establish between the MNO and the credential issuer establishing protocols in this situation	10.7 Removal of the Payment Application and Associated Credentials

11 LOYALTY & REWARDS

Loyalty & Rewards is a rapidly evolving space. Instead of establishing strict standards statements, this document instead established guidelines. Much of this section is dedicated to developing a common understanding of the current marketplace and the role of loyalty and rewards in the future of mobile payments.

The Loyalty & Rewards section includes the following sub sections:

- Overview of Loyalty
- POS Interaction
- Redemption (Loyalty Programs, Coupons, Vouchers and Incentives)
- Summary of Standards for Loyalty & Rewards

This document examines the types of loyalty programs that are available and those that could be integrated with NFC mobile payments, data standards for loyalty, rewards, coupons, vouchers and incentives and the end user experience for POS loyalty interaction.

11.1 OVERVIEW OF LOYALTY

11.1.1 OVERVIEW OF LOYALTY PROGRAMS

There are several loyalty programs currently in the marketplace. Each loyalty program has differing funding and redemption implications.

The below tables outline the various types of loyalty programs offered. The purpose of this section is to provide insight into the current loyalty and rewards environment and to suggest implications for the integration of loyalty and rewards programs with mobile payments.

11.1.2 LOYALTY PROGRAMS ANALYSIS

This section provides an overview of loyalty programs. Each of these programs is candidates for inclusion into a mobile wallet.

Types of Loyalty Programs	Description	Program Economics
Premier Merchant Funded Programs	This is a program that is offered in conjunction with credit or debit product offerings. In this program, the end users receive bonus points or cash back at participating merchants. These programs are typically offered for a short period of time.	Discounts are typically funded by merchants. Associated points and cash back are usually funded by the payment product issuers.
Payment Product Based Bonus Points and Cash-Back Programs	This is a program that is usually offered by the payment product issuer. This is typically an ongoing program where end users receive points or cash back for the payment	These programs are funded by payment product issuers to incentives spend.

Types of Loyalty Programs	Description	Program Economics
	product issuer.	
Member Coalition Programs	Both ongoing and one-time promotions where end users register payment products to receive discount and earn points at participating merchants. Program owners include membership organizations, payment networks and loyalty processors.	These programs are typically funded by merchants or manufacturers.
Online-Only Merchant-Funded Programs	Ongoing programs where end users receive points or cash back for using a payment product at specific online merchants.	These programs are typically funded by the merchant or manufacturer.
Merchant-Funded Discount Program	One-time promotions in the form of online discounts and in-store coupons. These programs are typically offered by payment product issuers, payment networks, or membership based organization.	These programs are typically funded by the merchant or manufacturer.
Proprietary Merchant Program	Ongoing and one-time promotions sponsored by merchant. These are programs that are not tied to a payment product and do not require financial institution involvement.	These programs are entirely funded by the merchant.

As outlined in the above table, each loyalty program has various stakeholders involved, introducing different ways of managing the redemption process. Due to the nature of these loyalty programs, only a few are to be considered from a POS interaction and redemption perspective on a mobile NFC service.

The programs considered to be good candidates for NFC payments include those programs which are integrated with payment products:

- Premier Merchant Funded Programs
- Payment Based Bonus Points and Cash-Back Programs
- Member Coalition Programs

These programs have a direct point of sale interaction component and a payment product component. The other programs excluded from this list do not meet these criteria.

11.1.3 OVERVIEW OF COUPONS, VOUCHERS AND INCENTIVES

This section examines the concept of couponing. Couponing is a way for a merchant or manufacturer to drive sales. It is anticipated that once coupons, vouchers and other sales incentives are incorporated into mobile devices, a significant amount of value will be created for the end user and for the merchants.

As mobile devices have become increasingly popular, marketers have sought new ways to integrate coupons into mobile devices. As such, there are several services available to end users that will make it easy to collect and redeem coupons via the end user's mobile device.

The below table outlines the various types of coupons, vouchers and incentive programs offered in the marketplace.

11.1.4 COUPONS, VOUCHERS AND INCENTIVES ANALYSIS

This section provides an overview of loyalty programs; these programs are candidates for inclusion into a mobile wallet.

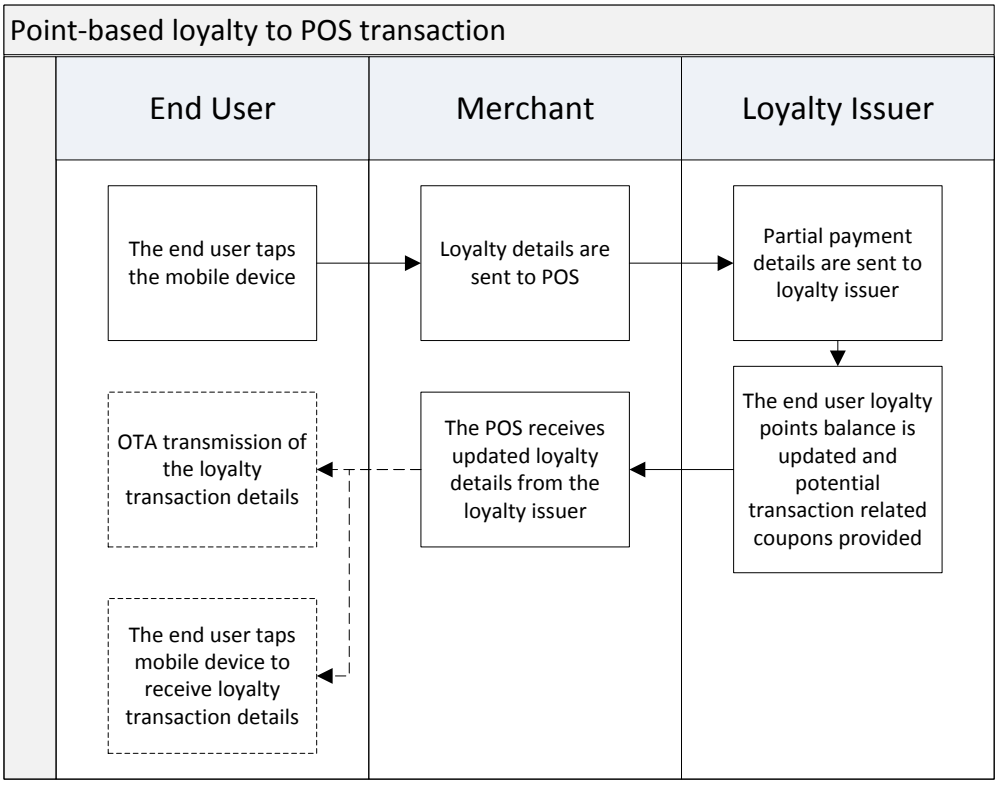
Coupon and Voucher Type	Type	Funding
Discount /Rebate	Discount and rebates are deducted from the cost of an item or a total purchase. Discounts are applied pre-payment and rebates are typically post-payment.	Discount and rebates are funded by merchants or manufacturers.
Buy One Get N Free	This is typically a merchant or manufacturer funded offer to incentivize purchased of goods or services.	Typically these are manufacturer or retailer funded offers.
Membership	Discounts are offered only to members of an organization, (e.g. wholesale clubs)	Discounts are usually funded by manufacturers or merchants.
Complimentary Promotion (e.g. item, shipping, tax)	Extra goods or services are usually added to the primary good or service that the end user purchase.	These are typically merchant and manufacturer funded programs.

11.2 LOYALTY POS INTERACTION

The POS communication between the POS terminal and mobile devices is another area that requires specific standards. This section reviews the various processes and guiding principles behind the POS integration and the Coupon, Voucher, Incentive redemption process. The POS systems are encouraged to receive and process the loyalty details from the end user's mobile device. If the merchant decides to accept NFC transmission of loyalty services, this section establishes guidelines and standards to follow.

11.2.1 POS INTERACTION PROCESS MAP

The following process map outlines how loyalty is transferred between the end user, merchant and loyalty issuer. The end user leverages standard payment methods (e.g. Visa, MasterCard) and provides their loyalty point payment product to receive the point balance. Based on the preferences set in the mobile wallet, the end user may receive coupons related to this transaction for future uses.



Depending on the mobile payment method for receiving electronic receipts, the loyalty transaction details will be sent over-the-air or when the end user taps the mobile device.

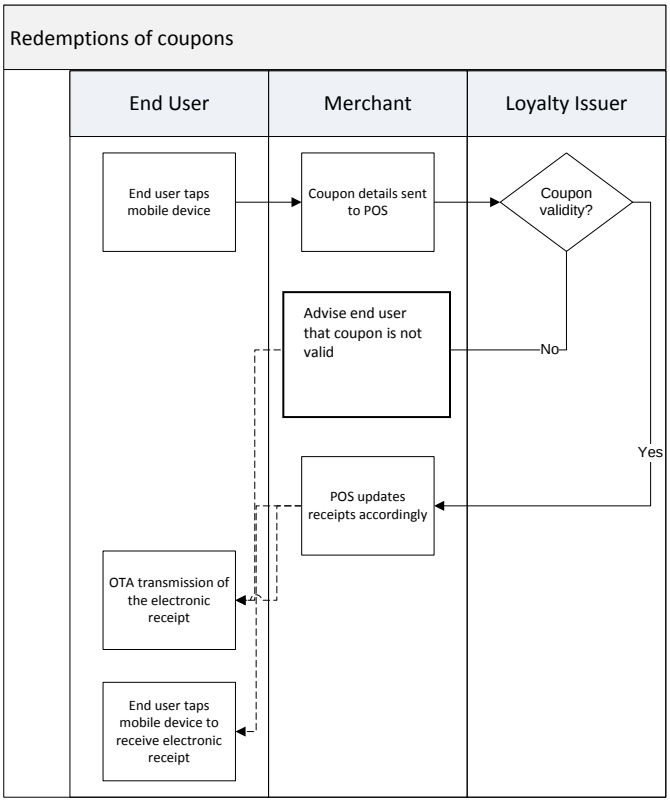
11.2.2 ANALYSIS OF LOYALTY POS INTERACTION EXPERIENCE

The following section compares the conventional loyalty experience with that of the loyalty experience using an NFC enabled mobile device. The NFC loyalty experience can offer a far richer experience for the end user.

Loyalty Experience	Current Interaction Experience	Mobile Interaction Experience	Implications
Redemption of Loyalty Program Points for a Purchase	The end user pays with the loyalty product and the payment product issuer credits the account in the back end using the loyalty points system.	The loyalty program details are integrated into the mobile wallet and are sent to the POS at the time of purchase.	The POS must be able to extract and process the loyalty details during the payment transaction.

11.2.3 COUPON, VOUCHER & INCENTIVES REDEMPTION PROCESS MAP

The coupon is sent during the payment steps and it is applied to final price balance.



Depending on the mobile payment method for receiving electronic receipts, the updated electronic receipts will be sent over-the-air or when the end user taps the mobile device.

11.2.4 ANALYSIS OF COUPONS, VOUCHERS AND INCENTIVES - POS INTERACTION

Incentive Type	Current Interaction Experience	Mobile Interaction Experience	Implications

Incentive Type	Current Interaction Experience	Mobile Interaction Experience	Implications
Discount /Rebate and BOGO and Complimentary tax rebate	The end user is provided with a paper-based coupon. The POS scans the coupon and the total price is adjusted.	The end user pays with the mobile device. The mobile wallet looks up the coupons that can be applied to the transaction and sends these coupons to the POS. Prior to the end user updating the payment method on their mobile device, the POS needs to extract and process the coupons from the payment transaction. Once all coupons have been processed, the payment is made.	The POS must extract the coupons and process the coupons prior to the payment. Without requiring the user to tap multiple times.

There are some standards and guidelines from the implications illustrated above:

Coupons and vouchers that are stored in the mobile wallet and that interact and transmit information to the NFC POS through NFC or other transmission methods, (e.g. barcode) must follow relevant standards in this document **[S83]**. The Merchant POS should be able to process coupons and vouchers transmitted by the NFC or other transmission methods and apply appropriate discounts for the end user.

11.2.5 POS TECHNOLOGIES

Protocols have been established for transmission of loyalty and coupon information, between the POS and the mobile device. ISO/IEC 14443 is an international standard that defines proximity cards used for identification and the transmission protocols for communicating. ISO/IEC 14443 must be used to transmit loyalty and reward information from the mobile device to the POS using NFC **[S84]**.

By reaffirming ISO/IEC 14443 as the standard for loyalty transmissions in Canada, this document seeks to limit the impact on merchants. Merchants would still need to make updates to the POS to appropriately route the loyalty transaction. However, using ISO/IEC 14443 as a standard will limit merchant hardware upgrade costs and employee retraining costs.

Several services exist which support transmission of mobile NFC services, these include: MiFare, FeliCa and Calypso. While this document does not directly promote any of these services, those organizations interested in offering loyalty and rewards services via the mobile device are encouraged to review these offering and the architecture.

11.3 REDEMPTION

Loyalty redemption is the process of rewarding end users for their loyalty by giving value back in the form of points, coupons or incentives. NFC mobile payments provides an opportunity to streamline the redemption process.

In this section, the current redemption experience will be described in detail with respect to the various loyalty programs, coupons, vouchers and incentives. After establishing an understanding of the current landscape for redemption, the experience from a mobile NFC perspective will be illustrated along with the implications necessary to roll out the redemption experience.

The redemption of loyalty points can traditionally be done in the following three ways:

- **Automatic Redemption:** The payment is made with the end user's loyalty points (assuming the balance is sufficient to cover the cost of the purchase).
- **End User Initiated Redemption:** Before a payment is made, the end user checks their point balance and chooses to pay with their loyalty points.
- **Merchant Initiated Redemption:** The end user attempts to pay with their standard payment method and the merchant advises that the end user has sufficient points. The end user chooses points or cash as the payment method.

11.3.1 ANALYSIS OF LOYALTY REDEMPTION EXPERIENCE

Type	Current Redemption Experience	Mobile NFC Redemption Experience	Implications
Premier Merchant-Funded Program	End user redeems their points for selected merchandise, flights, hotels, etc at the POS through the loyalty program website Points can fully or partially pay for the cost of the purchase.	End user pays with the mobile device and selects their card from their mobile wallet to receive instant redemption on their purchase using points that they have earned.	End user may need to select the option of paying with their points at the POS to initiate the redemption process.
Traditional FI bonus points and cash-back program	End user redeems their points or cash back amount either at the end of their billing cycle or end of year. Redemption is done automatically by the FI either through a deduction on the bill or a check at the end of the year.	At the end of the billing cycle, end user will receive an updated balance on their mobile wallet with the cash back reward.	No changes would be required when enabling this loyalty redemption experience on a mobile NFC service as it's managed by the back-end of the FI.
Member Coalition	End user receives a	End user pays with the	End user may need an

Type	Current Redemption Experience	Mobile NFC Redemption Experience	Implications
and Registered Program	discount for their purchase upon displaying the program information to the merchant.	mobile device using their mobile wallet and receives instant redemption on their purchase automatically.	additional tap to initiate the instant redemption process with the merchant unless there's a two way connection established.
Merchant-funded Discount Program	End user redeems their points for selected merchandise, flights, hotels etc at the point of sale through the loyalty program website. End user can alternatively redeem points at the merchant store when making their purchase. Points can fully or partially pay for the cost of the total purchase.	End user pays with the mobile device and selects their payment product from their mobile wallet to receive instant redemption on their purchase using points that they've earned.	End user may need to select the option of paying with their points at the point of sale to initiate the redemption process.
Proprietary merchant program	End user redeems their points for any merchandise available at participating stores at the point of sale Points can fully or partially pay for the cost of the total purchase.	End user pays with the mobile device and selects their payment product from their mobile wallet to receive instant redemption on their purchase using points that they've earned.	End user may need to select the option of paying with their points at the point of sale to initiate the redemption process.

Instant redemption of loyalty programs at the POS (i.e. using loyalty as currency) is an optional service offered at the discretion of ecosystem participants. If loyalty and rewards are offered as a form of currency, the loyalty and rewards credentials should be treated as payment credentials and securely provisioned and stored on the mobile device **[S85]**. For instant loyalty redemption, the end user must be required to choose to present loyalty points as a form of payment by selecting the loyalty program in the mobile wallet **[S86].**

11.3.2 ANALYSIS OF COUPON, VOUCHER & INCENTIVES REDEMPTION EXPERIENCE

	Current Redemption Experience	Mobile NFC Redemption Experience	Implications
Coupon, Voucher & Incentives	End User presents the coupon to the merchant The merchant scans it and the POS processes it.	The coupons are stored in the mobile wallet. The coupons are sent to the POS during the payment transaction.	Coupon integration into the mobile wallet would be required. The POS would be updated to process coupons sent during the payment transaction.

Coupons and vouchers should have the option (at the consent of the end user) to be automatically redeemed by the mobile wallet and integrated to the payment transaction.

11.4 LOYALTY & REWARDS SECTION SUMMARY

The loyalty and rewards section evaluates loyalty and rewards offers and the potential integration of these offers with NFC mobile payments. This section provides very few standards statements. Instead, the goal is to provide recommendations for implementing a loyalty and rewards solution.

This is a rapidly evolving space. As the ecosystem develops, loyalty and rewards standards will need to evaluated and updated.

The next and final section establishes Data & Security standards for all areas of mobile payments, including loyalty and rewards.

11.5 STANDARDS STATEMENTS

Number	Statement	Section
S83	Coupons and vouchers that are stored in the mobile wallet and that interact and transmit information to the NFC POS through NFC or other transmission methods, (e.g. barcode) must follow relevant standards in this document	11.2.4 Analysis of Coupons, Vouchers and Incentives - POS Interactions
S84	ISO/IEC 14443 is an international standard that defines proximity cards used for identification and the transmission protocols for communicating. ISO/IEC 14443 must be used to transmit loyalty and reward information from the mobile device to the POS using NFC	11.2.5 POS Technologies

Number	Statement	Section
S85	If loyalty and rewards are offered as a form of currency, the loyalty and rewards credentials should be treated as payment credentials and securely provisioned and stored on the mobile device	11.3.1 Analysis of Loyalty Redemption Experience
S86	For instant loyalty redemption, the end user must be required to choose to present loyalty points as a form of payment by selecting the loyalty program in the mobile wallet	11.3.1 Analysis of Loyalty Redemption Experience

12 DATA & SECURITY

The Data & Security section was designed around the general guideline that each ecosystem participant should only have access to the minimum information required to perform its primary role. The default for ecosystem participants should be to protect end user and merchant data. Access to and usage of data must be disclosed to the end user and the end users permission explicitly granted **[S87]**. Per S9, the credential issuer must also explicitly grant permission to use data. As indicated, S9 applies to this entire document.

12.1 DATA

Mobile wallets are a relatively new construct in the payment ecosystem. The ecosystem is expected to evolve. There are many new wallet providers who are developing mobile payment wallets and deploying them for end users. To be a part of a safe and secure payment ecosystem it is very important that the mobile wallet be compliant with payment industry guidelines. A key part of the guidelines and safety and security is what data can and cannot be captured by the mobile wallet. This section looks at the different kinds of data and draws standards on who has access to what information.

Beyond the stated data guidelines in this section, all mobile wallets will have to be PCI – DSS compliant and adhere to the PCI DSS guidelines. In case of a conflict, the stronger standard will prevail.

12.1.1 ACCESS TO WALLET DATA

This section outlines which ecosystem participants may have access different types of wallet information:

Data Types	Credential Issuer	Wallet Provider	Merchant	End User	MNO or SDM	Loyalty Issuer	Other Apps
Payment Products in Wallet	NO	YES[11]	NO	YES	NO	NO	NO
Loyalty Products in Wallet	NO	YES[12]	NO	YES	NO	NO	NO
Coupons in Wallet	NO	YES	NO	YES	NO	NO	YES

- **Payment Products in Wallet** – Only the **wallet provider** and the **end user** may access the **list of payment products** that are in a wallet, all others must not have access to the **list of payment products [S88]**. The wallet provider's access to **payment product** information must be restricted to only the information that is needed to service the wallet **[S89]**.
- **Loyalty Products in Wallet** – Only the **wallet provider** and the **end user** may access the **list of loyalty products** that are in a wallet, all others must not have access to the **list of loyalty products [S90].** The wallet provider's access to **loyalty product information** must be restricted to only the information that is needed to service the wallet **[S91]**.
- **Coupon in Wallet** – Only the **wallet provider**, the **end user** and **other end user approved loyalty applications** may access the **list of coupons** that are in a wallet, all others must not have access to the **list of coupons [S92].**

The above is based on the concept that only the end user and those that they explicitly give their consent to may access information in the wallet. This includes information such as how many and the type of payment products that a user has.

[11] Only the issuers of encrypted credentials have access to this information. The wallet provider may only have access to the minimum information to service products; additional awareness at the explicit consent of issuer and end user.

[12] Only the issuers of encrypted credentials have access to this information. The wallet provider may only have access to the minimum information to service products; additional awareness at the explicit consent of issuer and end user.

12.1.2 ACCESS TO CREDENTIAL DATA

This section outlines which ecosystem participants may have access to credential information, regardless of where this information is stored:

Data Types	Credential Issuer	Wallet Provider	Merchant	End User	MNO or SDM	Loyalty Issuer	Other Apps
Payment Product, Non-Encrypted Data	YES	NO	YES[13]	YES	NO	NO	NO
Payment Product, Encrypted Data	YES	NO	NO	NO	NO	NO	NO
Loyalty Credentials, Non-Encrypted Data	NO	NO	YES[14]	YES	NO	YES	NO
Loyalty Credentials, Encrypted Data	NO	NO	NO	NO	NO	YES	NO

- **Payment Product, Non-Encrypted Data** – Only the **credential issuer**, **merchants** and the **end user** may access **non-encrypted payment product data**; all others must not have access to **-encrypted payment product data [S93]**. Examples of Financial Non-Encrypted payment product details are: credit card number, name on credit card and CVV2. Merchants may only access this information as needed to process a payment. Merchant capture and storage of **non-encrypted payment product data** must be in line with payment network guidelines **[S94]**.
- **Payment Product, Encrypted Data** – Only the **credential issuer** may access **encrypted payment product data**, all others must not have access to **encrypted payment product data [S95]**.

[13] See clarification in the standards statement
[14] See clarification in the standards statement

- **Loyalty Credentials, Non-Encrypted Data** – Only the **loyalty issuer**, **merchants** and the **end user** may access n**on-encrypted loyalty credential data**; all others must not have access to n**on-encrypted loyalty credential data [S96]**. Merchant capture and storage of **non-encrypted loyalty credential data** must be consistent with the same care given to payment credentials and must only be used for rewarding or redeeming loyalty points **[S97]**.
- **Loyalty Credentials, Encrypted Data** – If loyalty points may be used for POS redemption, only the **loyalty issuer** may access **encrypted loyalty credential data**, all others must not have access to **encrypted loyalty credential data [S98]**.

12.1.3 ACCESS TO FINANCIAL DATA

This section outlines which ecosystem participants may have access financial transaction data:

Data Type	Acquirer	Credential Issuer	Wallet Provider[15]	Merchant	End User	MNO or SDM	Loyalty Issuer	Other Apps
Amount	YES	YES	NO	YES	YES	NO	NO	NO
Time	YES	YES	NO	YES	YES	NO	NO	NO
Merchant	YES	YES	NO	YES	YES	NO	NO	NO
Product (i.e. Which Credential)	YES	YES	NO	YES	YES	NO	NO	NO
Location	YES	YES	NO	YES	YES	NO	NO	NO
Transaction Details	NO	NO	NO	YES	YES	NO	NO	NO
Electronics Receipt	NO	NO	NO	YES	YES	NO	NO	NO

**Please note that S9 applies to this entire section

- **Financial Data, Amount** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **amount of a transaction**, all others must not have access to the **amount of a transaction [S99].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **amount of a transaction [S100]**.
- **Financial Data, Time** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **time of a transaction**, all others must not have access to the **time of a transaction [S101].** The wallet may collect and store this information for the end user but this

[15] See clarification in the standards statement

information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **time of a transaction [S102]**.

- **Financial Data, Merchant** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **merchant for a transaction**, all others must not have access to the **merchant for a transaction [S103].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **merchant for a transaction [S104]**.
- **Financial Data, Product** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **product used for a transaction**, all others must not have access to the **product used for a transaction [S105].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **product used for a transaction [S106]**.
- **Financial Data, Location** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **location of a transaction**, all others must not have access to the **location of a transaction [S107].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **location of a transaction [S108]**.
- **Financial Data, Transaction Details** – Only the **merchant** and **end user** may access the **transaction details** of a transaction (e.g. SKU level information), all others must not have access to the **transaction details [S109].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **transaction details [S110]**.
- **Financial Data, Electronic Receipts** – Only the **merchant** and **end user** may access the **electronic receipts** for a transaction, all others must not have access to the **electronic receipts [S111].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **electronic receipts [S112]**.

12.1.4 ACCESS TO LOYALTY DATA

This section outlines which ecosystem participants may have access loyalty transaction data:

Data Type	Acquirer	Credential Issuer	Wallet Provider[16]	Merchant	End User	MNO or SDM	Loyalty Issuer	Other Apps
Amount	YES	NO	NO	YES	YES	NO	YES	NO
Time	YES	NO	NO	YES	YES	NO	YES	NO
Merchant	YES	NO	NO	YES	YES	NO	YES	NO
Product (i.e. Which Credential)	YES	NO	NO	YES	YES	NO	YES	NO
Location	YES	NO	NO	YES	YES	NO	YES	NO
Transaction Details	NO	NO	NO	YES	YES	NO	NO	NO
Electronics Receipt	NO	NO	NO	YES	YES	NO	NO	NO

**Please note that S9 applies to this entire section

- **Loyalty Data, Amount** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **amount of a loyalty transaction**, all others must not have access to the **amount of a loyalty transaction [S113].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **amount of a loyalty transaction [S114]**.
- **Loyalty Data, Time** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **time of a loyalty transaction**, all others must not have access to the **time of a loyalty transaction [S115].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **time of a loyalty transaction [S116]**.

[16] See clarification in the standards statement

- **Loyalty Data, Merchant** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **merchant for a loyalty transaction**, all others must not have access to the **merchant for a loyalty transaction [S117].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **merchant for a loyalty transaction [S118]**.
- **Loyalty Data, Product** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **product used for a loyalty transaction**, all others must not have access to the **product used for a loyalty transaction [S119].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user gives their explicit permission to share the **product used for a loyalty transaction [S120]**.
- **Loyalty Data, Location** – Only the **acquirer**, **credential issuer**, **merchant** and **end user** may access the **location of a loyalty transaction**, all others must not have access to the **location of a loyalty transaction [S121].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **location of a loyalty transaction [S122]**.
- **Loyalty Data, Transaction Details** – Only the **merchant** and **end user** may access the **transaction details of a loyalty transaction** (e.g. SKU level information), all others must not have access to the **transaction details of a loyalty transaction [S123].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **transaction details of a loyalty transaction [S124]**.
- **Loyalty Data, Electronic Receipts** – Only the **merchant** and **end user** may access the **electronic receipts for a loyalty transaction**, all others must not have access to the **electronic receipts for a loyalty transaction [S125].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **electronic receipts for a loyalty transaction [S126]**.

12.1.5 PAYMENT PRODUCT AND LOYALTY BALANCE AND ACCOUNT INFORMATION

This section outlines which ecosystem participants may have access to payment product and loyalty and reward account information:

Data Type		Credential Issuer	Wallet Provider[17]	Merchant	End User	MNO or SDM	Loyalty Issuer	Other Apps
Payment Product	**Balance**	YES	NO	NO	YES	NO	NO	NO
	Account Details	YES	NO	NO	YES	NO	NO	NO
Loyalty Product	**Balance**	NO	NO	NO[18]	YES	NO	YES	NO
	Account Details	NO	NO	NO[19]	YES	NO	YES	NO

**Please note that S9 applies to this entire section

- **Payment Product, Balance Information** – Only the **credential issuer** and the **end user** may access the **payment product balance** information, all others must not have access to the **payment product balance [S127].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **payment product balance [S128]**.
- **Payment Product, Account Details** – Only the **credential issuer** and the **end user** may access the **payment product account detail information**, all others must not have access to the **payment product account detail information [S129].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the **payment product account detail information [S130]**.
- **Loyalty Product, Balance Information** – Only the **loyalty issuer** and the **end user** may access the **loyalty product balance information**, all others must not have access to the **loyalty product balance information [S131].** The wallet may collect and store this information for

[17] See clarification in the standards statement
[18] Yes only for redemption
[19] Yes only for redemption

the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **loyalty product balance information [S132]**.

- **Loyalty Product, Account Information** – Only the **loyalty issuer** and the **end user** may access the **loyalty product account detail information**, all others must not have access to the **loyalty product account detail information [S133].** The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the **loyalty product account detail information [S134]**.

12.2 FRAUD, MALWARE AND SECURITY

Fraud and security are serious concern with mobile payments. While this document does not include any specific standards on fraud and security, it is recommended that each ecosystem participant put processes in place to track, monitor and mitigate fraud and security concerns including malware, hacking and theft of mobile devices.

Ecosystem participants are encouraged to work together to combat risk to the safety and security of the mobile payments ecosystem.

12.3 DATA & SECURITY SECTION SUMMARY

This section addresses data and security concerns. This section was designed around the general guideline that each ecosystem participant should only have access to the minimum information required to perform its primary role.

It is critical that every ecosystem participant work together to ensure the safety and security of mobile payments.

12.4 STANDARDS STATEMENTS

Number	Statement	Section
S87	The default for ecosystem participants should be to protect end user and merchant data. Access to and usage of data must be disclosed to the end user and the end users permission explicitly granted	12 Data & Security
S88	Payment Products in Wallet – Only the wallet provider and the end user may access the list of payment products that are in a wallet, all others must not have access to the list of payment products [Continued in S89]	12.1.1 Access to Wallet Data
S89	[Continued from S88] The wallet provider's access to payment product information must be restricted to only the information that is needed to service the wallet	12.1.1 Access to Wallet Data
S90	Loyalty Products in Wallet – Only the wallet provider and the end user may access the list of loyalty products that are in a wallet, all others must not have access to the list of loyalty products [Continued in S91]	12.1.1 Access to Wallet Data
S91	[Continued from S90] The wallet provider's access to loyalty product information must be restricted to only the information that is needed to service the wallet	12.1.1 Access to Wallet Data

Number	Statement	Section
S92	Coupon in Wallet – Only the wallet provider, the end user and other end user approved loyalty applications may access the list of coupons that are in a wallet, all others must not have access to the list of coupons	12.1.1 Access to Wallet Data
S93	Payment Product, Non-Encrypted Data – Only the credential issuer, merchants and the end user may access non-encrypted payment product data; all others must not have access to -encrypted payment product data [Continued in S94]	12.1.2 Access to Credential Data
S94	[Continued from S93] Examples of Financial Non-Encrypted payment product details are: credit card number, name on credit card and CVV2. Merchants may only access this information as needed to process a payment. Merchant capture and storage of non-encrypted payment product data must be in line with payment network guidelines	12.1.2 Access to Credential Data
S95	Payment Product, Encrypted Data – Only the credential issuer may access encrypted payment product data, all others must not have access to encrypted payment product data	12.1.2 Access to Credential Data
S96	Loyalty Credentials, Non-Encrypted Data – Only the loyalty issuer, merchants and the end user may access non-encrypted loyalty credential data; all others must not have access to non-encrypted loyalty credential data [Continued in S97]	12.1.2 Access to Credential Data
S97	[Continued from S96] Merchant capture and storage of non-encrypted loyalty credential data must be consistent with the same care given to payment credentials and must only be used for rewarding or redeeming loyalty points	12.1.2 Access to Credential Data
S98	Loyalty Credentials, Encrypted Data – If loyalty points may be used for POS redemption, only the loyalty issuer may access encrypted loyalty credential data, all others must not have access to encrypted loyalty credential data	12.1.2 Access to Credential Data

Number	Statement	Section
S99	Financial Data, Amount – Only the acquirer, credential issuer, merchant and end user may access the amount of a transaction, all others must not have access to the amount of a transaction [Continued in S100]	12.1.3 Access to Financial Data
S100	[Continued from S99] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the amount of a transaction	12.1.3 Access to Financial Data
S101	Financial Data, Time – Only the acquirer, credential issuer, merchant and end user may access the time of a transaction, all others must not have access to the time of a transaction [Continued in S102]	12.1.3 Access to Financial Data
S102	[Continued from S101] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the time of a transaction	12.1.3 Access to Financial Data
S103	Financial Data, Merchant – Only the acquirer, credential issuer, merchant and end user may access the merchant for a transaction, all others must not have access to the merchant for a transaction [Continued in S104]	12.1.3 Access to Financial Data
S104	[Continued from S103] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the merchant for a transaction	12.1.3 Access to Financial Data
S105	Financial Data, Product – Only the acquirer, credential issuer, merchant and end user may access the product used for a transaction, all others must not have access to the product used for a transaction [Continued in S106]	12.1.3 Access to Financial Data

Number	Statement	Section
S106	[Continued from S105] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the product used for a transaction	12.1.3 Access to Financial Data
S107	Financial Data, Location – Only the acquirer, credential issuer, merchant and end user may access the location of a transaction, all others must not have access to the location of a transaction [Continued in S108]	12.1.3 Access to Financial Data
S108	[Continued from S107] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the location of a transaction	12.1.3 Access to Financial Data
S109	Financial Data, Transaction Details – Only the merchant and end user may access the transaction details of a transaction (e.g. SKU level information), all others must not have access to the transaction details [Continued in S110]	12.1.3 Access to Financial Data
S110	[Continued from S109] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the transaction details	12.1.3 Access to Financial Data
S111	Financial Data, Electronic Receipts – Only the merchant and end user may access the electronic receipts for a transaction, all others must not have access to the electronic receipts [Continued in S112]	12.1.3 Access to Financial Data
S112	[Continued from S111] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the electronic receipts	12.1.3 Access to Financial Data

Number	Statement	Section
S113	Loyalty Data, Amount – Only the acquirer, credential issuer, merchant and end user may access the amount of a loyalty transaction, all others must not have access to the amount of a loyalty transaction [Continued in S114]	12.1.4 Access to Loyalty Data
S114	[Continued from S113] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the amount of a loyalty transaction	12.1.4 Access to Loyalty Data
S115	Loyalty Data, Time – Only the acquirer, credential issuer, merchant and end user may access the time of a loyalty transaction, all others must not have access to the time of a loyalty transaction [Continued in S116]	12.1.4 Access to Loyalty Data
S116	[Continued from S115] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the time of a loyalty transaction	12.1.4 Access to Loyalty Data
S117	Loyalty Data, Merchant – Only the acquirer, credential issuer, merchant and end user may access the merchant for a loyalty transaction, all others must not have access to the merchant for a loyalty transaction [Continued in S118]	12.1.4 Access to Loyalty Data
S118	[Continued from S117] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the merchant for a loyalty transaction	12.1.4 Access to Loyalty Data
S119	Loyalty Data, Product – Only the acquirer, credential issuer, merchant and end user may access the product used for a loyalty transaction, all others must not have access to the product used for a loyalty transaction [Continued in S120]	12.1.4 Access to Loyalty Data

Number	Statement	Section
S120	[Continued from S119] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user gives their explicit permission to share the product used for a loyalty transaction	12.1.4 Access to Loyalty Data
S121	Loyalty Data, Location – Only the acquirer, credential issuer, merchant and end user may access the location of a loyalty transaction, all others must not have access to the location of a loyalty transaction [Continued in S 122]	12.1.4 Access to Loyalty Data
S122	[Continued from S 121] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the location of a loyalty transaction	12.1.4 Access to Loyalty Data
S123	Loyalty Data, Transaction Details – Only the merchant and end user may access the transaction details of a loyalty transaction (e.g. SKU level information), all others must not have access to the transaction details of a loyalty transaction [Continued in S124]	12.1.4 Access to Loyalty Data
S124	[Continued from S 123]]. The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the transaction details of a loyalty transaction	12.1.4 Access to Loyalty Data
S125	Loyalty Data, Electronic Receipts – Only the merchant and end user may access the electronic receipts for a loyalty transaction, all others must not have access to the electronic receipts for a loyalty transaction [Continued in S126]	12.1.4 Access to Loyalty Data

Number	Statement	Section
S126	[Continued from S125] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the electronic receipts for a loyalty transaction	12.1.4 Access to Loyalty Data
S127	Payment Product, Balance Information – Only the credential issuer and the end user may access the payment product balance information, all others must not have access to the payment product balance [Continued in S128]	12.1.5 Payment Product and Loyalty Balance and Account Information
S128	[Continued from S127] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the payment product balance	12.1.5 Payment Product and Loyalty Balance and Account Information
S129	Payment Product, Account Details – Only the credential issuer and the end user may access the payment product account detail information, all others must not have access to the payment product account detail information [Continued in S130]	12.1.5 Payment Product and Loyalty Balance and Account Information
S130	[Continued from S129] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the payment product account detail information	12.1.5 Payment Product and Loyalty Balance and Account Information
S131	Loyalty Product, Balance Information – Only the loyalty issuer and the end user may access the loyalty product balance information, all others must not have access to the loyalty product balance information [Continued in S132]	12.1.5 Payment Product and Loyalty Balance and Account Information

Number	Statement	Section
S132	[Continued from S 131] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the loyalty product balance information	12.1.5 Payment Product and Loyalty Balance and Account Information
S133	Loyalty Product, Account Information – Only the loyalty issuer and the end user may access the loyalty product account detail information, all others must not have access to the loyalty product account detail information [Continued in S134]	12.1.5 Payment Product and Loyalty Balance and Account Information
S134	[Continued from S133] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the loyalty product account detail information	12.1.5 Payment Product and Loyalty Balance and Account Information

13 DOCUMENT SUMMARY

The common reference model for NFC based mobile payments established in this document creates a set of expectations for ecosystem participants. These expectations and the associated interactions create a common foundation on which NFC mobile payment services in Canada may be built.

Each ecosystem participant must decide if they should adopt these standards. If they chose to, they are making a commitment not just to these standards, but to the vision of an open, safe and secure mobile payments ecosystem in Canada.

14 GLOSSARY OF TERMS

Terms	Definition
Acquirer or Acquiring Network	The acquirer is an institution that processes credit and/or debit card payments for a merchant.
Application/App store	Digital application distribution for Applications to your mobile device.
Canadian NFC Mobile Payments Reference Model	i.e. This document.
Cloud-Based Payments	Cloud-Based Payments store credentials remotely. For an end user to make a cloud based payment, they must use software and connections to remote servers. Cloud-Based Payments are NOT in scope for this document.
Collective Wallet	A mobile wallet that is designed by a group of credential issuers so that payment credentials from only this group of credential issuers may be bound and used for payment.
Companion Application (not pictured)	A companion application is associated with a payment application to increase functionality (by example: personal code management or transaction log). The companion application is provided at the discretion of the installer of the payment application.
Contactless	A method of communicating that does not require physical contact between two devices (see NFC for specifics).
Contactless Stickers	Stickers that use NFC technology to transfer information.
Controlling Authority (CA)	The CA manages key exchanges in an 'Open Wallet Model.' This is a model that is recognized but not mandated in the NFC Mobile Payments Reference Model. This document is an alternative to many–to-many relationships between a payment credential issuer's TSM and Secure Domain Manager's TSM.
Credential	The secure, encrypted information associated with a specific payment product.
Credential Issuer (CI)	The organization that issues and supports the payment product.

Terms	Definition
CVM	The Card Verification Method to ensure that the person presenting the card (embedded in the mobile device) is the person whom the card was issued.
CVV2	The "Card Verification Value 2" is the 3 digits at the back of the credit card
Default	A payment application or credential that is set to be used unless another payment application or credential is selected.
Delegated Mode	In a delegate mode the MNO or SDM rents (or gives access) to a portion of the secure element to the credential issuer. The MNO or SDM still has ownership on the secure element and can control what applications are loaded in the secure element. Keys are exchanged between the MNO or SDM and the credential issuer (or the credential loader) to provide that access to the secure element.
Device Software	When a payment application and payment credentials are stored on the embedded secure element, device software plays the role of the umbrella application (see below) to locate payment credentials and connect these with the NFC controller.
Dual Mode	In a dual mode the MNO or SDM has sold a portion of the secure element to the credential issuer. The credential issuer has full ownership and rights to that portion of the secure element. Keys are exchanged between the MNO or SDM and the credential issuer (or credential loader) as a part of the sale. The credential issuer can put any application on the secure element and does not need any permission from the MNO or SDM.
Ecosystem Participants	Organizations or individuals that play a formal role in the mobile payments ecosystem (i.e. offering or consuming mobile payment services).
Electronic Receipt	A receipt that is presented and stored as data only, no hard copy of this type of receipt is issued.
End User	(*Or the customer*) the end user is the end user of mobile payment and mobile connectivity services.

Terms	Definition
High Risk	Payments that meet risk criteria established by payment networks or credential issuers. High risk payments are subject to additional CVM steps.
High Value	Payments that exceed certain payment network or credential issuer value criteria or a combination of value and spend category criteria. High value payments are subject to additional CVM steps.
Industry Initiative Participants	Individuals committed to developing industry standards and guiding principles for mobile payments. Those involved in the creation of this document include: Bank of Montreal (BMO), Banque Nationale du Canada (BNC), Canadian Imperial Bank of Commerce (CIBC), Credit Union Central of Canada (CUCC), Desjardins Financial Group, Royal Bank of Canada (RBC), Bank of Nova Scotia (Scotiabank), Toronto Dominion Bank (TD).
Loyalty Service Providers	The administrator of loyalty and rewards programs.
Merchant	The merchant is the provider of goods or services for which the end user is providing payment.
Micro-SD Card	A memory card which is designed to integrate with the mobile phone and other mobile devices.
Mobile Device	Smart Phones, feature phone and tablet computers. This document is only interested on NFC enabled mobile devices. The term “mobile device” is also used interchangeably with “mobile handset” or “handset”.
Mobile Network Operator (MNO)	The MNO is the provider of mobile device connectivity services. For the purposes of this document, this role is sometimes used interchangeable with the OEM and Secure Domain Manager (SDM).
Near Field Communications (NFC)	Near field communication, or NFC, allows for simplified transactions, data exchange, and wireless connections between two devices in close proximity to each other, usually by no more than approximately 10 centimeters. NFC transactions for mobile payments will be transmitted using ISO 14443 A/B.
NFC Controller	The hardware and software that, in combination, control the NFC radio signals transmitted to and from the mobile device.
Open Wallet	A mobile wallet that is designed so that payment credentials from multiple credential issuers can be bound and used for a payment. Although ‘open,’ this type of wallet still requires agreements and business relationships between credential issuers and wallet

Terms	Definition
	providers before a wallet may be bound to credentials.
Operating volume	The strength and serviceable distance of the NFC radio on a mobile device.
Original Equipment Manufacturer (OEM)	The OEM produces the mobile device hardware that is used by the end user. For the purposes of this document, this role is sometimes used interchangeable with the MNO and the Secure Domain Manager (SDM).
OTA / Over-the-air	The transmission of data using a wireless network.
PAN	Or Primary Account Number based of 16 digits: a six-digit Issuer Identification Number (IIN), the first digit of which is the Major Industry Identifier (MII); a variable length (up to 12 digits) individual account identifier; a single check digit.
Pass Code	The mobile pass code is entered into the end user's mobile device as a card verification method.
Payment Application	A payment application provides the security requirements for making a payment and storing the payment credentials.
Payment Credential Issuer or Credential Issuer (CI)	The PCI (*or the Payment Application Owner*) is responsible for the encryption, safety and security of payment credentials. The relationship between the end user and the CI is based on financial services offerings and products.
Payment Network	(*Or the Payment Application Creator*) creates the non user facing payment application software and manages the payment network *(e.g. Visa, MasterCard and Interac, etc.).*
Payment Task Force	The Payments Task Force was working group formed by the Canadian Government in 2011 to evaluate the future of payments in Canada.
Peer-to-Peer Payments	Payments that occur directly between to end users, a merchant is not involved in this transaction.
POS	Point of Sale or the hardware that a merchant uses to capture payment credential information.
POS Application	The POS terminal hosts a payment application that complies with MasterCard PayPass, Visa or local scheme contactless specifications.

Terms	Definition
POS Device	Generic term that references a merchant acceptance terminal used to execute and process a financial transaction by communicating with an end user mobile device.
Proprietary Wallet	A mobile wallet that is designed so that only the payment credentials from the wallet provider may be bound and used to make a NFC mobile payment.
Return Transaction	A POS reversal transaction associated with the return of goods.
Secure Domain	A subdivision of the secure element.
Secure Domain Manager (SDM)	Manages access to the secure element; this role is often but not always combined with the role of the MNO. For the purposes of this document, this role is sometimes used interchangeably with the MNO and OEM.
Secure Element	Refers to the embedded secure area or secure area on the UICC where encrypted information is stored.
Secure Key	Secure key issuing is a variant of ID-based cryptography that reduces the level of trust that needs to be placed in a trusted third party by spreading the trust across multiple third parties.
Service Provider	The service provider is an organization such as a bank, a transport company, a retailer, etc. that provides services to be integrated with NFC mobile payments.
SIM	Subscriber identification module.
Simple Mode	In a simple mode, the MNO or the SDM allows the credential issuer to use its secure domain for the payment application. The right to the secure domain remains with the MNO or SDM. Any updates or changes to the payment application must be managed through the Secure Domain Manager or MNO.
Token	A cryptographic value provided by a Card Issuer as proof that a Delegated Management operation has been authorized.
Transaction	The action of executing a contactless proximity payment purchase between a POS terminal and a mobile device. A transaction includes the execution of the purchase at the point of sale and also the processing of authorization and clearing messages.
Trusted Service Manager (TSM)	(*Or Payment Application or Payment Credential Loader*) installs the payment credentials in the secure element.

Terms	Definition
UICC	The UICC (Universal Integrated Circuit Card) is the smart card used in mobile terminals in GSM and UMTS networks as defined by ETSI Project Smart Card Platform (EP SCP).
Umbrella Application	The umbrella application is used only when a payment application is stored on the UICC. The umbrella enables the communication between a wallet and all payment applications related to this wallet. The relationship of the umbrella application to payment applications is a one-to-many relationship. For an embedded secure element, this role is played by the device software.
Wallet Application or Wallet	The mobile wallet is the end user facing application which may be installed on the mobile device. The application allows users to enter and manage account specific information to be used in a NFC mobile transaction. It may be possible for one or more mobile wallets to reside on a mobile device at any given time.
Wallet Provider	Provides the end user facing interface (e.g. Google Wallet, ISIS, Visa, MasterCard, FIs, or other 3rd Parties).

15 REFERENCES

This document draws on a body of work of recently created standards in the NFC mobile payments space. This includes:

- GlobalPlatform System – message specification for management of mobile NFC devices v1.0
- GlobalPlatform's proposition for NFC Mobile – Secure Element Management and Messaging (White Paper
- GSMA - Mobile NFC Technical Guidelines
- 101203 - AFSCM TECH - LIVBL - Interface Specification - V1.2.1
- Visa rules for Merchants
- http://techcrunch.com/2009/12/01/square-receipt/

15.1 ISO REFERENCES[20]

Norm	Description
ISO-1	ISO/IEC 7816-1: 1998/Amd 1:2003 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics
ISO-2	ISO/IEC 7816-2:2007 Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of contacts
ISO-3	ISO/IEC 7816-3:2006 Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols
ISO-4	ISO/IEC 7816-4:2005 Identification cards – Integrated circuit(s) cards with contacts – Part 4: Inter-industry commands for interchange
ISO-5	ISO/IEC 7816-5:2004 Identification cards – Integrated circuit(s) cards with contacts –

[20] PayEz

Norm	Description
	Part 5: Numbering system and registration procedure for application identifiers
ISO-6	ISO/IEC 7816-6:2004/Cor 1: 2006 Identification cards – Integrated circuit(s) cards with contacts – Part 6: Inter-industry data elements
ISO-7	ISO/IEC 7816-15 Identification cards – Integrated circuit(s) cards with contacts – Part 15: Cryptographic information application
ISO-8	ISO/IEC 14443-3:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anti-collision
ISO-9	ISO/IEC 14443-4:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol

15.2 GSM REFERENCES[21]

Norm	Description
GSM-1	3GPP 31-111: Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)
GSM-2	3GPP 31-115: Secured packet structure for (Universal) Subscriber Identity Module (U) SIM Toolkit applications
GSM-3	3GPP 31-116: Remote APDU Structure for (Universal) Subscriber Identity Module (U) SIM Toolkit applications
GSM-4	3GPP TS 23.040: Technical realization of Short Message Service (SMS)
GSM-5	SGPP TS 23.048: Security mechanisms for the (U)SIM application toolkit; Stage 2

[21] PayEz

Norm	Description
GSM-6	GSM 11.11: Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface

15.3 ETSI REFERENCES[22]

Norm	Description
ETSI-1	ETSI TS 102-223: Smart Cards; Card Application Toolkit (CAT)
ETSI-2	ETSI TS 102 225: Secured packet structure for UICC applications
ETSI-3	ETSI TS 102 226: Remote APDU Structure for UICC based Applications
ETSI-4	ETSI TS 102 484 (Release 7): Smart Cards; Secure channel between a UICC and an end-point terminal
ETSI-5	ETSI TS 102 613 (Release 9): Smart Cards; UICC – Contactless Front-end (CLF) Interface Part 1: Physical and data link layer characteristics
ETSI-6	ETSI TS 102 622 (Release 10): Smart Cards UICC Contactless Front-end Interface (CLF): Host Controller Interface (HCI)
ETSI-7	ETSI TS 102 127: Reservation of CAT-TP <<well-known>> ports for standard applications

15.4 GLOBALPLATFORM REFERENCES[23]

Norm	Description
GP-1	GlobalPlatform Specification v2.2 – March 2006
GP-2	GlobalPlatform Specification v2.2 – Release Notes – March 25, 2006
GP-3	GlobalPlatform Card – Confidential Card Content Management v1.0 (Amendment A) – October 2007
GP-4	GlobalPlatform Specification 2.2 – UICC Configuration v1.0 – October 2008

[22] PayEz
[23] PayEz

Norm	Description
GP-5	GlobalPlatform Specification 2.2 – Contactless Services v1.0 (Amendment C) – February 2010
GP-6	GlobalPlatform Key Management System Functional Requirements 1.0 – November 2003
GP-7	GlobalPlatform Smart Card Management System Functional Requirements Version 4.0 21 December 2004

15.5 JAVA REFERENCES[24]

Norm	Description
JAVA-1	Java Card Specifications v2.2.2
JAVA-2	JSR 118: Mobile Information Device Profile v2.1
JAVA-3	JSR 177: Security and Trust Services API for J2ME v1.0.1
JAVA-4	JSR 257: Contactless Communication API v1.1
JAVA-5	JSR 211: Content Handler API (CHAPI) v1.0.1

15.6 EMVCO REFERENCES[25]

Norm	Description
EMV-1	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 1, Application Independent ICC to Terminal Interface Requirements V4.2
EMV-2	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 2, Security and Key Management V4.2
EMV-3	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 3,

[24] PayEz
[25] PayEz

Norm	Description
	Application Specifications V4.2
EMV-4	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 4, Cardholder, Attendant, and Acquirer Interface Requirements V4.2
EMV-5	EMV Contactless Specifications for Payment Systems Framework for Contactless Evolution Version 1.0 – October 2007
EMV-6	EMVCo – EMV Contactless Specification for Payment – Entry Point – version 1.0, May 2008
EMV-7	EMVCo Contactless Indicator Reproduction Standards for Cards and Payment Devices Last Update 05.31.07
EMV-8	EMVCo Contactless Symbol at POS Specifications Reproduction Specifications – Last Revised 06.01.07
EMV-9	EMVCo – EMV Card Personalization Specification V1.1 – July 2007
EMV-10	EMVCo – PayPass – ISO/IEC 14443 Implementation Specification V1.1 – March 2006
EMV-11	EMVCo – Contactless Mobile Payment Architecture Overview v1.0 – June 2010
EMV-12	EMVCo – Handset Requirements for Contactless Mobile Payment v1.0 – June 2010
EMV-13	EMVCo – Application Activation User Interface – Overview, Usage Guidelines and PPSE Requirements v1.0 – December 2010
EMV-14	EMVCo – EMV Profile of GlobalPlatform UICC Configuration v1.0 – December 2010

15.7 EPC REFERENCES[26]

Norm	Description
EPC-1	SEPA Cards Framework

[26] PayEz

Norm	Description
	Version 2.1 – December 2009
EPC-2	SEPA cards standardization volume – book of requirements Payments and Withdrawals with Cards in SEPA: Applicable Standards and Certification Process Version 4.0 – December 2009
EPC-3	EPC – GSMA – Trusted Service Manager – Service Management Requirements and Specifications v1.0 – January 2010

15.8 PAYEZ MOBILE REFERENCES[27]

Norm	Description
PM-1	Part I: Product Definition v1.0 – April 2011
PM-2	Part II: Technical Specification v1.0 – April 2011
PM-3	Security Guidelines for Standard Operational Environment v1.0 – June 2009
PM-4	Guidance for Payment Application Package Security Target v2.1 – July 2009
PM-5	(U)SIM Java Card TM Platform Protection Profile v2.0 – July 2010
PM-6	Payez *Mobile* MasterCard Implementation Guide – April 2011
PM-7	Payez *Mobile* Visa Implementation Guide – April 2011

15.9 AFSCM REFERENCES[28]

Norm	Description
AFSCM-1	Guidelines for Interconnection of Service Providers' and MNOs' Information Systems – Current document v1.0
AFSCM-2	Interface Specification between Telecom Operators and NFC Services Providers v1.1
AFSCM-3	Rules and Recommendations for MIDLet Design and Development v1.0

[27] PayEz
[28] PayEz

Norm	Description
AFSCM-4	Cardlet Development Guideline v1.0

16 CVM OPTION SUMMARY

This section summarized the options that were evaluated for CVM process. Tap and Confirm was selected as the method of choice in Canada.

Experience	Implications	Advantages	Disadvantages
Tap and Go (OTA Mobile Network)	• Consistent user experience for both high value and low value transactions • Best from a end user experience perspective	• One tap convenience • Similar experience to current contactless payment methods • Consistent with other mobile wallets	• Requires cellular connectivity for pass code and confirmation • End user pays for additional data charges
Tap and Go (Merchant POS)	• Convenient user experience for high value and low value transactions	• One tap convenience	• Has to interact with two interfaces • Requires cellular connectivity for confirmation • End user pays for additional data charges
Tap and Confirm (Approved Method)	• Need to educate end user on how to perform high value transactions • Balances the use of NFC and OTA	• Consistent with standards in Europe • Pass code confirmation done via NFC	• Requires OTA connectivity for confirmation and updates • No updates via NFC
Tap, Confirm and Reconfirm	• Good method for pure NFC based model • Has end user experience implications	• No OTA required for high value transactions • Mobile payment device can be used without cellular connectivity	• Long transaction time, given three taps required • Three taps may be confusing for the end user
Tap and Connect	• Difficult to maintain two way connection given the mobile device needs to be within 10cm of the NFC POS	• End user experience is seamless and consistent with low value transactions	• Mobile device has to be kept in close proximity during the entire transaction • Increased battery usage of the mobile device
Tap and Explore	• Merchant can define the payment user experience and offer coupons and loyalty offers for the end user	• Richer end user experience allows multiple user selection with payment method and loyalty options	• Long transaction time • Wallet providers and credential issuers have no additional benefit in this method

17 STANDARDS STATEMENTS

Some standards statements may appear to be repeated if concepts appear in separate sections within the document. For clarification and context, the relevant sections of the document should be referenced.

Number	Statement	Section
S1	All branding rules must be followed according to branding guidelines	6.1 Brand Acceptance Rule
S2	For MasterCard PayPass transactions, mobile device and contactless reader specifications must support PayPass Mag Stripe profile as defined in PayPass Mag Stripe specifications and Pass M/Chip or Mobile M/chip profile as defined in PayPass M/Chip specifications	6.2 Contactless And Mobile Payment Scheme Requirements
S3	For Visa PayWave contactless transactions, mobile device and contactless reader specifications must support MSD and VMPA implementation as defined in Visa Mobile Specifications	6.2 Contactless And Mobile Payment Scheme Requirements
S4	For Interac Flash contactless transactions, mobile device and contactless reader specifications must support Interac Flash Mobile contactless specifications	6.2 Contactless And Mobile Payment Scheme Requirements
S5	Other applicable operating rules should use the same authorization network and clearing systems as for standard debit and credit card transactions	6.3 Transaction Processing Requirements
S6	NFC card emulation mode must be used to execute a contactless mobile payment transaction between an end user's mobile device and a merchant's contactless reader using ISO 14443 Type A or ISO 14443 Type B radio frequency communication layer	6.7 NFC
S7	While this document and GlobalPlatform recognize three constructs (Simple Mode, Delegated Mode and Dual Mode), those that adopt these standards must use only the Delegated Mode or the Dual Mode as defined by GlobalPlatform; TSMs must operate in Delegated or Dual Mode	6.8 GlobalPlatform Messaging

Number	Statement	Section
Number	**Statement**	**Section**
S8	Access to and usage of data beyond what is required for an ecosystem participant to perform its primary role must be disclosed to the end user and the end users' permission must be explicitly granted	7.2 NFC Mobile Payments Reference Model – Solution Description
S9	For security and prevention of fraud, access to and usage of data beyond what is required for an ecosystem participant to perform its primary role must also be disclosed to the credential issuer and the credential issuer's permission must also be explicitly granted	7.2 NFC Mobile Payments Reference Model – Solution Description
S10	The mobile device must be able to accept credential provisioning and maintenance activities via an OTA or "Over-the-air" process	7.5 Software & Devices Overview
Number	**Statement**	**Section**
S11	POS contactless readers must comply with EMVCo contactless specifications [EMV-6] and MasterCard and/or Visa and/or Interac specifications	7.6 Contactless Reader/POS Requirements
S12	Regardless of functionality in pilots or initial commercial launches, those that adopt these standards expect to implement an open wallet and migrate away from proprietary and collective wallets within 18 months of the first open wallet being launched in Canada	8.1 Terminology & Solution Construct

Number	Statement	Section
S13	In furtherance of the goals of openness and interoperability, mobile wallets, mobile network operators, original equipment manufacturers, secure domain managers and credential issuers must not restrict access to payment applications from: • Debit payment products from Interac and other networks • Credit payment products from Visa, MasterCard and other networks • Prepaid payment products • Other payment products including transit and loyalty • Payment products issued in a foreign currency (e.g. US Dollar denominated products) This standards statement is subject to appropriate business relationships and technical capabilities being in place	8.2 Openness and Interoperability
S14	Payment applications or payment credentials must not be designed to prohibit a wallet from connecting with other payment applications or payment credentials, contingent on appropriate business relationships	8.2 Openness and Interoperability
S15	Mobile Wallet Access: for security, a mobile wallet must provide end users the option to lock the wallet and unlock the wallet using a user defined password	8.3 Wallet Features & Functionality
S16	Default Credential Selection: a mobile wallet must provide end users with the option to enable and disable a default payment credential	8.3 Wallet Features & Functionality
S17	Manual Default Override: a mobile wallet must provide end users with the option to override a default payment credential and manually select a payment credential to present	8.3 Wallet Features & Functionality
S18	High Value & High Risk Payments: a mobile wallet must have the ability to support entry of a pass code for end user verification of high value and high risk payments	8.3 Wallet Features & Functionality

Number	Statement	Section
S19	Transaction Data: a mobile wallet may capture transaction data for all linked payment applications; however, if it does capture this data, access to and usage of this data must be restricted as per the standards in the Data & Security section of this document	8.3 Wallet Features & Functionality
S20	Enabling a Return Transaction: a mobile wallet and payment application must be able to facilitate return transactions	8.3 Wallet Features & Functionality
S21	Payment Application Location: all elements of the payment application and payment credential (including the pass code) must reside in a secure element within the UICC or in an embedded secure element area on the mobile device [continued in S22]	8.4 Payment Application & Payment Credentials
S22	[continued from S21] However, for security reason, this document establishes only one approved method. Each credential issuer must store credential on separate supplemental security domains within the secure element	8.4 Payment Application & Payment Credentials
S23	Each Supplemental Security Domain must hold unique cryptographic keys which are required to establish a secure channel between a credential issuer's TSM and its associated security domain	8.4 Payment Application & Payment Credentials
S24	Payment Application Sharing: a payment application must only contain information from a single credential issuer	8.4 Payment Application & Payment Credentials
S25	Payment Application Openness: a payment application must not prevent connection to multiple wallets assuming that appropriate business and contractual relationships are in place	8.4 Payment Application & Payment Credentials
S26	Credential Identification: a payment application and payment credentials contain secure, encrypted information that must not be viewable by any other application	8.4 Payment Application & Payment Credentials

Number	Statement	Section
S27	Payment Application Storage Protocols: a payment application and associated payment credentials must be stored in accordance with appropriate EMVCo and payment network guidelines	8.4 Payment Application & Payment Credentials
S28	[Context: Companion Application: additional services may be added to a payment application using a companion application.] If a companion application is added, the credential issuer must approve of the addition of a companion application and the companion application must follow the same security protocols as a payment application	8.4 Payment Application & Payment Credentials
S29	The wallet application, umbrella application (if applicable) and payment application must go through a secure binding process	8.4 Payment Application & Payment Credentials
S30	NFC mobile payment solutions must ensure that only one payment application may be turned on, i.e. available for payment, at a time	8.4.1 Turning a Payment On and Off
S31	The payment application or payment credential that is turned on must be clearly identified in the list of the payment applications and payment credentials displayed in mobile wallet	8.4.1 Turning a Payment On and Off
S32	In the event that a default payment application has been setup, the default application must first be turned off before the selected payment application may be turned on	8.4.1 Turning a Payment On and Off
S33	The end user must not be able to select a blocked payment application to make a payment until approved steps are performed between the end user and the credential issuer to unblock the payment application	8.4.1 Turning a Payment On and Off

Number	Statement	Section
S34	Before a payment credential may be presented for a payment, a payment application and a wallet must be linked via a secure process that enables the wallet to access the payment application; this process is called binding	8.4.2 Linking a Wallet Application and a Payment Application
S35	Prior to a connection being established between a wallet application and a payment application, there must be a valid business relationship between the credential issuer and the wallet provider	8.4.2 Linking a Wallet Application and a Payment Application
Number	**Statement**	**Section**
S36	Convenience transactions must not exceed high value or high risk transaction thresholds as defined by the payment networks	9.1 Convenience Transaction Using a Mobile Device
S37	A convenience transaction must be performed as per existing payment network contactless guidelines; convenience transactions must not require more than a 'Tap and Go' to make a payment and must not require a Card Verification Method (CVM)	9.1 Convenience Transaction Using a Mobile Device
S38	High value and high risk transactions are defined by the credential issuer and/or the payment networks. High value and high risk transactions must be approved by the end user via a Card Verification Method (CVM)	9.2 High Value / High Risk Transactions Using a Mobile Device
S39	Once deemed acceptable by payment networks, high value and high risk transactions must be approved using the Tap and Confirm (i.e. also Tap-Enter and Verify Pass Code on Mobile – Tap) CVM	9.2 High Value / High Risk Transactions Using a Mobile Device
S40	Tap and confirm is the only approved method, all CVM must follow the tap and confirm process once deemed acceptable by payment networks	9.2.2 CVM Options Overview
S41	The standard CVM process in Canada for high value or high risk payments is 'Tap and Confirm' (i.e. double tap)	9.2.2 CVM Options Overview

Number	Statement	Section
S42	The final step in processing a mobile NFC transaction is receipt issuance. There are no unique mobile payment receipt issuance standards. Receipt issuance must be conducted as per existing guidelines	9.3 Electronic Receipts
S43	The "Offline" option, as defined by payment networks, must be followed for NFC mobile device return transactions in Canada	9.4.2 Returns Process
S44	Accordingly, NFC mobile payment returns will not require a CVM such as a signature, pass code or PIN	9.4.2 Returns Process
Number	**Statement**	**Section**
S45	A foundational concept in this section on enablement and lifecycle management activities is that interactions between ecosystem participants (including the wallet provider and credential issuer, the credential issuer and the TSM and the Credential Issuer and the MNO) must be preceded with steps to establish contractual business relationships	10.1 Business Relationships Between Ecosystem Participants
S46	As indicated in section 6.8, all messaging must be performed under the relevant guidelines from GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0	10.2 Key Management Mode
S47	Those that adhere to this document agree to use only the Delegated Mode or the Dual Mode as defined by GlobalPlatform for all enablement and lifecycle management activities	10.2 Key Management Mode
S48	For proprietary wallets, secure key management processes must be established between a credential issuer, a credential issuer's TSM, a SDM's TSM and a SDM	10.2 Key Management Mode

Number	Statement	Section
S49	For open wallets, protocols must be established to manage key between multiple parties	10.2 Key Management Mode
S50	In this process [key management process],the credential issuer's TSM, the credential issuer, the SDM's TSM and the SDM must have an established business relationship, either directly or indirectly	10.2 Key Management Mode
S51	Key exchange must be performed under the guidelines set out by GlobalPlatform	10.2.2 Single Credential Loader
S52	[Context: When this process is complete, the key exchange will facilitate a secure data transmission channel between the credential issuer's TSM, the credential issuer and the SDM's TSM.] This secure connection must exist for over-the-air provisioning to occur	10.2.2 Single Credential Loader
S53	The credential issuers' TSMs will then go through a process of exchanging keys among themselves to ensure that they can establish a secure connections – this exchange of keys must occur to facilitate the loading of credentials into an open or collective wallet	10.2.3 Multiple Credential Loaders (Hub and Spoke)
S54	In this model, all parties must perform key exchanges under the guidelines set out by GlobalPlatform. The central authority or hub of credential issuers' TSMs must develop and make available protocols to facilitate these interactions	10.2.3 Multiple Credential Loaders (Hub and Spoke)
S55	The end user must be able to request the payment application installation process via a mobile wallet	10.4.1 The End User Requests Access to the Payment Application

Number	Statement	Section
S56	In addition to requesting payment application installation via a mobile wallet, requests may also be initiated via other channels such as a website, branch, call center or mobile banking application. Whichever method of requesting the download of the payment application and payment credentials is used, the end user must give their consent prior to installation	10.4.1 The End User Requests Access to the Payment Application
S57	For mobile wallet initiated requests, the mobile wallet must display the names of credential issuer whose credentials can be loaded into that wallet	10.4.1 The End User Requests Access to the Payment Application
S58	Prior to installing the payment application and payment credentials on the mobile device, the identity of the end user must first be validated	10.4.2 End User Validation and Verification
S59	The end user validation and verification process will differ by credential issuer. It is the responsibility of the credential issuer to define the process of end user validation and verification	10.4.2 End User Validation and Verification
S60	Following validation and verification, the credential issuer must prompt the end user with messaging confirming the next step	10.4.2 End User Validation and Verification
S61	All parties involved in this process must establish a secure communication link with the credential issuer and the SDM to effect installation of the payment application and payment credentials	10.4.3 Mobile NFC Payment Application Installation
S62	Once the secure connection is established, the TSM must handle all activities including installation and activation of the mobile NFC service	10.4.3 Mobile NFC Payment Application Installation

Number	Statement	Section
S63	Binding must occur for a mobile wallet to access a payment application	10.4.4 Mobile Wallet and Payment Application Binding
S64	The umbrella application serves as a directory for the UICC and must be provided by the SDM	10.4.5 Secure Element on the UICC
S65	[Context: The umbrella application then informs the wallet application of where the payment application is stored and provides an identifier by which to locate the payment application.] The construct of the identifier must be provided by the SDM	10.4.5 Secure Element on the UICC
S66	Payment credentials are stored on the mobile device and must be able to be installed and updated over-the-air	10.4.7 OTA Provisioning of Credentials
S67	Upon a secure element update requested by the SDM (or SDM's TSM), the party must contact the credential issuer's TSM to reinstall the payment application once the SE has been updated	10.5.2 Update the Secure Element
S68	Change Mobile Device (Embedded SE): If the mobile payment application is stored in the embedded secure element, the end user must repeat the entire process of installing the mobile wallet and payment application (i.e. the end user, must setup a new device)	10.5.3 Change Mobile Device
S69	Change Mobile Device (UICC SE): When the end user changes or adds a secondary mobile device, they must go through initial setup activities again, including end user verification and binding of the payment credential to the mobile wallet	10.5.3 Change Mobile Device
S70	In the event of a lost or stolen mobile device, the end user must be instructed to contact both the MNO and the credential issuer	10.5.4 Lost or Stolen Mobile Device

Number	Statement	Section
S71	Once informed of a lost or stolen mobile device, the MNO or SDM (if different) must lock the mobile device – (including a SIM-lock for a SIM based mobile device or lock the secure area of the embedded element)	10.5.4 Lost or Stolen Mobile Device
S72	Once informed of a lost or stolen mobile device, the credential issuer must lock/block the payment method. (Additional internal steps may be followed which are similar to the current black listing of a card product)	10.5.4 Lost or Stolen Mobile Device
S73	Prior to a new mobile device being added and provisioned, the lost, stolen or old mobile device must have all payment credential information removed and positive confirmation of this action must be sent to the MNO, the SDM (if different) and the credential issuer	10.5.5 End User Replaces Device
S74	For mobile service and mobile device related issues, the end user will be instructed to contact their MNO	10.6.1 Mobile Service and Mobile Device
S75	An agreement must be reached with the MNO or SDM to support OTA provisioning and maintenance activities even if the end users mobile service is blocked	10.6.2 Failed Loading of Payment Credentials
S76	For a failed loading of payment credentials, the end user will be instructed to contact the credential issuer	10.6.3 Failed Transaction
S77	For a failed transaction, the end user will be instructed to contact the credential issuer of the payment instrument that is being used	10.6.3 Failed Transaction
S78	For all account servicing requests, end users will be instructed to contact the credential issuer	10.6.4 Account Servicing
S79	For a lost or stolen mobile device, the end user must be instructed to contact both their MNO and their credential issuer(s)	10.6.5 Lost or Stolen Mobile Device

Number	Statement	Section
S80	For binding issues where the wallet is working properly but the payment application is not, the end user will be instructed to call the credential issuer	10.6.6 Binding Process
S81	For issues with the payment application, the end user must contact the credential issuer	10.6.7 Payment Application Servicing
S82	If the mobile service is terminated by the MNO, the payment application will still continue to work. Agreements must be establish between the MNO and the credential issuer establishing protocols in this situation	10.7 Removal of the Payment Application and Associated Credentials
Number	**Statement**	**Section**
S83	Coupons and vouchers that are stored in the mobile wallet and that interact and transmit information to the NFC POS through NFC or other transmission methods, (e.g. barcode) must follow relevant standards in this document	11.2.4 Analysis of Coupons, Vouchers and Incentives - POS Interactions
S84	ISO/IEC 14443 is an international standard that defines proximity cards used for identification and the transmission protocols for communicating. ISO/IEC 14443 must be used to transmit loyalty and reward information from the mobile device to the POS using NFC	11.2.5 POS Technologies
S85	If loyalty and rewards are offered as a form of currency, the loyalty and rewards credentials should be treated as payment credentials and securely provisioned and stored on the mobile device	11.3.1 Analysis of Loyalty Redemption Experience
S86	For instant loyalty redemption, the end user must be required to choose to present loyalty points as a form of payment by selecting the loyalty program in the mobile wallet	11.3.1 Analysis of Loyalty Redemption Experience
Number	**Statement**	**Section**

Number	Statement	Section
S87	The default for ecosystem participants should be to protect end user and merchant data. Access to and usage of data must be disclosed to the end user and the end users permission explicitly granted	12 Data & Security
S88	Payment Products in Wallet – Only the wallet provider and the end user may access the list of payment products that are in a wallet, all others must not have access to the list of payment products [Continued in S89]	12.1.1 Access to Wallet Data
S89	[Continued from S88] The wallet provider's access to payment product information must be restricted to only the information that is needed to service the wallet	12.1.1 Access to Wallet Data
S90	Loyalty Products in Wallet – Only the wallet provider and the end user may access the list of loyalty products that are in a wallet, all others must not have access to the list of loyalty products [Continued in S91]	12.1.1 Access to Wallet Data
S91	[Continued from S90] The wallet provider's access to loyalty product information must be restricted to only the information that is needed to service the wallet	12.1.1 Access to Wallet Data
S92	Coupon in Wallet – Only the wallet provider, the end user and other end user approved loyalty applications may access the list of coupons that are in a wallet, all others must not have access to the list of coupons	12.1.1 Access to Wallet Data
S93	Payment Product, Non-Encrypted Data – Only the credential issuer, merchants and the end user may access non-encrypted payment product data; all others must not have access to -encrypted payment product data [Continued in S94]	12.1.2 Access to Credential Data

Number	Statement	Section
S94	[Continued from S93] Examples of Financial Non-Encrypted payment product details are: credit card number, name on credit card and CVV2. Merchants may only access this information as needed to process a payment. Merchant capture and storage of non-encrypted payment product data must be in line with payment network guidelines	12.1.2 Access to Credential Data
S95	Payment Product, Encrypted Data – Only the credential issuer may access encrypted payment product data, all others must not have access to encrypted payment product data	12.1.2 Access to Credential Data
S96	Loyalty Credentials, Non-Encrypted Data – Only the loyalty issuer, merchants and the end user may access non-encrypted loyalty credential data; all others must not have access to non-encrypted loyalty credential data [Continued in S97]	12.1.2 Access to Credential Data
S97	[Continued from S96] Merchant capture and storage of non-encrypted loyalty credential data must be consistent with the same care given to payment credentials and must only be used for rewarding or redeeming loyalty points	12.1.2 Access to Credential Data
S98	Loyalty Credentials, Encrypted Data – If loyalty points may be used for POS redemption, only the loyalty issuer may access encrypted loyalty credential data, all others must not have access to encrypted loyalty credential data	12.1.2 Access to Credential Data
S99	Financial Data, Amount – Only the acquirer, credential issuer, merchant and end user may access the amount of a transaction, all others must not have access to the amount of a transaction [Continued in S100]	12.1.3 Access to Financial Data
S100	[Continued from S99] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the amount of a transaction	12.1.3 Access to Financial Data

Number	Statement	Section
S101	Financial Data, Time – Only the acquirer, credential issuer, merchant and end user may access the time of a transaction, all others must not have access to the time of a transaction [Continued in S102]	12.1.3 Access to Financial Data
S102	[Continued from S101] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the time of a transaction	12.1.3 Access to Financial Data
S103	Financial Data, Merchant – Only the acquirer, credential issuer, merchant and end user may access the merchant for a transaction, all others must not have access to the merchant for a transaction [Continued in S104]	12.1.3 Access to Financial Data
S104	[Continued from S103] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the merchant for a transaction	12.1.3 Access to Financial Data
S105	Financial Data, Product – Only the acquirer, credential issuer, merchant and end user may access the product used for a transaction, all others must not have access to the product used for a transaction [Continued in S106]	12.1.3 Access to Financial Data
S106	[Continued from S105] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the product used for a transaction	12.1.3 Access to Financial Data
S107	Financial Data, Location – Only the acquirer, credential issuer, merchant and end user may access the location of a transaction, all others must not have access to the location of a transaction [Continued in S108]	12.1.3 Access to Financial Data

Number	Statement	Section
S108	[Continued from S107] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the location of a transaction	12.1.3 Access to Financial Data
S109	Financial Data, Transaction Details – Only the merchant and end user may access the transaction details of a transaction (e.g. SKU level information), all others must not have access to the transaction details [Continued in S110]	12.1.3 Access to Financial Data
S110	[Continued from S109] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the transaction details	12.1.3 Access to Financial Data
S111	Financial Data, Electronic Receipts – Only the merchant and end user may access the electronic receipts for a transaction, all others must not have access to the electronic receipts [Continued in S112]	12.1.3 Access to Financial Data
S112	[Continued from S111] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the electronic receipts	12.1.3 Access to Financial Data
S113	Loyalty Data, Amount – Only the acquirer, credential issuer, merchant and end user may access the amount of a loyalty transaction, all others must not have access to the amount of a loyalty transaction [Continued in S114]	12.1.4 Access to Loyalty Data
S114	[Continued from S113] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the amount of a loyalty transaction	12.1.4 Access to Loyalty Data

Number	Statement	Section
S115	Loyalty Data, Time – Only the acquirer, credential issuer, merchant and end user may access the time of a loyalty transaction, all others must not have access to the time of a loyalty transaction [Continued in S116]	12.1.4 Access to Loyalty Data
S116	[Continued from S115] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the time of a loyalty transaction	12.1.4 Access to Loyalty Data
S117	Loyalty Data, Merchant – Only the acquirer, credential issuer, merchant and end user may access the merchant for a loyalty transaction, all others must not have access to the merchant for a loyalty transaction [Continued in S118]	12.1.4 Access to Loyalty Data
S118	[Continued from S117] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the merchant for a loyalty transaction	12.1.4 Access to Loyalty Data
S119	Loyalty Data, Product – Only the acquirer, credential issuer, merchant and end user may access the product used for a loyalty transaction, all others must not have access to the product used for a loyalty transaction [Continued in S120]	12.1.4 Access to Loyalty Data
S120	[Continued from S119] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user gives their explicit permission to share the product used for a loyalty transaction	12.1.4 Access to Loyalty Data
S121	Loyalty Data, Location – Only the acquirer, credential issuer, merchant and end user may access the location of a loyalty transaction, all others must not have access to the location of a loyalty transaction [Continued in S 122]	12.1.4 Access to Loyalty Data

Number	Statement	Section
S122	[Continued from S 121] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the location of a loyalty transaction	12.1.4 Access to Loyalty Data
S123	Loyalty Data, Transaction Details – Only the merchant and end user may access the transaction details of a loyalty transaction (e.g. SKU level information), all others must not have access to the transaction details of a loyalty transaction [Continued in S124]	12.1.4 Access to Loyalty Data
S124	[Continued from S 123]]. The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the transaction details of a loyalty transaction	12.1.4 Access to Loyalty Data
S125	Loyalty Data, Electronic Receipts – Only the merchant and end user may access the electronic receipts for a loyalty transaction, all others must not have access to the electronic receipts for a loyalty transaction [Continued in S126]	12.1.4 Access to Loyalty Data
S126	[Continued from S125] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the electronic receipts for a loyalty transaction	12.1.4 Access to Loyalty Data
S127	Payment Product, Balance Information – Only the credential issuer and the end user may access the payment product balance information, all others must not have access to the payment product balance [Continued in S128]	12.1.5 Payment Product and Loyalty Balance and Account Information

Number	Statement	Section
S128	[Continued from S127] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the payment product balance	12.1.5 Payment Product and Loyalty Balance and Account Information
S129	Payment Product, Account Details – Only the credential issuer and the end user may access the payment product account detail information, all others must not have access to the payment product account detail information [Continued in S130]	12.1.5 Payment Product and Loyalty Balance and Account Information
S130	[Continued from S129] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and credential issuer give their explicit permission to share the payment product account detail information	12.1.5 Payment Product and Loyalty Balance and Account Information
S131	Loyalty Product, Balance Information – Only the loyalty issuer and the end user may access the loyalty product balance information, all others must not have access to the loyalty product balance information [Continued in S132]	12.1.5 Payment Product and Loyalty Balance and Account Information
S132	[Continued from S 131] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the loyalty product balance information	12.1.5 Payment Product and Loyalty Balance and Account Information
S133	Loyalty Product, Account Information – Only the loyalty issuer and the end user may access the loyalty product account detail information, all others must not have access to the loyalty product account detail information [Continued in S134]	12.1.5 Payment Product and Loyalty Balance and Account Information

Number	Statement	Section
S134	[Continued from S133] The wallet may collect and store this information for the end user but this information must not be accessible by the wallet provider or other 3rd party unless the end user and loyalty issuer give their explicit permission to share the loyalty product account detail information	12.1.5 Payment Product and Loyalty Balance and Account Information