Payments Security White Paper

BMO Bank of Montreal

CIBC

National Bank of Canada

RBC Royal Bank

Scotiabank

TD Bank Group

July 13, 2015

Contents

Introduction

It is essential to promote innovation and competition to drive the introduction of new mobile payments products and services in Canada. It is equally important to maintain the integrity of the Canadian payments infrastructure. The following white paper was developed by six of Canada's largest financial institutions: BMO Bank of Montreal, CIBC, National Bank of Canada, RBC Royal Bank, Scotiabank and TD Bank Group. The paper encourages market openness, supports innovation, and suggests that new mobile payments products and services maintain the high level of payments security in the Canadian market in order to maintain consumer and merchant confidence and provide continued protection against payment card fraud.

A significant development for the payments ecosystem is the recent introduction of open mobile wallets that hold credentials from multiple issuers. The intent of the white paper is to ensure that the industry is well-positioned to evaluate and adopt innovative products and services. In the evaluation of new technologies and business models, the Payments Security White Paper is based on the following objectives:

- Maintain industry-level payment security that is equivalent to or better than the payment card loaded into an open mobile wallet.
- Take appropriate steps to identify and protect consumers and merchants against technology and operational risks.
- Create the capability to allow consumers to load any payment credential into a wallet of their choosing and transact across all channels (point of sale and remote).

The ultimate objective is to maintain Canada's position as a leader in payments security.

SCOPE

This white paper reviews emerging mobile payment technologies and business models, identifies security and interoperability risks or issues that could impact on the Canadian payments ecosystem, and explores barriers to the development of the mobile payments ecosystem in Canada. The white paper provides an overview of key events in the Canadian market that have occurred since the *Canadian NFC[1] Mobile Payments Reference Model* was published in early 2012 and reviews the key aspects of HCE, an emerging technology, and highlight areas of opportunity and concern. Additionally the white paper reviews open mobile wallet solutions available in Canada, as well as those being launched by large global companies, and then considers the impacts of these open mobile wallet solutions on the Canadian market if they were to enter the market as currently designed.

[1] Near Field Communication.

This paper considers transactions initiated at the physical point of sale (POS) where the mobile device communicates with the merchant's payment terminal through a contactless communications protocol (e.g., NFC, QR code), remote payments completed within a mobile application that has been downloaded to the mobile device (in-app), and internet payments initiated by a mobile device that leverage a payment credential stored on the device. Remote payments that leverage "card on file" information to complete transactions, mobile banking applications, mobile payment applications that are strictly proprietary, and peer-to-peer payments that might be initiated from the mobile device are not within the scope of this paper. This paper does not define technical solution(s) or propose amendments to existing industry technical standards, data protection requirements, or anti-money-laundering requirements.

GUIDING PRINCIPLES

– **Security.** Maintain the level of security that consumers and retailers have come to expect from payment service providers in Canada, equivalent to that provided by EMV chip and PIN. Identify and protect consumers and merchants against technological and operational risks.

– **Openness.** Create and support an open mobile payments environment that allows consumers to pay for goods and services using any mobile wallet on any mobile device, leveraging the contactless payment terminals that many retailers already have.

– **Innovation.** Support innovation in mobile payments by creating an environment that promotes consumer choice and is conducive to the development, evaluation and introduction of new products and services.

AUDIENCE

The white paper may be of interest to Canadian mobile payments stakeholders including consumers, payment credential issuers, payment network providers, merchants, acquirers, mobile network operators (MNOs), mobile device manufacturers, wallet providers, and other interested parties.

Overview of the Canadian market

Over the past decade, the pace of payments innovation has been accelerating. The development and implementation of EMV chip and PIN, contactless EMV cards, peer-to-peer payments, SIM-based mobile payments, and most recently host card emulation (HCE) mobile payments have transformed the Canadian market. The introduction of new payment products presents both opportunities and challenges to the security of the ecosystem. Innovation should maintain or strengthen the security and overall integrity of the payments ecosystem.

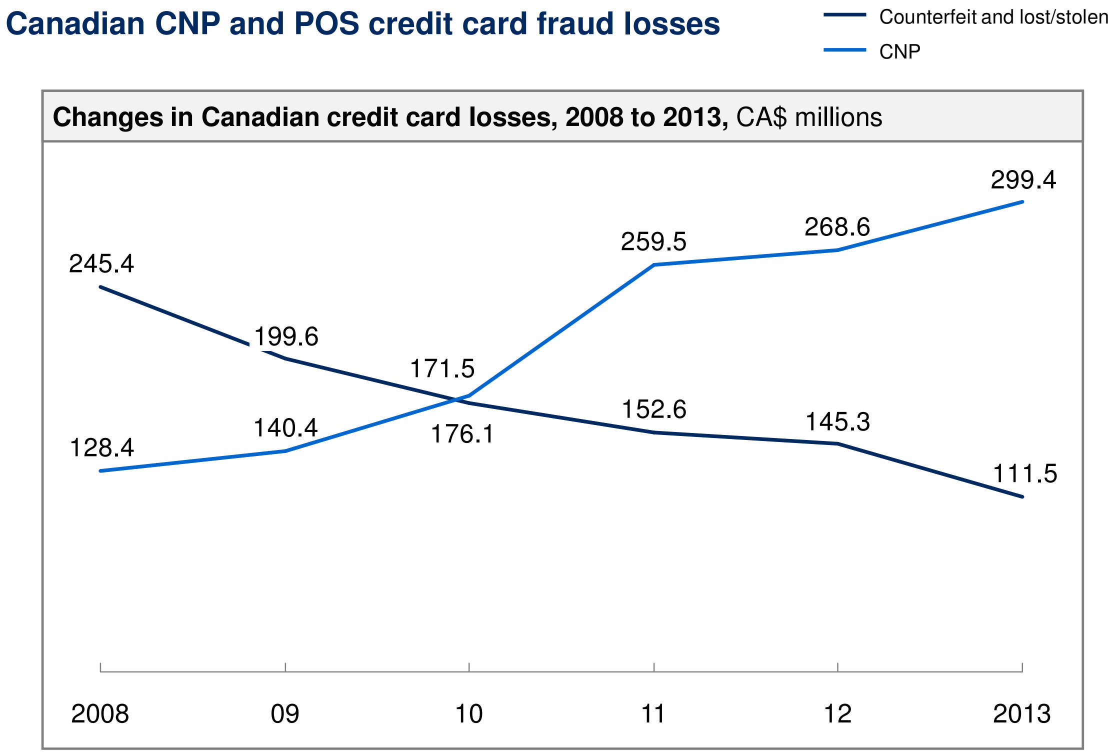
EMV MIGRATION

The national rollout of EMV chip and PIN technology began in earnest in 2008, and was largely completed by 2013. Moving away from magnetic stripe technology required a substantial infrastructure investment (e.g., POS devices, ATMs, retailer & issuer proprietary systems) and the mass reissuance of payment cards. Consumers learned to modify the payment process to insert, rather than swipe, their payment cards, and to switch from a signature to a four-digit PIN on credit cards.

The migration to EMV was viewed to be an industry initiative; a necessary investment to maintain the integrity of the payments ecosystem in Canada. Payments stakeholders from across the industry, led by the payment networks, worked closely together to manage customer and merchant impact by quickly identifying and resolving issues affecting interoperability (all cards at all devices) and customer experience. Initial consumer and merchant communications were managed at an industry level to ensure a consistent level of staff training and the use of common language across all merchant and consumer communications. Canada has been internationally recognized for its effective implementation of EMV.

EMV has had the intended impact on counterfeit fraud, which continues to decrease. Canada has also seen the expected increase in card not present (CNP) fraud driven by substantial growth in remote transactions, and by an increased focus by fraudsters on CNP transactions. Although measures have been put in place by retailers (proprietary fraud monitoring tools) and payment networks (Verified by Visa, Securecode), CNP transactions remain an area of weakness.

EXHIBIT 1 – FRAUD LOSSES IN CANADA 2008-2013



Source: *Canadian Bankers Association*

INTRODUCTION OF CONTACTLESS PAYMENTS

Contactless payments began gaining momentum on the heels of EMV. Contactless payments are quick and convenient: consumers just tap the card at an NFC-enabled POS – there is no need to insert the card or enter a PIN. This method of payment is especially attractive to merchants where throughput is important, such as quick service restaurants (QSR) and grocery. Contactless payments present risk to issuers as there is no customer verification method (CVM) and issuers are liable for fraud. When contactless payment was first introduced, the payment networks (MasterCard, Visa) determined that consumers could tap to pay for transactions less than $50. This limit was increased to $100 in 2013 by all of the payment networks (including Interac) based on detailed analysis that evaluated operational risks associated with a higher maximum transaction value.

Aggressive deployment of NFC-enabled terminals and cards has made Canada one of the top countries in the world for NFC penetration[2]. By the end of 2014, over 70 percent

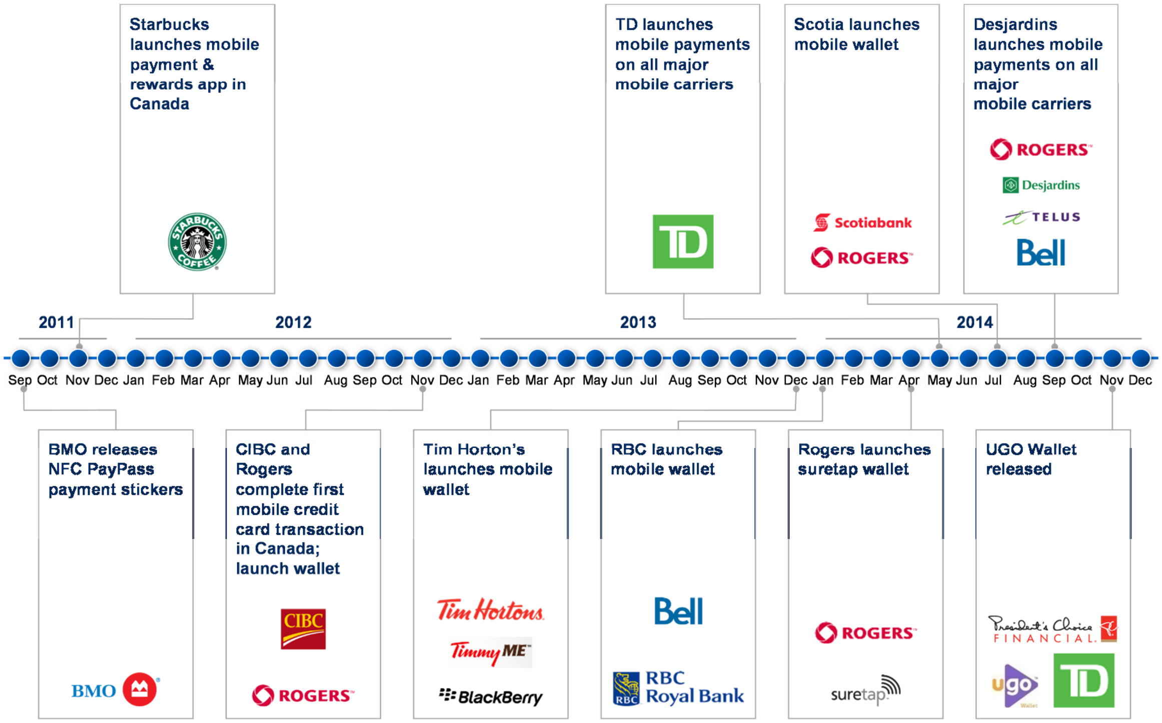
[2] MasterCard Mobile Payment Readiness Index, May 2012; Industry interviews

of credit cards and 40 percent of debit cards in Canada supported contactless payment. Over 80 percent of merchant POS devices in targeted categories (e.g., QSR, pharmacy, grocery) are NFC-enabled, and about 30 percent of all POS devices are NFC-enabled. At time of writing, contactless transactions represent between 10 to 20 percent of total transaction count.[3]

EVOLUTION OF THE CANADIAN MOBILE PAYMENTS LANDSCAPE

Canada's banks and credit unions worked together to develop the *Canadian NFC Mobile Payments Reference Model*, which focused on the creation of an open ecosystem that would support continued innovation in mobile payments. The Reference Model was focused on SIM-based mobile payments solutions that leveraged EMV architecture and security and contactless payment processes and policies. The document also considered additional wallet functionality, including electronic receipts, loyalty, and coupons/vouchers. The Reference Model proposed 134 voluntary standards aimed at accelerating and supporting the introduction and adoption of safe and secure mobile payments in Canada. Our view is that these standards have been helpful in guiding the development of mobile payments in Canada.

EXHIBIT 2 – EVOLUTION OF THE CANADIAN MOBILE PAYMENTS LANDSCAPE



Starbucks launches mobile payment & rewards app in Canada
TD launches mobile payments on all major mobile carriers
Scotia launches mobile wallet
Scotiabank
ROGERS
Desjardins launches mobile payments on all major mobile carriers
ROGERS
Desjardins
TELUS
Bell
2011
2012
2013
2014
Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
BMO releases NFC PayPass payment stickers
BMO
CIBC and Rogers complete first mobile credit card transaction in Canada; launch wallet
CIBC
ROGERS
Tim Horton's launches mobile wallet
Tim Hortons
TimmyME
BlackBerry
RBC launches mobile wallet
Bell
RBC Royal Bank
Rogers launches suretap wallet
ROGERS
suretap
UGO Wallet released
President's Choice FINANCIAL
ugo Wallet
TD

Source: *Company websites*

[3] Industry interviews

Since the *Canadian NFC Mobile Payments Reference Model* was published in May 2012, several Canadian payment credential issuers have developed and launched SIM-based mobile payments solutions. The first open mobile wallet to support payment was launched in Canada in November 2014[4]. Ideally, consumers should be able to load any of their payment credentials (credit, debit) from any network (American Express, Interac, MasterCard, Visa), onto any mobile device (Android, Apple, Blackberry, Windows, etc.) on any mobile network (Bell, Rogers, TELUS, etc.). This is not possible today. Although there have been several products introduced into the market, consumer adoption remains low due to the deployment challenges associated with SIM-based solutions. These challenges include:

- **NFC-enabled devices.** To support NFC payments, the mobile device must be NFC-enabled. When CIBC first launched its mobile payment application, only one mobile handset (BlackBerry Bold 9900) was NFC-enabled. Every mobile device must be certified by the MNO before a payment credential is loaded, a time consuming process. The number of NFC-enabled devices has increased dramatically over the past three years, and NFC has virtually become a standard feature on new devices. At the time of writing, not all devices that support NFC are certified for payment by all MNOs, meaning a consumer may have an NFC-enabled device that will not support mobile payments.
- **Supported MNOs**. To support mobile payments, payment applications owned by issuers must be loaded onto SIM cards owned by MNOs. This requires each credential issuer and each MNO to negotiate a commercial arrangement. For this reason, issuers are only able to support deployment as these agreements are implemented. At the time of writing, some issuers' proprietary solutions are only available to customers of a single MNO.
- **Payment-ready SIMs.** Until recently, the SIM shipped with a mobile device would not support payment applications, and consumers were required to purchase a replacement payment-ready SIM. Issuers initially faced wallet registration failure rates of 80 to 90 percent as a result of incompatible SIMs.[5] This was a substantial barrier. To remedy this, Canada's largest MNOs now sell NFC-enabled Android and BlackBerry handsets with payment-ready SIM cards.
- **Digitized credentials.** The first digital credentials available for mobile payment were credit products. Issuers have been increasing the number of products available for consumers, but it is not yet possible for most consumers to pay using a mobile device for all of the payment cards in their wallets. Interac's mobile debit application has only been available since 2012 and, at the time of writing, only one issuer is supporting mobile debit payment.

[4] Ugo press release, cnw.ca

[5] Issuer interviews

– **Provisioning credentials.** Provisioning of credentials, installing the mobile payment application onto the SIM card in the mobile device, has been challenging from the outset. The digital credential is provisioned "over the air" to the consumer's mobile device. This process can take several hours and, if internet connectivity is lost, it may fail. In 2012, EnStream – a joint venture founded by Bell, Rogers, and TELUS – introduced issuer trusted service manager (TSM) services and launched a common mobile interface between the Canadian issuers and MNOs with the objective of improving the provisioning experience. Although improved, provisioning challenges remain.

It is estimated that despite the number of relationships created between issuers and MNOs, fewer than 25% of consumers have all the required elements to participate in mobile payments.[6] Because mobile payment capability is available to a small subset of the consumer population, it is challenging for issuers to communicate and promote mobile payments broadly and awareness of mobile payment remains low.

CODE OF CONDUCT

The Code of Conduct for the Credit and Debit Card Industry (the Code) first came into effect in August 2010. It was created to address concerns raised by merchants regarding the business practices of credit and debit card networks, issuers, and acquirers, and it applies to debit and credit cards used to conduct transactions with merchants in Canada. The Code's objectives were to ensure that merchants in Canada benefit from cost transparency, pricing flexibility and choice in payment options accepted. Compliance with the Code is monitored by the Financial Consumer Agency of Canada (FCAC).

The Code was recently revised in April 2015 to include mobile payments. The revisions provide new consumer protections for mobile payment users to ensure that the consumer has full control of the default settings on the mobile wallet(s) and device(s). The Code also ensures that merchants can choose not to accept mobile payments should fees for mobile payments increase relative to card-based contactless payments.[7] The revised code also provides new protections for merchants. The Code requires that co-badged debit cards[8] be represented as two separate payment applications in mobile wallets or on mobile devices. This will be a change for consumers as many debit cards in circulation support two payment networks.

The government consulted extensively with the industry before introducing the Code in 2010 and continues to meet regularly with key stakeholders. The creation of and

[6] Proprietary analysis

[7] "Code of Conduct for the Credit and Debit Card Industry in Canada," Financial Consumer Agency of Canada, April 24, 2015

[8] Co-badged cards are debit cards that support two or more payment networks.

continuing revisions to the Code demonstrate government engagement and interest in the payments industry broadly, as well as a desire to ensure that fair and transparent business practices protect merchants and consumers. It is expected that the Code will continue to evolve.

Mobile payment technologies

Mobile payment is a broad term that includes payments effected through the use of bar codes, QR codes, the internet, and NFC. Fundamentally, mobile payments success is driven by consumers' perception of convenience, security, and value above and beyond that provided by the payment card. The growing penetration of "smart" devices is enabling traditional and non-traditional payments players to focus on developing mobile solutions to drive engagement and deliver value for merchants and consumers.

Bar code and QR code solutions have been deployed in Canada, typically as part of proprietary closed loop mobile payment solutions (e.g., Starbucks, Tim Hortons). These solutions require software and often hardware upgrades as part of the deployment. Merchant unwillingness to invest in additional hardware that can take up valuable counter space may be a challenge in the broader deployment of these solutions.

NFC acceptance capability has become a standard feature on POS devices, and most retailers in Canada now have the capability to accept NFC payments should they so choose. NFC acceptance is on the increase: at the time of writing, approximately 30 percent[9] of POS devices in Canada are enabled to support NFC payments, with significantly higher acceptance penetration in key verticals such as quick service restaurants (QSR). Consumers are becoming increasingly aware of the contactless payment capability that exists on the majority of payment cards in Canada. The value proposition of a quick POS experience without a CVM (e.g., PIN) is resonating, despite the limited number of campaigns in market to promote the use of contactless payment.

MOBILE PAYMENT TECHNOLOGY OPTIONS

Early NFC mobile payment solutions leveraged the hardware secure element physically located in the mobile device. Hardware solutions offer a high level of security because of the tamper-proof secure storage of payment credentials. The two leading hardware SEs are an embedded SE (eSE) that is built into the device by the device manufacturer, and a SIM-based SE that is owned and provided by the MNO.

A hardware SE can be described as a "smart card in the phone." Testing and certification processes are in place to ensure solutions meet the requirements defined by the payment networks and other industry bodies. The SE is protected by a restricted access interface and strong encryption to render it tamper resistant. The hardware SE is connected directly to the NFC controller in the mobile device; the mobile device operating system has no access to the data that is exchanged between the SIM and the NFC controller. The SE on a mobile device contains the payment credential information and other information necessary to create payment cryptograms for *that device only*, limiting the attractiveness to fraudsters. SIM-based solutions have been in the market

[9] Industry interviews

for several years and are well-supported by brand specifications and testing and certification processes.

More recent mobile solutions have leveraged Host Card Emulation (HCE) technology, a capability that was introduced by Android in 2013. In an HCE solution, the secure element is not located on the device: payment credentials are instead stored in the cloud. *HCE represents a fundamental paradigm shift for security.* The assumption is that the mobile device is insecure: payment security risks need to be mitigated by layering multiple alternative security mechanisms including dynamically generated, limited use payment credentials. HCE is an evolving technology with early deployments in several countries. Supporting documentation, including testing and certification processes, will continue to evolve over the next several years.

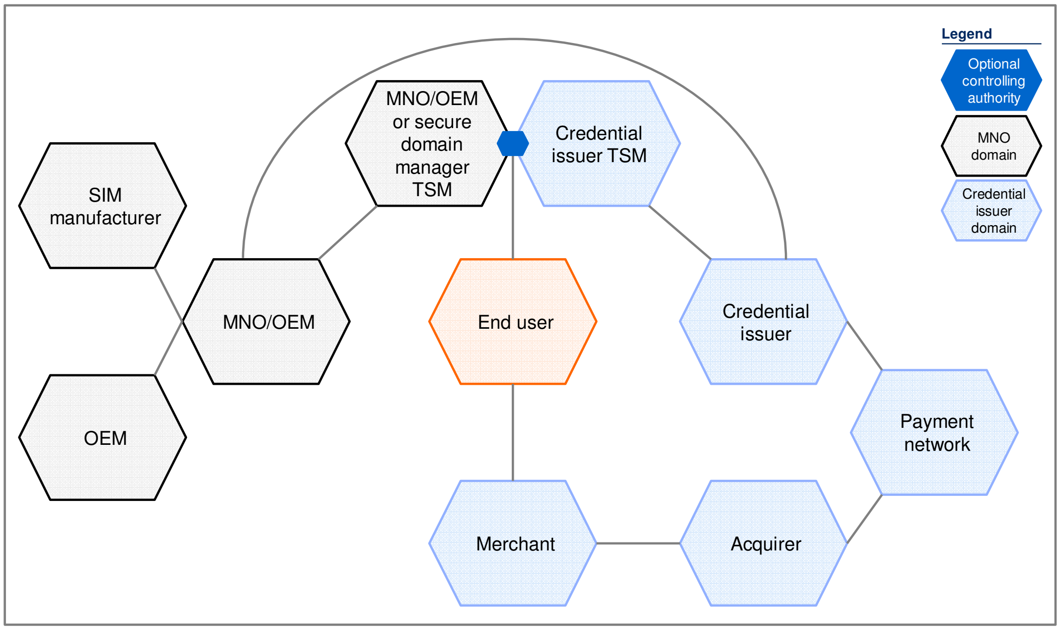
A conceptual overview of the security and maturity of payments technologies can be found in Appendix A.

SIM-BASED SOLUTIONS

Traditional card payments involve four parties: the card issuer; the customer; the merchant; and the acquirer. Payment networks connect the acquirer and the issuer to enable transaction authorization. Mobile payment solutions that leverage the SE or eSE require the introduction of new players into the ecosystem to create and manage digitized cards, and to deploy the digitized card to the consumer’s mobile device. New roles and responsibilities that have been introduced to support NFC mobile payments can be found in Appendix B.

The placement of these additional players in the ecosystem to support SIM-based NFC mobile payments is shown in the following exhibit.

EXHIBIT 3 – SIM-BASED MOBILE PAYMENTS ECOSYSTEM



Source: *Canadian NFC Mobile Payments Reference Model*

Table 1 outlines some of the possible risks associated with SIM-based mobile payment solutions.

TABLE 1 – POSSIBLE RISKS ASSOCIATED WITH SIM-BASED SOLUTIONS

Risk	Description	Consumer/merchant impact
Technology ***Assessment: Low risk***	■ Payment information is stored in a hardware secure element that is tamperproof ■ Specifications are clearly written; based on EMV specs ■ Certification criteria are clear and consistent ■ Some interoperability issues – collisions between credentials stored in different wallets	■ Good user experience (device does not need to be powered on/device does not need connectivity/offline transactions supported) ■ No upgrade required at POS other than NFC-enabled terminals ■ Interoperability issues between apps on the same device may limit consumer adoption
Operational	■ Complex ecosystem requiring multiple participants,	■ Mobile payment is not ubiquitously available (the

Risk	Description	Consumer/merchant impact
Assessment: Medium risk	partnerships, and associated governance ■ Provisioning is lengthy and sometimes unreliable ■ Lifecycle management can present challenges if new payment product or device is not supported	right payment card, right phone, and right network are all required). Friction can cause consumers to drop out of the registration and provisioning process ■ Consumers may not be able to carry payment capability over to a new payment product or mobile device
Reputational ***Assessment: Low to Medium risk***	■ Not all devices and payment products are supported	■ Consumer adoption will be limited until ubiquity is achieved

Hardware SE mobile payment solutions are based on robust and proven EMV specifications, and the level of security provided at POS is equivalent to that provided by the payment card. Fraud risk presented by not requiring a CVM have been mitigated by implementing a dollar value ‘cap’ on contactless transactions that, if surpassed, requires the consumer to insert the payment card into the POS terminal. Challenges with deployment have been related to user experience and the unexpected interaction of multiple wallet applications loaded on the same device. Detailed testing is required to ensure that there is no interaction between multiple payment applications that could result in a negative customer experience.

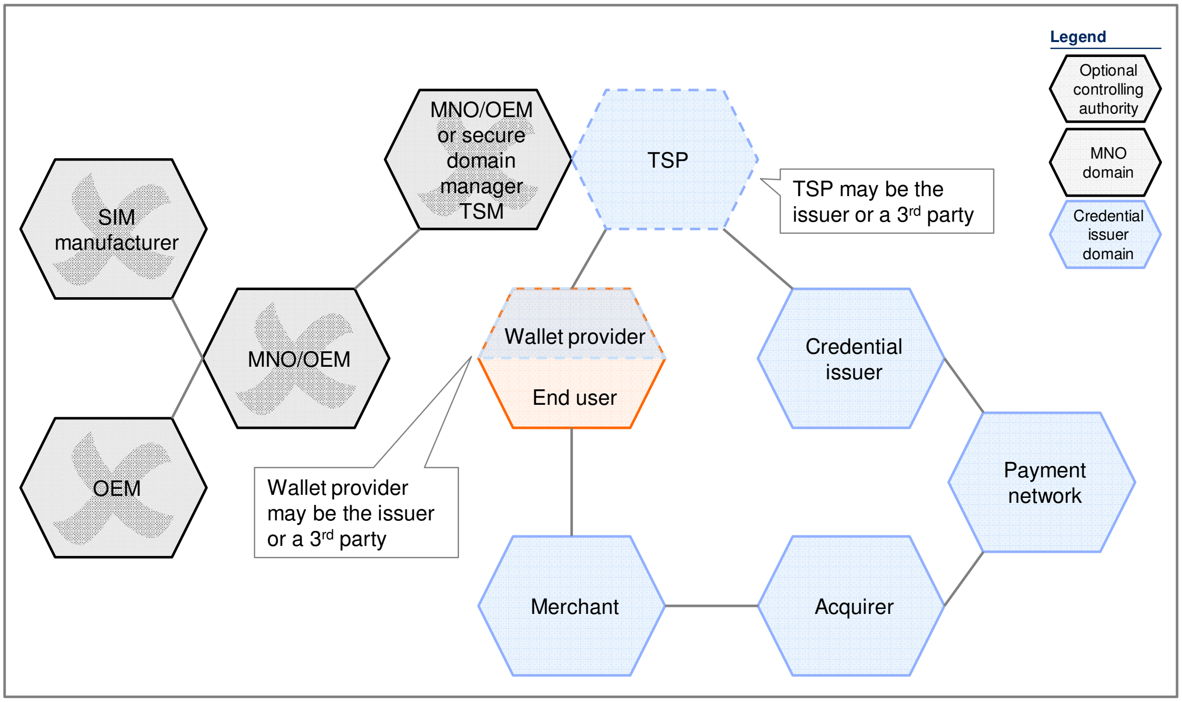
At the time of publication, there are five Canadian issuers with SE-based solutions in market (CIBC, Desjardins, RBC, Scotiabank, and TD). More and more devices are supported by the issuers as new NFC-enabled devices become standard.

HOST CARD EMULATION SOLUTIONS

Host card emulation (HCE) describes on-device technology that permits an NFC-enabled mobile device to emulate a payment card without relying on access to a secure element. HCE solutions use only software.

HCE dramatically simplifies the mobile payments applications ecosystem. Consumers can download the payment / wallet application from the internet (bank website, app store, etc.). HCE solutions eliminate the need for credential issuers to obtain space on a third-party secure element, removing the MNO and OEM roles from the ecosystem. This also eliminates the need for the MNO TSM and issuer TSM roles. As with SIM-based solutions, HCE solutions require an open operating system that grants NFC antenna access to third-party applications.

EXHIBIT 4 – HCE MOBILE PAYMENTS ECOSYSTEM


Legend
Optional controlling authority
MNO domain
Credential issuer domain
SIM manufacturer
OEM
MNO/OEM
MNO/OEM or secure domain manager TSM
TSP
TSP may be the issuer or a 3rd party
Wallet provider
End user
Wallet provider may be the issuer or a 3rd party
Credential issuer
Payment network
Merchant
Acquirer

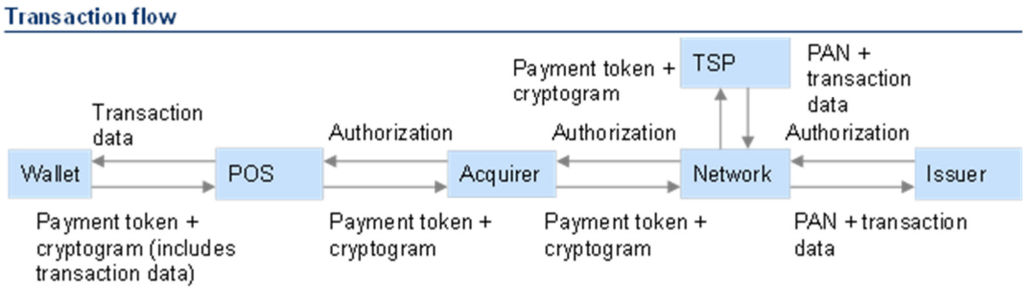
Elements required by an HCE solution

Many aspects of HCE solutions are similar to those of SIM-based solutions, with enhancements to support communication between the device and the cloud.

- **Cloud-based payments platform.** HCE solutions require software to manage the cloud-based payments account. Functions include managing primary account numbers (PANs) and limited-use keys, validating dynamic data replenishment requests, provisioning dynamic data to the device, verifying CVM, and managing the consumer mobile application account lifecycle and payment functions. Cloud-based payments platforms can be built and managed by credential issuers or outsourced to third parties.
- **Mobile application (wallet).** The mobile application includes a customer interface that supports enrolment in the cloud-based payment service and is involved in the provisioning of credentials at activation and on an ongoing basis. The mobile application must communicate securely with the payments platform. Mobile application development and management can be provided by issuers (proprietary mobile wallets) or outsourced to third parties (open mobile wallets).

- **Token Service Provider (TSP).** The need for dynamic data has created a new role in the HCE ecosystem for Token Service Providers. Tokenization consists of replacing the actual primary account number (PAN) [10] with an alternate PAN – a token. The attributes of the token are described to allow token PANs to flow through the payment system exactly as real PANs do. These tokens have the ability to impact every stakeholder in the ecosystem as they flow through the transaction from end to end, so it is important that they function as expected. Exhibit 5 demonstrates where the EMV Payment Tokenization Specification proposes TSPs should sit in the ecosystem.

EXHIBIT 5 – PAYMENT TOKEN PROVISIONING OVERVIEW



Note: TSP role could be performed by the issuer, network, or a 3rd party.

Source: *EMV Payment Tokenization Specification*

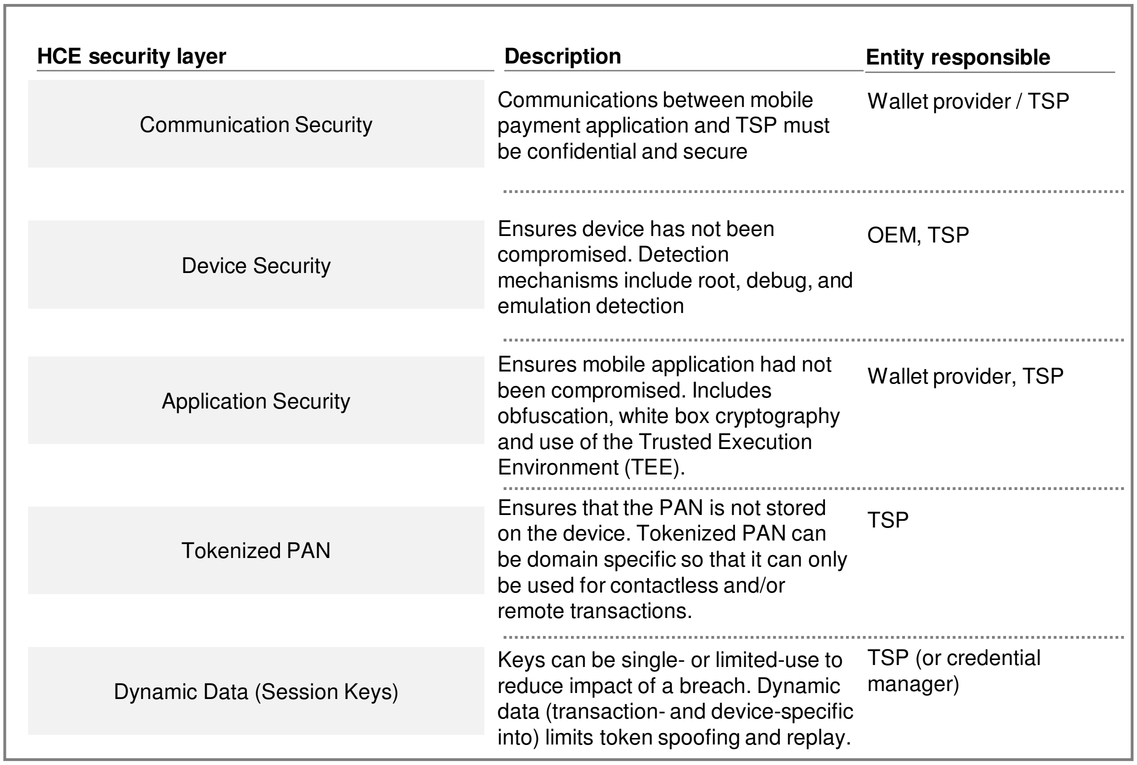
HCE TECHNOLOGY RISKS

Because HCE solutions do not require the secure storage of payment credentials on the device, payment security is provided through the layering of multiple security solutions in order to provide the security provided by a hardware solution. Because the mobile device is viewed to be less secure than a hardware secure element, all aspects of the HCE solution are continually monitored. Layered security is designed to make it difficult for fraudsters to steal tokens from the device, and use the tokens once they're stolen. Application security, device security, and communications security are essential to protect the storage of tokens on the device and prevent token theft. In the event of token theft, dynamic data is critical to prevent tokens from being used and/or limiting how they may be used. Dynamic data provides issuers and TSPs with a rich source of information on which to base authorization decisions, and limits the risk associated with token replay.[11]

[10] The PAN is the 16 to 19 digit number on the front of the credit card.

[11] Token replay is an attempt by a fraudster to use a single-use token multiple times. If the token incorporates robust dynamic data (such as incorporating transaction-specific information, or being single-use), a fraudster will not be

EXHIBIT 6 – HCE SOLUTION SECURITY COMPONENTS



HCE security layer	Description	Entity responsible
Communication Security	Communications between mobile payment application and TSP must be confidential and secure	Wallet provider / TSP
Device Security	Ensures device has not been compromised. Detection mechanisms include root, debug, and emulation detection	OEM, TSP
Application Security	Ensures mobile application had not been compromised. Includes obfuscation, white box cryptography and use of the Trusted Execution Environment (TEE).	Wallet provider, TSP
Tokenized PAN	Ensures that the PAN is not stored on the device. Tokenized PAN can be domain specific so that it can only be used for contactless and/or remote transactions.	TSP
Dynamic Data (Session Keys)	Keys can be single- or limited-use to reduce impact of a breach. Dynamic data (transaction- and device-specific into) limits token spoofing and replay.	TSP (or credential manager)

Source: *Consult Hyperion, HCE and Tokenisation for Payment Services; Sequent, Beyond Tokenization White Paper*

Dynamic data

Because payment credentials cannot be stored securely on the device, HCE requires the use of payment data that is constantly changing. Payment is enabled by loading limited use, domain-specific payment credentials on the device and storing them on the device until needed for a transaction. These dynamic credentials may be limited by number of uses, a time period, or both, before they expire. The short lifespan and dynamic nature of these credentials limits the risks associated with possible theft and interception. In the event a credential is stolen, TSPs and issuers should be able to identify inconsistencies in the dynamic data and decline the transaction. If dynamic data parameters are absent or not robust, fraudsters may be able to modify and transact (“replay”) with the stolen token. Issuers and TSPs may not be able to distinguish a “replayed” token from a legitimate token.

Issuers have options in the creation of dynamic data. One is to use a dynamic PAN that changes with every transaction. If dynamic tokenization is the selected approach, the

able to use/replay the token. The TSP and issuer will be able to identify inconsistencies in the dynamic data and decline the transaction.

dynamic token is provided by the TSP in advance of the transaction and stored on the mobile device. When the consumer transacts using the token, the transaction must pass through the TSP, where the original PAN is detokenized, and the transaction information, including the original PAN, is then passed on to the issuer to support authorization. Another option is to use session keys, which are cryptographic keys that are valid for one transaction. The transaction authorization process will evaluate the dynamic data for any errors and decline transactions where a mismatch occurs.

Issuers deploying HCE solutions will potentially have to determine how to manage the provisioning of dynamic data to the payment application on the mobile device. It is not possible to download dynamic data “as needed” because of the possible negative impacts on the transaction experience (credential must be present before payment can be initiated or latency issues may occur and offline transactions wouldn’t be possible). Issuers must determine how to authenticate the dynamic credential request coming from the mobile payment application and how many transactions will be supported in a single download of dynamic data (the lower the number of transactions, the lower the associated risk). Parameters need to be determined by issuers to ensure that a customer always has enough dynamic data (tokens or session keys) to be able to transact without interruption. It is important that dynamic data be provisioned using secure communication channels.

HCE solutions must continually evaluate the components of the solution to confirm that transaction risk is managed and payment security is maintained. This involves initial (and potentially ongoing) validation of the customer, and ongoing validation of the payment application, the mobile device, and the communications between the application and the cloud SE related to the request and provisioning of dynamic data.

Application security

Application security ensures that the payment application stored on the device has not been compromised in any way. Additionally, payment keys and other sensitive data stored on the device should be protected. One option is white-box cryptography, which prevents exposure of keys in memory or code. Another option is the use of a Trusted Execution Environment (TEE), which also allows for the secure storage of keys.

These measures prevent fraudsters from using malware or other methods to steal payment credentials and cryptographic keys from the device. If this material were stolen, fraudsters may be able transact using the credentials on the device.

Device security

HCE solutions assume that the mobile device is a less secure storage environment than a hardware-based SE, and implementations should include software detection mechanisms linked to the mobile device operating system that can determine if the device has been compromised. Mechanisms should be able to detect if a device has been rooted, is operating in a developer/debug mode, or is running on an emulator (among others). These scenarios compromise the security of the HCE solutions by exposing areas of the device that are normally protected. Fraudsters may be able to steal and use credentials from a mobile payment application that is run on a compromised device.

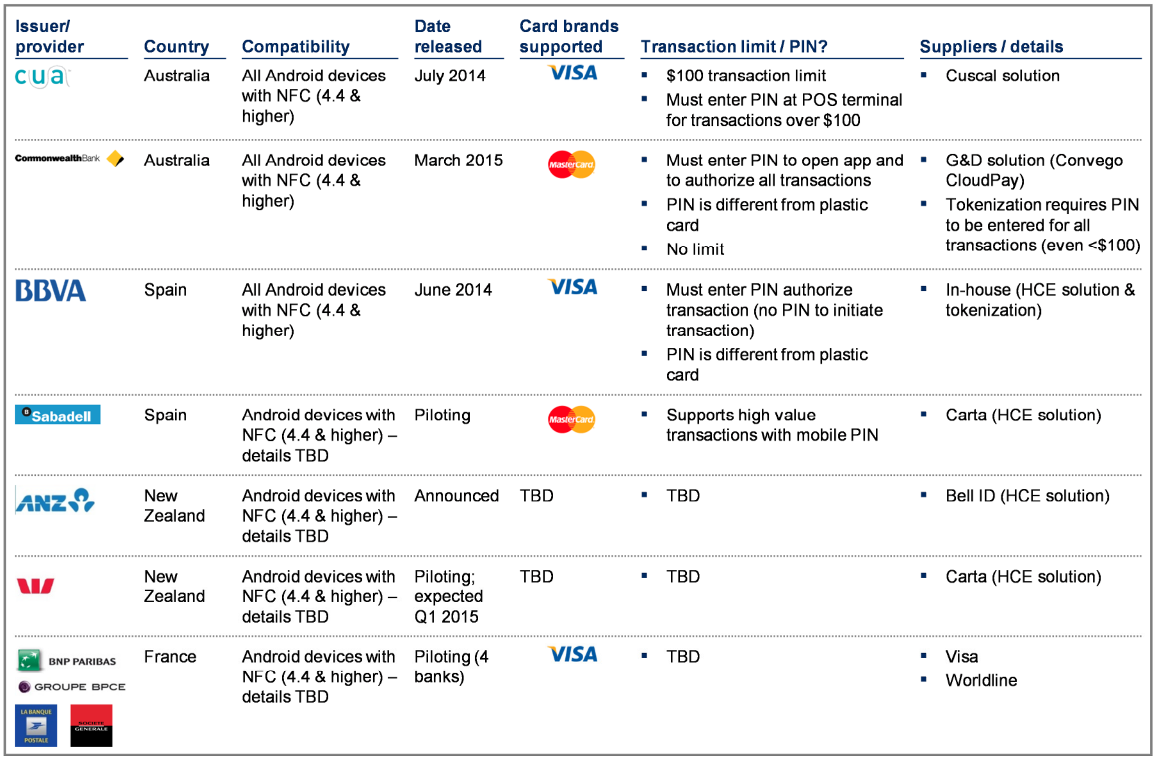
Communications security

The ongoing need to replenish dynamic data to support HCE means that there is frequent communication between the cloud and the device to support dynamic data provisioning. Communications between the handset application and the issuer cloud are confidential and must be protected (for instance, with strong encryption). If communications are intercepted and cracked, fraudsters may be able to steal the dynamic data provisioned to the device and perform transactions. Fraudsters may be also be able to spoof requests from the device to the cloud to get more dynamic data and perform more fraudulent transactions.

HCE DEPLOYMENT

Since HCE became available in late November 2013, proprietary HCE wallets have been launched in Australia, Spain, New Zealand, and France. Pilots are occurring in other countries, including Canada.

EXHIBIT 7 – SELECTED HCE IMPLEMENTATIONS IN MARKET



Issuer/ provider	Country	Compatibility	Date released	Card brands supported	Transaction limit / PIN?	Suppliers / details
cua	Australia	All Android devices with NFC (4.4 & higher)	July 2014	VISA	▪ $100 transaction limit ▪ Must enter PIN at POS terminal for transactions over $100	▪ Cuscal solution
CommonwealthBank	Australia	All Android devices with NFC (4.4 & higher)	March 2015	MasterCard	▪ Must enter PIN to open app and to authorize all transactions ▪ PIN is different from plastic card ▪ No limit	▪ G&D solution (Convego CloudPay) ▪ Tokenization requires PIN to be entered for all transactions (even <$100)
BBVA	Spain	All Android devices with NFC (4.4 & higher)	June 2014	VISA	▪ Must enter PIN authorize transaction (no PIN to initiate transaction) ▪ PIN is different from plastic card	▪ In-house (HCE solution & tokenization)
Sabadell	Spain	Android devices with NFC (4.4 & higher) – details TBD	Piloting	MasterCard	▪ Supports high value transactions with mobile PIN	▪ Carta (HCE solution)
ANZ	New Zealand	Android devices with NFC (4.4 & higher) – details TBD	Announced	TBD	▪ TBD	▪ Bell ID (HCE solution)
W	New Zealand	Android devices with NFC (4.4 & higher) – details TBD	Piloting; expected Q1 2015	TBD	▪ TBD	▪ Carta (HCE solution)
BNP PARIBAS GROUPE BPCE LA BANQUE POSTALE SOCIETE GENERALE	France	Android devices with NFC (4.4 & higher) – details TBD	Piloting (4 banks)	VISA	▪ TBD	▪ Visa ▪ Worldline

Source: *Company websites*

Given its infancy, concerns about HCE relate to insufficient details to support secure implementations, and lack of clarity regarding the roles and responsibilities of participants in the HCE ecosystem. The broader deployment of payment credentials into open mobile wallets may dramatically increase the impact of any specification inconsistencies and/or security gaps that are discovered.

Table 2 outlines some of the possible risks associated with HCE mobile payment solutions.

TABLE 2 – POSSIBLE RISKS ASSOCIATED WITH HCE MOBILE PAYMENT SOLUTIONS

Risk	**Description**	**Consumer/Merchant impact**
Technology Risk ***Assessment:***	Payment tokens are stored on the device. If the device is not secure, there is a danger of token capture and replay	User experience may not be as compelling as for SIM (device must be powered on, device

Risk	Description	Consumer/Merchant impact
Medium to High risk	Specifications are in early iterations and will require updating as the technology becomes better understood and more stable. This applies in particular to application security, device security, and tokenization The implementation approach can have a significant impact on the security provided by an HCE solution Certification criteria are unclear There are likely to be some interoperability issues as HCE solutions deploy globally and consumers load multiple HCE wallets on a single device	needs connectivity to replenish tokens, offline transactions may not be supported), although provision process is quicker Interoperability issues may impact the consumer and merchant experience
Operational Risk ***Assessment: Medium risk***	Reliance on new suppliers will require additional governance Transaction fraud risk is possible due to token capture/replay; insufficient risk management provided by token parameters Lifecycle management is simplified with HCE as HCE wallets are more easily moved from one mobile device to another	Mobile payment could be virtually ubiquitous, accelerating adoption (can work on all NFC-enabled devices, regardless of MNO)
Reputational Risk ***Assessment: Medium risk***	Lack of industry standards could lead to implementations that are not EMV equivalent	Security lapses can harm the integrity of the Canadian payments system, undermines consumer and merchant confidence

HCE is a new technology that is rapidly evolving. Although specifications exist to support cloud payments, they are early iterations (Visa was the first network to publish specifications in February 2014). Specific areas of concern related to HCE solutions include the following:

– **Early HCE implementations may not provide EMV-level security.** Interpretation of the specifications may deliver HCE solutions that are not optimally implemented to deliver EMV equivalent security (e.g., wallet apps, tokenization). If security layers are insufficient or lacking (e.g., device security and application security), it may be possible for fraudsters to intercept payment data/tokens and transact with that data. Strong device and application security, using techniques such as white-box cryptography and obfuscation make it more difficult to steal tokens.

– **Strategies to manage dynamic data must be comprehensive.** Token parameters must be carefully considered. Parameters such as domain restrictions limit risk in the event a token is stolen. Clear and prescriptive guidelines do not yet exist to guide the optimal selection of dynamic data parameters. HCE implementations must support the continuous management of data parameters to limit risk exposure.

– **Interoperability issues may emerge.** Interoperability is an ongoing concern as HCE wallets are deployed more broadly. Differences in implementation may result in acceptance issues or unintended customer and merchant impacts. Consumers may choose to have multiple HCE wallets, and may load the same credential into several wallets. Consumers may also have an SE wallet and an HCE wallet on the same device. Managing access to the NFC controller may be challenging. At present, there is no industry-level coordination to ensure multiple wallets will work in concert on the same device.

From a consumer and merchant perspective, there is little, if any difference in the transaction experience at POS between an SE and HCE technology. Both solutions leverage NFC and both solutions will respond to messaging from the POS if a CVM is required.

The table below outlines some of the important differences between SE and HCE solutions that should be considered by issuers.

TABLE 3 – COMPARISON OF HCE AND SIM SOLUTIONS

Solution Aspect	SIM SE	HCE
Device requirements	Mobile device with NFC capability NFC-enabled SIM card Device must be certified by MNO and issuer	Mobile device with NFC capability
Provisioning	Requires Issuer TSM and Telco TSM to deploy payment application and credentials to the device.	Customer downloads wallet app; payment credentials are initially delivered and replenished over the air

Solution Aspect	SIM SE	HCE
	The customer downloads the wallet UI or it may be preinstalled by the MNO Changing mobile devices will require the customer to reload the wallet and all credentials; the new mobile device may not be supported	HCE wallets can be more easily migrated to a new mobile device
Usability	Works at online and offline terminals Works whether mobile device is on or off (depending on implementation) Passcode can be entered directly into the device Data connection required for initial provisioning; not required for transacting	Offline transactions are challenging to support due to relevance of dynamic data Offline PIN is not supported Device must be on and payment app must be running to transact Data connection is required for initial provisioning and ongoing token replenishment; it is not required for transacting
Security	Credentials stored in hardware-based and tamper-proof secure element on the SIM PAN may or may not be tokenized	Credentials stored on secure element in the cloud Payment tokens stored on the device are single- or limited-use to manage the risk of storing in software Layered security is required to manage the risk of not having a hardware-based secure element
Business model	Relationship with individual MNOs to support the loading of the credential on SIM Trusted Service Manager to manage payment application	Relationship with TSP to manage payment credentials
Maturity	Backed by robust and mature standards Certification process is well	Specifications continue to evolve and may need to be harmonized across OEMs and payment networks

Solution Aspect	SIM SE	HCE
	defined by payment brands	Certification process is not yet well defined by all payment brands
Interoperability	Standards are available to support interoperability at most key interaction points	Interoperability will need to be monitored as deployments increase

Open mobile wallets

The early days of mobile payments saw the launch of proprietary closed-loop solutions like Starbucks, where the credential issuer is able to control all aspects of the ecosystem. These early solutions relied on static credentials (e.g., barcodes), and leveraged existing POS capabilities (e.g., scanners).

The deployment of open-loop mobile payments requires acceptance at POS, which has been facilitated by the rollout of NFC-enabled terminals. Financial institution proprietary wallets leveraged NFC and hardware secure elements (SIM) to deliver secure contactless mobile transactions. Issuers created the mobile application, engaged a trusted service manager (TSM) to deploy and manage the application, and rented space from an MNO on the secure element to install the application on the mobile device.

The evolution in mobile payment business models has been supported by the evolution in the technology. In the past six months, several major announcements have indicated continued change in the mobile payments space. The launch of Apple Pay in October 2014 has brought the “open mobile wallet” business model to the forefront.

A detailed overview of Canadian and U.S. open mobile wallet solutions can be found in Appendix C.

OPEN MOBILE WALLETS – POTENTIAL IMPACTS ON ISSUERS

Some inferences can be drawn from the mobile payments announcements of the past six months. Large technology companies are serious about mobile payments and are launching solutions that emphasize industry-leading customer experience. Moreover, it is our view that it is critical that open mobile wallets launching in Canada deliver EMV-equivalent security.

In the event that Apple Pay remains the only viable platform for iPhone, the battle for relevancy will likely be carried out on the Android platform. The introduction of HCE has removed many of the barriers to rapid deployment of mobile payment solutions. The entry of payment networks into new business lines (e.g., tokenization) offers another opportunity to accelerate the development and deployment of open payment wallets by creating solutions that dramatically simplify the loading of a payment credential. Large payments players are shoring up their positions through the introduction of new products and services (e.g., Android Pay, Samsung Pay) and through acquisition (e.g., Google’s purchase of Softcard, PayPal’s purchase of Paydiant).

This rapidly changing market presents some substantial issues and risks that may have an impact on mobile payments in Canada. It is assumed there will be a proliferation of open mobile wallets supported by HCE technology and products/services like Android Pay. It is also assumed that consumers will want to load their payment credentials in multiple wallets.

POTENTIAL RISKS ASSOCIATED WITH OPEN MOBILE WALLETS

With proprietary wallet applications, issuers are able to tightly manage the security of the solution and the customer experience. Issuers control the availability of the mobile payment application, and ensure that they know the customer who is requesting a digital credential. Issuers manage the selection of the CVM (PIN/passcode), define the dynamic data parameters, manage token generation and oversee the provisioning process. In open mobile wallet business models, the issuer relinquishes control to the wallet provider and the TSP for many of these functions.

Participation in open mobile wallets may require the issuer to “outsource” key elements of the registration and provisioning process and overall transaction security to the wallet provider and TSP. While issuers may not manage all potential points of security weakness in an open mobile wallet solution, they continue to bear liability for the end-to-end transaction. This presents several risks.

Inadequate customer identification and verification may increase the incidence of account takeover fraud

The ability to truly confirm a customer’s identity will be critically important with respect to open mobile wallets. An open mobile wallet that provides the highest level of security can still present fraud risk if the identity of the customer requesting the credential is not confirmed.

For example, a fraudster that steals a payment card or card number could attempt to enroll that card in an open mobile wallet. If the process to identify and validate the user is weak, the fraudster may be able to successfully register the card and enable the wallet. If this occurs, the fraudster will be able to transact at POS or remotely with impunity until the legitimate cardholder or issuer detects the fraud. Even the most secure mobile payment solution will not be able to compensate for poor ID&V. Robust ID&V is critical element that supports the integrity of the payments system.

In an open mobile wallet solution, the payment credential issuer continues to manage the relationship with the customer, and all of the obligations associated with that relationship. For this reason, every payment credential request should be referred to the issuer of the credential for review and decisioning. As the owner of any liability associated with the account, the issuer – not the wallet provider or the TSP – would be best positioned to determine whether to approve a credential request. In this way, issuers remain responsible and accountable for the validation of the consumer requesting the credential. If issuers wish to outsource the authentication process, it could be to a vendor of their choosing who will meet issuer ID&V requirements.

To date, issuers have generally not been required to respond to requests for payment credentials from third parties and will need to develop processes to confirm the identity of the customer. Additional information is available as part of the open mobile wallet registration process, and issuers should request that data pertaining to the mobile device (e.g., “device fingerprint”) and the mobile payment application (e.g., application

ID) are captured and provided by the wallet provider as well as customer and payment credential information. Information regarding the verification method (e.g., fingerprint, passcode) should also be requested by issuers and provided by the wallet provider. All of this data will assist the issuer to effectively bind the customer, the credential, the payment application and the device. Data captured at registration can also be used to support transaction authorization decisions.

ID&V will be the cornerstone of open mobile wallet security. It will be critical to identify account takeover attempts at the time of registration. Weak ID&V at a single issuer could potentially undermine consumer and merchant confidence in the Canadian payments system. It is critical that the customer's identity be assured.

If there are inconsistent approaches to ID&V among issuers, fraudsters will be able to quickly determine which issuers have inadequate processes. Issuers in the United States have had to address this problem, and other jurisdictions can learn valuable lessons from their experience. It is in the Canadian payment industry's interest that ID&V be reliable at an industry level. The challenge will be implementing robust ID&V practices without introducing too much friction into the provisioning process.

New customer verification methods (CVMs) are emerging

In the payments ecosystem, robust authentication methods exist to ensure only authorized customers can transact. An individual can be authenticated in three ways:

Knowledge factors. Something the user **knows**

– Examples: Password, passphrase, PIN, pattern, challenge response

Ownership factors. Something the user **has**

– Examples: ID card, payment card, hardware token, device with software token

Inherence factors. Something the user **is** or **does**

– Examples: signature, biometrics (fingerprint, facial recognition, voice recognition, retinal scan, heartbeat recognition)

Issuers have relied on two factor authentication consisting of something the user has (e.g., a payment card, a mobile device) and something the user knows (e.g., a PIN). Traditionally, inherence factors – something the user is – have been the weakest method of authentication. Handwritten signatures are difficult to reliably validate in person, let alone remotely.

Recent technology innovation, including hardware that supports biometric authentication, has brought inherence factors back to the forefront. Smartphones, such as the iPhone 6 and Galaxy S6, support fingerprint scanners. Consumers can use the fingerprint reader to unlock the device as well as to provide access to applications on the mobile device. Apple Pay leverages the iPhone Touch ID capability to authenticate each payment transaction; Samsung Pay is expected to leverage the fingerprint in a similar way.

Fingerprints can be problematic and an unintentional source of family fraud (credit card fraud that is perpetrated by a family member). The user can often register between five and ten fingerprints in the device that can be used to do many things in addition to authorizing payment. For example, children of the device-owner may register their fingerprints to be able to unlock device. This could allow the children of the cardholder to make unauthorized purchases without the cardholder's knowledge.

Moreover, these devices are typically covered with fingerprints and, in the event that the device is stolen or lost, fraudsters could potentially create a fingerprint and gain access to everything on the device, including the ability to make payments. This is not a theoretical problem – instructions on how to crack several fingerprint scanners in the market are available on the internet.

Additional biometric options (e.g., voice, facial, and heartbeat recognition) are expected to be made widely available in the foreseeable future. The projected benefits to customers are clear: the payment experience is faster and more convenient.

The CVM used for open mobile wallet payment probably won't be an issuer CVM

With EMV chip and PIN cards, the customer is advised to select a four digit PIN that is unique to that payment card. With open mobile wallets, the verification method to make a payment may be the same verification method for all payment credentials in the wallet and is very likely to be the same verification method used to unlock the device.

With an EMV chip and PIN transaction at POS, the issuer receives confirmation that the PIN entered into the POS device matches the PIN stored on the card (the match is confirmed by the POS) or the PIN stored on file (PIN is confirmed by the issuer host). With open mobile wallets, the verification method may not be a PIN, and the match between the verification method provided by the consumer and the verification method stored on the mobile device will be confirmed by the device. Issuers have no line of sight to the actual verification method, and must 'trust' the device to confirm the match. Biometric verification methods may not be as secure as PIN. Knowledge-based factors, like passwords and PINs, require an exact match to succeed. However, biometrics are "noisy" – finger position and pressure impact fingerprint impressions. Lighting conditions may impact facial recognition. To accommodate for "noise", levels of tolerance are set to allow for a certain amount of variation.

The verification method becomes relevant for issuers for transactions at POS that are over the contactless high value transaction limit of $100. Until the reliability of biometric verification methods have been proven, we would prefer a verification method that is something the customer knows, rather than something the customer is.

There may be customer impacts related to mobile verification methods. There will be additional security considerations related to mobile device-based verification options that will have consumer impacts. It will be important to educate customers of these impacts so that they are aware of the risks and learn to differentiate and protect their mobile verification methods as they protect their PINs today.

The CVM landscape is changing with the introduction of emerging biometric recognition options. As consumers increasingly transact with a mobile device, issuers may need to reduce their reliance on the mobile device verification method and increase their reliance on other data (i.e. device and application information) to identify and validate the customer.

Minimum standards, certification and/or review processes for open mobile wallets are unclear

Although there are cloud payment specifications available from the payment networks, it is not clear how these specifications are to be implemented by open mobile wallet providers. Additionally, there are no clear certification and/or review and approval processes to ensure open mobile wallets meet minimum standards and adhere to payment network specifications. Validation of token requestors, including wallets, is the responsibility of the TSP. At the time of writing, no guidelines exist on how to evaluate these requestors. Fundamentally, issuers need confidence that third parties can deliver adequate security to protect the customer and payment credentials.

Issuers may have to rely on transaction security provided by third parties

Open mobile wallets that rely on HCE technology could present more risk as issuers may have limited control over how the wallet solution protects the mobile device (e.g., application security, device security, communication security) and the parameters that define the nature of dynamic data, and how dynamic data is provisioned to the mobile device. The wallet provider and/or its partners/contractors may not deliver the same level of security as an issuer’s proprietary solution. Issuers will need to truly understand all aspects of security associated with an open mobile wallet HCE solution in order to evaluate any technology risk associated with the wallet solution.

The roles and responsibilities of the TSP are likely to evolve

Open mobile wallets have introduced the concept of PAN tokenization into the payments flow. Instead of the actual card number, an alternate card number (a tokenized PAN) is provided. Merchants never see the actual card number, only the tokenized PAN. Tokenization is not a new concept, but it has not been deployed as part of the payment process before.

At time of writing, large open mobile wallet providers (e.g., Apple, Samsung, Android) have all announced relationships with the payment networks, and it is expected that tokenization services for these open mobile wallet solutions will be provided by

American Express Token Service, MasterCard Data Enablement Services, Visa Tokenization Services, and by Interac in Canada. Partnership with the networks provides open mobile wallet providers with a single point of connection per network to all the associated card issuers (the reverse is also true). This model dramatically increases speed to market for the wallet provider, but limits choice of suppliers for issuers.

EMVCo published its Payment Tokenisation Specification in March, 2014. This document is a first version and will be updated over time. In its current version, it provides minimal guidance regarding the building and maintenance of token requester APIs, token vaults, token storage and security, token provisioning platforms and token registries. For more information on concerns regarding the EMVCo specification, please see Appendix D.

Although not a defined function in the EMVCo tokenization specification, payment network TSPs have also taken on the role of provisioning digital credentials to a secure element. With the introduction of open mobile wallets that rely on HCE technology, it is expected that the roles and responsibilities of the TSP will be expanded further to include the provisioning of dynamic data. It is important that these roles and responsibilities are clearly described.

Ideally issuers will not be required to rely upon a third party to define dynamic data parameters, and will be in a position to define and monitor the effectiveness of a dynamic data strategy. However, business models are evolving rapidly, and issuers may choose to provide credentials to requesting entities that they know little about, and over which they have little control. In the situation where the TSP is the intermediary, it is assumed that the TSP will take accountability for ensuring that all aspects of the tokenization service and dynamic data provisioning service are secure and protect all involved parties from risk.

Open mobile wallet transactions will generate more data for more entities

Mobile payments have the potential to generate more data than traditional chip and PIN transactions at POS. What is certain is that there will be more data, seen by more entities, and stored in more places. This presents both opportunities and challenges for issuers and the payments ecosystem.

Transactions initiated from a wallet could provide additional information to the issuer about the device (e.g., IMEI, MEID, IP address), about the hardware (e.g., specifications, Android ID, iPhone UDID), about the wallet (e.g., App ID), and about location (e.g., GPS). There may be an opportunity for issuers to support transaction authorization and fraud monitoring by integrating this data into existing transaction systems.

This data, including transaction data, will likely also be seen by other parties (e.g. the open mobile wallet provider) who may find this information useful. It is not clear which parties should have access to and own this data. Wallet providers may use this data to better understand their customers; merchants may use this data to drive customer loyalty and deliver custom offers.

The increased availability of data presents opportunities and risks. Transaction data will now potentially be stored by third-party wallet providers and TSPs. Issuers do not have control over how third parties secure this data. It is not clear how to prevent these entities from seeing this information, and the issuer has no control over the security to be used in storing this information. It is important that issuers are aware of where transaction data is captured and stored in order to protect data commitments to cardholders, and to share obligations with third parties as appropriate.

Considerations to accelerate adoption of open mobile wallets in Canada

To truly drive the adoption of mobile payments, the customer experience with the mobile device would need to be as to be as good as, or better than the experience with the payment card. Consumers should be able to load any of their payment credentials into any wallet of their choosing. They should be able to pay for any transaction of any value through any channel with their mobile device. Until the mobile device provides the same or more functionality as the payment card, adoption of mobile payments may continue to increase slowly.

It is estimated that ~30% of the POS devices in Canada support NFC contactless payment[12]. In order for consumers to transact exclusively with a mobile device, this penetration must continue to increase to the point where 100 percent of POS devices support NFC. Contactless payment is currently available for transactions less than $100. Providing consumers with the ability to pay for transactions of any value at the POS will be a precursor to increasing the acceptance footprint. Terminal upgrades are being deployed that will support high value transactions. It is anticipated that it will take until 2018 for these upgrades to be deployed.

A substantial challenge for Canadian consumers in the adoption of mobile payments is the inconsistent availability of SE solutions. It is not possible for any Canadian financial institution to market mobile payments broadly across its customer base. Consumers struggle to confirm their eligibility for mobile payments ("*Is my payment card available for mobile payments? Is my carrier supported? Is my mobile device supported?*"). Despite the fact that there are five Canadian banks that are issuing mobile credentials and that all of the large MNOs support mobile payment across multiple devices for one or more issuer, it is estimated that fewer than 25%[13] of Canadian consumers have the required overlap between payment credential, carrier relationship and mobile device to participate in mobile payments.

Canadian issuers are exploring HCE mobile payment solutions to address many of these deployment challenges. HCE is an emerging technology, and over the next several years the industry intends to work towards clarifying specifications, and identifying and managing technology and interoperability risks.

Technology companies like Apple, Samsung and Google will likely change the way consumers, and payments stakeholders, think about mobile payments. These players will likely leverage new technologies, introduce new business models and deliver compelling customer experiences. These solutions will provide options for Canadian consumers. The adoption of these solutions will depend on the wallet value proposition, the penetration of mobile devices in market that support the wallet (operating system and NFC capability) and the NFC acceptance footprint.

[12] Industry interviews

[13] Proprietary analysis

Until consumers are able to use the mobile device for all payments, adoption will be limited. High value transactions at point of sale should become available over the next few years as terminal upgrades roll out. It will likely be necessary for proprietary Canadian wallets to support remote payment capability to compete with large global wallets. In-application payments are expected to increase dramatically. Canadian issuers will need to determine whether to and how to support payments of this nature.

To date there have been two Canadian open mobile wallets that have launched. One of the main challenges for open mobile wallet providers and credential issuers is how to support the requisition and loading of a proprietary mobile payment credential into another party's open mobile wallet. This can be particularly challenging in an SE environment where every issuer may not have a relationship with every MNO, and may not support every device. For HCE solutions, challenges may exist related to dynamic data parameters and issuer requirements for minimum levels of security.

To achieve rapid deployment of open mobile wallet solutions, it may be helpful to identify opportunities for issuers and wallet providers to easily exchange information and payment credentials.

Potential areas of focus to achieve guiding principles

Mobile payments are rapidly evolving and have the potential to change the way goods are bought and sold across Canada. Open mobile wallets have the potential to benefit all industry participants, especially consumers and merchants, by reducing friction and providing value-added services. Adoption of mobile payments throughout the ecosystem will require a compelling value proposition for consumers and merchants and security that is equivalent or better than that provided by payment cards. Only then will consumers leave their wallets at home.

Deliver security equivalent to the EMV payment card

The pace of payments evolution has been accelerating in Canada, which presents both opportunities and risks. The launch of open mobile wallets in the United States has caused Canadian issuers to consider impacts to payment security and to learn from the US experience. Canada has invested heavily in EMV infrastructure and Canadian consumers and merchants have come to rely upon and expect this level of security. Open mobile wallet providers operating in Canada should provide solutions that deliver transaction security that is equivalent to that of the Canadian market.

HCE is the most recent payments technology to be launched in Canada and is likely to be widely deployed in both proprietary issuer wallets and open mobile wallets. The integrity of HCE solutions depends on the thoughtful implementation of layered security, including a rigorous approach to dynamic data, in order to deliver required levels of payment security. Canadian issuers will need to determine how to work effectively with the payment networks, wallet providers and Token Service Providers to ensure solutions in market deliver EMV-equivalent security.

It will likely be some time until robust industry standards and payment network specifications are in place to support HCE. In the interim, roles and responsibilities will continue to evolve and security and interoperability issues may arise. Issuers will have to navigate this landscape carefully.

Innovation in mobile payment solutions should strengthen the security and integrity of the Canadian payments ecosystem and provide payment security equivalent to current EMV payment credentials in market.

Robust ID&V is required to adequately protect consumers against payment card fraud

With proprietary mobile wallets, issuers are able to manage the entire solution and associated risks. Participation in open mobile wallets may require the issuer to “outsource” key aspects of the solution to the wallet provider. Issuers will continue to manage the relationship with the customer, and should consider reviewing all digital credential requests received from open mobile wallet providers. Robust ID&V will be critical to protect consumers against account takeover fraud. Even an open mobile wallet with strong transaction security can be compromised if a payment credential is fraudulently loaded.

As part of the registration process, issuers should consider requesting a minimum set of data pertaining to the device, wallet application, and verification method (e.g., fingerprint, passcode). This data will support strong binding between the consumer, the payment credential, the device, and the wallet application that can support transaction authorization decisions.

Canadian issuers currently rely on the PIN to authorize POS transactions. Canadian payments stakeholders communicate as an industry about the importance of protecting the PIN, and the importance of having a unique PIN for each payment card. With open mobile wallet solutions, consumers will likely use the same verification method for all payment cards in the wallet, and that verification method may also be used universally across all applications on the device. Issuers may not receive any information about the verification method other than a 'match' between the information about the verification method that is stored on the mobile device and the actual verification method presented by the consumer. For wallets that support a transaction 'preauthorization' process (verification method, tap) the verification method will be used to initiate payments of all values across all channels.

Best practices related to EMV payments call for a four digit PIN that is unique to the payment card. The use of a biometric verification method that is not unique to the card, and perhaps not unique to the wallet, and is not something that the consumer knows (like a passcode) may create risk for issuers and consumers. Ideally the industry will support a payment process for transactions that are over $100 through all channels (POS and remote and in-app payments) that is consistent across payment products and wallets.

Issuers may have to leverage data other than the verification method to confidently approve transactions. Effective ID&V processes should result in strong binding between the consumer, the credential, the payment application and the device. Additional data provided as part of the registration process could be requested by issuers and supplied by wallet providers to confirm the cardholder. Issuers could leverage this additional data to support transaction authorization decisions, potentially reducing the reliance on verification method while maintaining overall transaction security.

Provide a compelling value proposition to consumers

To truly drive the adoption of mobile payments, the customer experience with the mobile device would need to be as to be as good as, or better than the experience with the payment card. Ideally consumers should be able to load any of their payment credentials into any wallet of their choosing. They should be able to pay for any transaction of any value through any channel with their mobile device.

Canada boasts a reasonable NFC acceptance footprint with strong acceptance in key verticals. Ultimately all POS devices would need to support NFC mobile payment in order to fully convert consumers to mobile payments.

Although mobile payment solutions exist in market today, consumers require alignment between their issuer, MNO and device in order to participate. Coverage is limited within and between issuers and MNOs. HCE solutions that launch over the near term are expected to address challenges related to carrier, and to some degree, the device. The expected launch of Apple Pay in Canada will provide mobile payment capability for consumers who carry iPhone mobile devices.

Canadian issuers will need to consider the attributes of their proprietary mobile payment solutions in light of the functionality expected to be included with global wallet providers such as Samsung, Android and Apple. Canadian solutions do not support transactions over $100 at POS, and there is currently no capability to transact remotely or in-app. Issuers should identify and consider options to support remote acceptance.

Open mobile wallets are expected to help to drive adoption of mobile payments. The use of ‘one to many’ interfaces could dramatically accelerate the availability of open mobile wallets in Canada. An industry level service capability that connects wallet providers and payment credential issuers could be leveraged to support credential requests, offer industry level fraud monitoring, interoperability testing, and dynamic data provisioning and management.

Canada presents a mobile payments environment supported by stakeholders with aligned interests. The global payments landscape is evolving. Technology advancements will support rapid deployment of mobile payment capability. Large players are positioning themselves as meaningful players in the mobile space. Canadian issuers will continue to manage the relationship with the customer, and the responsibilities that accompany this relationship. In the evaluation of new opportunities to provide consumers with additional mobile payments options, it is important that issuers maintain the focus on payment security, ensure that consumers and retailers remain protected against fraud and that risks are adequately managed. In this way Canada’s investment in payments security will be upheld.

The Proposed Path Forward

Robust customer authentication on enrollment

Due to the distributed nature of enrollment in open mobile wallets, authentication of customers will be the cornerstone of maintaining open mobile wallet/payment credential integrity. It will be critical for issuers to identify account takeover attempts at the time of mobile wallet registration, prior to provisioning a payment credential. Because issuers continue to hold the liability for fraud, every payment credential request should be referred to the issuer of the credential for scoring and decisioning. Canadian issuers are encouraged to ensure consumers continue to be protected against account takeover fraud by implementing adequate Identification and Verification of Customer (ID&V) activities. Ideally 100% of mobile wallet payment credential requests would be sent to issuers and scored against issuer proprietary risk management protocols. It would be helpful to define minimum data requirements to support credential provisioning, and determine how open mobile wallets would provide this data to issuers as part of the credential provisioning process. It may be possible to include the data as required elements of the payment credential request. This approach would potentially require every TSP operating in Canada to have the capability to capture this data and to pass it from wallet providers to issuers. Ideally, the required ID&V data will be the same across all payment networks (American Express, Interac, MasterCard and Visa).

Customer authentication at time of transaction

In addition to introducing new business models into the Canadian payments environment, open mobile wallets will introduce new verification options (i.e. fingerprint) and new transaction types (i.e. in-app transactions). Issuers have traditionally relied on the PIN, a proven Customer Verification Method (CVM), to confirm the presence of the cardholder at the time of purchase. Open mobile wallets may be designed to use customer verification information that is stored on the mobile device, not stored or known by the issuer. In this situation, when the customer transacts, issuers will have to rely on the wallet provider to determine if the verification information presented to support the transaction is a true match with the verification information stored on the mobile device. The inability to verify the customer will be problematic for issuers who must comply with industry codes of practice and payment network zero liability policies. Canadian issuers prefer a payment process that requires the provision of verification information for high value transactions (currently >$100) that they can validate as a control on their fraud liability. When the transaction exceeds the HVT limit of $100, consumers will be asked to provide verification information to confirm they are present at the transaction. Ideally, the HVT payment experience will be consistent across all credentials within a single wallet, and across all wallets the consumer may choose to use to drive consumer adoption and ease of use.

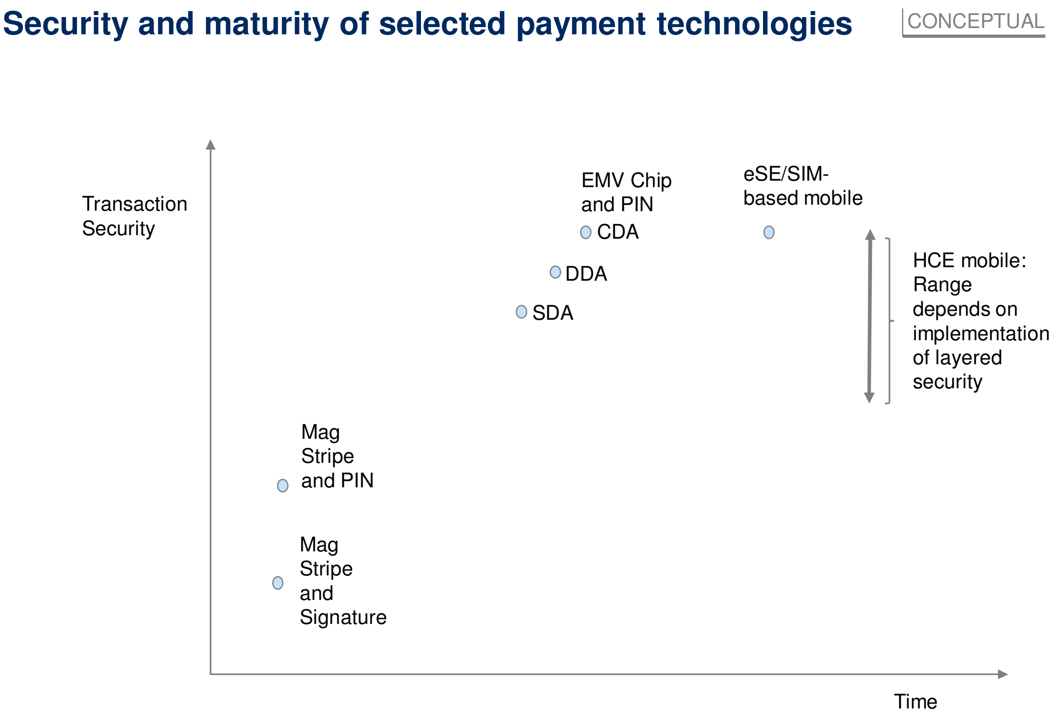
EMV equivalency and issuer management of dynamic data

Open mobile wallet providers and TSPs should introduce solutions and services that support the level of payment security already established in Canada. To protect the substantial investment that has been made in the Canadian payments infrastructure, and to continue to deliver the level of security that consumers and merchants have come to expect and rely upon, open mobile wallets that seek to launch in Canada should provide security equivalent to that provided by EMV Chip and PIN technology.

Cloud-based solutions require diligent management of payment-related data that is stored on the phone. In order to protect consumers and merchants, it is important that this payment data is not useful to fraudsters. This is accomplished by disguising the card number (tokenization) and regularly refreshing other important data elements (dynamic data). The more frequently the data is refreshed, the more secure the solution will be. Dynamic data, and the protection of dynamic data, are critical components of payment security. Issuers would like to be in a position to manage the key attributes of their tokenization and dynamic data strategies to support management of transaction liability. It is in the interest of all Canadian mobile payments participants that minimum industry standards related to dynamic data be developed to deliver EMV equivalency. Issuers ideally will be positioned to maintain control over dynamic data parameters to ensure EMV-level security is provided.

Appendix A – Security and maturity of selected payment technologies

Appendix A



Appendix B – New roles to support NFC Mobile Payments

Appendix B – New roles to support NFC mobile payments

Role	Description
Controlling Authority (CA)	The CA may manage key exchanges in an open mobile wallet. This is a model that is recognized but not mandated in the *NFC Mobile Payments Reference Model.* It is considered an alternative to many-to-many relationships between a payment credential issuer's Trusted Service Manager (TSM) and a Secure Domain Manager's TSMs.
Mobile Network Operator (MNO)	The MNO is the provider of mobile device connectivity services. Examples: Bell Mobility, Rogers, TELUS
Original Equipment Manufacturer (OEM)	The OEM produces the mobile device hardware that is used by the end user. Examples: Apple, Blackberry, HTC, Samsung
Secure Domain Manager (SDM)	The SDM manages access to the secure element; this role is often combined with that of the MNO.
Trusted Service Manager (TSM)	The TSM installs the payment credentials in the secure element. It provides a secure link between multiple parties (e.g., the credential issuer and the MNO) to facilitate the installation of payment credentials.
Wallet provider	The wallet provider provides the end-user-facing interface.

Source: *Canadian NFC Mobile Payments Reference Model*

Appendix C – Overview of open mobile wallet providers

Apple

Apple Pay

In October 2014, Apple launched Apple Pay – a mobile payment solution that supports POS and remote transactions. Initially supported by a handful banks, Apple Pay is now supported by over 200 U.S. partner banks as of April 2015. Commanding approximately 40 percent of the US smartphone market[14], Apple is in the process of altering the US payments landscape.

Apple has partnered with Visa, MasterCard, Discover, and American Express to provide a turn-key payment solution. To participate, issuers must set up an ID&V process to validate cardholders who register and provide an issuer master key to the payment network to generate a token PAN for Apple Pay.

Apple has leveraged many of the industry’s learnings in its launch of Apple Pay. The wallet is easily downloaded, and loading credentials is a simple process. The POS payment experience is quick and frictionless. Apple Pay requires no investment from merchants other than NFC-enabled terminals. In countries like Canada and Australia that have high contactless acceptance, retailers can already accept Apple Pay without doing anything. Apple has introduced a mobile payment process that is as easy as tapping a card. And although loyalty is not yet a part of Apple Pay, it is not hard to imagine how Apple will include loyalty in the near future.

Apple is also transforming online and remote payments. Apple has created its own “Acceptance Mark” that allows consumers to pay for goods on a retailer’s website or to pay in-app simply by selecting “Apple Pay” and authorizing payment with a fingerprint. The Apple Pay payment experience is well-suited to remote payments, and a number of retailers (Uber, Panera Bread, Target, Airbnb) have already deployed Apple Pay in-app acceptance.

At time of writing, Apple Pay is only available in the United States. Launches in other countries have not been formally announced.

Google

Google Wallet

Google launched its SIM-based wallet in September 2011. Partnering closely with MasterCard, the solution leveraged a virtual MasterCard credit card credential loaded on the SIM that allowed the user to pay using NFC at POS. The merchant was paid by Google; Google then charged the customer’s credit card on file. The business model

[14] ComScore MobiLens, March 2015

was challenged as Google Wallet earned lower card-present interchange on the POS transaction than the higher card-not-present interchange it paid to the issuer of the credit card on file. The business model as is created operational challenges for issuers and consumers related to loyalty cards, and allowed Google to capture all of the transaction data. This presented challenges to loyalty since issuers were unable to determine where cardholders were transacting and therefore unable to offer points multipliers (for example, double points at grocery stores). Deployment was challenging for Google as the only MNO that would support the wallet was Sprint (MNOs participating in Softcard, a SIM-based mobile wallet service backed by AT&T, Verizon, and T-Mobile, would not support the product).

In November 2013, Google announced that Android 4.4 KitKat would support Host Card Emulation (HCE), and in March 2014, Google announced that it was terminating NFC tap-and-pay support for Android operating system versions that were older than Android 4.4 KitKat. In February 2015, Google announced that it had acquired technology and patents from Softcard to improve its payments service. As part of the purchase, Google negotiated terms that will see Google Wallet preloaded on NFC-enabled Android devices sold by AT&T, Verizon, and T-Mobile. In early March 2015, Softcard announced that it would close down all accounts as of March 31, 2015 indicating that Google will not be providing support for SIM-based solutions. Google appears to be focused on HCE as the preferred technology platform for mobile payments.

At time of writing, Google Wallet is only available in the United States.

Android Pay

In early March 2015, Google announced Android Pay, a platform that will enable developers to integrate mobile payments into their applications using an API layer. The API will also be available for use by issuers and merchants to design their own payment applications on Android. The Android Pay platform will support HCE, tokenized card numbers, and NFC. Future enhancements will allow Android Pay to use biometric devices like fingerprint scanners. It is not known when Android Pay will be publicly available; further information about an expected 2015 launch is expected in soon.

Google has stated that Visa, MasterCard, and American Express will support Android Pay when it launches. It is possible that tokenization services will be provided by the payment networks, similar to Apple Pay. If this is the case, Android Pay will be able to provide an end-to-end solution for wallet creators that requires only the creation of the user interface. Issuers will be required to work with the payment networks' TSPs to support Android Pay.

PayPal

PayPal is a major player in online commerce, and this is still where the majority of transactions originate[15]. PayPal has been experimenting with physical POS payments for a few years, and announced the launch of its digital wallet in September 2013. The PayPal wallet app allows consumers to store credit cards, pay at bricks and mortar stores that support PayPal, ordering ahead from select restaurants, and sending and receiving money, and finding local deals. In 2014, just under 20 percent of PayPal total sales of $226 billion were made on mobile devices – a small percentage of which were physical POS transactions.

In March 2015, PayPal announced the purchase of Paydiant, a company that makes mobile wallet technology that is powering payment apps for merchants and issuers. Paydiant is a software-based solution that generates a Quick Response (QR) code either on a POS terminal or on a receipt. The customer takes a picture of the QR code and can select how to pay for the transaction from credentials stored in the wallet. Credential information is securely stored in the cloud and is never shared with the merchant. The credential information is sent securely to the acquirer, who processes the transaction as usual. Paydiant is the wallet supplier selected by MCX, a consortium of U.S.-based merchants that have joined together to build an open mobile wallet that provides merchants an alternative to credit and debit.

Samsung

Samsung Pay

In early March 2015, Samsung announced the expected summer launch of Samsung Pay in the United States and Korea. Samsung Pay offers two solutions: depending on the device model and country, the credentials will be stored either in hardware on an embedded secure element or in the cloud. Historically, Samsung devices in the North American market have shipped without an embedded secure element – it is possible this will continue. In either case, dynamic data will be generated in the cloud.

Like Apple Pay, Samsung Pay leverages tokenization – credit card numbers will be tokenized and replaced with a device-specific token. This solution will use HCE technology. Tokenization services are likely to be provided by payment networks as they are with Apple Pay.

In addition to supporting NFC, Samsung Pay will support mag stripe transactions in the U.S. only using a proprietary technology called Magnetic Secure Transmission (MST) that Samsung obtained by acquiring LoopPay in February 2015. This technology allows the customer to make contactless payments at traditional mag stripe POS devices without NFC. In theory, approximately 90 percent of merchants in the United States will

[15] www.paypal-media.com; Q4 2014 Fast Facts

have the capability to immediately accept contactless payments from Samsung Pay using MST[16].

Rogers

suretap wallet

Rogers launched the suretap wallet April 2014 – a SIM-based solution available only to Rogers customers. The suretap wallet supports the Rogers Prepaid MasterCard, which customers can load at their convenience. The card must be loaded prior to use, as transactions do not "flow through" to another card on file. Rogers charges fees to use this card: $2 to add value to the card and a $2.50 monthly maintenance fee. Users of the suretap wallet can purchase and load gift cards from select merchants, including Swiss Chalet, Indigo, and Harvey's.

At time of writing, suretap wallet is only available in Canada.

TD Canada Trust/PC Financial

UGO

UGO Wallet was announced in November 2013, and launched in November 2014 as Canada's first open mobile wallet that combines multiple payment and loyalty programs. A joint-venture between TD and PC Financial, UGO allows customers of both banks to load credit cards for mobile payments. The UGO Wallet supports multiple loyalty programs, including PC Plus. PC Plus members earn PC points automatically when making eligible purchases at participating grocery stores with TD Visa or PC Financial MasterCard payment credentials.

UGO is a SIM-based solution that is supported by the three largest Canadian MNOs: Bell, Rogers, and TELUS. NFC-enabled devices running Android KitKat 4.4 or higher and Blackberry 10 devices are supported. A version of the UGO wallet is also available for iPhone, but supports loading loyalty cards only (not payment cards).

As with other Canadian wallets, only point of sale transactions under $100 are currently supported. It is unclear when UGO will support high value transactions and what CVM will be used. Remote transactions are not yet supported, which limits consumer adoption.

At time of writing, UGO wallet is only available in Canada.

[16] Samsung LoopPay press release, businesswire.com February 18, 2015

Appendix D – EMVCo Tokenization Specification

The EMVCo specification was published in March 2014. In its current version, it provides minimal guidance regarding the building and maintenance of token requester APIs, token vaults, token provisioning platforms, or token registries. The TSP is a pivotal entity. Token vaults hold both PANs and token PANs and will be an attractive target to fraudsters. Token domain restrictions are expected to be instrumental in preventing cross-channel fraud, and clear requirements are needed to determine how token attributes are leveraged in authorization decisions.

The following table outlines areas of concern with the EMVCo Tokenization Specification.

Area of concern	Explanation
Security and controls	The specification states that token vaults shall be protected by strong physical and logical security measures according to industry standards, but it does not describe any requirements about the storage of the actual data (PAN and token to be stored in separate locations, etc.) or address other aspects of the TSP service where data is stored. Given the importance of payment tokens in HCE payments, requirements to define minimum standards regarding data security and storage would be expected. This is especially important in open mobile wallet models where issuers retain liability yet rely on the TSP to protect sensitive data.
Token requester registration and assurance	The specification states that each TSP determines the information to be collected from a token requester, including KYC and transaction controls (i.e., domain restrictions). No mandatory fields are defined. The TSP must determine a token assurance level for each token requester, but no guidelines exist regarding how the requester is to be evaluated and the assurance level (no assurance – 0 to high assurance – 99) assigned. Token requesters can include card-on-file merchants, acquirers, merchants, OEMs, digital wallet providers, and card issuers.
Identification and verification (ID&V)	The specification is unclear about who should perform ID&V and which elements should be captured as part of the process to derive a token assurance score. Examples of ID&V activities are provided, but they are not helpful. The specification is unclear about what is being validated to provide an assurance level: the token requester, the credential, or the owner of the credential. The specification indicates that the issuer ID&V should consider token assurance values in the payment token to PAN/cardholder binding, but it does not provide requirements to ensure the token assurance level has any value. It also does not define which entity should be responsible for determining the level of ID&V to be

Area of concern	Explanation
	performed. As the owner of the customer relationship and liability associated with the account, it is suggested that the credential owner determine how rigorous ID&V processes should be for different types of token requesters.
Payment token generation	The EMV specification does not provide any guidance as to how a token must be generated other than a requirement related to token expiry date. It is not clear which party determines the parameters that define token issuance. It is also not clear how token generation will incorporate domain restrictions relating to channel, merchant, wallet, etc., and any requirements for a cryptogram. The specification states that business functions must be integrated with the applicable payment network but does not refer the token provider to any payment network specifications related to tokenization.
Payment token issuance and provisioning	The specification declares that token provisioning is performed through an interface between the token requestor and the TSP. According to EMVCo, "methodologies associated with the provisioning may be proprietary to each Token Service Provider and are outside the scope of this specification." Requirements should be provided that define security protocols regarding the transmission of payment tokens from the TSP to the token requester.

Bibliography

Reports and white papers

Canadian Bankers Association[17], *Canadian NFC Mobile Payments Reference Model*, May 2012.

Consult Hyperion, *HCE And SIM Secure Element: It's Not Black And White,* June 2014.

Consult Hyperion and GSMA, *HCE and Tokenization for Payment Services*, October 2014.

European Central Bank, *Recommendations for the security of mobile payments*, November 2013.

European Payments Council, *Mobile Payments Initiatives*, December 2014.

European Payments Council, *Mobile Wallet Payments,* January 2014.

First Data, *EMV and Encryption + Tokenization: A Layered Approach to Security*, 2012.

Smart Card Alliance, *Card-Not-Present Fraud: A Primer on Trends and Authentication Processes,* February 2014.

Smart Card Alliance, *Host Card Emulation (HCE) 101*, August 2014.

Smart Card Alliance, *Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization*, October 2014.

Sequent, *Beyond Tokenization: Ensuring secure mobile payments using dynamic issuance with on-device security and management*, accessed April 2015.

TSYS, *Tokenization: FAQS & General Information,* 2014.

Specifications

EMVCo, *EMV Payment Tokenisation Specification Technical Framework*, March 2014.

[17] CBA publicly released the Reference Model on behalf of Canadian financial institutions

Glossary

These definitions were sourced from third party documents published by the Canadian Banking Association, Consult Hyperion, EMVCo., Global Platform, GSMA, Mobey Forum, Smart Card Alliance and Sequent.

Term	Definition
Acquirer	An organization that processes credit and/or debit card payment transactions for a merchant.
App Store	A vendor of applications for a mobile device. App stores are generally operating system specific (e.g., Apple Store, Google Play Store).
Bluetooth Low Energy (BLE)	A wireless personal area network technology designed to require reduced power consumption and cost. PayPal Beacon leverages this technology.
Cardholder Verification Method (CVM)	The Cardholder Verification Method used to ensure that the person presenting the credential is the person to whom the credential was issued.
Combined Data Authentication	An authentication technique used in offline chip transactions that calculates a cryptogram for each transaction that is unique to the specific card and transaction. The chip card must be capable of RSA cryptographic processing. During a payment transaction, the chip card generates a second dynamic signature which the terminal must verify using RSA cryptography. This is to confirm that the chip card that was authenticated using DDA, is the same card that is used to authorize the transaction
Credential	The secure, encrypted information associated with a specific payment card, loyalty card, government-issued card, etc.
Credential Issuer	The organization that issues a credential.
Cryptogram	An alphanumeric value that is the result of data elements entered into an algorithm and then encrypted commonly used to validate data integrity. Commonly used cryptograms are Authorization Request Cryptogram (ARQC), Authorization Response Cryptogram (ARPC), Transaction Certificate (TC), and Application Authorization Cryptogram (AAC).
Dynamic Data/Token	Limited use payment credentials that are provisioned to an application to support a transaction.
Dynamic Data Authentication (DDA)	An authentication technique used in offline chip transactions that calculates a cryptogram for each transaction that is unique to the specific card and transaction. DDA protects against card skimming and counterfeiting.
Embedded Secure	A tamper-resistant secure microcontroller that is embedded in a

Term	Definition
Element (eSE)	mobile device on a single chip. Several smartphones, such as the iPhone 6 and some Samsung S6 models ship with embedded secure elements.
EMVCo	A corporation that defines standards for the inter-operation of integrated circuit cards, POS terminals, and ATMs for authenticating credit and debit card transactions. Current EMVCo members are MasterCard, Visa, JCB, American Express, China UnionPay and Discover, who each have an equal interest in the corporation.
High-Value Transaction (HVT)	A payment transaction that exceeds the network-recommended threshold for no CVM. At the time of writing, the threshold for HVT in Canada is $100.00.
Host Card Emulation (HCE)	A software architecture that provides an exact virtual representation of electronic identity cards (including credit and debit cards) using only software. HCE allows mobile applications to offer NFC payment solutions without the need for a secure element on the phone (eSE or SIM).
Identification & Verification (ID&V)	A valid method through which an entity may successfully validate the cardholder and the cardholder's account in order to provision payment credentials.
International Mobile Equipment Identity (IMEI)	A 15- or 17-digit code that uniquely identifies mobile phone sets. The IMEI code can enable a GSM (Global System for Mobile communication) or UMTS (Universal Mobile Telecommunications Service) network to prevent a misplaced or stolen phone from initiating calls.
Issuer Identification Number (IIN)	The first six digits of the Primary Account Number (PAN).
Mobile Device	A portable computing device that has an operating system, can run application software, and can connect to communication networks (e.g., cellular data, Wifi, Bluetooth, NFC).
Mobile Equipment Identifier (MEID)	A globally unique number identifying a physical piece of CDMA mobile station equipment. It can be seen as an IMEI but with hexadecimal digits.
Mobile Network Operator (MNO)	A provider of wireless communications services that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure, back haul infrastructure, billing, customer care, provisioning computer systems and marketing and repair organizations. Also known as a wireless service provider,

Term	Definition
	wireless carrier, cellular company, or mobile network carrier.
Mobile Payment Application	See *Wallet.*
Mobile Wallet	See *Wallet.*
Near Field Communication (NFC)	A short-range wireless communication technology for smartphones and similar devices that enables data transfer between the devices. NFC operates at 13.56 MHZ, complies with ISO/IEC 14443 and ISO/IEC 18092 standards, and operates in ranges of less than 10 cm.
NFC Controller	A hardware contactless front end designed to encapsulate the data exchanged between the NFC reader and the target application, from the radio layer to the application layer.
Obfuscation	Code obfuscation is a technique to prevent the reverse engineering of a cryptographic algorithm. A method of obfuscation is *white box cryptography* (see below).
Open Mobile Wallet	A mobile payment wallet that supports credentials from multiple credential issuers.
Original Equipment Manufacturer (OEM)	An entity that acquires and assembles components into a new product that is rebranded and sold.
Over the Air (OTA)	The transmission of data using a wireless network.
Primary Account Number (PAN)	A 16-digit number that identifies a payment credential. The first 6 digits are the Issuer Identification Number (IIN).
Pass Code	A (four-digit) number that is entered into the mobile device that acts as a cardholder verification method (CVM).
Payment Credential	See *Credential.*
Payment Network	The system that provides specifications to support mobile payments and manages the network that is used to process the payment transaction (e.g., American Express, Interac, MasterCard, Visa).
Personal Identification Number (PIN)	A secret numeric code of 4 to 6 characters that is used to identify cardholders at a customer-activated PIN pad. PINs can be verified online by the issuer or sent to the chip card for offline PIN verification.
Point of Sale (POS)	Hardware deployed by a merchant that is used to capture credential information to process a transaction.
Proprietary Wallet	A mobile wallet that will only support the credentials issued by the wallet provider.
Quick Response (QR) Code	A type of matrix barcode (machine readable optical label) that contains information about the item to which it is attached. The

Term	Definition
	QR Code system became popular due to its fast readability and greater storage capacity compared to standard UPC barcodes.
Secure Element (SE)	A tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities (Global Platform).
Static Data Authentication (SDA)	An authentication technique used in offline chip transactions that uses a cryptogram using a static public key certificate and static data elements. With SDA, the data used for authentication is static—the same data is used at the start of every transaction.
Subscriber Identity Module (SIM)	Hardware owned by the MNO that is deployed on the handset. Issuer credentials can be securely stored here. Also called Universal Integrated Circuit Card (UICC).
Token (static)	A surrogate value that replaces the Primary Account Number (PAN) in the payments ecosystem. A token is *static* if the surrogate value remains constant with each use.
Token (dynamic)	A surrogate value that replaces the Primary Account Number (PAN) in the payments ecosystem. A token is *dynamic* if the surrogate value changes with each use, and may incorporate transaction-specific data such as amount and time.
Token Service	A system comprised of the key functions that facilitate generation and issuance of Payment Tokens from the Token BINs, and maintain the established mapping of Payment Tokens to PAN when requested by the Token Requestor. The service also provides the capability to support Token Processing of payment transactions submitted using Payment Tokens by de-tokenizing the Payment Token to obtain the actual PAN.
Token Service Provider (TSP)	An entity that provides a Token Service comprised of the Token Vault and related processing. The Token Service Provider will have the ability to set aside licensed ISO BINS as Token BINs to issue Payment Tokens for the PANs that are submitted according to this specification.
Token Vault	A repository, implemented by a Tokenization system that maintains the established Payment Token to PAN mapping. This repository is referred to as the Token Vault. The Token Vault may also maintain other attributes of the Token Requestor that are determined at the time of registration and that may be used by the Token Service Provider to apply domain restrictions or other controls during transaction processing.
Token Vault	An entity that develops and maintains a Token Vault.

Term	Definition
Provider	
Tokenization	A process by which the Primary Account Number (PAN) is replaced with a surrogate value called a Payment Token. Tokenization may be undertaken to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.
Trusted Execution Environment (TEE)	The Trusted Execution Environment (TEE) is a secure area of the main processor of a smart phone (or any connected device including tablets, set-top boxes and televisions). It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity.
Trusted Service Manager (TSM)	A trusted service manager (TSM) is a role in a hardware-based mobile payment ecosystem. It acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, phone manufacturers or other entities controlling the secure element on mobile phones. The trusted service manager enables service providers to distribute and manage their contactless applications and credentials remotely by allowing access to the secure element in NFC-enabled handsets.
Unique Device Identifier (UDID)	A unique alphanumeric number attached to an iOS device. Every single iPhone, iPad, and iPod Touch has one.
Universal Integrated Circuit Card (UICC)	Hardware owned by the MNO that is included in the mobile device. Issuer credentials can be stored securely in the UICC. Also referred to as a SIM.
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, open	A mobile payment application that will accept credentials from more than one issuer.
Wallet, proprietary	A mobile payment application designed for one issuer's credentials. The wallet provider is the issuer.
Wallet provider	Entity that designs, creates, and manages the mobile wallet application – the end-user-facing interface.
White Box Cryptography	A method of obscuring code to hide cryptographic processes and keys. The objective is to protect secret keys from being disclosed in a software implementation.

Note: All trademarks in this document are the property of their respective owners.