



HCE Payment Journey Whitepaper

September 2016

Driving Trust
www.insidesecond.com

Table of contents

- Executive Summary..... 2
- Introduction..... 4
- Market Potential..... 5
 - Online vs In-store..... 5
 - Accelerating Adoption 6
- Ecosystem..... 7
 - Near Field Communication..... 7
 - Universality 7
 - Tokenization..... 8
 - Host Card Emulation vs Secure Element..... 8
- Channels to Market 10
 - Complementary Channels..... 10
 - Third Party Wallets 10
 - Issuer Wallets..... 11
 - Reusable Assets 12
 - Remote Payments 14
- Deploying an HCE Solution 15
 - Benefits of HCE 15
 - Control over how the cardholder interacts with the service 15
 - Manage how the service interacts with other products..... 15
 - Freedom to Innovate 15
 - Building an HCE Product 16
- Conclusion..... 18

Executive Summary

Over the last few years, the Payment industry has been watching Mobile Payments evolve with a mixture of intrigue and caution. As with any new technology, the hype and enthusiasm is matched only by the naysayers. This leads to a lot of conflicting opinions and sometimes downright incorrect information being pushed into the market. As an active participant in the market, it is important to be able to analyze the facts with a clear head and clear objectives. Only then is it possible to make sensible decisions that will support your business in the long term.

When analyzing the facts, it becomes clear that Mobile Payments are beginning to realize their potential. It is also obvious that the traditional payment players are not going to be disrupted in the short term. The requirement for a near-ubiquitous acceptance network puts the established payment networks in a strong position. This means that the three and four party models will persist; and it will be the card issuing banks that will provide Mobile Payment services to consumers - either directly or indirectly.

Given this, it seems clear that Issuer Banks need to be actively considering and developing their Mobile Payment products - their cardholders will expect them to provide one in the near term.

The challenge for the Issuers is to decide which channel (or channels) to use to reach their cardholders: Third Party wallets like ApplePay or develop their own Issuer Wallet. Ultimately, the channel(s) will depend on what the Issuer wants to achieve. For most Issuers this will result in a multi-channel strategy - mixing Third Party wallets with their own HCE (Host Card Emulation) based payment solution - with each channel providing a different value proposition.

With a clear strategy and smart decision-making, this multi-channel approach can be achieved without additional overheads. Allowing Issuers to pool the benefits of each channel.

It is recommended that card Issuers give serious consideration to deploying their own HCE payment application as this gives them control and freedom to build a Mobile Payment product that reflects their own business needs. When developing the solution, it is important to focus on those needs; which will be reflected in the User Experience and Security of the product. This should drive any technology selection decisions.

INSIDE Secure is a Visa Token Service integration partner making it ideally placed to accelerate issuing banks' integration to scheme tokenization services. This provides banks with a smooth route to utilize the aggregation ability of these token services to develop their own wallet product.

Couple this expertise with INSIDE Secure's MatrixHCE technology, which provides HCE functionality based on the leading payment brand standards, Mobile Banking and Payment Application developers are able to accelerate their development and time to market by combining HCE, Payment and Security as a packaged solution.

Securing Mobile Payment applications requires more than just data encryption. In addition, developers must secure the overall application code with its vital logic & processes, data, *and* cryptographic keys. MatrixHCE utilizes INSIDE Secure's software protection tools to make it extremely difficult and time-consuming for attackers to understand how a payment application works in order to compromise it.

Introduction

Mobile Payment is an exciting, fast moving arena to operate within. For all the hype and enthusiasm there are equally as many naysayers. This is natural for a market that has yet to settle down and mature; but leads to a lot conflicting opinions and sometimes downright incorrect information being pushed into the market. All this noise makes short term, never mind long term, planning appear difficult.

As an active participant in the market, it is important to be able to analyze the facts with a clear head and clear objectives. Only then is it possible to make sensible decisions that will support your business in the long term.

A common approach to dealing with the noise is to “wait and see”. Unfortunately, given that currently 30% of payments globally originate from mobile devices¹ and in developed markets it is already reaching 50%, consumers are starting to expect Mobile Payment services. This means that delaying will leave space in the market for new players and the traditional providers will be left playing catch up - never a good position to be in.

Very simply, the time to start developing Mobile Payment services is now.

To quiet the noise, allowing the decision making process to progress, key questions need to be answered:

- What is the market potential of Mobile Payment services?
- What ecosystem will support the market?
- Which of the competing solutions within the ecosystem will win out?
- What does my business gain from this new market?

By taking a logical approach, each of these questions can be answered in a straightforward manner. These answers can then form the basis of a positive business strategy.

This paper answers the questions for payment card issuing banks, quieting the noise, to allow a sensible business strategy to be put in place.

¹ <http://www.fierceretail.com/story/30-global-transactions-happening-mobile/2015-10-09>

Market Potential

Online vs In-store

The market potential for Mobile Payments is huge. In the United States alone spending is expected to reach \$142 billion by the end of 2019². Admittedly, this is mainly being driven by online purchases where the trend is for consumers to switch to using their mobile phone (either through apps or mobile browsers) from laptops and PCs to make online purchases.

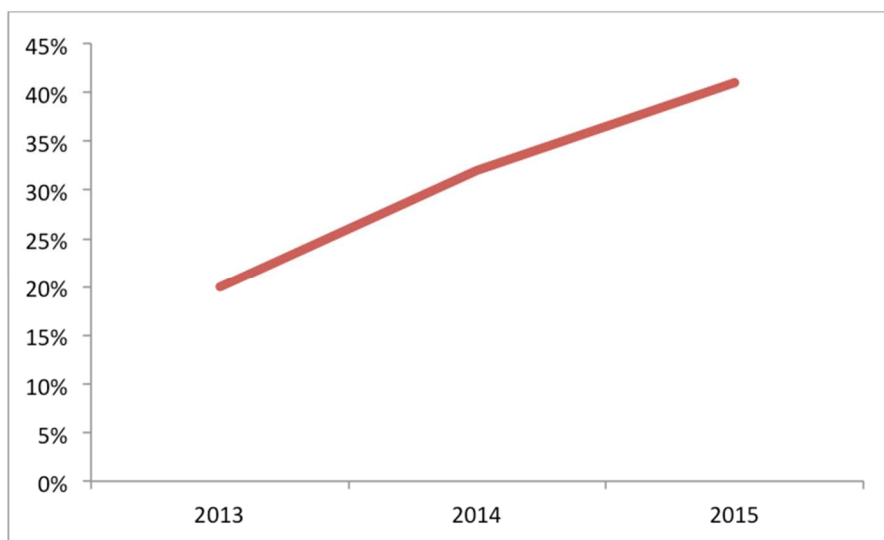


Figure 1 - Percentage of Online Transactions Performed with Mobile on "Black Friday"³

In-store Mobile Payments are still maturing in terms of market adoption (the technology is ready, proven and being successfully deployed). The reasons for this slower adoption are now being overcome and the sort of growth seen with online payments is starting to occur with in-store payments.

² http://blogs.forrester.com/denee_carrington/14-11-17-us_mobile_payments_will_reach_142b_by_2019

³ <http://www.marketwired.com/press-release/iovation-predicts-mobile-devices-account-48-percent-online-retail-transactions-from-2074930.htm>

Accelerating Adoption

There are two main reasons for the adoption of in-store payments to lag behind online payments: habit and too many barriers being put in front of the consumer.

The first reason is that the habitual change from plastic card to mobile phone is much harder than the change from laptop to mobile phone; especially in countries where contactless cards are not prevalent. Laptop (or PC) to mobile is a change that consumers are making for lots of services - not just payment; cash or card to mobile is a change that is unique to payments.

The second reason is that traditionally there were too many barriers put in the way of consumers that wanted to use Mobile Payments. Research showed a gap between interest (demonstrated by application downloads) and the uptake of services. The barriers were a key factor in this:

- The on boarding process was painful - there were far too many steps for the cardholder to complete. Mobile is all about instantaneous consumption so every setup step is painful. With the current range of solutions, these steps have been greatly reduced both in number and in size. HCE, Apple Pay, Samsung Pay etc. all offer a smooth and easy signup process.
- Acceptance was not ubiquitous. This meant that there would always be a question in the consumer's mind as to whether the phone would be accepted for payment. Much easier to just use plastic and save any embarrassment.

This too is changing (for contactless based solutions at least) as both Visa and MasterCard have mandated that all terminals will need to be contactless by the end of 2019⁴.

With these barriers being broken down, the adoption rates are finally starting to grow - and grow quickly.

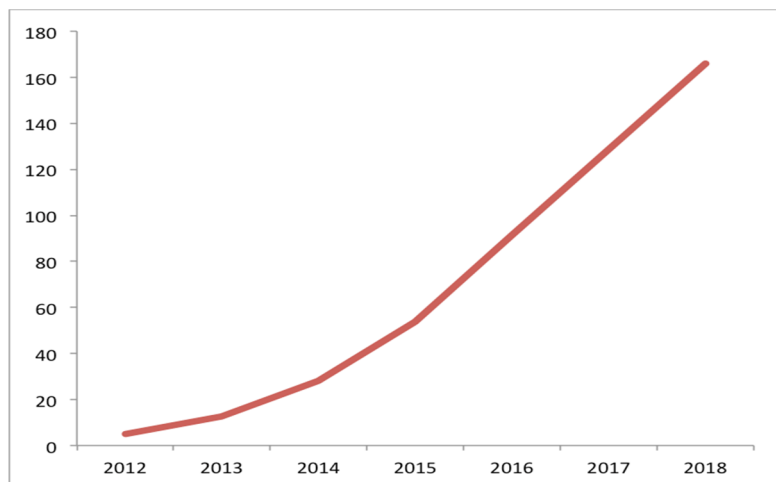


Figure 2 - NFC Payment Users Worldwide (in millions)⁵

⁴ <http://www.paymentscardsandmobile.com/contactless-cards-breakthrough-in-europe/>

⁵ DigiWorld Yearbook 2015, May 2015

Ecosystem

Near Field Communication

The first contactless payment cards and the first Mobile Payment products coincidentally, but independently, appeared in 1997 from Mobil and Coca-Cola respectively⁶. The technology that would become the standard for in-store proximity payments made its debut in 2004 when Visa launched its first contactless card in Malaysia⁷. By 2020, all Visa and MasterCard merchants will have to accept contactless payments.

The Near Field Communication (NFC) technology that these cards use is supported by all modern mobile phones. This means that the traditional card acceptance network is able to accept both plastic cards and Mobile Payments without modification.

Universality

Uncertainty in any market opens up opportunities for new ideas and new players. Mobile Payment is no different. A plethora of challengers to the traditional card schemes have appeared over the last couple of years - all using the mobile phone as a payment device.

For any payment scheme to be successful, it needs to have near-universal acceptance. Consumers have demonstrated that doubt about retailer acceptance limits their confidence in mobile payments; and as such they will revert to cash or cards - both payment methods where that doubt does not exist.

It is their existing acceptance network that will mean the traditional payment schemes will win out. Visa and MasterCard - as well as American Express, China UnionPay, JCB and Discover - do not have to spend time and money building a ubiquitous acceptance network, they already have one. By building their in-store Mobile Payment solutions on the existing technology base, the traditional payment schemes instantly gain a mobile solution that is universally accepted.

This acceptance network means that the existing three and four party payment schemes⁸ will become the basis for in-store Mobile Payments; and the existing card Issuers will be the channel to consumers for Mobile Payment services.

⁶ <http://nearfieldcommunication.org/payment-systems.html>

⁷ <https://www.globalplatform.org/implementationsfinancial.asp>

⁸ <http://www.brimstone-consulting.com/three-and-four-party-card-schemes>

With in-store Mobile Payments starting to gain traction in the market, and the traditional payment networks being the route to a universal solution, this means that now is the time that the issuing Banks need to start developing Mobile Payment facilities for their cardholders.

Tokenization

Tokenization⁹ is the act of replacing a sensitive credential with a pseudo credential that has restricted use cases. This pseudo credential can be mapped back to the original by a management service when the credential is used - provided the use case is allowed.

Tokenization has become a crucial part of the security architecture for Mobile Payments (along with mobile application protection). In this case, the account number (PAN) is replaced with a digital PAN that is in the same format as the real PAN and treated by the acquiring network as if it was a real PAN. Either the Issuer or the payment scheme can perform the mapping between the real PAN and the digital PAN.

Host Card Emulation vs Secure Element

There are two competing technologies for implementing contactless payments on a mobile phone: Host Card Emulation and Secure Element.

Secure Element

The classic model is to use a Secure Element (SE). The SE approach replicates “chip” cards within a mobile phone; with the payment processing and credentials contained in a separate tamper-resistant computer chip - traditionally the phone’s SIM card but now more commonly embedded within the handset. This chip is known as the SE. The SE has a direct connection to the phone’s NFC controller so payment traffic does not pass through the phone’s operating system.

An application on the phone can communicate with the SE to provide a user interface but this interface is not directly involved in the payment transactions.

Modern Secure Element solutions tend to use tokenization but it is not mandatory.

⁹ It is beyond the scope of this paper to discuss the details of tokenisation but more information can be found at <https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf>

Host Card Emulation

The alternate model is to use Host Card Emulation (HCE). HCE allows an application on the mobile phone to directly drive the phone's NFC controller. This allows a purely software approach where an application on the phone implements all the payment logic as well as a user interface.

For security reasons, HCE solutions need to use some form of Tokenization as well as strong application protection - such as INSIDE Secure's MatrixSSE¹⁰.

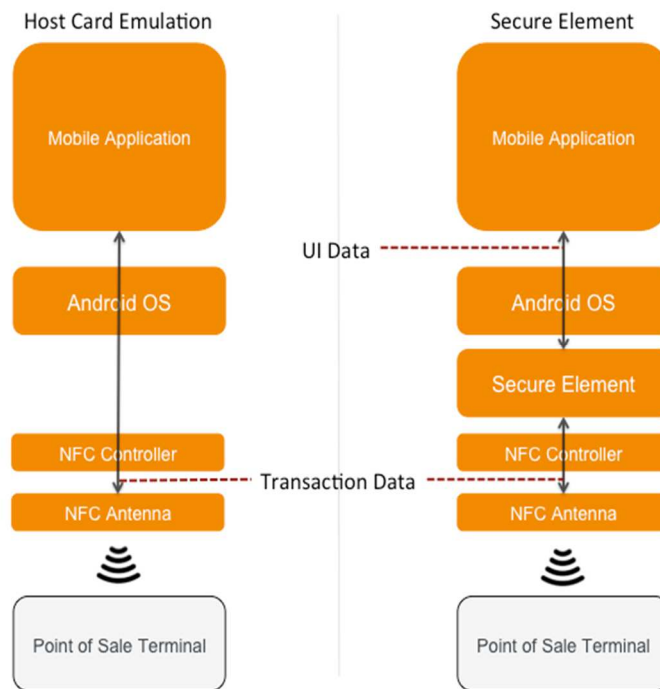


Figure 3 - Host Card Emulation vs Secure Element

Proponents of the Secure Element approach highlight its proven security model that is analogous to chip-and-pin cards. While the pure software approach of Host Card Emulation provides an easier route to market without the need to involve third parties. This means that the Secure Element model is only practical for the Secure Element owners (e.g. a handset manufacturer who has embedded a chip in their devices). Other players, such as issuing banks, will find Host Card Emulation the only feasible route to market.

¹⁰ <https://www.insidesecond.com/Products-Technologies/Mobile-Payment-and-Banking/MatrixSSE>

Channels to Market

Complementary Channels

Mobile Payment Channels available to Issuers (and their cardholders) can be split into two groups: Third Party wallets such as the OEM Pays from Apple, Samsung, Google, etc.; and Issuer wallets where the issuing bank develops their own application.

Third Party Wallets

Third Party wallets provide an easy route to market for Issuers. The Issuers connect to the payment scheme tokenization services (VTS¹¹, MDES¹², etc.) and the schemes handle the aggregation to the different Third Party wallets.

Often, these Third Party wallets integrate closely with the cardholder's mobile device. Couple this with the fact that the wallet providers have undertaken a lot of market education to increase consumer awareness, then "discovery" of the service is likely.

The challenge for Issuers from Third Party wallets is that the user interface (and therefore the conversation with the customer) is controlled by the Wallet provider, not the Issuer Bank. There is a risk that the customer will subconsciously move their payment relationship from the bank to the Wallet provider - thus disintermediating the bank.

The highest profile Third Party wallets come from the handset manufacturers and operating systems developers. Table 1 below gives a breakdown of these third party wallets.

¹¹ <https://usa.visa.com/partner-with-us/payment-technology/visa-token-service.html>

¹² <http://newsroom.mastercard.com/2014/09/10/mastercard-digital-enablement-service-mdes-making-digital-payments-happen/>





				
Provider	Apple	Samsung	Google	Microsoft
Headline Features	In-store NFC payments In-app purchases In-browser purchases Only option on iPhones	In-store NFC payments In-app purchases MST ¹³ for use at non-contactless terminals	In-store NFC payments In-app purchases In-browser purchases	In-store NFC payments
Devices	iPhone 6 and above AppleWatch	Samsung Galaxy S6 and above	All Devices running Android 4.4 or newer	Windows Phone 10
Model	Secure Element	Secure Element	HCE	HCE
Countries	Australia, Canada, China, France, Hong Kong, Singapore, Switzerland, UK, US	Australia, Brazil, China, Spain, Singapore, South Korea, US	Australia, Singapore, UK, US	US

Table 1 - Third Party Wallets¹⁴

Issuer Wallets

Issuer Wallets are generally provided using Host Card Emulation (HCE). HCE is the easiest route for an Issuer to provide their own wallet, as they do not need to interact with non-payment organizations (such as mobile network operators to gain access to a secure element).

¹³ MST: Magnetic Secure Transmission - <http://www.samsung.com/us/support/answer/ANS00043865/>

¹⁴ Table is correct at time of publication

This paper would recommend that Issuers consider developing an Issuer Wallet. This allows them to benefit from a channel over which they have full control over and therefore complete freedom to develop a solution that reflects their business needs.

The table below summarizes HCE in a similar manner to the Third Party wallets above.

Wallet	Issuing Bank (standalone application or integrated to m-banking app)
Provider	Issuing Bank
Headline Feature	Issuing Bank in control to add any feature they desire.
Devices	Android running 4.4 (KitKat) and newer Windows Phone 10 Blackberry 7 and 10
Model	HCE
Countries	Any

Table 2 - Issuer Wallet

Reusable Assets

Discussions around the different channels available to Issuers are often couched in “either-or” terms. That does not have to be the case. Issuing banks need to evaluate each channel on its own merits - adopting *all* those that make business sense, not just selecting a single winner.

A multi-channel approach allows the Issuer to enjoy the benefits that each channel brings. It also allows them to respect consumer choice when it comes to selecting how to interact with Mobile Payment products.

One of the concerns of adopting a multi-channel approach is the duplication of effort, complexity and ultimately cost; but with smart decision-making, duplication can be avoided.

All the Mobile Payment channels identified rely on tokenization. Tokenization is a security technique to separate the payment credentials on the mobile devices from the real account. By using a common tokenization service across all channels, the duplication is greatly reduced. The reason for this is because, as well as its security objectives, a tokenization service can also act as an aggregator to the different channels.

An Issuer only has to connect to the tokenization service once and they are connected to all the different Third Party wallets¹⁵. They also gain most of the infrastructure to deliver their own HCE wallet as well.

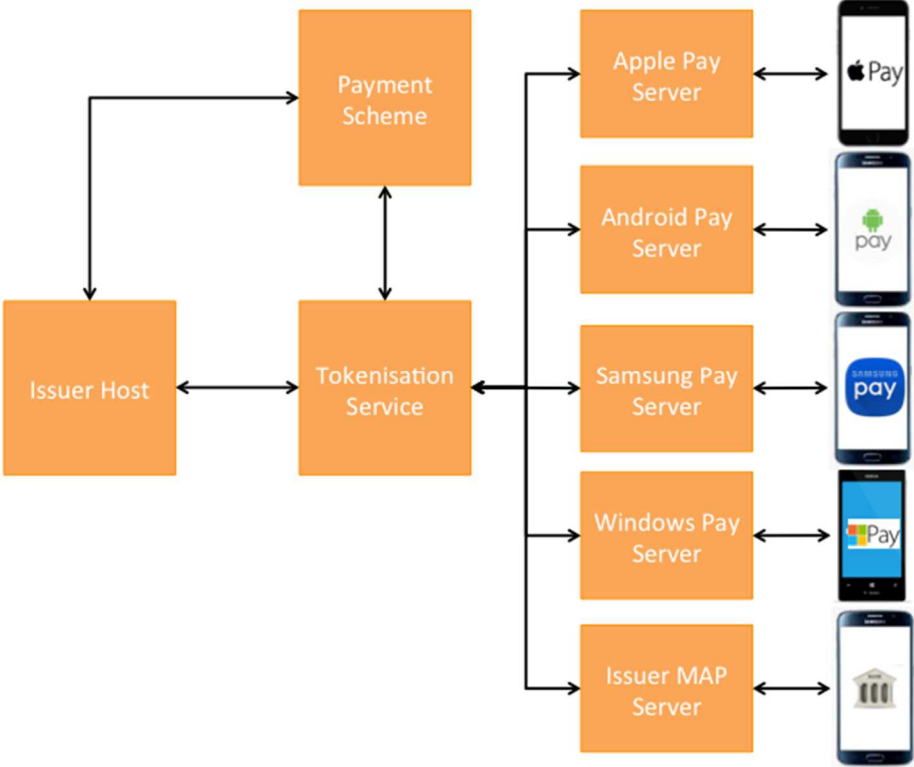


Figure 4 - Tokenization Service acts as an Aggregator to Multiple Wallets

The other concern is of customer confusion - if there are multiple Mobile Payment services available which one should the customer choose?

There is no evidence of this confusion occurring in the market. In fact, this competition is positive as it significantly raises awareness (through 3rd party wallet marketing) and market maturity. Consumers are used to having competing services and will ultimately choose the one that works best for them.

¹⁵ From a technical perspective at least, there may still be commercial agreements required

Remote Payments

The boundary between card present (in-store) and card not present (online) payments is blurring. The technologies that deliver in-store Mobile Payments can also be used to provide Remote Payments.

These are payments for online purchases but instead of performing a traditional card not present transaction, the card instances that are deployed onto the mobile handset are used to perform a card present-like transaction - reusing the same security model as for in-store payments to reduce the fraud risk of online payments. The difference being that instead of communicating with a physical Point of Sale, the transaction is completed against online services.

Remote payments also improve the user experience by removing the requirement to manually enter card details for each transaction.

Deploying an HCE Solution

Benefits of HCE

One of the highest profile HCE rollouts is Capital One. Paul Moreton, Vice President of Digital Product Management defines a clear objective for his organization: *“We are focused on innovation and the evolution of digital products and services. Our goal is to provide our customers with payment options that help them succeed and simplify their lives.”*

The real strength of an HCE Payment solution for an Issuer is that it is under their control - freeing the issuer from third party constraints. This allows Issuers space to innovate and evolve their products and services, achieving goals such as Capital One’s.

Control over how the cardholder interacts with the service

Many HCE adopters state their reason as wanting to help their cardholders to have control over their money. To be able to devolve power to its cardholders, an Issuer needs to be in control of the solution in the first place. HCE gives Issuers that control. With HCE, the Issuer builds the user interface and so has control over how the cardholder interacts with the service.

Manage how the service interacts with other products

Another commonly quoted reason for developing an HCE solution is to achieve more seamless money management. With HCE, the Issuer can manage how the service interacts with other products and services within the Issuer’s portfolio. The Issuer can decide on a loose coupling between services by building a stand alone payment application or a tighter coupling by embedding Mobile Payment into an existing mobile banking application.

Freedom to Innovate

The flexibility and control an Issuer has over their HCE solutions allows them to innovate in the market place. Some examples that have already been deployed include:

Instant Card Replacement

If a card is lost or stolen, BarclayCard offer an instant replacement in the form of a virtual card to the cardholder's Android mobile application¹⁶. This means that the consumer is not cut-off from their funds while waiting for a new card to be sent through the post.

Installment Plans

The BBVA Wallet allows consumers to convert a purchase into an Installment Plan either at the time of purchase or later¹⁷ - linking together two BBVA services: card payments and loans.

Loyalty Schemes

Mobile is about reducing friction by joining up data and services. One of the highest levels of friction at the checkout is the separate step needed to collect loyalty points - another card needs to be found and scanned. If that loyalty card can be embedded in the HCE application then it can be read automatically as part of the payment tap.

Building an HCE Product

It is relatively straightforward to identify the technological building blocks of a HCE payment solution, select vendors to supply them and then put the blocks together. This will give a working, functioning solution; but it will be a technology led solution not one focused on customer or business objectives.

The crucial question for any HCE project team to answer is "what do we want to get out of it?". By defining a clear objective at the start, the developed solution will be something that adds value to the issuing bank's business.

With the question answered and the objective defined, it is possible to start to define the User eXperience (UX) of the solution. Supporting the desired UX should be one of the key drivers in any technology decisions - the other driver is the security of the solution.

To deploy an HCE service, the issuing bank needs to have two components: a backend service (consisting of a tokenization service and a token requestor mobile application platform aka a MAP) and a mobile application. The tokenization service

¹⁶ <http://www.nfcworld.com/2015/11/16/339607/barclaycard-to-use-hce-to-instantly-replace-lost-and-stolen-cards/>

¹⁷ <https://contactlessintelligence.com/2014/04/02/37389/>

has been discussed above. The MAP is a server component that manages the link between the tokenization platform and all the instances of the mobile application(s). While the mobile application is responsible for delivering the issuing bank's chosen UX to the cardholder.

It is the recommendation of this paper that the Issuer takes the path of least resistance to support their UX and security requirements when sourcing each of these components.

If the Issuer is supporting multiple Mobile Payment channels, then the tokenization service already provides the ideal place to reduce duplication. One tokenization service can be selected to power all the different channels. The tokenization service then becomes a common integration point.

The Mobile Payment application is the consumer's point of interaction with the mobile system. It is the application that delivers the UX. This means that the Issuer needs control over the application's user interface. This does not mean that the Issuer needs control over the whole application though. There is a lot of common functionality that any Mobile Payment application needs to provide. This common functionality can be provided by a secure Software Development Kit (SDK) - again reducing duplication and cost.

Provided the SDK does not make any assumptions about the user interface, the Issuer can keep control over the UX without needing to take on responsibility for the underlying complexities and security of delivering Mobile Payments.

Conclusion

Mobile Payments are fast becoming an accepted way to make online purchases; and this trend is emerging for in-store payments as well.

Despite the noise in the market, the traditional payment players are not going to be disrupted in the short-term. The requirement for a near-ubiquitous acceptance network puts the established payment networks in too strong a position, therefore it is the card issuing banks that become the preferred and trusted providers of Mobile Payment services to consumers.

Given this, it is clear that the Issuers need to be actively considering and developing their Mobile Payment solutions - their cardholders will expect it in the near term.

The challenge for the Issuers is to decide which route to market to take: use a Third Party wallet like ApplePay or develop their own Issuer Wallet. Ultimately, the channel(s) to use depends on what the Issuer wants to achieve. For most Issuers, this will result in a multi-channel strategy - mixing Third Party wallets with their own HCE payment solution - with each channel providing a different value proposition.

It is recommended that card Issuers strongly consider deploying their own HCE payment application as this gives them control and freedom to build a Mobile Payment product that reflects their own business needs. When developing the solution it is important to focus on those needs; which will be reflected in the User Experience and Security of the product. This should drive any technology selection decisions.

INSIDE Secure is a Visa Token Service integration partner making it ideally placed to accelerate issuing banks' integration to scheme tokenization services. This provides banks with a smooth route to utilize the aggregation ability of these token services to develop their own wallet product.

Couple this expertise with INSIDE Secure's MatrixHCE technology, which provides HCE functionality based on the leading payment brand standards, Mobile Banking and Payment Application developers are able to accelerate their development and time to market by combining HCE, Payment and Security as a packaged solution.

Securing Mobile Payment applications requires more than just data encryption. In addition, developers must secure the overall application code with its vital logic & processes, data, *and* cryptographic keys. MatrixHCE utilizes INSIDE Secure's

software protection tools to make it extremely difficult and time-consuming for attackers to understand how a payment application works in order to compromise it.



Figure 5 - MatrixHCE provides a rapid and secure development platform for Issuer HCE applications

About INSIDE Secure

INSIDE Secure provides comprehensive embedded security solutions. World-leading companies rely on INSIDE Secure's mobile security and secure transaction offerings to protect critical assets including connected devices, content, services, identity and transactions. Unmatched security expertise combined with a comprehensive range of IP, software and associated services gives INSIDE Secure customers a single source for advanced solutions and superior investment protection. For more information, visit www.insidesecond.com.

INSIDE Secure S.A.

Arteparc Bachasson • Bât. A
Rue de la carrière de Bachasson
CS 70025 • 13590 MEYREUIL • France

Tél: + 33 (0)4 42 90 59 05

Fax: + 33 (0)4 42 37 01 98

© INSIDE Secure 2013. All Rights Reserved. INSIDE Secure[®],
INSIDE Secure logo and combinations thereof, and others
are registered trademarks or tradenames of INSIDE Secure
or its subsidiaries. Other terms and product names may be
trademarks of others.

www.insidesecond.com

