HCE and Tokenisation for Payment Services

discussion paper

consult hyperion
securing tomorrow's transactions

GSMA

Contents

EXECUTIVE SUMMARY 4

1. INTRODUCTION 5

1.1 Background and objectives 5
1.2 What is card emulation? 6
1.3 What is host card emulation 6
1.4 The role of tokenisation 7
1.5 The secure element vs HCE debate 9

2. NFC PAYMENT ECOSYSTEMS 10

2.1 HCE ecosystem 10
2.2 Secure element ecosystems 12
2.2.1 SIM SE 12
2.2.2 Embedded SE – Apple Pay 13
2.2.3 ApplePay vs SIM Secure Element: Additional considerations 14

3. CONSIDERATIONS 15

3.1 Provisioning 15
3.1.1 Provisioning dynamic data 16
3.1.2 Tokenisation 18
3.2 User experience 19
3.2.1 Downloading data 21
3.2.2 User experience considerations 23
3.3 Security 24
3.3.1 Controls and risk management 25
3.4 Business model 26
3.4.1 HCE in software 26
3.4.2 With secure hardware 26
3.5 Maturity 28

4. CONCLUSION 30

Executive summary

In July 2014, to help understand the opportunities and challenges between SIM secure element (SE) and host card emulation (HCE) services, the GSMA commissioned Consult Hyperion to produce a guide, *HCE and SIM Secure Element: It's not Black and White*, comparing the approaches. Following its publication, readers have asked for more information regarding the use of HCE. This paper aims to provide deeper analysis for banks and mobile network operators investigating the use of HCE and tokenisation within a mobile payment service.

Alongside the growing penetration of contactless acceptance infrastructure, there is increasing momentum behind the migration to mobile. This migration covers the full range of implementation options, HCE, SIM based and embedded, with the entry of Apple.

HCE offers the promise of an additional mechanism for banks to support their customers. It:

- Simplifies the ecosystem for provisioning applications at the expense of increasing payment transaction risk management,
- Removes the cost and complexity of application management using a third party supported secure element, but
- Increases the complexity of issuer host systems, as these systems now have to provide dynamic data for each transaction.

Dynamic data (e.g. transaction specific cryptographic keys) is needed to address the vulnerabilities exposed by the lack of a secure hardware platform in the customer's handset. The use of a dedicated static PAN for HCE, or per-transaction dynamic PANs will help limit the option cross-contamination into e-commerce. Issuers can choose to undertaken PAN management themselves or use one of the commercial tokenisation services that are coming to market.

As the user has to download (either by choice or on a pushed basis) dynamic data for use in transactions prior to the transaction occurring, the security of HCE relies on the authentication of the customer for this download. It is important that sufficient emphasis is placed on securing customer authentication over the whole lifetime of the products. To address this, issuers should consider the use of additional hardware security for authentication credentials.

The additional costs required for the new issuer processes require careful consideration. During a cost analysis, we suggest that issuers work with partners to explore the potential benefit gained by the integration of a secure element into their back-end processes for HCE. This should result in an understanding of how the hybrid approach could control the cost and complexity of a solution implemented to a population scale.

It is still early in the lifecycle for HCE, with the initial scheme specifications being published or under development. Assuming HCE follows the development path of other card payment technology deployments, it will be a year or so before specifications and product stabilises.

The findings from Consult Hyperion's initial HCE guide continue to ring true.

- Begin by understanding your local market conditions and your target transaction profile
- Maintain flexibility in your strategy, as secure hardware is likely to continue to be a significant part of the most appropriate solution, and
- Work collaboratively with industry partners to ensure that customers and merchants are brought along with the ease-of-use promise that the HCE can bring.

1. Introduction

1.1 Background and objectives

Near field communications (NFC) is the most widely supported technology for a mobile phone to be used in a payment transaction at point-of-sale (POS). NFC allows consumers to use mobile phones for secure services including payment, ticketing, access, loyalty and vouchers.

Today, conditions are in place for NFC services, including significant smart phone penetration, the app store ecosystem and the more than 225 mobile phone models that support NFC as well as the proliferation of contactless card payment terminals.

For around five years, NFC services using a secure element have been piloted and commercially launched around the world. The use of a secure element to perform this process within an NFC capable phone is called "card emulation". To the POS terminal the mobile phone behaves exactly like a smart payment card. There are already more than 50 commercial and pilot services in action including OrangeCash in France, SmartPass in Germany, Tapit in Switzerland, SureTap in Canada and Softcard in US and the Mobile Wallet from China Mobile.

In October 2013, Google announced the inclusion of "host card emulation" (HCE) functionality in Android 4.4 KitKat, which allows the payment app to communicate directly with NFC controller/antenna credentials and payment credentials to be stored on payment app on the mobile phone operating system (the "host") instead of in the secure element. In 2014, Visa and MasterCard released specifications, requirements and guidelines for payment applications using HCE, including a software development kit to enable its clients to deploy mobile payments using HCE. Banks in Spain and Australia have started pilots using HCE technology for payment applications.

To help understand the opportunities and challenges between SIM Secure Element and HCE services, the GSMA commissioned Consult Hyperion to produce a guide, *HCE and SIM Secure Element: It's not Black and White*, comparing the approaches. The guide was endorsed by MasterCard, UK Cards Association and the Mobey Forum.

The banks have asked for more information regarding the use of HCE. This paper aims to provide deeper analysis for banks and mobile network operators investigating the use of HCE and tokenisation within a mobile payment service.

1.2 What is card emulation?

Card emulation was the precursor to host card emulation (HCE) and therefore a brief description of this is necessary to provide context.

Card emulation as the name suggests is about making a mobile phone act like a smart card. This could allow, for example, a mobile phone to be used in a payment transaction at point-of-sale instead of a contactless smart card.

Prior to HCE, an actual smart card device (e.g. a secure element such as a SIM) was required to be accessible to the mobile phone and was used to store the card payment application. This is called "Card Emulation". The payment app in the secure element provides transaction and risk logic such that the payment application itself is involved in the process of approving or declining a transaction, managing critical data in the tamper-resistant environment of the secure element.

When NFC card emulation is performed with a secure element, the interface to the payment reader (e.g. a point-of-sale or POS) is the same as for a traditional payment card. Similarly, with HCE, a standard EMV payment transaction is performed from an application residing in the mobile phone's host operating system and the POS sees a mobile app which looks like a mobile payment card.

The NFC controller is a hardware contactless front-end (CLF) designed to encapsulate the data exchanged between the NFC reader and the target application, from the radio layer to the application layer. A SIM secure element is directly connected to the CLF by a single physical wire link and as such the mobile operating system (OS) has no access to the exchanged data.

1.3 What is host card emulation?

With HCE, a secure element device is not required. The payment application is held in the mobile phone operating system (the device host or "host" for short). As the device host is not secure, an HCE payment app cannot fully protect sensitive data and must ensure that the usefulness of data in it is restricted such that the liability associated with the compromise of this data is limited. This is done by using different payment data on each transaction.

NFC SECURE ELEMENT CARD EMULATION AND HOST CARD EMULATION

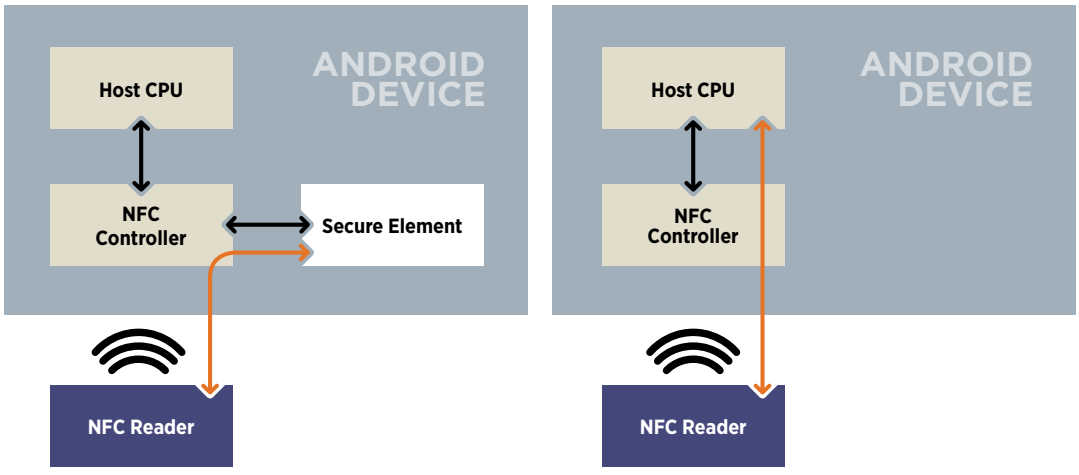

Figure 1 (Source: Google http://developer.android.com/guide/topics/connectivity/nfc/hce.html)

In HCE, the NFC controller is connected to the application through the mobile OS, which in theory allows the OS to read the data exchanged. This may be an issue for some applications, but for card payments there is no particular requirement for data confidentiality between an application and reader. In EMV, data is exchanged between the application and the terminal in the clear. The integrity of transactions is managed by using transaction cryptograms that can only be verified by the issuer and by using different data in different channels, such as requiring the use of the secure code for card not present (CNP) transactions or by using different primary account numbers (PANs) over different channels.

HCE is currently supported in Android 4.4 KitKat and Blackberry OS 10.

1.4 The role of tokenisation

We have seen that HCE allows payment applications residing on the handset to emulated cards on the NFC interface. What HCE does not provide is the way to secure these applications in the absence of a hardware secure element. Since the security of payment data cannot be relied on in the same way as traditional card products and secure element NFC, and alternative approaches to security are needed. Typically, these involve provisioning limited use payment credentials (e.g. PANs and cryptographic keys) into the app prior to each transaction. Provisioning limited use PANs is commonly referred to as tokenisation.

Tokenisation is the process of substituting the account PAN with a single use or limited use "token PAN", where use can be limited by consumer device, channel or merchant. This reduces the impact of data breaches significantly as, for example, the capture of PANs from the systems at one merchant would not impact any others. The aim is to make sure that if a "token PAN" is captured it will have limited and possibly no value. Tokenisation is a layer that can be applied on top of HCE.

To employ this service, the issuer would call a token service provider (TSP) to generate token PANs (and, potentially, payment keys) which would be delivered to the mobile app and used in HCE transactions. When these transactions are processed through the payment network, the TSP would be called to convert token PANs back into a real PAN to allow the issuer to process the transaction in the normal way.

TOKENISATION OF PANS

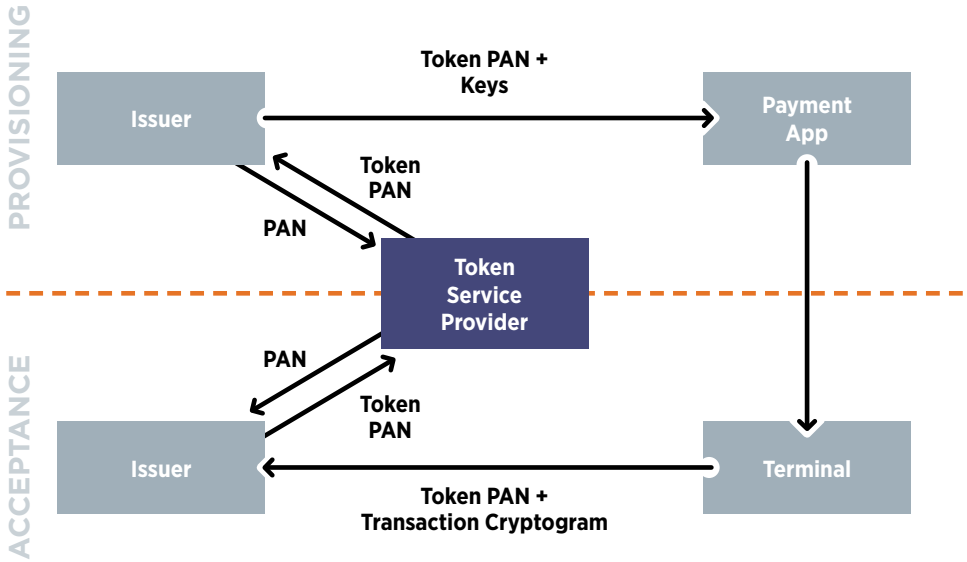

Figure 2

Although not a new technique in retail payments, tokenisation is now being formally defined with EMVCo[1]. Principally created in an attempt to address steadily rising e-commerce card-not-present (CNP) fraud, one of EMVCo's identified 'use cases' for the tokenisation is to support HCE contactless payments.

It is worth noting that EMV tokenisation is not required for HCE contactless EMV payments. Issuers are free to use their own security schemes that do not rely on external tokenisation providers. Typically, these would be the use of static PANs used solely for HCE apps and dynamic data for individual transactions, such as using limited-use session keys which are only valid for a single transaction (each application transaction counter [ATC) value], as allowed for within the existing EMV payment specifications. Also note, that session keys can be used with tokenised PANs. Either way, transaction-specific data (token or session keys) will need to be distributed and managed.

SESSION KEYS WITHOUT TOKENISATION

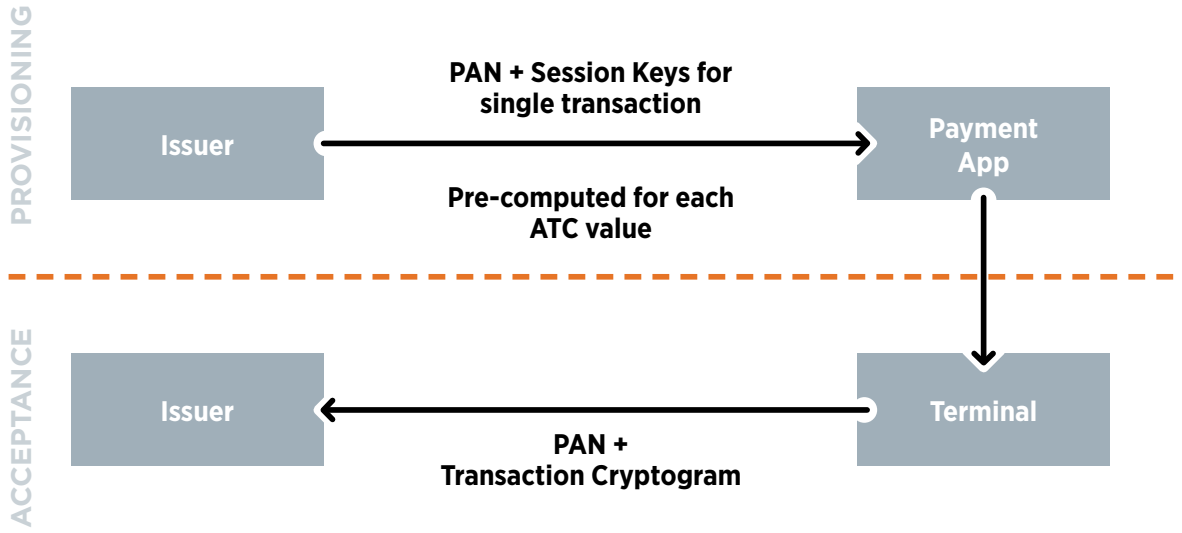

Figure 3

1. EMV Payment Tokenisation Specification – Technical Framework, http://www.emvco.com/specifications.aspx?id=263

1.5 The secure element vs HCE debate

A high-level discussion of the secure element vs HCE debate is presented in the recent Consult Hyperion guide, *"HCE and SIM Secure Element: It's not Black and White"*, comparing each approach. The debate can be summarised as follows.

As secure hardware is not used, the NFC HCE solution for mobile contactless payments is believed to remove some of the complexity associated with SIM SE-based NFC payments and reduce the need for mobile network operator involvement.

Although HCE does indeed simplify some aspects of the NFC ecosystem, it requires a new approach to security which, for now, means issuers will need to either build new capabilities in-house or work with specialist suppliers. Issuers will also need to work with the payment networks to obtain certification waivers until the rules for HCE are fully developed.

By contrast, the processes around SIM SE are mature but with a more complex ecosystem, which the operators are actively working to simplify. In markets with a mature SIM SE NFC ecosystem, taking a SIM SE approach should be quicker and lower risk than HCE, as from an issuer's point of view risk management for SIM SE payment apps is very similar to risk management for card payment apps.

The SIM SE and HCE approaches to NFC payments should not necessarily be viewed as mutually exclusive. There is significant overlap in the functionality required to support contactless payments for each of them and complementary features should be explored.

To make sense of the choices involved, it helps to consider a structured view of the key elements of the mobile contactless payments proposition, including: ecosystem, provisioning, user experience, security, business model and infrastructure maturity. Each of these key aspects is considered for HCE in more detail in the remainder of this document.

2. NFC payment ecosystems

2.1 HCE ecosystem

The emerging HCE ecosystem for mobile contactless payments is illustrated in Figure 4.

THE HCE NFC ECOSYSTEM

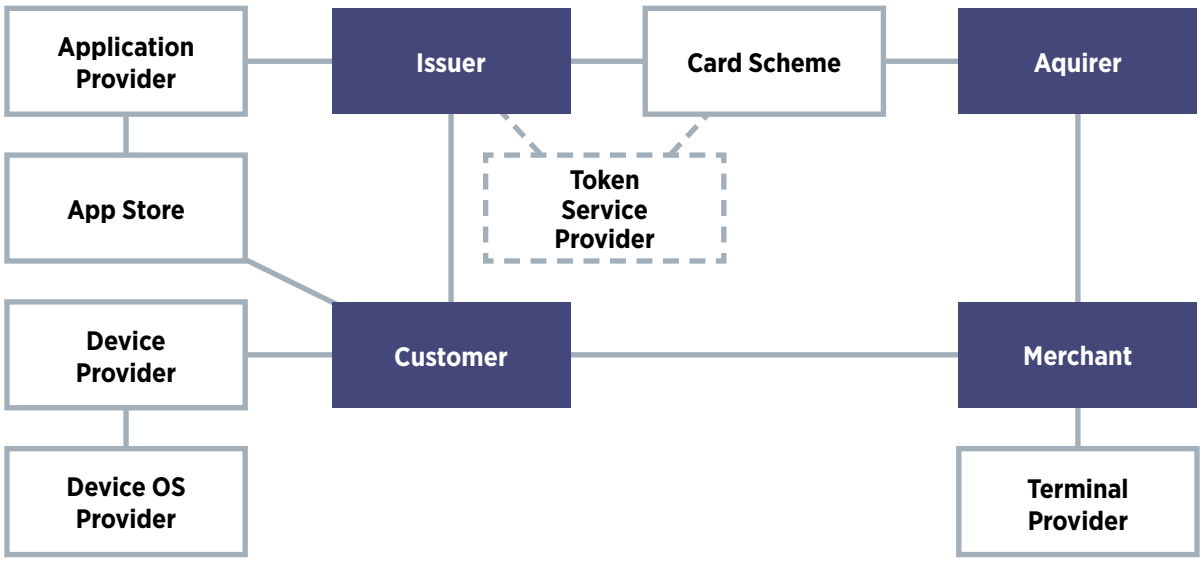

Figure 4

The relationships needed for the processing HCE payment transactions remain the same as for traditional card payments (the four corner model), with the potential for the inclusion of a TSP if tokenisation is to be used. As noted, the issuer is responsible for choosing the security scheme to be used in its HCE apps and the use of EMV tokenisation is optional.

The issuer maintains its relationship with a card scheme for the payment product issued. The card scheme runs the payment network providing the transaction acceptance relationships with merchants through acquirers and processors.

HCE NFC transactions accepted by the merchants are directly equivalent to contactless card or SE NFC transactions – termed “card present” transactions. This means issuers and acquirers have the same liability rules as cards (as defined by the card scheme) and merchants are offered the same settlement terms. In agreement with the scheme rules, issuers have to ensure that the card-present liability model matches their risk management policy for HCE transactions. For example, issuers may choose not to authorise particular transaction types from HCE apps, such as those requiring offline data authentication, Customers receive handsets from devices providers (in many markets these are mobile network operators) independent of the payment application process. Customers download HCE payment apps to their devices from an app store in the same way as for any other app. App stores are normally run by the OS provider for the device. The payment application provider may publish the app to an app store on behalf of an issuer or the issuer may publish the app themselves. As this is just the standard general purpose approach for app management, the issuer has less control over the distribution mechanism for the app and cannot necessarily rely on its integrity or the integrity of the data that gets loaded into it. This is significantly different to distributing smart card apps to cards or secure elements where the integrity of the device can be relied on through relationships with the Personalisation Bureau for cards or trusted service managers (TSMs) for secure elements. Therefore, issuers must use new means to ensure the integrity of apps through the use of software hardening techniques, and to protect transaction data through the generation and use of dynamic data for transactions, that is of limited use and which may or may not include tokenisation of PANs. These aspects are examined further in later sections of this paper.

TSMs are not required for HCE. This is one of the key differences between the secure element ecosystem and the HCE ecosystem. For secure elements using TSMs interoperability is achieved using GlobalPlatfom standards. For HCE, there is no single standard as to how the integrity of payment applications and data is to be ensured. This may lead to a fragmentation in solutions and to usability issues for customers. These aspects are examined further in later sections of this paper.

2.2 Secure element ecosystems

2.2.1 SIM SE

The SIM secure element ecosystem for mobile contactless payments is based on the provisioning of smart card payment applications, including the sensitive payment credentials, inside the SIM secure element. The payment app performs the contactless EMV payment transaction with the POS across the NFC interface, which looks like a contactless payment card to the POS. A mobile app also resides on the handset (outside of the SE) which provides the user interface to the consumer – but the transaction is managed by the application running in the SIM.

The model allows issuers and card schemes to work with mobile operators to install their payment app on the SIM through the mobile operator's TSM. Once provisioned, the issuer will use their own TSM to manage the payment credentials within their payment app. To simplify the provisioning of NFC payment applications, mobile network operators and third parties (such as the cards schemes or consortia of issuers) created TSM hubs[2] and the common TSM for issuers to connect to all operators in a given market. The approach is illustrated in Figure 5.

AN EXAMPLE SIM SE ECOSYSTEM USING A TSM HUB

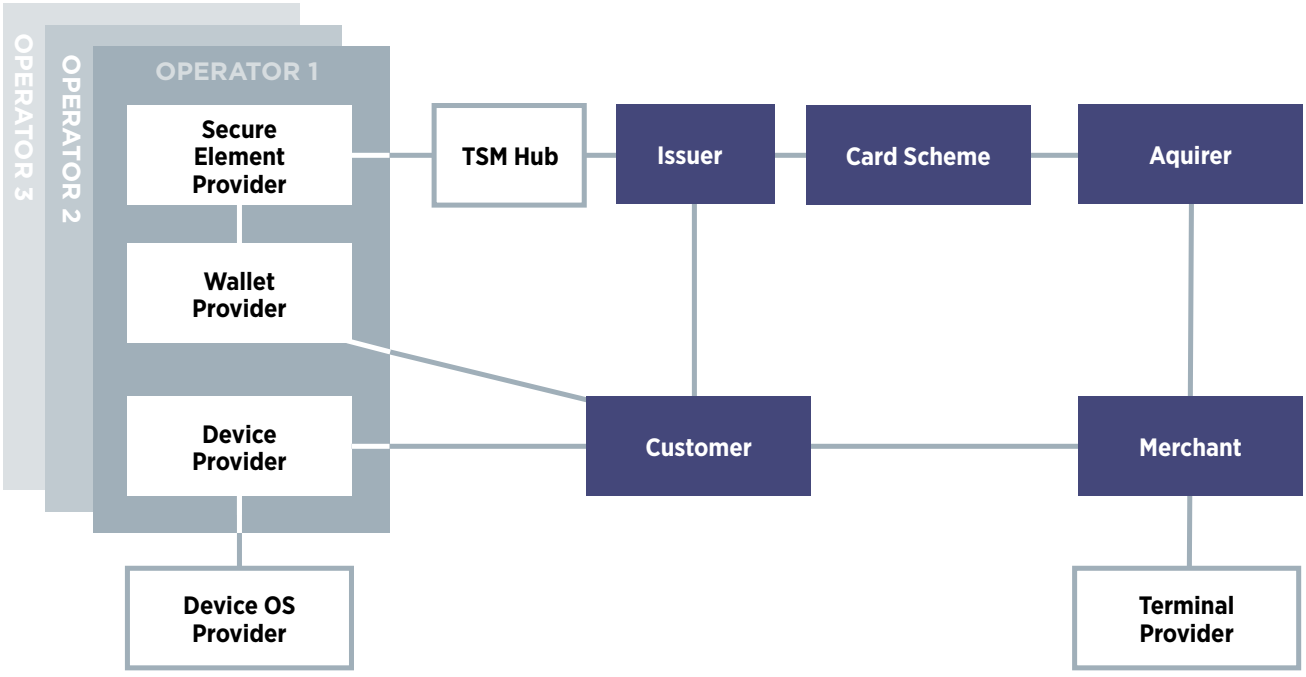

Figure 5

Another common tool is to preinstall payment applications from the main card schemes onto the SIM which can be instantiated remotely for each issuer. This avoids the need to download a complex application for each issuer. A similar approach is also used by ApplePay (Chapter 2.2.2).

In applicable markets, operators now offer a packaged approach to issuers, via TSM hubs that combine the reach of multiple operators, fit with the standard acceptance infrastructure, and offer a well understood security model.

2. http://nfctimes.com/news/tsm-hubs-and-aggregators-can-they-help-banks-roll-out-nfc

2.2.2 Embedded SE – Apple Pay

The approach selected by Apple is very similar to the existing SIM SE approach. Apple has also created its ecosystem for mobile contactless payments based on smart card payment applications running in a secure element embedded in their devices. From the information available publically[3], Apple have agreements with card schemes that allows the schemes to map a payment app installed on the secure element to an issuer customer account through the scheme's own service provider (SP) TSM service.

Issuers must sign up to the Apple Pay service before their card accounts can be mapped to payment applications on the SE by the schemes. The contract arrangement between the issuer and Apple is facilitated by the card schemes.

The ecosystem for this approach is illustrated in Figure 6.

THE APPLE PAY ECOSYSTEM

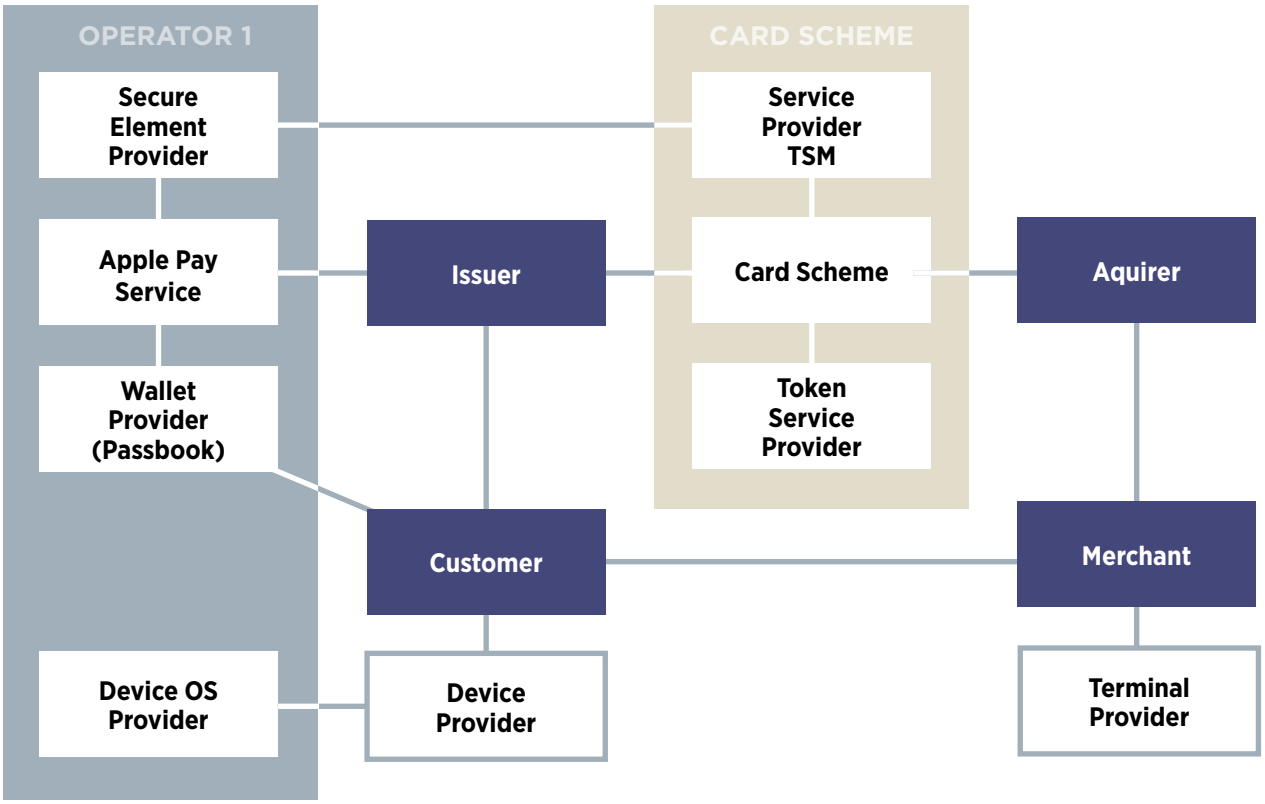

Figure 6

3. http://www.apple.com/apple-pay/

The payment transaction is the standard card present transaction at a merchant terminal. Card schemes personalise a static tokenised PAN (and associated keys and data) into a payment application on the embedded secure element on behalf of the issuer. The cardholder's funding card account with the issuer is mapped to SE PAN in the card scheme service. The difference between this approach and the SIM approach described in 2.2.1 is the PAN is replaced by an alias that is tokenised. For example, to renew personal account information, card schemes can reissue a token to a new card without re-provisioning a new token. This tokenisation model is different to the HCE model, as due to the token being securely stored on a secure element it does not need to be renewed for every transaction or dynamic, making the system simpler to manage.

The handset user interface is provided by Apple Passbook. On the Apple iPhone, the user authenticates to Passbook using the home button fingerprint reader. On the Apple Watch, the user activates the SE payment app by a double tap on a side button. This means that the issuer does not decide the authentication approach for the cardholder on the handset but uses Apple's implementation for Passbook.

As the service is being launched in the US, which has not yet migrated to EMV terminals, some questions remain as to its fit with existing payments when it rolls out internationally. For example, it is not clear whether offline data authentication is supported and whether Passbook cardholder verification can fully replace online PIN at POS terminals in markets using this method of cardholder verification for higher value contactless payments.

In summary, issuers are being offered a packaged approach from Apple, via the card schemes, in which the ecosystem and user experience are managed and defined by Apple.

2.2.3 ApplePay vs SIM Secure Element: Additional considerations

The similarity between Apple's and operators' approaches suggests a consistent, secure and simple payment services on Apple and non-Apple operating systems.

Typically, SIM secure element could offer more flexibility within the user interface than within the restrictions of the Apple approach. The selection of a payment product from the list of installed applications is often done from an operator wallet interface, but the payment user interface itself may be a separate application.

The static tokenisation of the PAN is an interesting idea for the SIM approach. This would simplify the card lifecycle management and would allow issuers to connect to mobile network operators through the same tokenisation platforms.

While outside the scope of this paper, it is also worth noting that both the operator SIM SE and embedded SE approaches offer the potential for transactions initiated from the secure element to be used for remote e-commerce transactions. The GSMA have published a discussion paper, *Mobile and Online Commerce, Opportunities provided by the SIM*[4], that looks at this topic in detail. ApplePay also addresses both contactless and remote transactions, albeit in different way, with in-app payments being the immediate use case for its devices.

4. http://www.gsma.com/digitalcommerce/mobile-and-online-commerce-opportunities-provided-by-the-sim

3. CONSIDERATIONS

3.1 Provisioning

As an HCE payment app running in device host software does not offer the same levels of security as a hardware secure element, alternative approaches to security are required which result in a different provisioning model.

Typically, the approach will involve provisioning limited use payment credentials (that is cryptographic keys and data) to the app on the mobile device that become useless after a transaction using the credentials is performed.

The limited use payment credentials are referred to as the dynamic data for the HCE app. The dynamic data will need to be provisioned into the app for each transaction (or for a small number of transactions depending on scheme rules and issuer risk appetite) to be performed. For HCE, therefore, the provisioning of payment credentials is required prior to a transaction, unlike secure element applications where payment credentials are provisioned once. This is a major difference in terms of service management.

Figure 7 gives an overview of the provisioning model for HCE mobile contactless payments.

HCE PROVISIONING MODEL

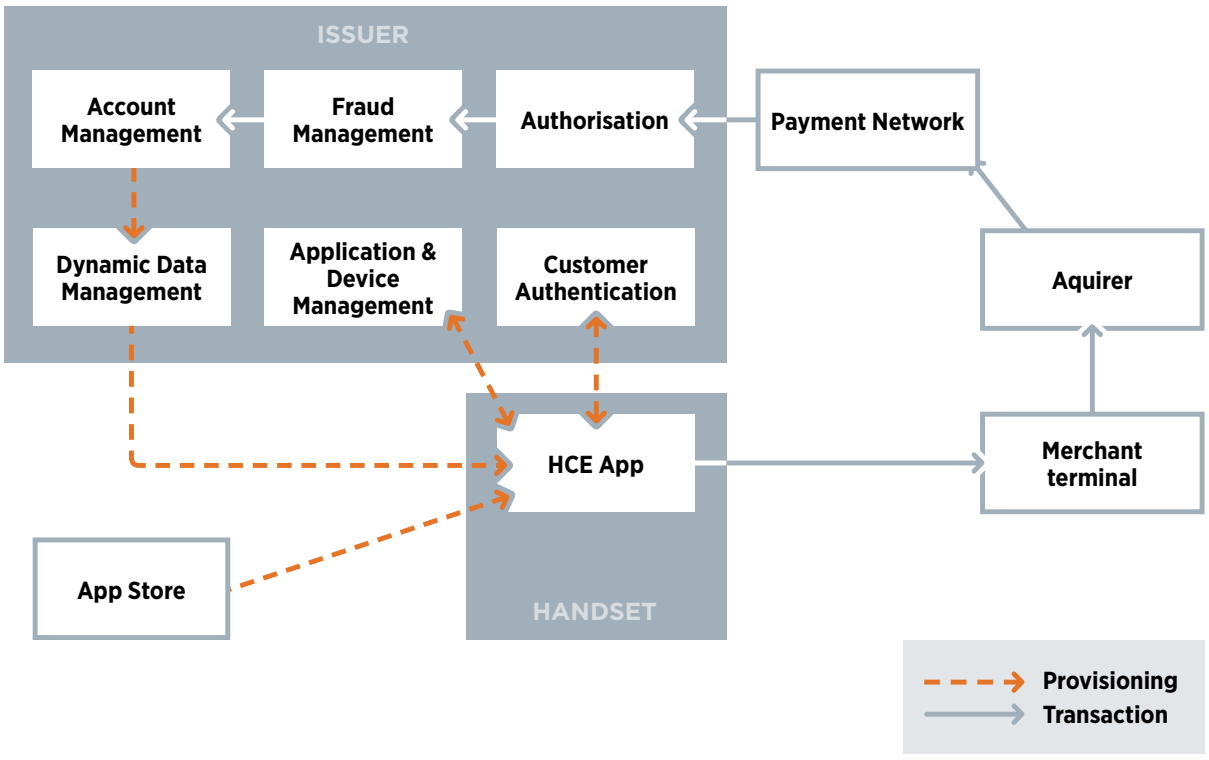

Figure 7

As noted in Chapter 2, the issuer does not control the distribution of the app to its customer base. To ensure that the correct app is used by customers, the following functionality will need to be provided by issuers:

- Application management to protect the integrity of the HCE app and ensure there are only uniquely identifiable app instances installed throughout its customer base. Although issuers may have existing apps, the management of HCE may need to include additional features to protect integrity.

  Similarly, HCE app integrity will require functionality not necessarily required in apps supporting secure element transaction. For example, an HCE-based app may want to detect if the mobile OS has been rooted, is running a debugger or the app is running in a simulator.

- Device management to identify and track each device used for HCE apps, and to track any changes. Without access to secure hardware on the device, issuers must rely on weaker authentication methods to uniquely identify the device. These will include software profiles and software reported environment information (e.g. location).

- Customer authentication that provides binding functions to tie the customer to their device and to the HCE app instance installed on it. The stronger the customer authentication the more confident issuers can be that provisioning is being performed to the correct customer and device.

3.1.1 Provisioning dynamic data

Issuers need to decide how to generate and manage the dynamic data to be used in each transaction during the design of the end-to-end service. For example, should an issuer generate a tokenised dynamic PAN for each transaction or use cryptographic session keys?

Dynamic PANs are unique pre-computed PANs where each one is used in a single transaction. A dynamic PAN may be used in the generation an application card key which is used in the transaction to generate a transaction cryptogram. In this approach, the dynamic PAN and the card key make up the dynamic payment credentials to be downloaded to the HCE app prior to the transaction.

Since EMV version 4.0 (published in 2000), issuers have had the option of using session keys. Session keys are cryptographic keys that are valid for one transaction only, based a transaction counter maintained by the issuer. These will be used to generate cryptograms for transactions that will mean there is no requirement for PAN tokenisation, although an alternative PAN for the HCE channel is always recommended.

GENERATING PER TRANSACTION SESSION KEYS

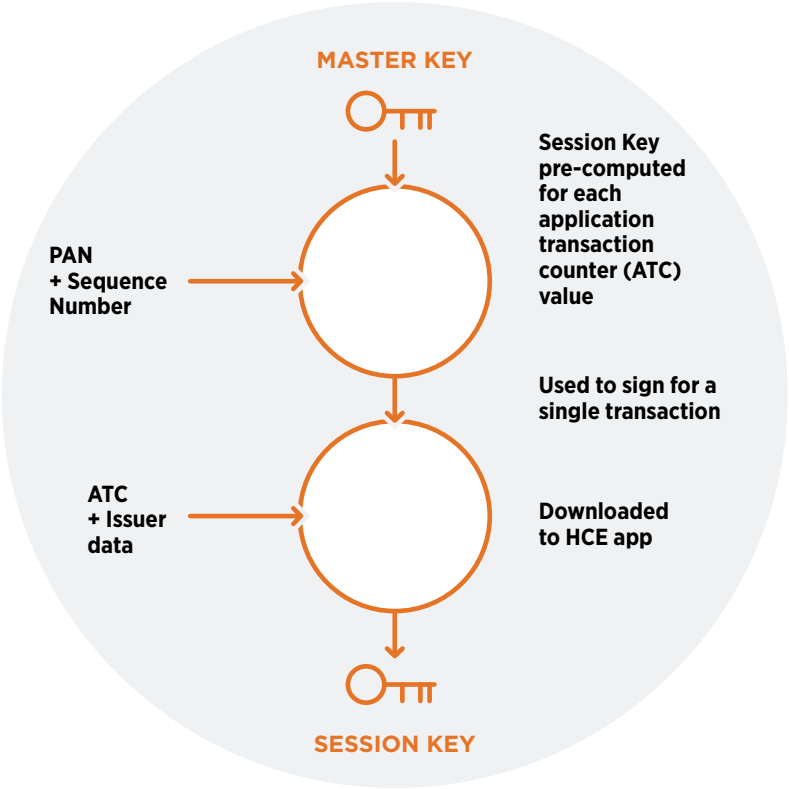

Figure 8

Whatever the dynamic data method selected, the transaction authorisation process (e.g. checking transaction data integrity and cryptograms) is required to implement a corresponding process that correctly detect errors in transaction data and mismatched cryptograms.

TRANSACTION CRYPTOGRAM PROCESS FLOW USING SESSION KEYS

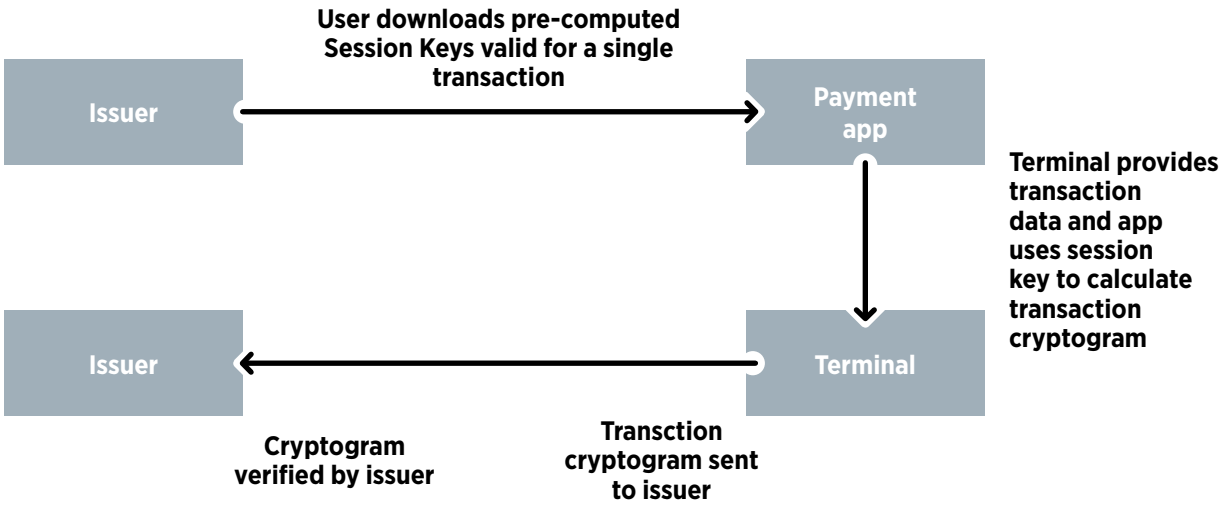

Figure 9

As well as transaction authorisation systems, the impact of the provisioning choices needs to be assessed for other issuer systems. For example, there may be different limits applied to HCE transactions, offline transaction are not likely to be supported and should not be cleared if clearing records are received, HCE apps may be only made available to a specific segment of customers, etc. Issuers need to be aware that choices made for provisioning, may result in changes being required to other systems.

3.1.2 Tokenisation

As pointed out in Chapter 3, the use of tokenised PANs at a transaction level is optional for issuers (although using the real account PAN is never recommended), and will likely depend on whether session keys are supported in the current issuer systems and whether tokenisation is being implemented by the issuer for other use cases (such as for e-commerce payments).

If tokenisation is to be used and an external TSP is being employed, the provisioning model changes to that illustrated in Figure 10.

HCE PROVISIONING WITH TOKENISATION

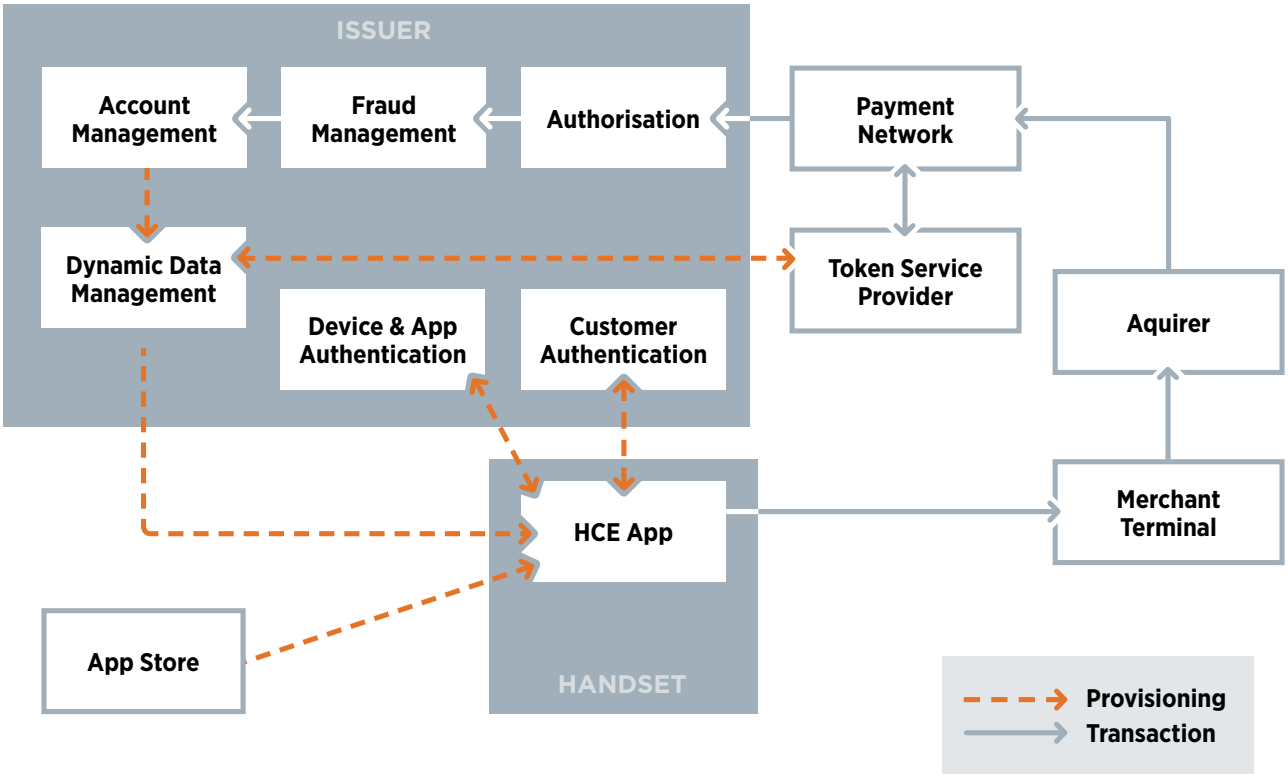

Figure 10

Here, the TSP provides the dynamic data to be downloaded to the HCE app. This means that the TSP must verify the result of the transaction using this data before passing equivalent de-tokenised transaction data to the issuer for authorisation.

3.2 User experience

With the need to provision payment credentials frequently, issuers need to be careful not to introduce usability issues. This aspect is considered further in this section.

While the user experience for the payment transaction in a merchant with an HCE application is the same as for a secure element initiated payment transaction, the journey for the customer to provision data to the mobile app is very different and more involved.

As it is not possible to dynamically retrieve credentials from the issuing bank during a transaction itself, due to the latency in the network and the lack of universal connectivity in merchants, payments credentials (such as dynamic PANs and single use keys) will need to be delivered to the mobile phone ahead of the transaction occurring.

This is illustrated in Figure 11.

CUSTOMER JOURNEY

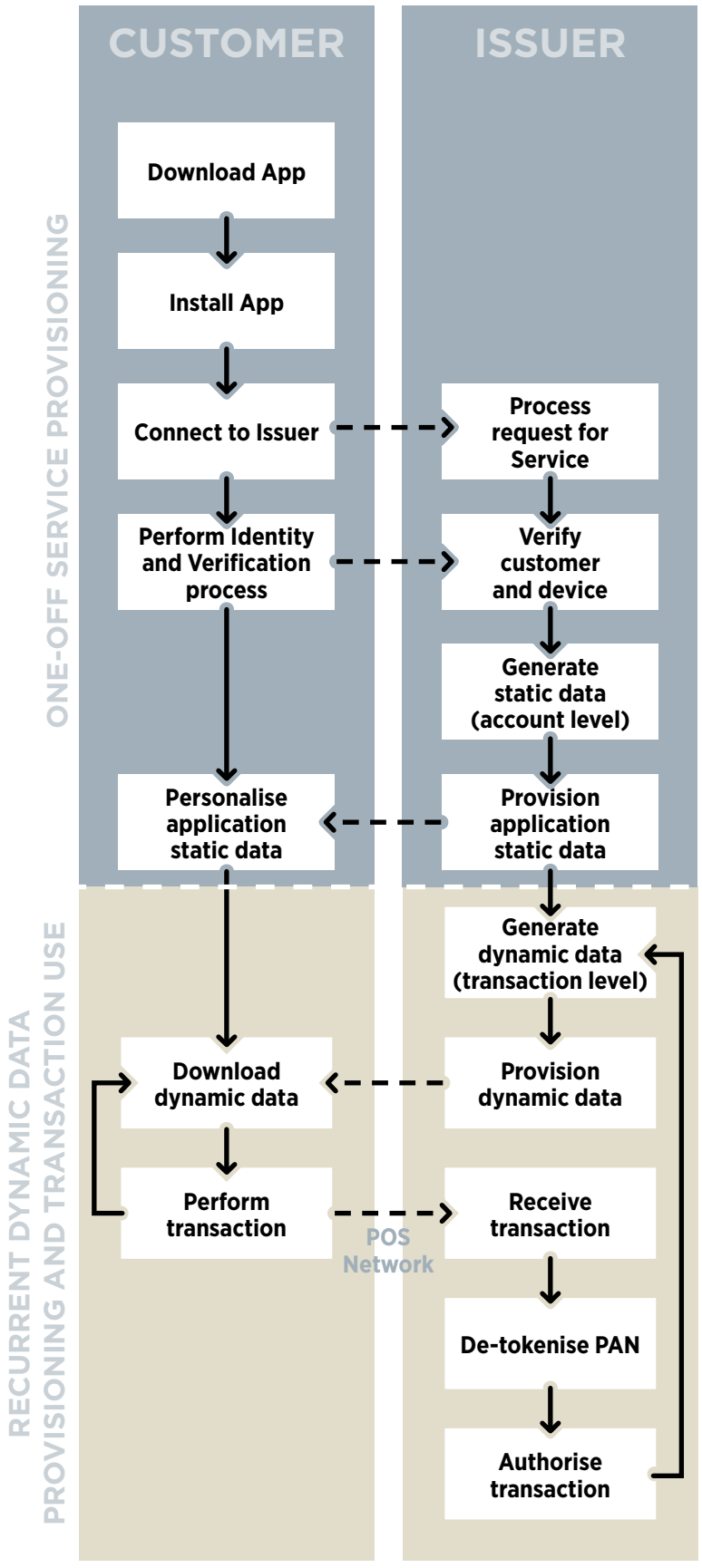

Figure 11

As illustrated in Figure 12, HCE and secure element-based NFC have similar payment experiences at the POS. HCE apps have a few differences that affect the usability that issuers need to be aware of. For example, Android currently requires that the screen is switched on for the host processor to run apps, meaning that when there is low or no power, HCE apps will not work. Secure element apps are meant to be able to work when the handset has no or low power as the controller can be driven passively by the reader.

Additionally, different card scheme implementations may have different requirements that affect the user experience. For example, with one scheme requires the entry of a PIN into the HCE app for cardholder verification prior to a transaction being performed.

PAYMENT TRANSACTION USER EXPERIENCE

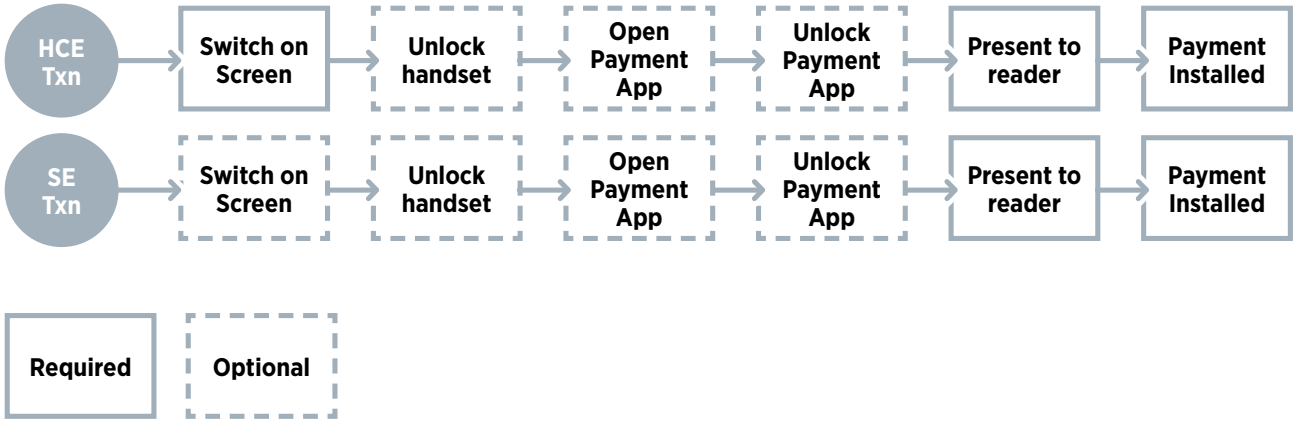

Figure 12

3.2.1 Downloading data

As indicated in the customer journey in Figure 7, the requirement to download dynamic data prior to transactions, and how it's implemented, will affect the user experience. Issuers need to decide how many transactions will be supported in a single download of dynamic data and how often customers are required to be authenticated (e.g. with every download or less frequently).

Typically, these aspects are set and controlled by issuer risk management, who are responsible for assessing the exposure should an HCE app be compromised. The key questions are:

- How many 'sessions' will be available on the handset at one time?
- Should the cardholder be authenticated for every download and update?
- Can other factors such as device location be used to enhance the experience (e.g. less frequent authentication when at home/work)?

In the initial deployments, issuers will need to track and learn behaviour such that the user experience is optimised for customers while controlling overall risk. For example, to make sure the user does not run out of 'sessions'.

Customer interaction is only required for the authentication step, as illustrated in Figure 13. If the issuer decides that no authentication is required for a particular download, then it can be performed automatically in the background. If customer authentication is required, then the user should receive a notification to complete authentication.

DYNAMIC DATA REFRESH USER EXPERIENCE

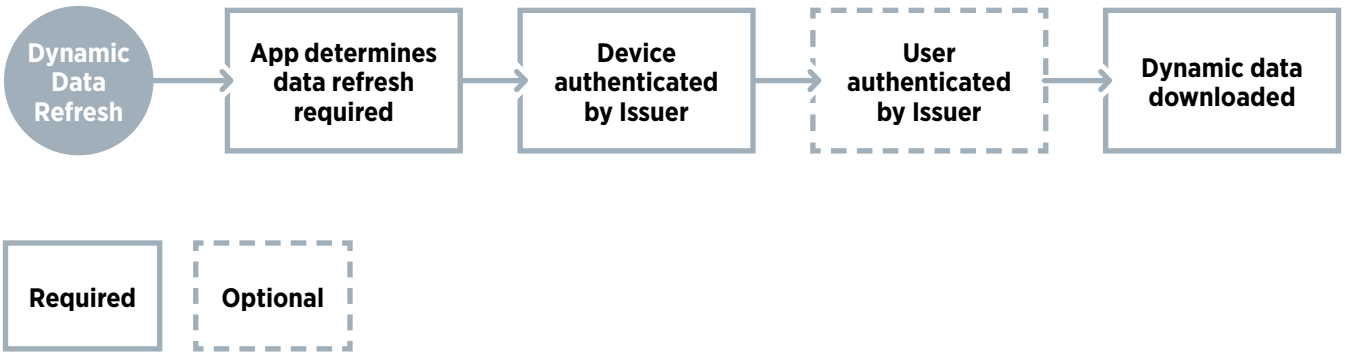

Figure 13

Additionally, issuers' account management systems and processes (such as customer care) need to be kept up-to-date with developments for HCE apps. As customers' user experience for HCE apps is ongoing (as dynamic data needs to be refreshed), keeping track of activity on accounts (while protecting users' privacy) is important to be able to service customers effectively and deal with usability problems as they arise. This will be a key part of the overall customer experience.

3.2.2 User experience considerations

Table 1 provides a summary of the key features of the user experience that issuers need to consider to support HCE.

TABLE 1: USER EXPERIENCE SUMMARY

FEATURE	COMMENTS
Default payment app	Selection of the default application is defined in Android and is, in principle, user controlled.
Power-off / Low-power	HCE apps always require the processor to operate normally for transactions to be possible.
Online transaction	HCE are designed to be online authorised. HCE offers a similar experience to contactless card and secure element online transactions in the majority of situations.
Offline transaction	Offline data authentication at standard offline terminals require an appropriate public key certificate chain, signed by a scheme key at the root. The payment app key pair and certificate needs to be protected in software for long enough that their discovery do not allow further transactions offline and compromise the integrity of the scheme. The current HCE specifications do not support offline transactions. The impact of this is market specific, as although many offline terminals are also online capable, some acceptance points will be impacted in markets supporting offline transactions.
Transit	Transit transactions are delayed authorisations – a combination of offline data authentication and an online transaction. As previously noted, offline data authentication would need to be supported by the card scheme specifications. Proposals are in place for a transit specific public key hierarchy but such support is not yet standardised.
Higher value payments – Online PIN markets	In principle, HCE offers a similar user experience to contactless card or secure element for online PIN transactions. The transaction is accepted by the POS reader and the PIN entered on an attached PIN pad.
Higher value payments – Offline PIN markets	Although, a PIN cannot be verified offline in a standard mobile app, PINs can be checked by issuer host systems through the use of transaction cryptograms that use the PIN as an input, or, depending on scheme rules and issuer risk management, by using an additional device feature or service (such as a hardware secure element or trusted execution environment). The functionality to achieve this is not standardised across scheme specifications and may vary by issuer.
Remote payments	In principle, in the same way that secure element mobile payment apps can perform e-commerce transactions, HCE apps using single use credentials can be used remotely. Customer authentication will need to be implemented differently to payments at POS. Currently, there is no interoperable approach defined by the card schemes.

3.3 Security

As there is no secure hardware for HCE, solutions propose to use dynamic data (e.g. dynamic PANs and cryptographic session keys) delivered to the mobile app to enable it to perform a single transaction based on these credentials. As these payment credentials aim to be single use only, the security risk for transactions should be less than credentials expected to be valid for a number of years (as is the case with secure element solutions). However, it is of key importance that credentials are delivered precisely to the correct device under the control of the cardholder and over the lifecycle of the device. The use of dynamic data method generally implies increased transaction profiling and monitoring.

While the actual risk for HCE service will depend on its actual implementation, Table 2 introduces key risk areas for payments and expected countermeasures.

TABLE 2: HCE RISK EXAMPLES

RISK	IMPACT	COUNTERMEASURE / CONTROLS
Counterfeit	Clone application and use it on another or reuse it same device. Change app code to allow use when normal logic would decline a transaction.	Downloadable limited use payment keys for use in online transactions. Limits on the use of offline transactions. Software protection for the HCE application itself, and keys and other sensitive data. No risk management logic should be included in application code. Fraud monitoring for suspicious device use or transaction patterns. Incorporate hardware security using a secure element or trusted execution environment.
Lost & Stolen	Stolen device used for transactions.	Customer authentication for the refresh to dynamic data and at POS for higher value transactions. Incorporate application and device management to ensure each app is a distinct and identifiable instance.
Cross-contamination	Data capture and reuse in different channel.	Use HCE specific PANs for HCE applications or dynamic PAN from a tokenisation service.

3.3.1 Controls and risk management

Addressing the previously introduced threats will require a risk-based application and device management system that can manage the entire estate of app instances that are able to make decisions allowing provisioning or transaction use. The controls required to support HCE apps necessitate the following types of security functions to be included in issuer deployments:

- Application security – to provide protection for the app itself (that is to ensure it has not be tampered with, stolen or otherwise compromised), the payment keys and other sensitive data, through software protection (e.g. perhaps using white box cryptography where appropriate) in the handset app and/or by adding support for secure hardware (that is a secure element or trusted execution environment) to store sensitive data;
- Device security – to assess whether the device can be trusted, using software detection mechanisms linked to the OS (e.g. root detection, emulator/debug detection) and/or including support for secure hardware.
- Communications security – to ensure that communications between the handset app and the issuer host servers are confidential with trusted integrity.

Accepting an electronic payment transaction involves the management of risk. Risk management aims to reduce the likelihood that the risk will occur or limit the impact of the risk, while achieving the desired usability and supporting the target transaction types. Issuers implement this through a combination of technical authorisation of the transaction data and sophisticated fraud management systems and processes (which may be outsourced with appropriate policies in place). Upgrades to fraud management may include monitoring the characteristics of HCE transactions, such as linking transactions to device and application identities and customer behaviour and transaction activity monitoring.

It is important that customer user experience is not adversely impacted with the introduction of the controls needed to protect against the identified risks. This balance needs to be assessed in conjunction with issuers' existing environment and applications to ensure a consistent approach is delivered across services.

It is worth noting that the reputational risk associated with security failures may be more costly than the monetary losses incurred by an issuer, particularly in offline markets for which contactless transactions are limited to lower value.

3.4 Business model

3.4.1 HCE in software

The business model for HCE appears to offer a "no fee" provisioning model. However, the issuer has to invest in its host platforms to support the HCE services as downloadable dynamic data for contactless EMV applications is new functionality.

The tangible benefit for an issuer would be the transaction revenue model that applies to contactless cards in their market, with an expected transaction uplift due to the convenience of having a payment product in the mobile form factor. With the cardholder authentication, mobile allows for higher value contactless payments. As such, any transaction uplift seen may also include an uplift in the value of contactless transactions, as well as their frequency.

The key cost components to issuers for the development of the system required to support HCE transactions are likely to be:

- Dynamic data generation (e.g. limited use cryptographic session keys)
- Device and customer authentication
- Upgrades to transaction authorisation and fraud management (if needed)
- Upgrades to account management to service customer requests and product lifecycle
- HCE app development and support, perhaps with integration into existing mobile applications
- Lifecycle management of deployed HCE apps to identify, track devices and app instances (including binding to users, upgrades and revocation).

Operationally, these have to be managed by the issuer (or its outsourcer). The provisioning functions to and from the customer device should be automated. However, as previously shown, the user experience is significantly different to using a standard contactless card or secure element NFC device such that additional customer support and problem management is likely to be required (such as filtering calls to the appropriate staff).

If the issuer would to choose to use the third party tokenisation services, these are likely to attract fees but may reduce the need for upfront investment in bank developed services.

A generalised statement on the likely size of the initial investment is not appropriate for this paper, as issuers' current capabilities and existing systems will have a significant impact (e.g. whether services are outsourced). Naturally, before issuers engage on a change programme, they will need to have worked through a comprehensive cost assessment.

3.4.2 With secure hardware

As noted in chapter 3, to reduce some of the complexity of managing the downloaded dynamic data stored in the insecure software components of a handset, secure hardware could be used (if available). Generally, a reduction in complexity leads to some removal of cost. More importantly, perhaps, if a secure element were available from HCE apps, it could be used as to improve the security of device, app and customer authentication, reducing its complexity and potentially reducing the need for additional transaction fraud management. This is illustrated in Figure 14.

HCE COMBINED WITH A SECURE ELEMENT

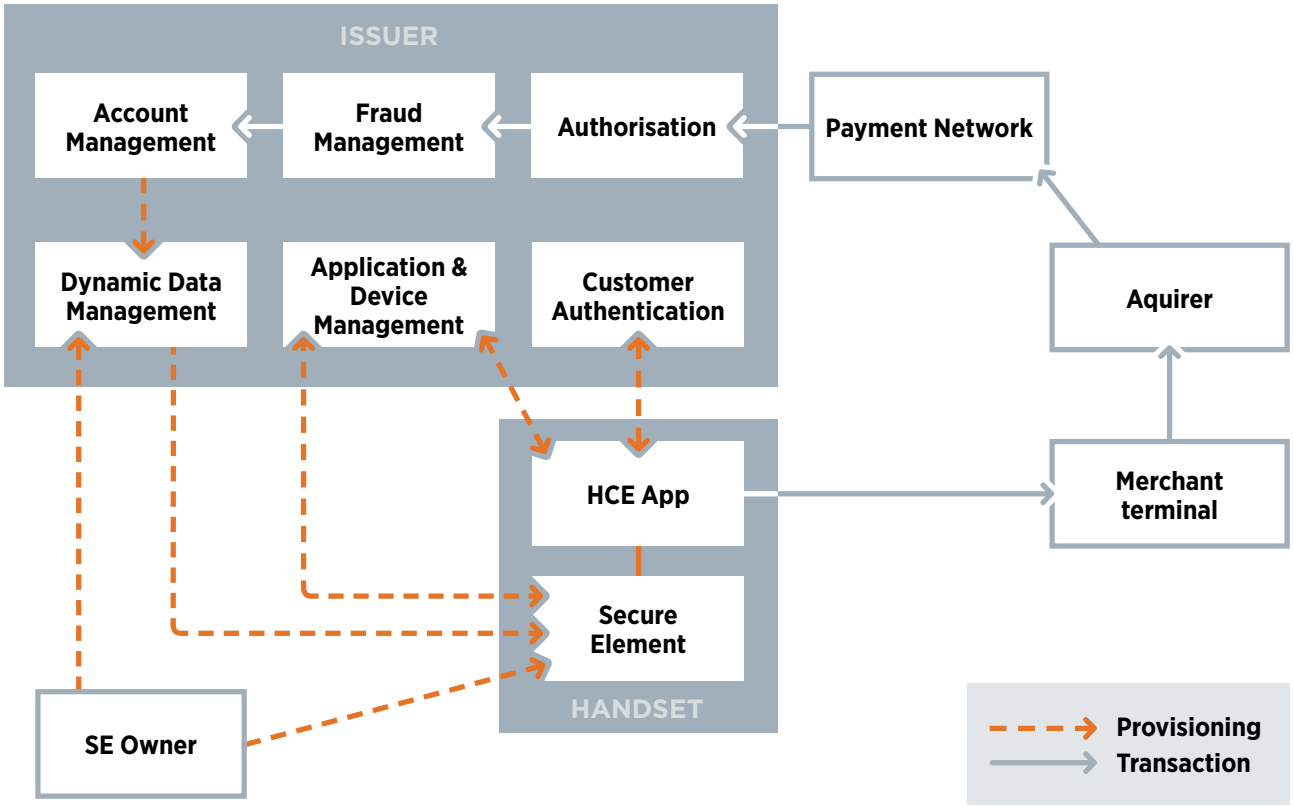

Figure 14

This approach, sometimes referred to as a hybrid model, has not been fully defined and, as such, issuers would need to work with suppliers and partner organisations to investigation its possibility and assess whether it represents an actual cost saving. The benefit may be an improvement in the user experience for customers as dynamic data would likely need to be downloaded less frequently. There may also be a benefit if customers' perception that an increase in security is provided.

3.5 Maturity

The card payments ecosystem is defined by the card schemes working together within EMVCo to provide technical interoperability at transaction acceptance in merchants. This approach has been very successful in creating stable specifications and global interoperability covering many hundreds of millions of cards and devices, and many millions of payment terminals.

For contactless payments, the payments industry (and its partners) has evolved from contactless EMV card payments, to mobile NFC payments using secure elements and most recently now to include HCE NFC payments. The timeline for this evolution is illustrated in Figure 15.

ILLUSTRATIVE HCE TIMELINES

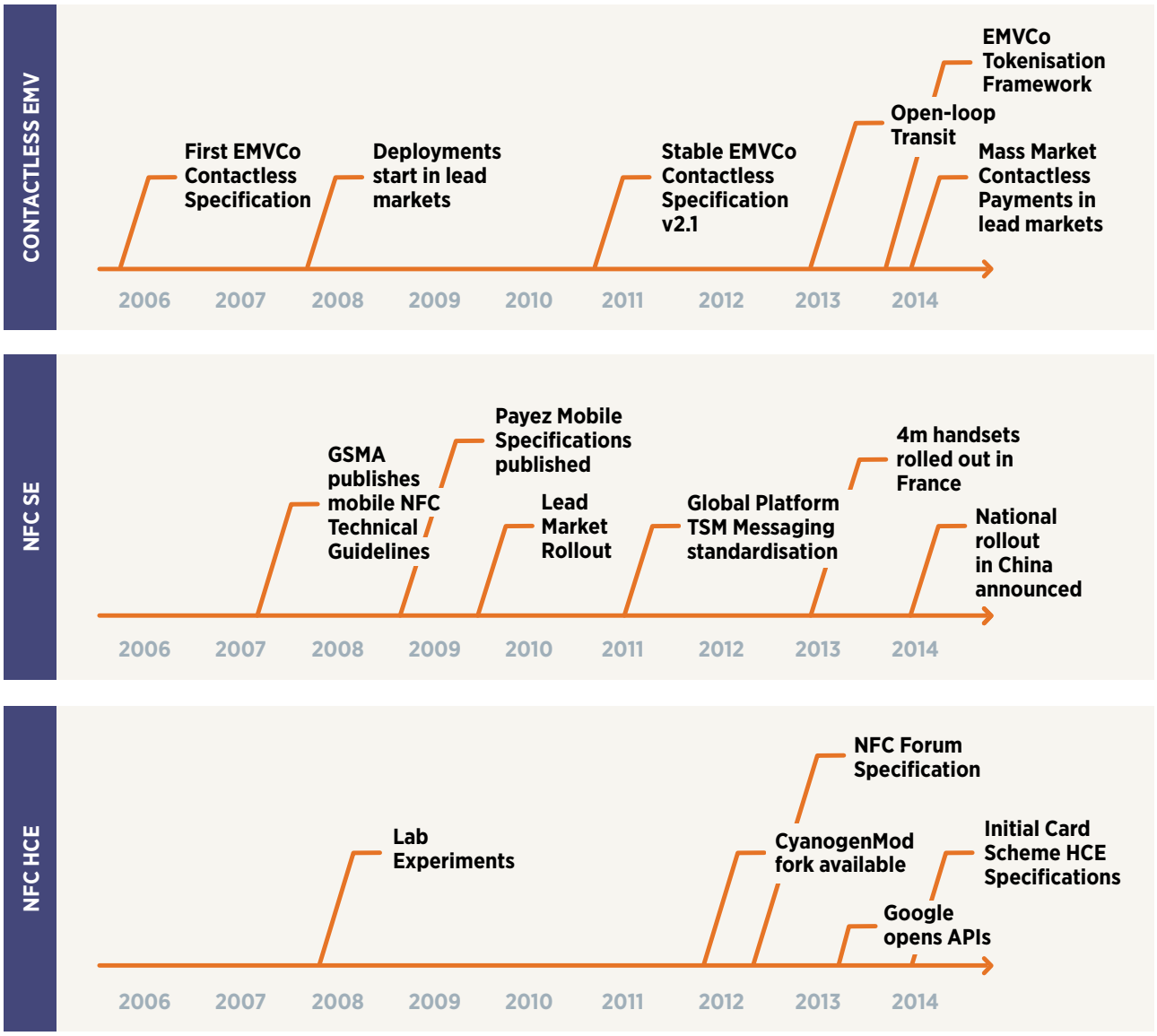

Figure 15

As the Figure 10 shows, for retail payments the timescale for the evolution from an idea and initial specification to a mass market population scale product deployment is considerable. This is because payment ecosystems involve relationships between many parties whose interests must be aligned, and products tend to be deployed into markets that have existing, generally well-functioning, alternatives acting to dampen consumer take up.

In comparison with other contactless products, the evolution of HCE to population has only just started. HCE products will inevitably go through a series of refinements as trials and pilots continue. For now, trials and pilots will likely be on a limited scale and will require waivers from the card schemes.

The lifecycle stages in a typical product development and deployment is illustrated in Figure 11.

TYPICAL PAYMENT DEVELOPMENT LIFECYCLE

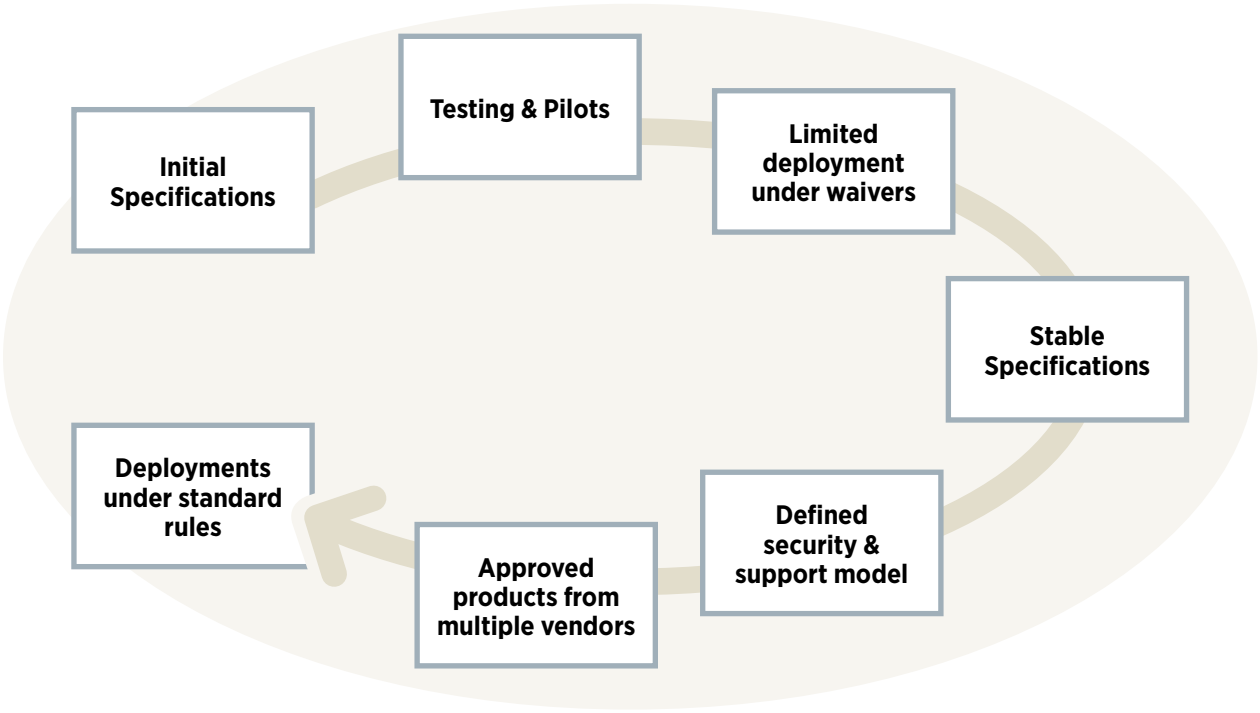

Figure 16

Historically for retail payments, each significant functional adaption follows this type of cycle over a period of at least two to three years, and if terminal changes are required, the timescale can be significantly longer. Issuers should be aware of this and, if market readiness dictates, consider drawing up a suitable roadmap with plans to come to market with an alternative, more mature, product.

4 CONCLUSION

The attractiveness of mobile NFC payments increases with the growing penetration and stability of the contactless acceptance infrastructure. Whereas as little as two years ago, contactless acceptance for general purpose in-store payments was unproven, today the penetration and use of contactless cards and terminals is expanding in many markets around the globe. Contactless payments are migrating into mobile with the rollout of secure element NFC payment applications (where local market conditions are suitable), and now with the entry of Apple into NFC mobile payments, momentum is likely to increase further.

HCE offers the promise of an additional mechanism for banks to support their customers. It:

- Simplifies the ecosystem for provisioning applications at the expense of increasing payment transaction risk management,
- Removes the cost and complexity of application management using a third party supported secure element, but
- Increases the complexity of issuer host systems, as these systems now have to provide dynamic data for each transaction.

Dynamic data (e.g. transaction specific cryptographic keys) is needed to address the vulnerabilities exposed by the lack of a secure hardware platform in the customer's handset. For secure element solutions, one cryptographic key is generated per account for the life of the product. This will need to be changed to generate tens of keys per month for each HCE payment app. Careful process design (e.g. such batch pre-generation) and management of resources is required to ensure system performance and user experience are not adversely affected, and incremental costs are not prohibitive.

The use of a dedicated static PAN for HCE or per-transaction dynamic PANs will help limit the option cross-contamination into e-commerce. Issuers can choose to undertaken PAN management themselves or use one of the commercial tokenisation services that are coming to market.

As the user has to download (either by choice or on a pushed basis) dynamic data for use in transactions prior to the transaction occurring, the security of HCE relies on the authentication of the customer for this download. An attacker does not need to break the security of the app if they are able to use legitimate credentials to download payment data. It is important that sufficient emphasis is placed on securing customer authentication over the whole lifetime of the products, including integration of device authentication and, perhaps, with links to transaction fraud management. To address this, issuers should consider the use of additional hardware security for the long-lived authentication credentials.

The additional costs required for the new issuer processes require careful consideration. During a cost analysis, we

suggest that issuers work with partners to explore the potential benefit gained by the integration of a secure element into their back-end processes for HCE. This should result in an understanding of how the hybrid approach could control the cost and complexity of a solution implemented to a population scale. The secure element offers an option for the local storage of dynamic data, improving usability, as data can be trusted and does not need to be downloaded as frequently, and can help to secure device and customer authentication when a download from the issuer is required, to address this key vulnerability in the process.

It is still early in the lifecycle for HCE, with the initial scheme specifications being published or under development. Assuming HCE follows the development path of other card payment technology deployments, it will be a year or so before specifications and product stabilises.

The findings from Consult Hyperion's initial HCE guide continue to ring true:

- Begin by understanding your local market conditions and your target transaction profile.
- Maintain flexibility in your strategy, as secure hardware is likely to continue to be a significant part of the most appropriate solution, and
- Work collaboratively with industry partners to ensure that customers and merchants are brought along with the ease-of-use promise that the HCE can bring.

ABOUT CONSULT HYPERION

“Thought leaders in digital money and digital identity”

Consult Hyperion is an independent strategic and technical consultancy, based in the UK and US, specialising in secure electronic transactions. We help organisations around the world exploit new technology for secure electronic payments and identity transaction services from mobile payments and “chip and PIN” to contactless ticketing and smart identity cards. Our aim is to assist customers in reaching their goals in a timely and cost-effective way.

We support the deployment of practical solutions using the most appropriate technologies and have globally recognised expertise at every step in the electronic transaction value chain, from authentication, access and networks, to transactional systems and applications.

For more information, visit www.chyp.com

ABOUT THE GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world’s mobile operators with 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities. The GSMA also produces industry-leading events such as Mobile World Congress and Mobile Asia Expo.

The GSMA’s Digital Commerce program works with mobile operators, merchants, banks, payment networks, transport operators and services providers to support the deployment of mobile commerce services. By fostering the ecosystem to encourage and facilitate collaboration, the program collaborates with the mobile ecosystem to develop specifications and guidelines for technical implementation and build value propositions for adjacent sectors.

For more information visit www.gsma.com

GSMA Head Office
Level 2, 25 Walbrook
London, EC4N 8AF,
United Kingdom
Tel: +44 (0)207 356 0600

www.gsma.com

©GSMA 2014