HCE and SIM Secure Element:

It's not black and white

A Discussion Paper from Consult Hyperion

Date: June 2014
Authors: Steve Pannifer, Dick Clark, Dave Birch

steve.pannifer@chyp.com

consult hyperion
securing tomorrow's transactions

Supported by:

MasterCard

mobey forum

THE UKCARDS ASSOCIATION

Consult Hyperion
Tweed House
12 The Mount
Guildford
GU2 4HN

t: 01483 301 793
f: 01483 561 657

www.chyp.com

Executive summary

The recent inclusion of Host Card Emulation (HCE) into Android 4.4 KitKat opens up the possibility of performing mobile NFC payments without using a SIM Secure Element (SIM SE). HCE may potentially remove a lot of the complexity associated with SIM SE-based NFC payments and reduce the need for mobile network operator (MNO) involvement. This is, however, only part of the story.

This paper shows that whilst HCE does indeed simplify some aspects of the NFC ecosystem (most notably the application provisioning process), it requires a new approach to security. For now, issuers will need to either build new capabilities in house or work with specialist suppliers. They 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 MNOs are actively working to simplify.

There are also some usability considerations with HCE that need to be addressed, as the use of the technology matures. Whether or not these impact a particular issuer will depend on the types of transaction that the issuer needs to support.

The SIM SE and HCE approaches to NFC payments should not be viewed as mutually exclusive. There is a lot of overlap in the capabilities required to support each of them. Whilst this paper contrasts payments using SIM SE to payments using HCE, the two approaches will not stay this polarised as the markets develop. Combining the approaches may allow solutions to be optimised for different markets whilst reusing existing infrastructure that has already been developed.

The incorporation of HCE into the smart phone mainstream has tapped into significant latent demand for mobile contactless transactions. This will stimulate a new interest in MNO NFC services in the mass-market. For issuing banks contemplating which approach to NFC payments is right for them, this paper shows that there are a number of factors to consider. The biggest single factor is likely to be the local market. In markets with a mature SIM SE NFC ecosystem, taking a SIM SE approach should be quicker and lower risk than HCE. In other markets, a deeper analysis will be needed as both solutions develop.

Introduction

Retail payments in face-to-face environments continues to be an area of considerable innovation. The mobile phone is at the centre of these initiatives. Many mobile devices are now equipped with Near Field Communication (NFC) technology that allows the mobile phone to communicate with contactless-enabled terminals, just as contactless EMV[1] cards can. The use of mobile banking is also growing rapidly and many banks are seeking to determine the best way to enable payments at point of sale (POS) from within mobile banking applications.

Host Card Emulation (HCE) is being proposed[2] as a short-cut for mobile NFC payments. It could allow banks to launch mobile NFC products without needing to make use of the SIM or other Secure Element (SE), by allowing the mobile device operating system (OS) to communicate directly over the NFC interface in card emulation mode. This would allow banks to issue mobile NFC products over the top, removing the need to cooperate with mobile operators, with the aim of reducing cost and complexity.

Is this the right approach for card issuing banks to take?

This paper seeks to provide a balanced view on this development to help card issuing banks better evaluate the approaches they should take to NFC payments.

At the same time as the payments industry is experimenting with these new approaches to NFC payments, there are other developments in the card payments world. In October 2013[3], the three largest global card brands came together to announce a standardised approach to tokenisation – the process of substituting the real PAN (Primary Account Number) with a "token" to reduce PCI DSS (Payment Card Industry Data Security Standard) risks. The primary focus of this initiative is "card not present" (e.g. eCommerce) payments. As this paper will show HCE implementations may benefit from single or limited use PANs. Therefore, no discussion about HCE is complete without reference to this tokenisation initiative.

What is HCE?

Host 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 SIM) was required to be accessible to the mobile phone and was used to store the card payment application. This was called "Card Emulation".

With HCE, no smart card device is required. The payments application is held in the mobile phone operating system (the "host").

Note that the term "host" in this context does not refer to the issuer host although, as we will show later, supporting HCE will impact the issuer host.

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

1. "Europay MasterCard Visa", the standards body for smart card based retail payments.
2. http://nfctimes.com/news/hce-moves-forward-promise-and-not-little-hype
3. http://newsroom.mastercard.com/press-releases/mastercard-visa-and-american-express-propose-new-global-standard-to-make-online-and-mobile-shopping-simpler-and-safer/

Mobile is the future

It is clear that the mobile consumer device has a very significant role to play in the delivery of services to consumers. In many markets smart phone penetration is already well above 50% with the majority of those smart phone owners using the mobile internet and mobile apps on a daily basis.[1]

Mobile banking is no exception to this trend. The Federal Reserve recently reported continued growth in mobile banking[2]. 51% of US smart phone owners used mobile banking services in 2013. Many banks are adopting a "mobile first" approach realising that the mobile channel allows them to interact with customers more frequently and in new ways. Payments should be high on the list of services a bank wishes to offer. They allow the bank to engage frequently with the customer, providing greater insight into their behaviour and increasing the opportunities to build trust.

Why has it taken so long?

NFC mobile payments have been talked about for a long time. The NFC Forum standards body was founded in 2004. The first commercial trials were seen in 2007 with live products being launched from 2011.[3]

There are several reasons why it has taken this long for the NFC payments momentum to build:

- The first Android smart phone (not including NFC) was released in 2008. Whilst some early NFC products were launched on "feature phones", mobile payments really only make sense in the context of full smart phones and the associated app store ecosystem.
- Until recently only a limited number of phones supported NFC. This is no longer an issue. There are now many more NFC handsets. At the time of writing there are 224 mobile phone models supporting NFC, with more coming soon.[4]
- Mobile NFC is dependent on the rollout of contactless card payment terminals. Without them no mobile NFC transactions can be performed. Contactless acceptance now exists in many markets[5] across the globe and is a widely supported interface for payments at POS.
- The different priorities and expectations of banks and mobile operators caused delays in the establishment of the required ecosystem. In a growing list of markets, these parties are now working closely together.

We are now at the point where the right conditions for NFC payment have been created in many markets. The question is then for issuers to consider which approach they should take to NFC – SIM SE or HCE?

1. http://think.withgoogle.com/mobileplanet/en/
2. http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf
3. See http://www.nfcworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/ for an extensive list of trials and live deployments
4. See http://www.nfcworld.com/nfc-phones-list/#available for an exhaustive list of handset that currently support NFC.
5. http://newsroom.mastercard.com/press-releases/mastercard-to-use-host-card-emulation-hce-for-nfc-based-mobile-payments/

Figure 1, Live SE NFC Deployments

As illustrated in Figure 1 there are numerous live NFC deployments around the world, these however have had mixed success due to those market conditions. In the US, for example, until EMV[1] contactless technology replaces magnetic stripe, contactless may struggle. In China and Canada, on the other hand, where the contactless acceptance is relatively high and the banks and mobiles operators are collaborating, the required conditions for the ongoing NFC launches appear to be met.

What's the difference between SE and HCE?

Before comparing the SE and HCE it is helpful to understand what the difference between the two approaches really is.

Figure 2 illustrates the difference between SE and HCE in the handset.

In SE NFC payments, the application (or "payment app") containing the payment credentials (i.e. secret cryptographic keys) are stored in a tamper resistant hardware module referred to as the SE. The SE has a direct connection with the NFC controller/antenna. Typically this would be the SIM SE (also referred to as the UICC) owned by the mobile operator, meaning that the mobile operator would need to be involved in provisioning of the payment app. Up until Android 4.4 KitKat, this was the only supported way of emulating a payment card on an Android device[2].

Android 4.4 KitKat now additionally allows a payment app located in the mobile phone operating system (i.e. held in software) to also communicate directly with the NFC controller/antenna. This allows app providers to load payment apps directly into the handset via an app store and, as the SIM SE is not being used, without needing to involve the mobile operator.

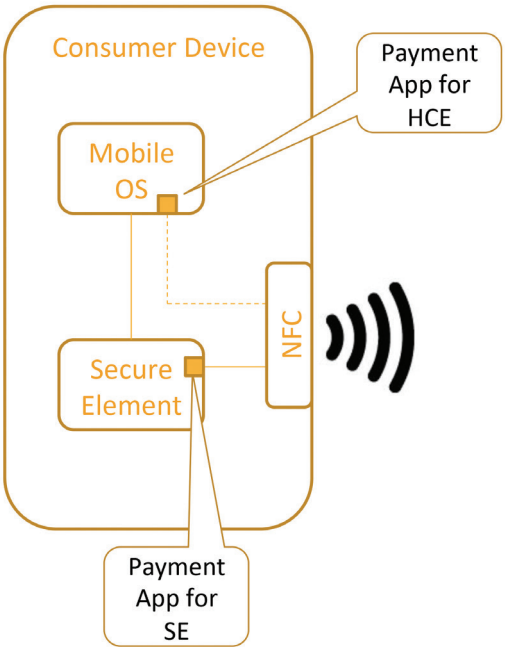


Figure 2,
SE and HCE in the Handset

The mobile handset is only one element of an end-to-end mobile payments system. Each approach, SIM SE or HCE, requires a supporting ecosystem for provisioning, management and usage. In the following sections we outline the ecosystems for the SIM SE and HCE and evaluate their strengths and weaknesses.

1. EMV migration is ongoing in the US
2. Not including non-standard Android OS versions such as CyanogenMod

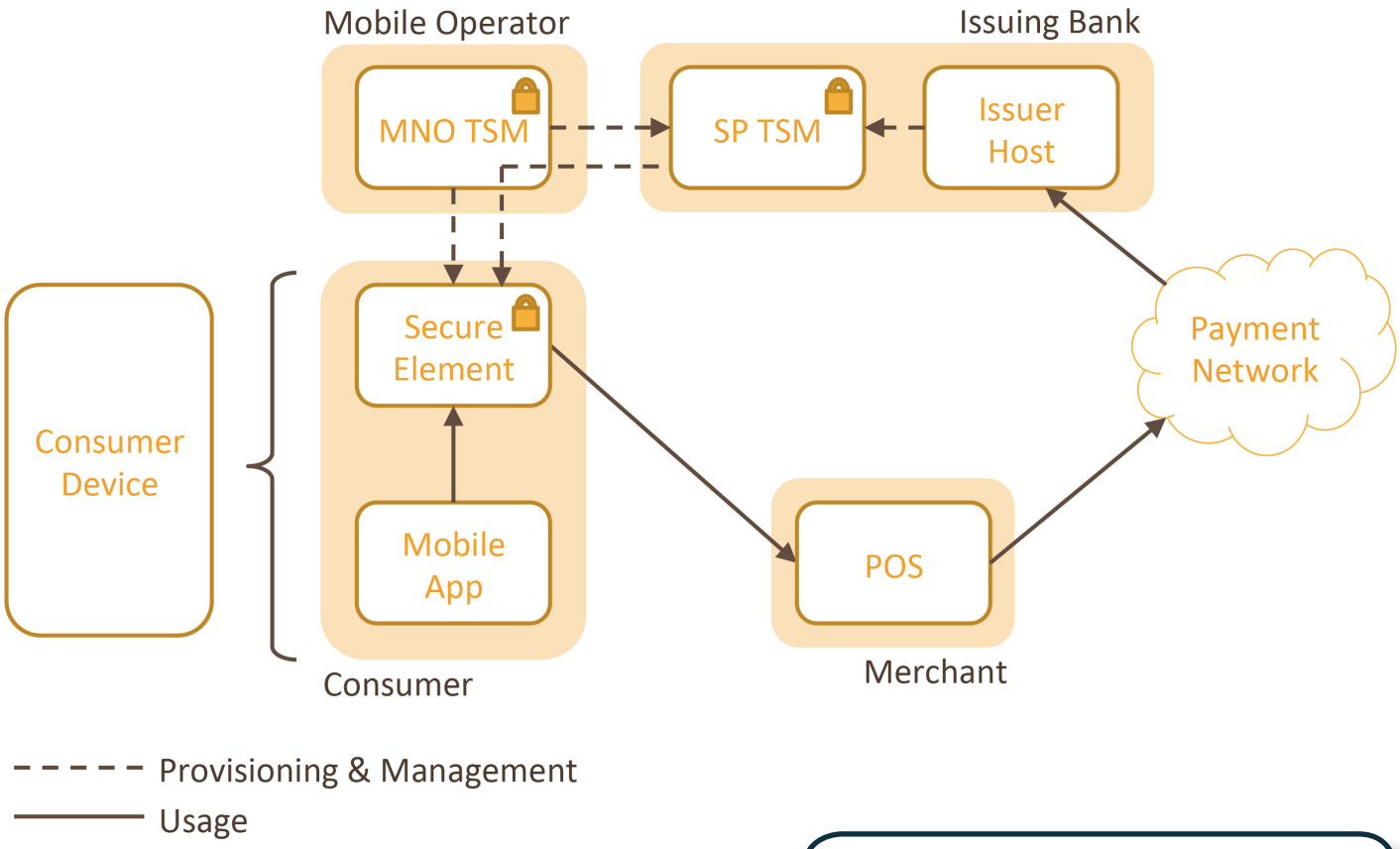


Figure 3, The SIM SE NFC Ecosystem

Figure 3 illustrates the ecosystem that has developed to support SIM SE element based NFC payments, as follows:

The consumer has a mobile handset that contains the hardware SE (e.g. a SIM provided by the mobile operator). The payment app, including the sensitive payment credentials, resides inside the SE. This payment app performs the contactless EMV payment transaction with the POS across the NFC interface. To the POS the payment app looks like a contactless payment card.

A mobile app will also reside on the handset (outside of the SE) which provides the UI (User Interface) to the consumer allowing him or her to interact with the payment app to, for example, check balances or enter a passcode.

The payment app is owned by the issuing bank. It needs to be securely provisioned into the SE before any transactions can take place (indicated by the padlocks and dotted arrows in Figure 3). This requires collaboration with the owner of the SE (i.e. the mobile operator in the case of a SIM SE) who will, via their TSM (Trusted Services Manager), grant the issuer access to the SE. Once provisioned, the issuer will use their own SP TSM (Service Provider TSM) to manage the payment credentials within their payment app.

Hub TSMs

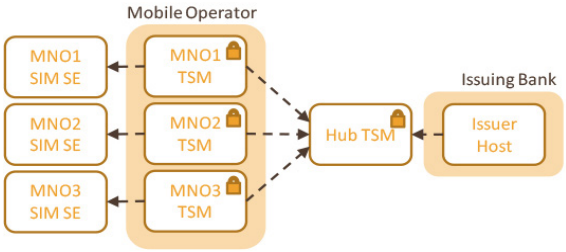


Figure 4, Hub TSM

An issuing bank will usually want to be able to provision payment apps onto SIMs from all mobile operators in the market. In the past this meant integrating with multiple MNO TSMs which is complex commercially and technically. In several markets (e.g. Canada, China, Germany, Italy, Norway, Poland and Spain) Hub TSMs are being established, that will provide issuing banks with access to SIMs from multiple MNOs through a single TSM integration. This, together with the GlobalPlatform and GSMA initiatives to simplify the end-to-end process, should lead to less complex and more interoperable solutions going forwards.

The HCE NFC ecosystem

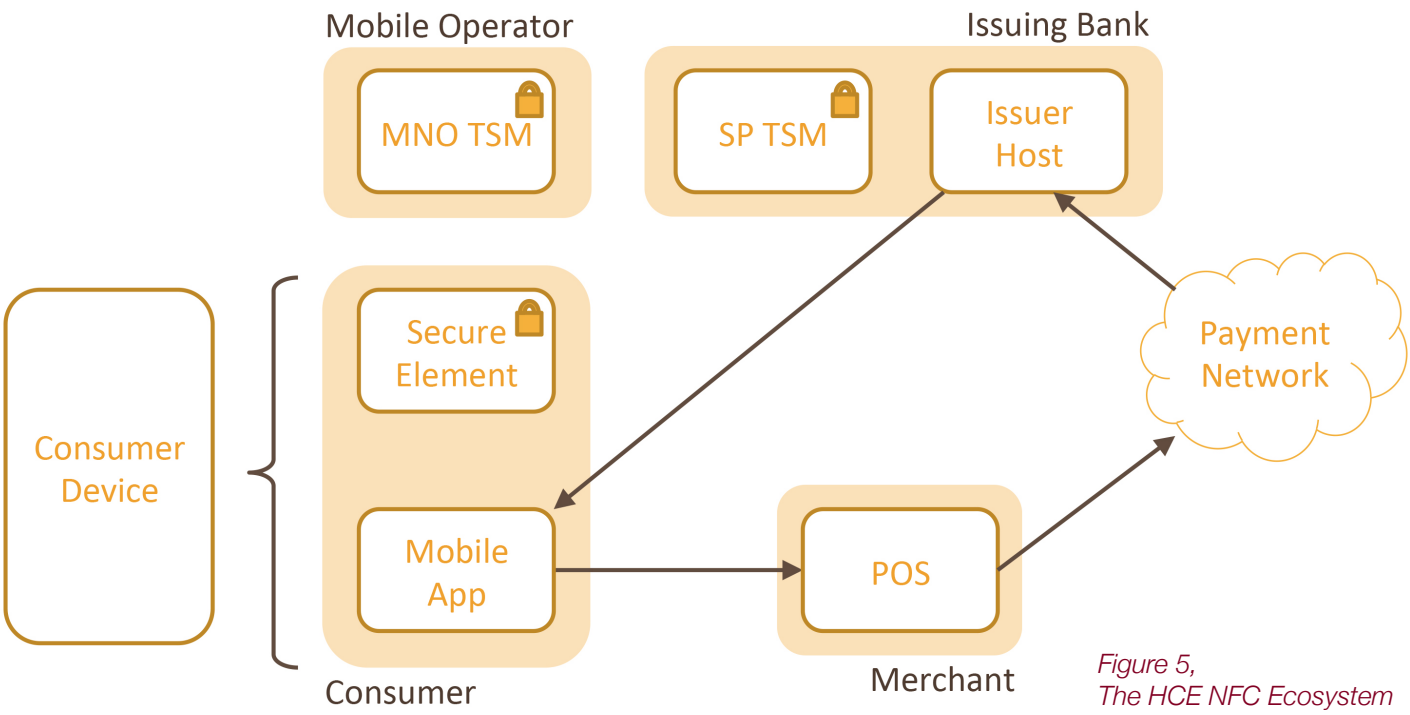


Figure 5, The HCE NFC Ecosystem

Figure 5 illustrates the ecosystem that has developed to support HCE-based NFC payments. There are a number of key differences compared with conventional SE-based NFC payments, as follows:

An SE is not used. Instead the EMV payment transaction is performed from an application residing in the mobile phone's operating system. To the POS, this mobile app now looks like the payment card.

The mobile app can be downloaded from an app store, in the same way as any other app, directly onto the handset. There is no need to involve the mobile operator or other third party. Whilst this makes provisioning of the mobile payment product very simple it comes at a cost – security and usability.

The mobile app (and the operating system on which it depends) does not offer the same levels of security as a hardware secure element and therefore alternative approaches to security are required. Typically, these will involve provisioning single use or limited use payment credentials to the mobile device, to minimise the impact of compromise. No long term storage of sensitive data, such as PANs, PINs and keys, is appropriate within the mobile handset OS.

The need to provision limited use payment credentials frequently may also introduce usability issues. For example, if the mobile phone does not have network connectivity it will not be able to receive new payments tokens.

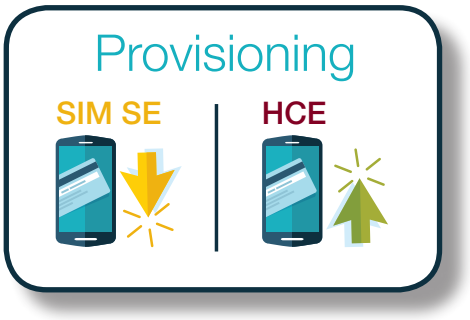
The two approaches presented above are now considered in more detail.

Tokenisation

Figure 6, Tokenisation

Tokenisation is the process of substituting the card PAN with a single use or limited use "tokenised PAN". This reduces the impact of data breaches significantly. If a "token" is compromised 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 tokens 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 tokens back into a PAN to allow the issuer to process the transaction in the normal way.

Comparing SIM SE NFC and HCE NFC



Provisioning

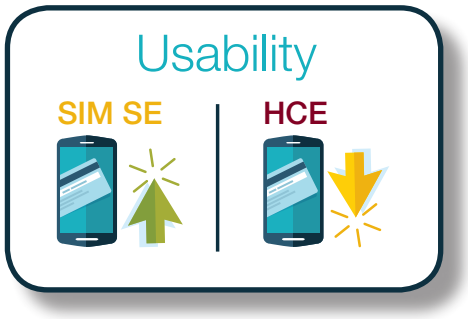
In order to be able to provision SIM-based SE NFC payment apps, two key things need to happen:

- The consumer needs to have an NFC-enabled SIM. If a new SIM is required this will add cost and friction to the provisioning process. In China, for example, this obstacle is being removed by linking the rollout of NFC-enabled SIMs to the switch to 4G, which also requires SIM replacement.[1]
- The SIM owner (the mobile operator) needs to grant access to the issuing bank so that the bank can provision and personalise the payment app on the SIM. This will require to the bank to integrate with mobile operator TSM. There are, however, a number of markets where hub TSM services will help to reduce this complexity.

Provisioning an HCE NFC payment app on the other hand is more straightforward, requiring no cooperation with the mobile operator and no integration with an external TSM. As a result, the issuing bank then bears the entire responsibility for delivering the provisioning and management of the payment app to all supported handsets and OS versions. Furthermore, HCE provisioning is likely to be a frequent activity, with payment credentials being provisioned ahead of every few transactions. As noted above, this will require integration with new services such as TSPs.

Whilst there are significant questions concerning HCE provisioning, the issuing bank will be able to address these concerns unilaterally. Therefore, on balance, we believe that HCE may be more attractive to banks than SIM SE provisioning. As the number of standardised and hub services increase, this may change especially if the pricing reflects the commodity nature of the service.

Usability



The consumer experience is a very important factor in payments. Increased convenience is arguably the primary benefit of contactless payments to consumers. Mobile payments have the potential to go further than just payment, providing news ways to engage with the consumer, through the mobile phone. Convenience remains, however, fundamentally important.

For a mobile payment product to be convenient it must be easy to set up, simple to use and work everywhere.

The friction associated with setting up a mobile payment product is already touched on above. From a consumer perspective, HCE has the edge as there will never be the need to obtain a new SIM, although an Android OS upgrade may be necessary. Apart from this there should be little difference to the consumer when setting up a product, although clearly this depends on the specific implementation of the payment product.

The key usability differences arise in usage and coverage.

SIM SE NFC payments products build on card payment technology which is designed to work anywhere a contactless card will work. This includes at online and offline POS terminals, and should work regardless of whether the mobile handset is powered up or not. In some cases SIM SE NFC payments are better than contactless cards. For example, offline PIN verification, where the PIN is verified in the card, is cumbersome using contactless cards, requiring a second interaction with the card after the initial tap. With SE NFC the PIN (or "passcode") can be entered directly into mobile UI prior to the transaction.

There are a number of potential usage differences with HCE NFC to be considered:

- Limited use payments credentials, such as single use keys, will be delivered to the mobile phone ahead of the transaction occurring. It will not be possible to dynamically retrieve credentials from the issuing bank during a transaction, even if the phone is online, due to the network latency. If new credentials have not been successfully delivered to the mobile phone, transactions will not be possible.
- Offline cardholder verification may need to be implemented in new ways due to there being no secure storage on the device. This should not impact markets already using online PIN.

1. http://www.gw.com.cn/news/news/2014/0314/200000324078.shtml

- HCE requires the phone to be turned on and the relevant payment app running in the mobile phone OS. In high throughput environments, such as mass transit payment at gate, this may be a particular issue.

SIM SE NFC is likely to be better than HCE NFC from a usability perspective for mobile contactless payments. The usability issues with HCE can be mitigated, however as it stands HCE may not provide a totally seamless user experience.

Security

Security is clearly a significant concern with HCE; the primary security component in SIM SE NFC (i.e. the SE) is removed and so new measures to protect payment credentials are required.

The phrase "SE in the cloud" is used a lot in connection with HCE NFC payments. Here the idea is that the valuable account-level payment credentials (such as secret cryptographic keys), that were previously held in the SE, are moved into a secure data centre (in the "cloud") which is accessible to the mobile app. Single use credentials ("session" keys for example) are then delivered to the mobile app to enable it to perform a single transaction. The risks to these single use credentials should be much lower than the risk to those at the account-level. The actual risk will depend on the specific implementation.

PAN data is also at risk in HCE payments, especially if the issuer allows the same PAN value to be used across HCE NFC and other channels. Tokenisation, where PANs are replaced with temporary surrogate values, addresses this concern. An industry wide tokenisation initiative is underway (outlined above) which issuers are likely to integrate into their HCE solutions.

A key issue with putting the SE "in the cloud" is one of authentication. How does the issuing bank know that the "SE in the cloud" is being accessed by a legitimate device and user. Without the use of the SE, the issuing bank is likely to need to employ a range of measures (such as device fingerprinting and risk based authentication) to maximise their chances of detecting unauthorised access. Mobile security capabilities will be required as well to detect devices that have been rooted or compromised in some other way. These capabilities will need to support a range of devices and changing OS versions.

Payments have always been about managing risk down to an acceptable level. We believe that through appropriate risk management that issuing banks will be able to achieve good enough security for low value transactions using HCE. However, the security will not, at least in the short term, achieve the recognised levels of SIM SE-based security and may require new risk management systems.

Business Model

The costs associated with SIM SE NFC have been a source of contention between mobile operators and banks. Issuing banks wishing to provision and manage payment apps have been faced with various charges including renting space on the SIM, setup charges for TSM services and usage charges for each management operation performed by the TSM during the lifecycle of the payment product. This issue is recognised by the mobile industry. The GSMA is leading an effort to significantly reduce these costs to issuing banks[1]. The ongoing efforts to simplify the end-to-end processes and the emergence of hub TSMs will all help in achieving this goal.

Against this HCE may appear to offer a "no fee" model for NFC payments. The issuing bank clearly has to invest in server side platforms to manage its "SE in the Cloud" services. If these are fully owned by the bank, the bank may be able to avoid paying ongoing fees to external vendors. The problem is that the size of the upfront investment and ongoing operational costs of in-house solutions are difficult to gauge, and the specialist skills required to deliver HCE services may necessitate engaging external vendors. Where external vendors are used we would expect charges to be per user or per transaction to reflect the increased frequency with which provisioning processes are performed (e.g. provisioning a single use payment credential for every transaction). In addition, the solutions that are currently being developed by vendors are proprietary and could lead to supplier lock-in or multiple integrations where a bank wishes to dual source.

If an issuing bank chooses to leverage the industry tokenisation services, these will have an impact. However banks may well need to build support for tokenisation anyway, irrespective of HCE.

1. http://www.gsma.com/digitalcommerce/simplification

Branding and control has also been an area of concern for SIM SE implementations. We believe banks will wish to locate payment services within their wider mobile banking services, where their brand is visible to the consumer. This is in contrast to the model where the payment instrument is held in an MNO wallet but not that visible to the consumer. Technically, there is no difference between SIM SE and HCE on this point, both can support either approach. We believe that MNOs are now much more open to bank-branded apps directly accessing the SIM SE. With HCE the bank clearly has the freedom to take whichever ever approach they wish.

There are many factors affecting the commercial aspects of the NFC payments services. The attraction of fewer commercial relationships, simpler fee structures and the greater control promised by HCE will be appealing to banks. However, as the costs of delivering and supporting HCE are not clearly defined at the current time, we cannot say whether SIM SE or HCE has a more attractive business model.

Maturity

SIM SE NFC is more mature than HCE NFC. All of the international card schemes and several national schemes, such as China UnionPay, have stable specifications and established certification processes. These build directly on their contact and contactless card specifications, and have been informed by the various trials and pilots performed over the past seven years.

In contrast, HCE NFC is the subject of much ongoing work to establish best practices, determined optimum transaction models and to understand implications for certification. Visa has recently released initial specification and guidelines concerning HCE[1]. MasterCard has announced similar plans. These will inevitably go through refinement as trials and pilots continue. For now trials and pilots will require waivers from the card schemes.

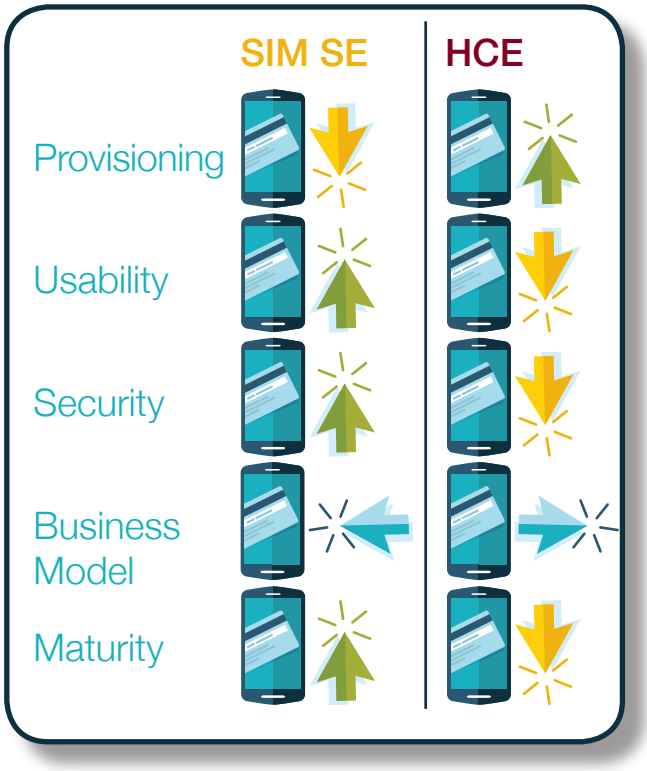
Summary

Comparing all aspects there are good reasons for focusing on SIM SE NFC payments and good reasons for focusing on HCE NFC payments.

The SIM SE approach may provide the fastest route to market in more mature markets, whereas HCE may be faster in others. The SIM SE approach is likely to provide a more robust, secure and usable solution, although it may also be possible to build an HCE solution that works acceptably well.

As has been the case to date, commercial viability is likely to be a significant factor in the choice of SIM SE or HCE. The bank will need to choose between known costs with the lower delivery risk of SIM SE and the promise of lower costs, but with the chance of unexpected delivery costs and increased delivery risk of HCE.

In reality, the choice of SIM SE and HCE is not mutually exclusive. As suggested below every bank should develop services that build on competencies that are common to both approaches, providing flexibility going forwards.



1. http://investor.visa.com/news/news-details/2014/Visa-to-Enable-Secure-Cloud-Based-Mobile-Payments/default.aspx

What does this mean to banks?

NFC remains the most widely support contactless interface for mobile payments at POS and should therefore be an important part of any bank's payments strategy.

Consult Hyperion suggests that there are a number of key points for banks to consider as they plan mobile NFC payments:

- **Understand the local environment:** The local conditions will play a big role in determining the best approach. In mature markets, especially where contactless acceptance is sufficiently wide and aggregated TSM services are available the SIM SE is likely to be quicker and cheaper to deliver than HCE. In other markets, this may not yet be the case but this will change as plans to simplify the SIM SE take effect.
- **Understand your target transactions:** It is possible that HCE will be less suited to certain transaction types (e.g. offline, high value) than SIM SE. Understanding which transactions are driving contactless acceptance in your market (e.g. transit) will be critical to ensuring that you build services that are relevant.
- **SIM SE and HCE are not mutually exclusive:** For simplicity this paper has contrasted conventional NFC payments using the SIM SE with HCE payments not using an SE. In reality the two approaches may not be this polarised. The most effective solutions over the medium term may be hybrid models where, for example, the SIM is used to address the security and authentication gaps in HCE. This will be especially attractive if it can be achieved without needing to issue new SIMs.
- **Build flexibility into your strategy:** There is likely to be considerable overlap between SIM SE and HCE in terms of the systems and capabilities that are required. Banks should ensure that whichever direction is taken services are designed with flexibility in mind.
- **Collaborate with the industry:** Until there is a level of standardisation around HCE, there remains the risk that banks could adopt solutions that are insufficiently flexible or lock the banks in. Collaboration is needed with the card schemes and other players, such as mobile operators, who can help address some of the issues to develop standards and define the complete NFC ecosystem.

Despite all the interest around HCE, the SIM SE approach for mobile payments still has many advantages. Both approaches have their merits and the right approach will be dependent on the needs of banks in each of their operating markets.

"Thought leaders in digital money and digital identity"

About Consult Hyperion

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.

consult hyperion
securing tomorrow's transactions

First published June 2014
Consult Hyperion
Tweed House
12 The Mount
Guildford
GU2 4HN
United Kingdom
www.chyp.com

This report was commissioned by the GSMA, 5 New Street Square, London, EC4A 3BF, United Kingdom. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of the GSMA or its members.