mobey forum

The Host Card Emulation in Payments: Options for Financial Institutions

HCE Workgroup

www.mobeyforum.org

HCE Workgroup

Chair

Zaf Kazmi	CaixaBank

Vice Chair

Kristian T. Sørensen	Nets

Editor

Zilvinas Bareisis	Celent

Contributors

Sverker Akselsson	Nordea
Bent Bentsen	DNB
Jonathan Bye	Royal Bank of Scotland
Pablo Chepalich	BellID
Yuri Grin	Intervale
Jordi Guaus	CaixaBank
Douglas Kinloch	INSIDE Secure (Metaforic)
Bastien Latgé	INSIDE Secure
Tom Pawelkiewicz	ScotiaBank
European Payments Council	Mobile Channel Workgroup Members
Douglas R. Peters	HSBC
Philippe Roy	Nordea
Ville Sointu	Ericsson
Rajasekaran Soruban	Mahindra Comviva
Julien Traisnel	Oberthur Technologies The M Company
Tapio Vailahti	Giesecke & Devrient

Supporting and adjacent documents

Mobile Wallet Part 2: Control Points in Mobile Wallets
Mobile Wallet Part 3: The Hidden Controls

Visit Mobey Forum Knowledge Centre at www.mobeyforum.org

Table of Contents

1. Executive Summary

Near Field Communication (NFC) technology has been around for quite some time now. Yet after numerous great promises, NFC payments haven't really managed to take off in most parts of the world. At the end of last year, Google announced it would make Host Card Emulation (HCE) technology available in its Android operating system. Given the payment schemes' (Visa, MasterCard and American Express) endorsement of the approach, HCE might become a game changer for the mobile payments ecosystem.

The objective of this paper is to provide guidance to the financial institutions considering their options for implementing NFC payments. The paper aims to highlight the implications of HCE technology along with its pros and cons compared to a physical Secure Element (SE) based mobile payment solution, as seen from the financial institution's point of view. Not surprisingly, security considerations take a central stage in this discussion.

The paper describes two main HCE solution alternatives – card emulated by the cloud system and card emulated by the phone application. The paper analyses the roles of different stakeholders within this new ecosystem and contrasts it with the traditional physical SE-based implementation. While a Mobile Network Operator (MNO) or a handset provider are no longer involved as an SEI (Secure Element Issuer) and there is no need for a Trusted Services Manager (TSM), there are possibly two new entities – the HCE Payment Solution Provider and the Token Service Provider (TSP) – with a serious stake within this new ecosystem.

The paper also summarises the results of an HCE survey conducted in September 2014 by Mobey Forum. The survey provides valuable insights into the banks' attitudes to seeking external help for HCE solutions and into criteria the banks consider as most important when selecting an HCE solution provider.

Finally, the paper analyses the HCE approach by applying the control point model created and published by Mobey Forum in its Mobile Wallet White Paper Series.

The conclusions of our analysis are:

- Broad adoption of HCE would imply significant changes in the mobile payments landscape. It gives different entities, including financial institutions, more freedom to decide to what extent they want to work with other players of the value chain. Therefore, we view HCE as an important driver behind the NFC-based mobile payments adoption as well as other services such as vouchers, couponing, ID management, and others.
- However, HCE is not an easy fix to NFC mobile payments challenges – while the issuing might become simpler, there are other areas to consider, such as new roles and new business models.
- Some financial institutions will clearly be attracted by HCE, while others may continue with physical SE-based solutions or even consider deploying both.
- HCE represents a fundamental security paradigm shift. In the traditional physical SE-based NFC world, we need a physical space on device to secure our data. In HCE, the starting assumption is that the phone is NOT secure, and we use tokenization and other techniques to mitigate risk.

- Overall, HCE provides more options for financial institutions and is perceived more of an opportunity than a threat or complication.
- Understanding the market dynamics and the control points will be essential to success.

2. Introducing Host Card Emulation

2.1. HCE: Another Option to Implement NFC Payments

The first thing to know about Host Card Emulation (HCE) is that it represents an alternative to the "traditional" NFC payments. It still relies on the NFC technology for proximity payments, and the mobile device always has to be NFC-enabled.

In the **traditional NFC** payments implementation, payments application and the actual card credentials reside on a physical Secure Element (SE), usually a SIM card or a dedicated chip embedded inside the phone – see Figure 1. Many mobile network operators (MNOs) around the world have launched or have piloted physical SE-based NFC payments, often in partnership with banks. Examples include Deutsche Telekom's MyWallet service in Germany, Softcard (formerly known as Isis) in the US, various initiatives by Orange in France, Poland and the UK, and many other operators around the world. Also, La Caixa in Spain launched NFC payments in partnership with Telefónica, Vodafone, Orange, and Visa Europe, while Telenor and DNB partnered in Norway for the rollout of Valyou mobile wallet.

By contrast, in **HCE**, the payments application resides on the phone's operating system (OS), the "host," and interacts with the cloud system and the NFC controller directly – see Figure 1. There is no need for a card issuer to use SIM or other secure element for making contactless NFC mobile payments. Examples of HCE implementations and pilots include initiatives at a number of Spanish banks, such as Bankinter, BBVA, and Banco Sabadell, and Sberbank in Russia, the biggest bank so far to announce its decision to test HCE technology.

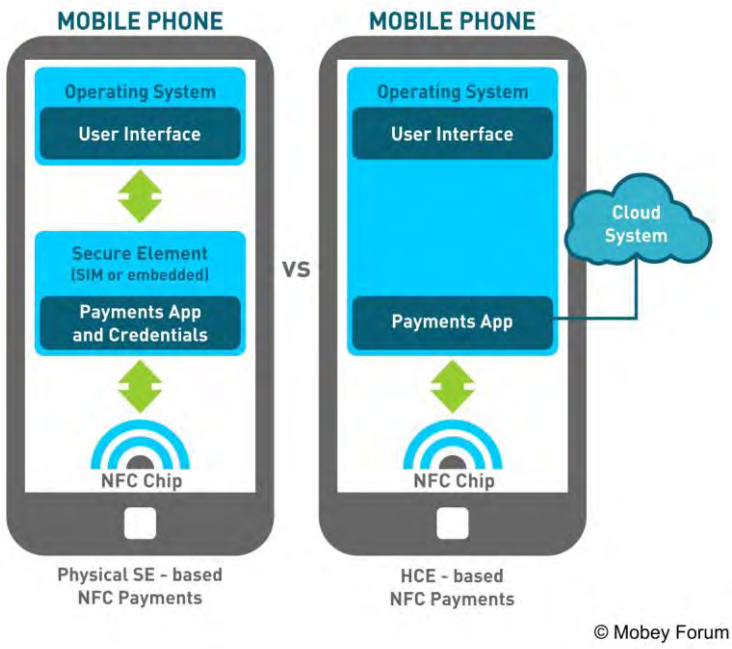

Figure 1: Differences between Physical SE Card Emulation and Host Card Emulation-Based Implementations on a Mobile Device

HCE is currently available only on Android 4.4 KitKat and Blackberry OS 10 operating systems. By contrast, traditional NFC payments are supported by most operating systems, such as Android, Blackberry and Windows. Apple has been refusing to support NFC for a long time, but it recently announced Apple Pay, which will also utilise NFC technology. While the reported details are scarce, it appears to be a unique implementation of physical SE-based NFC payments.

Finally, it is possible to have **hybrid** solutions which make use of a physical SE (SIM) as well as cloud-based services. Royal Bank of Canada launched such a solution, provided by Bell ID[1], in February 2014; as reported by NFC Times[2], "RBC Secure Cloud puts the full payment applets on the bank's servers, while loading only one small applet, along with tokens, on the SIM."

2.2. HCE: A Brief History

It has been a long and winding road for NFC. It has become a running joke in the industry to predict NFC's take-off "next year." Despite the hard work done by various stakeholders in the industry, there seemed to be no easy solution for the equation needed for successful take-off. Of the original three alternatives of physical secure elements (SIM Card, SD card or embedded SE), the SIM card rapidly became the main feasible option in most developed markets for implementing NFC mobile payments.[3]

[1] Bell ID has a patent pending
[2] http://nfctimes.com/news/canada-s-largest-bank-combines-cloud-sim-new-model-nfc-ecosystem
[3] Australia as one of the exceptions

While NFC was struggling, software-based payment solutions started to emerge allowing consumers to download the wallet and register their card details "in the cloud." In March 2012, MasterCard said they would consider introducing a fee for digital wallets such as PayPal, and Visa Inc. soon followed[4].

In the meantime, NFC Forum decided in 2009 to standardise the Host-NFC chip interface so that device manufacturers could switch suppliers more easily. Before that, those interfaces were proprietary by each manufacturer and therefore different. A "side effect" of such a common interface was that it made it much easier to implement HCE.

NFC Forum chose at that time to create its own protocol, NFC Controller Interface (NCI), rather than rely on the Host Controller Interface (HCI) as used in a Single Wire Protocol (SWP) by the European Telecommunications Standards Institute (ETSI). NCI defines a standard interface within an NFC device between an NFC controller and the device's main application processor. From the very beginning, interworking between ETSI HCI and NCI was a priority, and interworking with other secure elements (embedded SE, SD, SIM, etc.) was always a consideration. But those other elements were "out of scope" of the actual NFC Forum work.

However, Blackberry enabled its operating systems to support open protocol from the very beginning. Plenty of developers had also begged Google to support the software-based API to secure element in the Android OS (instead of SWP), but Google did not take this into consideration. This is where small start-up SimplyTapp stepped in and forced its way by opening the API (the developers often speak of "rooting" or "jail-braking" the device, possibly against Android license).

SimplyTapp and Bankinter[5] became the very early pioneers in software secure element. SimplyTapp had the first trials in August 2012; Mobey Forum's member meeting in 2013 in San Francisco[6] was the first public event where Bankinter introduced its solution, which immediately raised a lot of interest among the banks attending.

In November 2013, Google released HCE architecture in Android 4.4 KitKat, allowing any organisation to gain access to NFC technology at a relatively low cost. With HCE, any application on an Android 4.4 device can emulate an NFC smart card and support payments, loyalty programs, card access and transit passes except Mifare and Calypso[7].

Finally, during Mobile World Congress (MWC) 2014, Visa and MasterCard also decided to support the software secured wallets themselves. The payment schemes asked EMVCo to draw up the specifications for tokenisation, a new direction which enabled the schemes to strengthen their role in the payments value chain.

[4] Mobile Payments World http://www.mobilepaymentsworld.com/visa-ceo-calls-digital-wallet-fee-on-paypal-appropriate/
[5] NFC World http://www.nfcworld.com/2013/02/27/322783/bankinter-develops-nfc-payments-service-that-eliminates-need-for-secure-elements/
[6] Mobey Forum's member meeting in SF, April 2013, hosted by SAP
[7] HCE is currently technically not feasible for following contactless technologies: MIFARE® Classic, MIFARE® DESFire (in native mode), Calypso.

3. Security Considerations

3.1. Review of Risks

A physical secure element has one big advantage on its side: as a separate smart card, it is a dedicated secure hardware with dedicated access rules and certification, and hence is the most secure way to execute mobile payments. It eliminates any application code running in the device's operating system (OS) which might interfere with the NFC-based mobile payment message exchange. No device malware and no viruses can embed themselves in-between and spy on data flowing along this chain. The solution is tamper-resistant and can also work even without battery for specific uses cases, such as, for example, transit and access control.

HCE-enabled mobile payment applications run on the mobile device's central processing unit ("Host CPU"). If present in the same phone, malware, spyware, and viruses also run on the same CPU. Theoretically, "intruder" applications can spy on the traffic between the NFC Controller and the HCE-enabled mobile payment application, although, of course, the real PAN is not transmitted. Rooted[8] mobile devices are especially vulnerable here. Even in non-rooted phones, the only protection the OS provides to the HCE-enabled application is the native OS "sandbox," which is not as secure as hardware SE.

Basically, the HCE enabled mobile payment application has to have everything the real card needs for the execution of the standard contactless transaction with the POS. Yet, that application can be simply downloaded from the app store. While it is much easier to provision the credentials, the application is the most critical point of the solution from a security perspective.

There are two critical elements in securing the HCE app, which is sometimes called Software Secure Element:

1. Protection of the application itself (application integrity).
2. Protection of critical data and cryptographic functions.

3.2. Application Integrity

Integrity of the application and its function is achieved by tamper-proofing the app code. Tamper-proofing is achieved by a series of techniques making an app resistant to analysis, change, or manipulation by a hacker. Such techniques have to be "stand alone" and not reliant on security functions within the operating system of the device. Indeed, the safest assumption when planning protection is that the device will be compromised; in that case, the app has to defend itself by retaining its integrity.

At the heart of this is a runtime integrity network embedded throughout the app code, which detects and responds to any attempts to analyse, reverse-engineer, or otherwise manipulate code or

[8] Rooting is often performed with the goal of overcoming limitations that carriers and hardware manufacturers put on some devices, resulting in the ability to alter or replace system applications and settings, run specialised apps that require administrator-level permissions, or perform other operations that are otherwise inaccessible to a normal user.

memory. Attackers trying to compromise the app will find their room for manoeuvre highly restricted to the point that they cannot do any malicious work.

3.3. Protection of Critical Data and Cryptographic Functions

Critical data and cryptography are protected by creating an obfuscated, cryptographic boundary within the app itself which can transact and process data in memory without revealing any of the data or any secrets used to process that data. It subsequently outputs the data in a form that can be used securely by other processes, locally or remotely.

Like traditional SE hardware, a software secure element also has to be tamper-resistant, and its logic has to be impenetrable, in order to protect the complete application. Unlike hardware, this software secure element is present at the application layer, ideally within the application and unique to that application. This same technique also binds the cryptographic functions to the app, rendering them indivisible from the whole app.

These techniques allow the paradigm of HCE to work securely so that any app can continue to use HCE to make payment. This broad applicability and the software's inherent flexibility can help drive adoption.

It is worth clarifying the differences between standard, Black Box cryptography and White Box cryptography to help understand why White Box cryptography is a useful technology for data processing on hostile devices, such as smartphones. Black Box cryptography is what most people recognise as cryptography. On mobile devices this requires the private key to be embedded so that data can be processed. The key is kept secret when the walled garden security is in place, which, of course, is completely unrealistic in the face of jail-breaking, rooting and exploits of the device OS and security "sandbox."

White Box cryptography is an expanded, arithmetically derived implementation of standard cryptography, where the private keys and encryption algorithms are dissolved into the binary such that they cannot be recovered. This allows processes that rely on cryptography to be kept secure, even in hostile, exploited, and jail-broken environments.

Mobile payment technology solution providers may also decide to store main payment credentials (including all sensitive payment-related cryptographic keys and card data like PAN, Expiry Date, etc.) in the secure cloud / server-based Hardware Secure Module (HSM). They might provision the HCE-enabled mobile payment app on-demand (for example just in advance of the payment transaction) with "temporary" PAN, "temporary" Expiry Date, "temporary" "session based" cryptographic keys, etc. This provisioning would have to happen via OTI (over the Internet), using secure channel established between secure cloud and Mobile Payment Application (using SSL for example, or similar technique).

If the payment credentials are made temporary and short-lived, then even if there is malware and spyware embedded along the contactless transaction payment chain, those "intruder" programs would obtain the information, which would become useless either immediately or very soon after the transaction has been completed. Please note that "temporary" here can be fine-tuned depending on the risk tolerance.

One another key aspect to note here is, such dissolved private keys and encryption algorithms can be dynamically updated by the application itself, per user application wise, without requiring the users to periodically upgrade the application by themselves or without needing to rely on automatic app store upgrade notifications, because if a user wallet application or handset environment is compromised the issuer should be able to selectively upgrade the compromised app without needing to do a mass upgrade of millions of wallet applications. This in addition to ensuring the protection is individualized and unique per user mobile application, also helps to keep such protection mechanism independent of the mobile wallet application release process.

3.4. Device Identity

It is critical for the app to "know" on which device it is being used. Once enrolled and activated, it should only run on that particular device. The potential for cloning payment apps and creating a simple card-skimming system has been a concern for all since HCE was first considered.

Traditionally, in the context of a device or application, proof of "identity" is based on:

1. A secret, proving the uniqueness of the user;
2. An algorithmically derived device state, proving the uniqueness of the device and the use.

Examples of the secret would include a PIN code, a user password, and, increasingly, biometrics such as fingerprint scans. A complex and arithmetically derived ID of the device's state upon enrolment and through time is one of the most advanced techniques today; these ID solutions are growing in use across many mobile markets.

The intention of such IDs is to ensure that they cannot be understood in order to replicate the device state to allow cloning. As a further defence, they render it very difficult to mimic a user, again to prevent cloning. These techniques then are placed within the protected application, and thus are further defended by the software secure element, something that is actually difficult to replicate in traditional Secure Elements.

3.5. Tokenisation

Tokenisation in the context of digital payments is a method that replaces the Primary Account Number (PAN) by a token(s), which is a disguised representation of the original PAN value. If the token is compromised, it has limited or no value. Tokens can be protected for example by limiting the number of transactions or time for which the token is valid.

This new card number value is used in a payment transaction without much impact on the actual value chain. Of course, the issuer has to reconcile the original related PAN and the token in the transaction authorisation flow.

EMVCo has issued a tokenisation framework to describe the requirements for creation and use of payment tokens in the context of digital transactions (mobile or digital wallet). The framework introduces a third party entity, Token Service Provider, which can generate and resolve tokens on the issuer's behalf. However, this does not prevent the issuers from doing it in-house, as the issuer

and validator of the token can be the same institution. Although the concept is intended mainly for m-/e-commerce transactions, it can also be used for card present environments including any bearer channel such as QR codes or NFC/HCE.

There are two different types of tokens – **alternate and dynamic**. Alternate tokens are a static representation of a real PAN and can only be used for Card Present (CP) transactions. To ensure the security levels required by the payment schemes, variable keys are used in each transaction, and the tokens may have limits on the number of transactions or time to live. This model is used in other sectors such as transport.

The **dynamic** tokens are alternative PANs valid for a single transaction and limited time only. They are used for Card Not Present (CNP) transactions.

Given that tokens have to be provisioned ahead of the transaction, the user experience might be negatively impacted if the device runs out of tokens before it can connect online again. Appropriate authentication of the user by the token server is crucial to ensure that the tokens are loaded to a device of the legitimate user.

3.6. Paradigm Shift

HCE represents a fundamental security paradigm shift. In the traditional physical SE-based NFC world, we need a physical space on device to secure our data. In HCE, the starting assumption is that the phone is NOT secure, and we use tokenization and other techniques to mitigate risk.

Overall, HCE provides more options for financial institutions and is perceived more of an opportunity than a threat or complication.

4. HCE Solution Alternatives

Host Card Emulation has two solution options when it comes to payments or other services that require a high level of security: **card emulated by the cloud system** and **card emulated by the phone application**. This section describes and compares these solutions.

4.1. Card Emulated by the Cloud System (Full Cloud Solution)

In a full cloud HCE solution, card emulation is done in the cloud with both the transaction flow logic and the actual payment credentials residing on a remote server. The application on the phone authenticates the user, provides user interface, and manages the secure connection to the cloud and the pass-through of data to the NFC controller – see Figure 2.

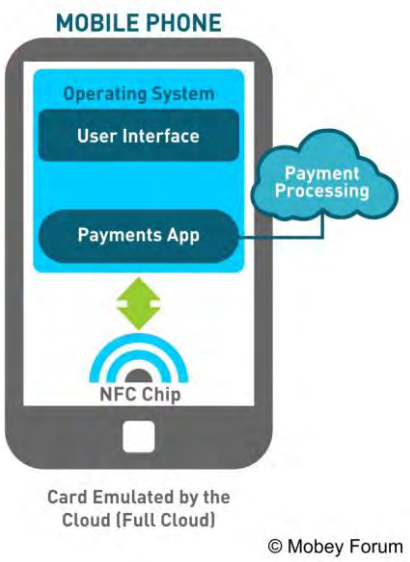

Figure 2: Full Cloud Based HCE Solution

In a full cloud-based solution *each transaction* needs to connect to the remote server in order to obtain the payment credentials – see Figure 3 on page 13. The server has access to card data with keys and creates the cryptogram, and then transfers that data to the mobile phone. The payment is then done in the same manner as in the solution with physical SE – the phone transfers payment data to POS via NFC, and the POS sends it on to the processor, which sends it to the issuer for authorisation. There is no need to modify anything regarding acceptance infrastructure. Because payment credentials are stored in the cloud, the solution is also suitable for e-/ m-commerce payments.

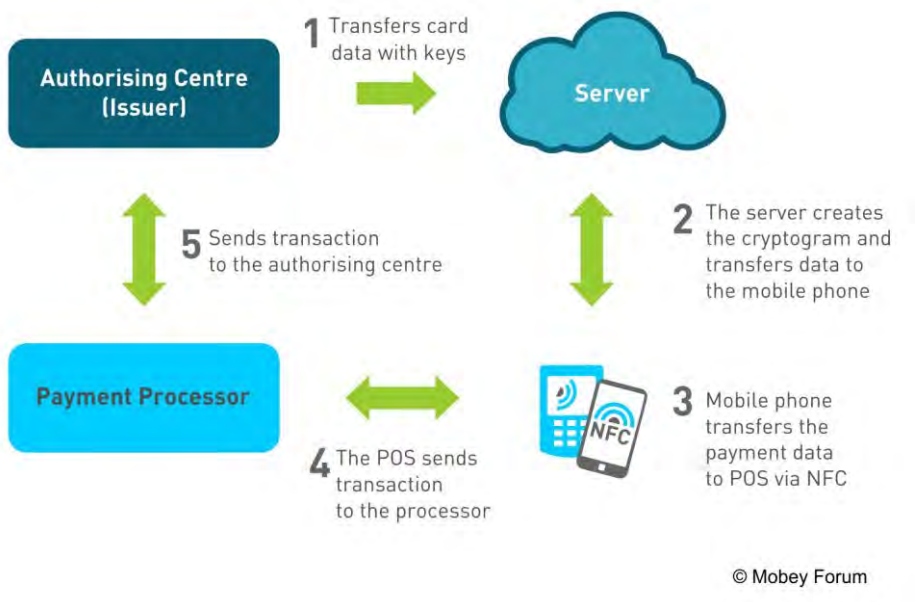

Figure 3: Transaction Flow in a Full Cloud Based HCE Solution

A key challenge for a full cloud-based HCE implementation is that for each transaction the client is connected to a server to download the payment credentials. While that enhances security, it requires a phone with data connectivity, and the response time can be slow depending on the network. The solution usually works reasonably well in countries with very high speed 4G or even 5G networks, but in other countries it is not fast enough for a satisfactory user experience. The transaction speed is usually slower than 500 milliseconds (including POI processing) required for many environments with high throughput, such as transport.

While there are plenty of cloud security solutions in the market, a security-related challenge is authentication to ensure that the credentials in the cloud are being accessed by a legitimate user and device. It also stores data in the cloud, which can raise some privacy concerns. Device fingerprinting, risk-based authentication, or biometrics can be used to manage the transaction risk.

4.2. Card Emulated by Phone Application with Tokenisation

The alternative to a full cloud solution is to have card emulation done entirely by the application on the phone. Given the sensitive nature of the application – it would hold the keys necessary to generate a transaction cryptogram – it has to be well protected (see the Security Considerations section). Also, it would not be prudent to hold the actual payment credentials on the app; hence, this approach is made more secure in conjunction with tokenization– see Figure 4 on page 14.

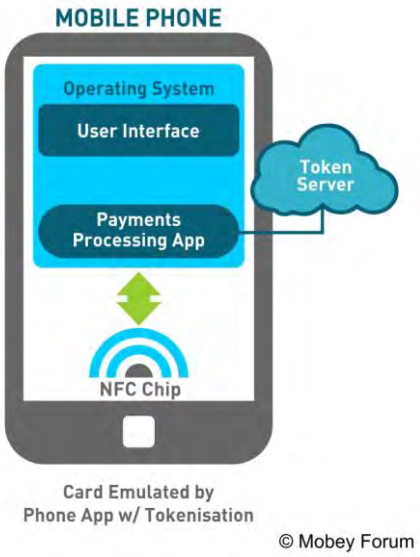

Figure 4: Card Emulation by Phone Application Solution

As Figure 5 demonstrates, the authorising centre shares the actual card credentials with a Token Service Provider (TSP), which may be an in-house solution or a third party entity, such as the card network (e.g., Visa/ MasterCard), a processor, or another provider. This step typically happens once upfront and whenever the actual cards credentials have to be replaced (e.g., at expiry). TSP generates and issues tokens, which the authentication server periodically downloads to the phone. Then, for each transaction, secure mobile app on the phone creates the transaction cryptogram and transfers payment data to POS via NFC, from where the transaction is sent to the processor. A filter detects which transactions are based on tokens and sends them to the TSP to be detokenized, in other words, to return the actual PAN value so that the issuer could authorise the transaction.

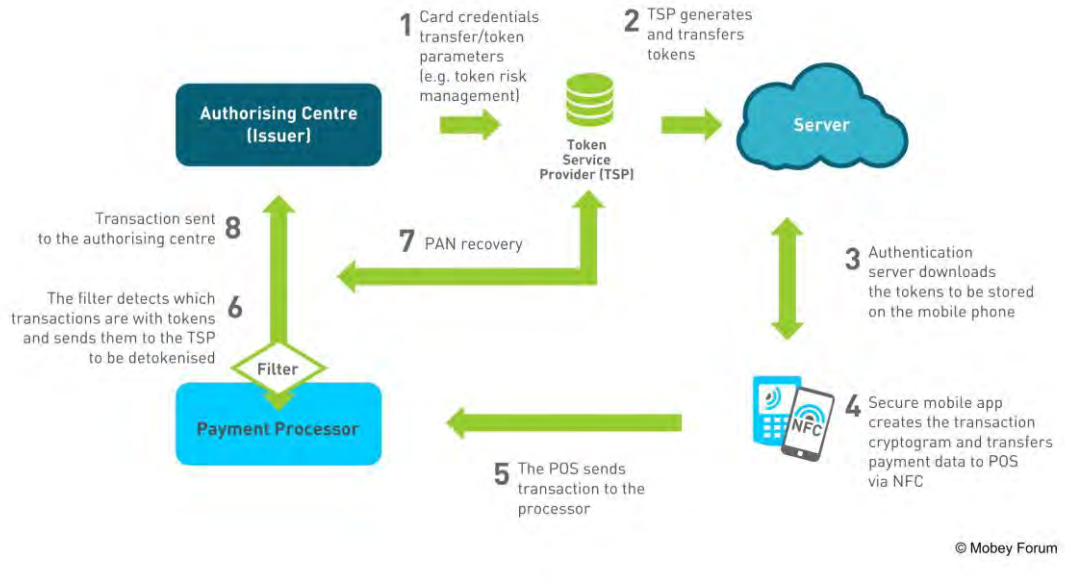

Figure 5: Transaction Flow in the Card Emulation by Phone Application Solution

5. Implementing HCE

5.1. Business Model Considerations

One of the major challenges for "traditional" NFC payments is the complexity of the overall ecosystem and the business model. Issuers have to negotiate how the SE owners will be compensated for storing the payment credentials in the SE and whether the SE owners would collect any transaction fees. Furthermore, agreements with one or more Trusted Service Managers may be needed to help provision payment credentials onto the SE.

Compared with physical SE-based NFC payments, an HCE-based business model is much more straightforward – in theory, the issuers can do it all themselves. Such a full in-house implementation might help avoid recurring fees; however, the issuers would have to invest upfront to develop a solution, and would likely engage specialist **HCE solution providers**. For token-based HCE solutions, the issuers may also want to utilize a third party **Token Service Provider**, which would likely charge for its services[9].

In September 2014, Mobey Forum surveyed over 100 banks and technology and service providers on their views on HCE. One of the questions directed to the banks was which part of an HCE solution they would consider doing in-house vs. enlisting the help of a third party. Figure **6** below shows the breakdown of the banks' responses.

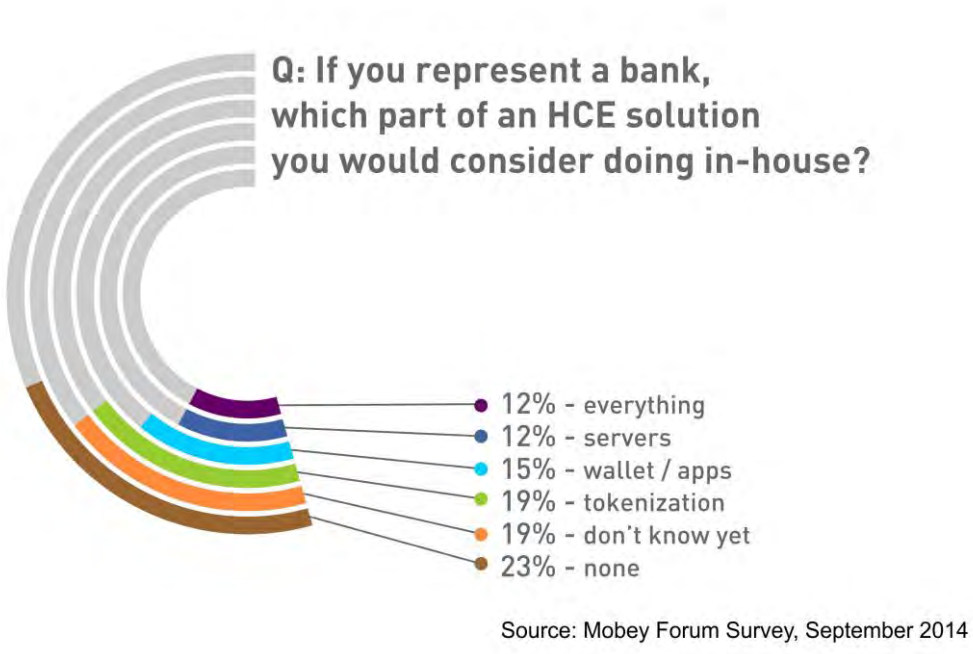

Figure 6: Banks' Attitudes about HCE Implementation Choices

[9] Reportedly, Visa was planning to waive its tokenisation fees throughout 2015 http://www.digitaltransactions.net/news/story/Apple-Pay_-No-Charge-for-Merchants_-But-Transaction-Security-Fees-for-Issuers

Only 12% of respondents said they would do everything in-house; 19% are prepared to do tokenisation themselves, while 15% would keep in-house the development of wallet/apps. Further 12% wanted to keep control of the servers: *"as long as the server is sited in-house … for the rest, would prefer solution providers."* At the other end of the spectrum, 23% said they would like to outsource everything to a third party solution provider.

19% did not know what they might do. Most of those respondents represent organisations at the early stages of considering HCE. Example comments include:

- *"We are currently looking for solutions in the market. Depending on the outcome we could outsource everything or do some things in-house."*
- *"Still evaluating the best option for our organisation."*
- *"Challenging question, given that set-up (what is done in-house, what with partners) varies a bit from country-to-country. HCE could potentially even be good at unifying some of the current set-ups [across] countries."*

By the way, the answers should not be interpreted that the remaining 81% who answered what they would outsource or keep in-house were all planning to launch HCE solutions. The responses included those who had no plans, but simply knew their organisation's attitudes to outsourcing, as demonstrated by the following comment:

- *"Not currently planning to implement HCE. However, the most likely outcome would be to outsource all activities."*

5.2. Selecting the Solution Provider

Given that only 12% of respondents are prepared to implement HCE solution themselves and 23% would like to outsource everything, Mobey Forum wanted to understand which criteria would be considered most important in selecting the HCE solution provider. The question was open to all respondents and listed nine criteria; the tenth option was "Other," allowing the respondents to offer a criterion not on the list. The respondents were asked to rank criteria in order of importance. Figure 7 on page 17 shows weighted importance of selection criteria based on the survey participants' responses.

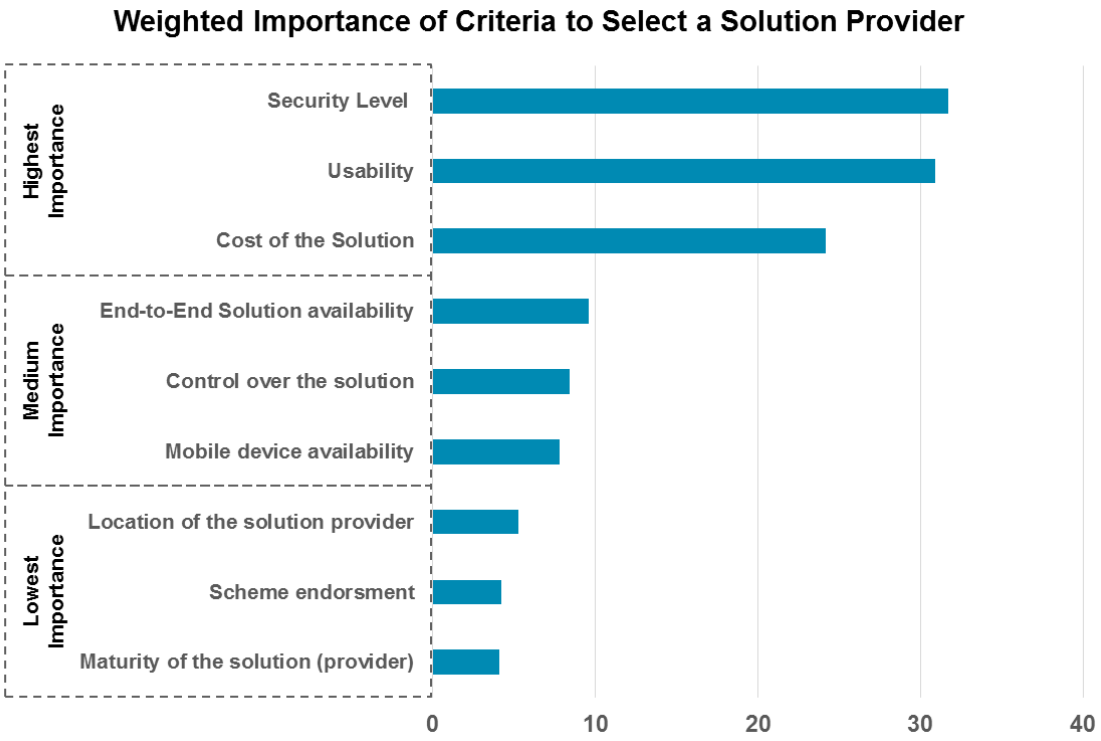

Figure 7: Criteria for Selecting an HCE Payments Solution Provider

Not surprisingly, security level and usability were viewed as by far the most important criteria, followed closely by the cost of the solution. End-to-end solution availability was ranked only as medium importance, consistent with the desire of many respondents to do at least parts of the solution in-house. Similarly, having control over the solution and ability to change the provider easily if needed was ranked as medium importance, alongside with mobile device availability.

We were also not surprised to see the location or maturity of the solution provider being ranked among the least important criteria. While having people on the ground during the project still remains important, the actual location of technology providers matters less in our global economy. Similarly, this is a relatively new area of expertise, so the respondents do not expect vendors or their solutions to be already mature. What did surprise us a little was the low score for the importance of solution endorsement by schemes, such as Visa and MasterCard. Of course, even a low score does not mean that the factor is not important; it simply indicates its relative importance considering all other criteria. We would also expect this factor to rise in importance if only banks answered the question, not including the responses of technology and service providers.

"Other" responses revealed interesting insights into what the survey participants also consider as important criteria. A number of responses focused on two additional criteria – **solution/vendor flexibility** and **vendor implementation and support capabilities**. For example, comments regarding solution/vendor flexibility include the following statements:

- *"Geographic / 'universality' of the solution, i.e. ideally it fits for many markets with differing payment infrastructure & providers."*

- *"Flexibility of implementing additional (scheme) requirements."*
- *"Tokenisation expertise and flexibility."*

Comments around implementation and support capabilities include the following:

- *"Lead time for end-to-end implementation."*
- *"Post implementation support."*

Also, some respondents are keen to look beyond HCE, recognising that they are unlikely to deploy HCE solutions in isolation. For them, it is important how the **HCE solution fits into their overall strategy**, as illustrated by their comments:

- *"Roadmap on top of the HCE Solution."*
- *"Co-existence with other NFC solutions."*

Finally, the survey asked the respondents to list the providers they were aware of offering HCE solutions and related services in the market. The resulting list is included in Appendix A.

6. HCE Control Points Analysis

HCE has the potential to fundamentally change the market dynamics by shifting the balance of power compared to the traditional physical SE ecosystem for mobile contactless (NFC) payments.

While the technical and security related questions and issues raised by HCE are addressed elsewhere in the paper, this section focuses on the change of roles and aforementioned balance of power that HCE can cause.

The analysis is done by applying the control point model that Mobey Forum created and published in the second and third white paper in the Mobile Wallet White Paper Series.[10] Control points from all three layers have to be analysed in order to understand the changing dynamics for a particular solution in a particular market.

Internal Control Points	HCE Perspective
Connection to/from mobile wallet: Controls which types of mobile device, operating system, and mobile wallet implementation can be connected to relevant services and controls the delivery of content according to the designated user level.	This is still a central control point. Mobile devices supported by HCE are bound to be a subset of current NFC-enabled devices, since HCE-based solutions are dependent on both compatible hardware and a compatible operating system.
Distribution channels for the mobile wallet: Controls the distribution of the mobile wallet and application to the user.	TSMs have traditionally had a significant role in SE-based NFC payment solutions. With HCE, mobile wallet applications can be distributed more easily by a broader set of players.
Customer acquisition and enrolment: Controls how users are signed up to mobile wallet services. Acquisition and enrolment are key because they control the main access route to existing customer segments and marketing channels.	With HCE the responsibility for this control point lies even stronger with the wallet providers, as they can no longer rely on the operator distribution channels.
Bearer/connection technology: Controls the various bearers and connection technologies needed for	With HCE the connection technologies are no longer “physically” shielded from the OS on the phone, making these interactions potentially more vulnerable. Securing these through various

[10] http://www.mobeyforum.org/whitepaper/mobile-wallet-whitepapers-part-2-control-points-in-mobile-wallets

http://www.mobeyforum.org/whitepaper/mobile-wallet-part-iii-the-hidden-controls/

interaction between the mobile wallet on the device and relevant services.	security measures increases the importance and value of this particular control point.
Channels to get value into and out of the mobile wallet: Controls how users put funds into their mobile wallets and how they can transfer value to a merchant or other individual.	With HCE, especially combined with (closed loop) prepaid[11], the entry barrier for issuing a means of payment to a mobile wallet has been significantly lowered, which opens this control point for many new players outside of the traditional issuing space. This is also the control point that the Token Service Provider role will be aiming for.
Data flow: The data flow to and from the mobile wallet can be controlled by a variety of stakeholders and intermediaries.	The data flow to and from the mobile wallet can be controlled by a variety of stakeholders and intermediaries. With hardware based SE and Single Wire Protocol the communication between the NFC antenna and the SE is isolated from the OS. With HCE the data used for the NFC interaction will flow through a software layer in the OS and thus put the OS provider in a very strong position from a control point perspective. Having said that, the OS provider will not know the real PAN and other transaction data.
Data ownership: There is a wide variety of data around mobile wallets, encompassing payments, commerce, products, location, preferences, loyalty, and more. The use of such data should always be under the consent of the end user.	While there is no direct change to this control point due to HCE, the lower entry barrier for content providers brings more players and services to the market – all of which will generate data when used.

[11] For more insights into the changing market dynamics driven by prepaid and mobile, please refer to Mobey Forum's whitepaper Prepaid Mobile Wallet: http://www.mobeyforum.org/whitepaper/prepaid-mobile-wallet/

External Control Points	HCE Perspective
Point of interaction (POI)	The fact that there are no immediate changes to the POI control point is a key element for the potential success of HCE since it relies on the existing and well defined NFC specifications and hence does not require any changes on the hardware side with the merchants.
Value and payment services	No immediate changes.
Merchant back end	No immediate changes.

In the original third mobile wallet white paper, the Environmental Control points were listed, but only briefly discussed since they were seen as peripheral compared to the more central Internal and External control points. With the introduction of HCE, these will have increased relevance for the mobile wallet issuers that are considering applying this technology to their solution.

Environmental Control Points	HCE Perspective
Regulation	It is possible that different regions will apply different regulatory regimes – we have already seen interested parties like the European Central Bank suggest that payments should be secured by hardware-based security solutions.
International use	Since HCE is gaining support from the major schemes, the options for international use in terms of acceptance should remain unchanged compared to the existing solutions; however, since HCE-based solutions in most cases depend on data connectivity, international use would imply reliance on Wi-Fi or data roaming, which many users would be reluctant to switch on.
Connectivity	Similar to the control point above – the dependency on data connectivity in most HCE implementations requires not only mobile coverage, but also a certain quality of the connection. Some implementations have requirements of 4G or even 5G connection for a satisfactory user experience.

Looking through the control points, it is evident that broad adoption of HCE would imply significant changes in the mobile payments landscape.

7. Summary and Conclusions

If provided with a suitable software-based payment solution, HCE is another option to implement NFC payments. As this paper and the summary table below demonstrate, compared with physical SE-based NFC payment implementations, HCE has some advantages but also comes with its own complexities.

Consideration	Physical SE-Based Solution	HCE Solution
Issuing/ provisioning	Requires provisioning of the payments app and credentials to a physical SE on the phone. May need a new SIM card.	Payment app can be downloaded from the app store; payment credentials supplied as needed by the solution.
Security	Very secure, chip-based, tamper-resistant environment.	Need to manage risk of exposing the payments app to malware and viruses. Need risk-based authentication to ensure a legitimate device and user are accessing payment credentials. Security ensured by utilising limited-use payment credentials (e.g., tokens, transaction keys) and other risk management techniques.
Current OS support	Android, Blackberry, Windows	Android 4.4 KitKat Blackberry OS 10
User experience	Seamless. Works with low-power or without any user interaction.	Without access to a fast network, users may experience slow transactions (4.1-full cloud solution). Tokens have to be delivered to the phone ahead of the transaction (risk of not having a token if the phone can't connect to the network). Battery power may be required.
Transaction support	Currently for physical POS (card present) only.	Physical POS and e-/m-commerce (card present and card not present).
Business model	Complex ecosystem and business model; issuers need agreements with both SE owners and TSM suppliers.	Fast time to market – no need for complex issuer-MNO-TSM negotiations. However, issuers may want to partner with HCE solution providers or utilise third-party Token Service Providers.

It is evident that broad adoption of HCE would imply significant changes in the mobile payments landscape. It gives different entities, including financial institutions, more freedom to decide to what extent they want to work with other players of the value chain. Therefore, we view HCE as an important driver behind NFC-based mobile payment adoption as well as other services such as vouchers, couponing, ID management, and others.

However, HCE is not an easy fix to NFC mobile payments challenges – while the issuing might become simpler, there are other areas to consider, such as new roles and new business models. Some financial institutions will clearly be attracted by HCE, while others may continue with physical SE-based solutions or even consider deploying both. Understanding the market dynamics and the control points will be essential to success.

8. Appendix: Solution Providers

Mobey Forum's HCE Survey included a question asking for the names of companies providing HCE services and solutions. The aim of the question was to provide added value for those who are in process of drafting a Request for Information (RFI) or Request for Proposal (RFP). Mobey Forum has not qualified the suggested companies, and does not imply all of these have relevant solutions. The Forum is also aware of the fast-changing situation in the market.

Solution Providers as of September 2014	
ABNote	*www.abnote.com.au*
Accarda	*www.accarda.com*
Bell ID	*http://www.bellid.com/*
CA Technologies	*http://www.ca.com/us/default.aspx*
CartaWorldwide	*http://www.cartaworldwide.com/*
C-Sam - A Mastercard Company	*http://www.c-sam.com/about-us*
Gemalto	*http://www.gemalto.com/*
Giesecke & Devrient	*http://www.gi-de.com/en/index.jsp*
Helixion	*http://www.helixion.com/*
INSIDE Secure	*http://www.insidesecure.com/*
Mahindra Comviva	*http://www.mahindracomviva.com/products/mobile_financial_solutions.htm*
MasterCard	*http://www.mastercard.com/index.html*
Nexperts	*http://www.nexperts.com/*
Oberthur Technologies	*http://www.oberthur.com/*
Proxama	*http://www.proxama.com/*
Redsys	*http://www.redsys.es/*
Seglan	*http://www.seglan.com/*
Sequent	*http://www.sequent.com/*
SimplyTapp	*https://www.simplytapp.com/*
Visa	*http://usa.visa.com/about-visa/index.jsp*
WincorNixdorff	*http://www.wincor-nixdorf.com/internet/site_EN/EN/Home/homepage_node.html*