HOST CARD EMULATION:
NFC’S MISSING LINK
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>1. WHAT IS HCE?</td>
<td>4</td>
</tr>
<tr>
<td>2. IMPLEMENTATION OPTIONS</td>
<td>8</td>
</tr>
<tr>
<td>3. HCE BUSINESS BENEFITS FOR SERVICE PROVIDERS</td>
<td>12</td>
</tr>
<tr>
<td>4. THE IMPACT OF HCE ON MNOS</td>
<td>15</td>
</tr>
<tr>
<td>5. HCE BEYOND PAYMENTS</td>
<td>18</td>
</tr>
<tr>
<td>6. THE FUTURE OF HCE</td>
<td>19</td>
</tr>
<tr>
<td>ABOUT BELL ID</td>
<td>22</td>
</tr>
</tbody>
</table>
Near field communication (NFC) technology and mobile wallets have traditionally stored all the data needed to make a transaction on a physical secure element (SE) within a mobile device. This has established the owners of the SE – such as carriers / mobile network operators (MNOs) or mobile device manufacturers – as the gatekeepers, both in terms of permission to access the SE as well as charging to access it.

As there are many SE owners operating worldwide, each with a unique business and technical model, service providers must establish a relationship with each in order to deliver their services via NFC. Many industry experts recognize the challenges surrounding integration between many of the players in the NFC ecosystem as the reason why mass market NFC services are yet to be deployed.

The industry has been given a huge boost with the advent of host card emulation (HCE): it allows NFC-based applications to be added to mobile devices without having to get permissions to connect with the SE.

This ebook will explore how HCE can overcome the challenges faced by service providers when implementing NFC services, with a particular focus on payments, and discuss the benefits of HCE over ‘traditional’ NFC SE implementations.
1. WHAT IS HCE?

Mobile payment credentials have traditionally been stored locally on the mobile device inside a piece of hardware called the secure element (SE). An SE is a tamper resistant hardware platform, capable of securely hosting applications and storing confidential and cryptographic data. It therefore plays a very important role in secure mobile computing.

For example, in the finance industry SEs are used to host personalized card applications and cryptographic keys required to perform financial (EMV) transactions at a point-of-sale (POS) terminal. SEs used in the identity market may hold biometric data or certificates which can be used for signing documents.

Whatever the purpose, the secure environment provided by the SE protects the user’s credentials ensuring the safety of the user’s data.

The physical presence of a SE in the device, however, creates dependencies and complexities that make it difficult and expensive for actors in an NFC ecosystem to interact efficiently. For example, an application issuer would need to have agreements with a number of SE issuers, who in turn need to connect with different types of mobile handsets.

HCE is a technology that emulates a payment card on a mobile device using only software. It uses the mobile operating system to enable a ‘virtual’ SE to be present outside the mobile device. By moving the SE to a remote environment, the complexities and associated costs can be bypassed: application issuers can directly provision their applications to a virtual secure element without any third-party involvement.
HCE essentially offers issuers an alternative solution where the use of a physical SE on the device adds insufficient value to justify the additional costs. It provides a bridge between the point-of-sale (POS), the remote SE and service provider, for example an issuing bank. Crucially, HCE does not require any changes to acquiring infrastructure nor optimization to specifically support NFC.

By moving the SE to the remote environment of the cloud, the cost and complexity of managing a physical SE can be reduced significantly, ensuring a consistent user experience. It allows consumers to make contactless payments, even without an internet connection, by using preloaded tokens.
HOW HCE IS REINVIGORATING NFC SERVICES

According to analyst firm IHS, just 18.2% of mobile phones were NFC-ready in 2013; it predicts that by 2018, penetration will be 64%. Android, which dominates global smartphone shipments at 81% in the third quarter of 2013, supports HCE on Android 4.4 (KitKat). This brings HCE service delivery options to in excess of three quarters of the entire smartphone market.

THERE ARE A NUMBER OF LARGE INDUSTRY PLAYERS THAT ARE SUPPORTING HCE

• In early 2014, Google announced that from 14 April 2014 it will only be possible to use Google Wallet to make a NFC payment using a device that supports HCE. Its decision was based on the fact the Google’s ‘tap and play’ operates on different technology on Android 4.4 (KitKat) and so would no longer support physical SEs.

• In January 2014, the GSMA and Consult Hyperion published a study to help banks and mobile operators understand HCE and SIM SE approaches to NFC payments. The guide concludes that the SIM SE and HCE approaches to NFC payments each offer important benefits for financial institutions and should not be viewed as mutually exclusive. Indeed, a combination of the approaches may be appropriate for differing applications and markets.

• In February 2014, MasterCard and Visa announced their support of HCE technology. Technical specifications have been released to support this deployment.
These announcements mean that HCE is now a viable alternative for many card emulation projects, where no physical SE is needed in the device. Coupled with the significant increase in NFC-enabled devices and the exponential rise in the number of handsets shipped, NFC services will soon become a mainstream technology.
2. IMPLEMENTATION OPTIONS

While HCE is currently supported by Android and BlackBerry, it is creating different opportunities and solutions in the marketplace. These promote choices and give service providers the ability to easily and effectively deploy NFC services to their customers in a manner that supports their commercial objectives, technical capabilities and security requirements.

As well as delivering alternative payment technologies, HCE may also encourage MNOs to cooperate on hybrid solutions which are less onerous to implement. This will accelerate the development of NFC services and may be the catalyst needed to deliver the benefits of this contactless technology to both the industry and the consumers they serve.

Currently there are two HCE NFC models available to service providers:

1. **Pure HCE**

   This offers issuers an alternative solution where the use of a physical SE on the device adds insufficient value to justify the additional costs. For example, low value payments, loyalty, couponing, access control, transit and other low value applications.

   The pure HCE configuration does not require an SE in the device as the payment application is hosted remotely within a secure data center in the cloud such as the application issuer’s own environment. When making a transaction using pure HCE, it simulates the SE in its communication with...
a POS terminal and will connect to the cloud to receive the data required to make a payment. This configuration allows card issuers to retain their role as the manager of the payment ‘token’ with responsibility for risk within the payments ecosystem, while the MNO is a data carrier.

2. HYBRID HCE
This configuration offers all the benefits of HCE coupled with the enhanced security of a physical SE (either SIM/UICC or embedded SE), which is used for authentication purposes only. The main benefit of this model is that as it can be implemented onto a wider range of handsets. It does require some MNO / mobile handset manufacturer involvement, depending on the owner of the SE, to load the cardlet into the SE. The lifecycle management of the application (such as update, delete and other functions), however, is managed on the remote server in the cloud, not in the SE. This means that involvement of the MNO / mobile handset manufacturer is minimal.

Another advantage to the MNO is that it does not require large capacity NFC SIMs since the majority of the data is stored in the cloud. Therefore, the SIM does not need to be replaced to allow the end-user to enable NFC capabilities.

When there is no internet available, both HCE models pre-authorized EMV tokens which the mobile device can use in order to process an entire payment transaction.
HOST CARD EMULATION - NFC'S MISSING LINK
3. HCE BUSINESS BENEFITS FOR SERVICE PROVIDERS

Ultimately, the main benefit of HCE is that it allows the service providers to be in control, including control of costs, security, partners and, most importantly, management of a solution’s position in the value chain. Players in the NFC ecosystem want to work under mutually beneficial and productive relationships, which will ultimately drive the technology forward and add value to the end-user.

Here are just some of the other benefits that HCE offers:

1. INDEPENDENCE

By deploying services to HCE, no intermediaries are necessary to access the SE. This narrows the gap between application issuers and customers, ensuring a consistent brand and end-user experience across all available NFC services.

2. EASIER INTEGRATION WITH THIRD PARTIES

Being in control of the SE allows easy integration with any third party provider and business model. These include MNOs, NFC device manufacturers and trusted service managers.

3. LOWER COSTS

SE integration in mobile devices is expensive and subject to SE domain fees. By deploying the SE remotely, the NFC value chain will be shortened as fewer parties in the ecosystem need to be involved; this leads to lower provisioning costs.
HCE ALLOWS SERVICE PROVIDERS TO BE IN CONTROL OF THE COSTS, SECURITY, PARTNERS AND MANAGEMENT OF A MOBILE PAYMENTS SOLUTION.
4. GREATER SECURITY AND IMPROVED RISK MANAGEMENT
Direct access to the SE enables instant fraud detection and allows immediate blocking of an application. Additionally, the computing power of HCE is higher than that on a mobile device. This offers the option for more advanced on-device risk management. Enhanced security means better customer satisfaction and higher adoption in the long-term.

5. MULTIPLE CARDS, EMV APPLICATIONS AND PAYMENT SCHEMES
Storage capacity on a physical SE is limited. Using HCE, storage is scalable and can be expanded to meet individual requirements and to support any card, application and payment scheme. The greater the choices available, the more options for developing and expanding the solution in the future.

6. COMPATIBILITY WITH READERS AND POS
As the transaction emulates an EMV payment, no changes are needed to existing contactless terminals or the payment acceptance infrastructure.
4. THE IMPACT OF HCE ON MNOs

HCE is not side-lining MNOs / carriers, but instead giving them innovative technology to immediately expand their capabilities, proposition and revenues in the NFC industry. The solution offers a new strong and flexible form factor of the SE in order to support the industry’s drive towards full-scale NFC deployments.

It is likely that a portion of the market will adopt the hybrid HCE model which requires some MNO involvement. The potential to have more applications hosted in the cloud, in combination with using the SIM for strong authentication, confirms the position of the MNO as the important authentication authority for mobile devices.

HCE working with MNOs offers the following benefits to the NFC ecosystem:

1. **SAVE ON THE REISSUANCE OF SIM CARDS**
   By utilizing HCE, MNOs can roll-out NFC services to consumers immediately (provided the handset is NFC enabled) without the need to invest in new additional infrastructure or issuing updated SIMs with a SE, as existing SIMs already offer the capability required to authenticate a user.

2. **PROVIDE STRONGER AUTHENTICATION**
   A hybrid HCE implementation means that MNOs, as the owner of the SIM card, provide an additional strong authentication mechanism. This coupled with their expanding infrastructure integrates well with the improved processing power of HCE. These complementary technologies will increase transaction security, speeds and network availability.
WITH HCE, MNOs CAN ROLL-OUT NFC SERVICES IMMEDIATELY WITHOUT INVESTING IN A NEW INFRASTRUCTURE AND SIM CARDS.
3. **SUPPORT A WIDER SERVICE PORTFOLIO**

Hosting the functionality of the SE remotely expands storage capacity and processing power. This means that HCE delivers flexibility when launching and managing mobile services. HCE allows many more service provider applications to be supported and the increased processing power decreases the amount of time taken to provision the application (and its credentials), and execute transactions.

4. **FUTURE PROOF**

HCE is adaptable to future technology developments. Updates and service launches are made much easier, cheaper and quicker without the need to upgrade hardware. HCE also makes the bundling of services such as loyalty and couponing more effective. MNOs can work with service providers to leverage existing real-time consumer context information to add value to mobile financial services.

5. **ENABLE FLEXIBLE AND SCALABLE BUSINESS MODELS**

HCE offers a simple and strong business model to MNOs. Extended capacity allows for additional revenue generating services to be hosted. The non-physical nature of HCE requires reduced integration effort, allowing the MNO to efficiently adapt to different business models. MNOs can offer packages to service providers active in specific industries which prioritize their applications’ network requests, enabling quicker processing times for key services.
5. HCE BEYOND PAYMENTS

HCE FOR TRANSIT, REWARD AND ID
NFC payment is a clear use case for HCE based solutions; the cloud based payments specifications now issued by several of the payment brands are reliant on HCE as part of their global mass market NFC payment strategy. The advantages of the technology, in terms of market reach, control and cost of deployment, also lend the technology to many other NFC based use cases where a secure token needs to be managed and supports some form of transactional behavior. E-tickets and e-vouchers for a number of industries are already being looked at including travel (such as flight, rail), rewards (retail), and closed loop payments for store cards, transit and universities.

HCE ON OTHER CHANNELS AND PLATFORMS
A key advantage of the mobile platform is that the same management of secure tokens, credentials, and entitlements (tickets/value) can also be used outside of HCE for NFC to enable support for remote transactions over the network (WiFi, 4G, etc.) in any form of m-commerce. Combining that secure token management capability with other technologies (such as a trusted platform module) already deployed on laptops and tablets means that the same solution can enable secure and cost effective deployment of multiple applications in the m-commerce and e-commerce remote transactions area.
6. THE FUTURE OF HCE

Although some markets have achieved NFC success, such as Canada where an established infrastructure has been introduced that has meant MNOs and service providers are working together in a USIM-based ecosystem, NFC has yet to realize mass-market rollout globally. The introduction of HCE and its simplicity, therefore, has been seen by many industry commentators as a game-changer.

CASE STUDY – AUSTRALIA

Australia is a marketplace where HCE can solve a number of issues and achieve traction quickly, with many Australian banks and service providers now sprinting to develop this technology and become first movers within the marketplace. But why is HCE perfect for Australia?

To begin, Australian banks, MNOs and service providers have been unable to work together effectively to create a joint and common NFC infrastructure. The release of Google’s Android KitKat 4.4 allows financial institutions and service providers to take control of their implementations and come to market independently, avoiding the need for complex business relationships with other entities in the NFC ecosystem.

The marketplace does, however, have a strong contactless infrastructure, with over 100,000 contactless POS terminals across Australia already and twelve million contactless cards already in circulation. As HCE mobile payments use the same contactless POS infrastructure as contactless cards, this provides a springboard for the technology; Australian consumers are
WITH A STRONG CONTACTLESS INFRASTRUCTURE, AUSTRALIAN CONSUMERS ARE ALREADY ACCUSTOMED TO ‘TAP-AND-GO’ BEHAVIOR.
already accustomed to ‘tap-and-go’ behavior. Finally, Australia is one of the few countries where embedded SEs were launched for mobile payments. Commitment from the handset manufacturers, however, is now wavering as embedded SEs represent an additional expense. With NFC prevalent in handsets but embedded SEs receiving less support, HCE can become the dominant technology for fast and widespread mobile payments deployment.
ABOUT BELL ID

Banks, governments and enterprises worldwide rely on Bell ID software to safely issue and manage credentials on many millions of smartcards, smartphones and connected devices. Our software integrates with any third party technology and simplifies the issuing complexities of payment, identity, loyalty and transit applications. Whether it’s EMV payments data stored on a chip card, in an NFC-enabled mobile device or in the cloud leveraging HCE, Bell ID has the expertise to manage the lifecycle of any application on any form factor. Our award winning solutions meet the demanding requirements of international standardisation bodies and payment networks.

In June 2013, Bell ID launched Secure Element in the Cloud. The award winning technology enables credentials and information related to mobile service to be securely stored and the associated processes to be executed in a cloud environment. This removes many of the complexities and cost implications related to the deployment of secure mobile services.

As a pioneer in the cloud-based mobile payments sector, Bell ID has taken steps to protect this intellectual property by filing an international patent application (WO2014/048990) with the World Intellectual Property Organization (WIPO).

To learn more about Secure Element in the Cloud and host card emulation, please visit the webpage or watch our short video.