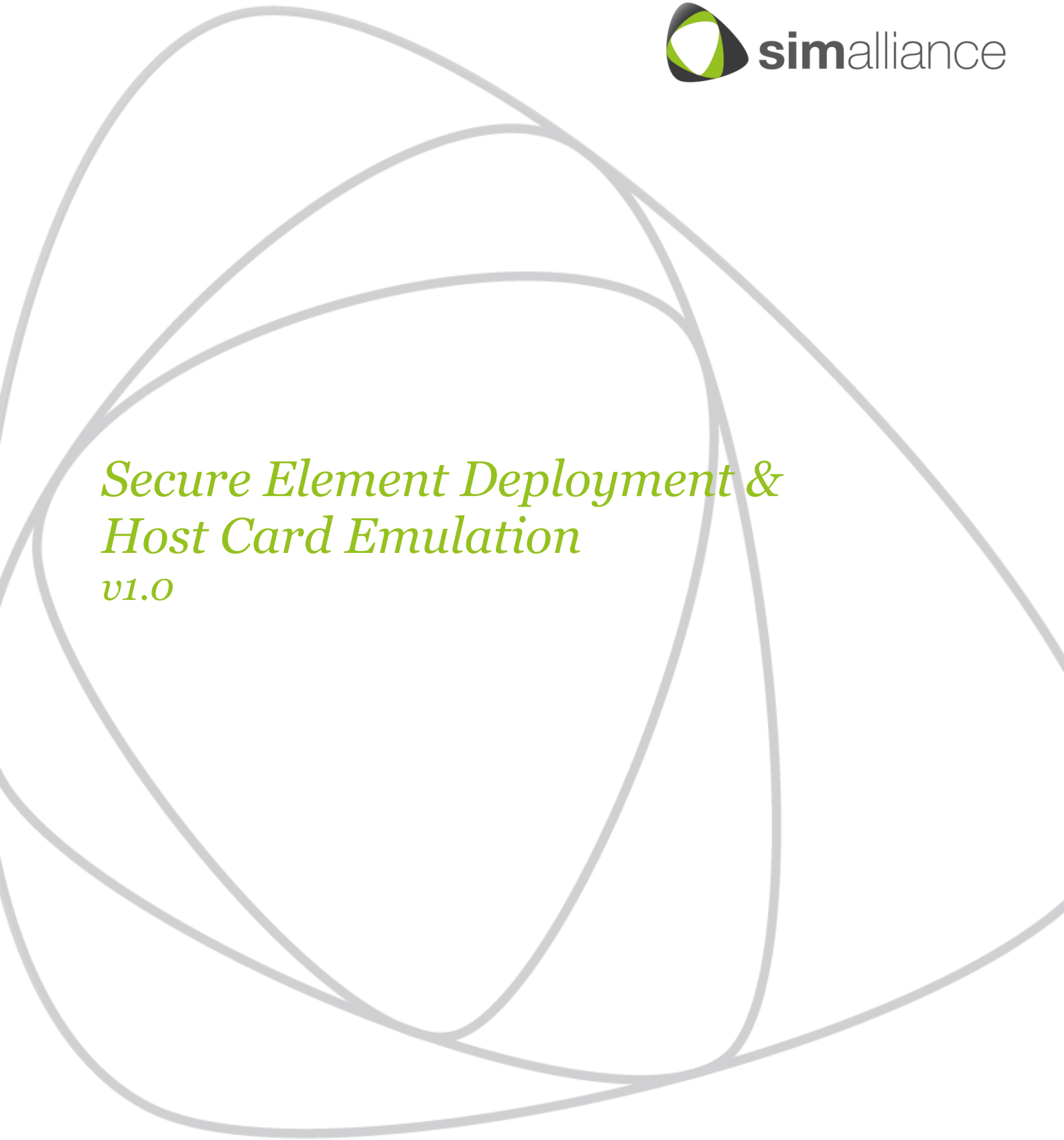

Secure Element Deployment & Host Card Emulation

v1.0

Document History

Version	Date	Editor	Remarks
1.0	29/04/2014	HCE Taskforce	Public release

Contents

1. Executive summary

This paper provides an introduction to Android's Host Card Emulation (HCE) and explores its value to the NFC ecosystem relative to the Secure Element (SE). SIMalliance contends that while HCE is good for the NFC ecosystem as a whole (increasing end-user familiarity with NFC through additional services, driving adoption and encouraging new developers into the ecosystem), the technology remains immature, un-standardised and, relative to SE-based deployments, vulnerable to malicious attack.

Given HCE's current and anticipated limitations, SIMalliance considered HCE to be best utilised in use cases where stringent security requirements, optimal transaction speeds and always-available functionality are not mandatory.

In order to distribute and manage valuable and/or sensitive credentials (for activities such as payment, transport, identity, or access) this paper asserts that a secure component in the device, together with a secure provisioning and management solution, remains a necessary requirement. Both the secure component and its corresponding management solution should be fully interoperable and mobile OS platform agnostic. The secure component should also be able to host applications in a 'black-box' manner and should not contain software that can be easily removed, decompiled, or otherwise interrogated to reveal the location of stored confidential data (either locally within the device or the credentials needed to gain access to such data in the cloud) which, as a result, could then be targeted and compromised.

SIMalliance maintains that it is necessary to have such a secure component and management system certified following extensive security testing by several recognised third-party laboratories, thus ensuring that the secure NFC ecosystem is audited using the latest generation of known attack path techniques.

2. Introduction to Host Card Emulation (HCE)

Defined initially by the NFC Forum and since its inception integrated in the "Card Emulation" part of the core set of NFC specifications, HCE (Host Card Emulation) allows the software emulation of a smart card-based application. Prior to December 2013, HCE was available only via Blackberry OS. Since then the feature has also been supported by Android OS, following the launch of version 4.4, codenamed "KitKat".

Android 4.4 provides an API set that helps developers to control the NFC interface and send commands to NFC-enabled devices. Applications could therefore be developed to emulate any classic contactless smartcard application using the ISO 14443-4 standard, such as loyalty, access control, ticketing or payment applications. HCE however does not enable the emulation of some hardware-based card scheme applications like Mifare or Felica.

2.1 Security and appropriate usage

Moreover, HCE does not provide any specific hardware or software-based security services; it behaves just like any other Android application and does not, therefore, offer the same level of security as conventional contactless smart card applications. Security concerns relating to HCE are further compounded by industry reports indicating that Android is, by some distance, the most attacked of all mobile environments.[1]

[1] Source CISCO 2013 Annual Security Report

HCE is not integrated into the secure management environments commonly used in today's mobile devices. Neither is it included in the frameworks for secure elements (SE), such as those specified by GlobalPlatform. As such, HCE does not benefit from the same level of interoperability, secure execution, remote management and ubiquitous acceptance required to manage both the mass roll-out and post-deployment life cycle of NFC applications in a secure, consistent and standardised way.[2]

SIMalliance assessment:

HCE is best suited to use cases where the user's stored credentials are of low value and where the emulated NFC application is not based on direct implementation of a current, pre-existing card application.

2.2 Benefit to NFC ecosystem

The key goal of HCE is to offer a basic model for simple card emulation, enabling developers and service providers to roll-out new NFC services to the market. SIMalliance anticipates that this capability will bring new creative players into the NFC ecosystem, many of which may not hail from the traditional smart card world. These players will be capable of developing innovative applications that attract new users, creating new NFC use cases and enhancing the NFC service experience of current users. Ultimately, this will be to the benefit of the whole NFC ecosystem, bolstering service adoption and driving user familiarity through an increased number of applications.

SIMalliance assessment:

HCE is good for the NFC ecosystem as a whole; it will make NFC more accessible and versatile to developers, and more familiar to end-users, increasing mass market adoption as a result.

2.3 HCE service delivery

In order to optimise HCE such that a level of service similar to that provided by existing card schemes can be delivered, additional technologies may be required, such as cloud-based credential management. Like HCE, these technologies remain proprietary and immature, and may also have a significant impact on existing card management systems. In addition to security restrictions, they may also bring other limitations relative to the end-user's experience and other supported features. An NFC transaction requiring back and forth exchanges with its corresponding IT system in the cloud, for example, will bring a critical dependence on the quality of the mobile network coverage or in-store Wi-Fi speeds, either of which could negatively impact transaction times at the point of sale.

A transition to these enabling technologies can be challenging as they have yet to be proven at scale. Authentication to the cloud to gain access to services must be secured with more than one factor (user name and password for example is insufficient to protect access to high-value cloud based services). Handling, storage and validation of tokens needs to be carefully considered in the light of a device which is not trusted. As a consequence, a service provider wanting to fully replicate and emulate its existing contactless smart card-based services on HCE, as it is today, may need to make significant investments in new, as yet non-standardised, technologies. It will take time to establish an industry standard that is agreed by all parties in

2 Technical recommendations on how to optimise interoperability in NFC deployment and management can be found in SIMalliance's NFC Secure Element Stepping Stones document, available here: http://www.simalliance.org/en/nfc/nfc_technical/

the ecosystem. Deploying a HCE based service ahead of this point in time carries an inherent risk for the service provider, which will need to be carefully evaluated.

SIMalliance assessment:

Early adopters should proceed with care; the quality of HCE service delivery is dependent on a variety of variable factors. Until industry standardisation has been achieved in a secure manner, technology investment will remain at risk (see Chapter 7 for more).

2.4 Market development and adoption

HCE on Android OS is limited today to Android v4.4, meaning it is currently available only on select, high-end handsets. Reaching a critical mass may take time; the Android mobile ecosystem is characterised by strong variation between device models and OS versions[3], which are further compounded by the slow rollout of new OS releases to legacy devices. Due to the size of Android's market share, there are also a high number of 'rooted' Android devices, which will also inhibit the rate of adoption amongst users. Although Android OS has now surpassed 80% global marketshare[4], these factors will limit HCE coverage. Mass deployment of HCE is likely to occur on other major smart phone OS platforms, like iOS and Windows Mobile, in a more consistent and interoperable way.

SIMalliance assessment:

HCE remains in its infancy. Until more OS providers support the HCE model, deployments will remain vulnerable to the prevailing challenges associated with global Android OS utilisation.

2.5 The Secure Element: a widely established, interoperable and secure alternative

Currently the only means of offering a device agnostic, standardised (and therefore interoperable) environment for the mass deployments of NFC applications is by utilising a Secure Element (SE). The SE offers the most stringent level of security available today, together with the largest number of secure services, all supported by mature certification schemes offering strong guarantees to service providers.

SEs are also supported by mature ETSI, 3GPP, GlobalPlatform and Java Card standards, offering an optimal level of interoperability and an unmatched, rich portfolio of essential services. This allows mass deployment in the field and comprehensive management of application life cycles for the vast majority of service providers' requirements (for banking, transport, access control, identity etc.).

3. Establishing certification

3.1 About SE certification schemes

One of the key advantages of the SE as a standalone component is the possibility to certify its security robustness against malicious operations. With security being a design fundamental of the SE, it presents strong countermeasures against the most sophisticated attacks. As a result, there are no demonstrated instances of unauthorised access to, or duplication of, the sensitive data stored in a SE. It is also a reliable 'second factor' in models of strong authentication (where the first factor is 'something you know' and the second factor is 'something you have').

[3] Android Fragmentation Visualised (OpenSignal)
[4] International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker

The sophistication of malicious attack techniques are evolving quickly, in line with the advancing computational capabilities of integrated circuit chips. This has given rise to an entire community of security experts dedicated to the discovery of potential attacks and the development of appropriate countermeasures.

The ability to guarantee the security of a service provider's or end-user's credentials is a pre-requisite for the adoption of mobile NFC services. The SE's certification scheme is well established; certification can only be achieved after deep analysis and extensively testing conducted by a number of independent certification laboratories, which work independently to verify a SE's robustness to a wide range of attacks (including, amongst others, malicious applets, fault attacks, masquerades and side channel attacks). The certification scheme also scrutinises the SE for strict adherence to functional specifications.

In a bid to reduce the risks of fraud and malicious operations even further, many service providers and payment associations have defined their own SE security certification frameworks and will only permit a device to perform their required task, like authenticating a payment, for example, once full certification has been obtained. SEs used in today's mobile payment solutions have already achieved certification from all corresponding payment associations and schemes (including EMVCo, Visa, MasterCard, American Express, etc.).

In addition to scrutinising the SEs themselves, SE certification schemes also require the specific auditing of each provider's processes and premises, in order to verify that the confidential data of both the user and service providers is handled with an appropriate level of security. This includes SE development centres, and the factories of SE providers, which are then certified again by the individual payment associations.

3.2 HCE certification: a big job ahead

In order to protect the payment schemes, issuing banks and their customers, certification schemes similar to those described above must be defined for new mobile payment solution technologies like HCE. Over time, this will be achieved by following a similar process, over a number of years, which has led to the establishment of SE certification schemes. Several key challenges must be faced on this road. An expert community must be assembled that is capable of identifying and developing countermeasures to possible threats to HCE, leading to the definition of a certification scheme that is sufficiently comprehensive to demonstrate the robustness of the solution to service providers and end-users. The fact that HCE is not a standalone piece of hardware but it is an integrated component in the Android OS (together, potentially, with other OSs in the future) is a serious challenge; it may be more difficult to identify the possible attack paths than it has been with the SE. Establishing the boundaries of stakeholder security responsibility is likely to be another big and related challenge.

SIMalliance assessment:

Given its current level of immaturity, HCE has a long way to go before it can establish a certification scheme that is comprehensive and robust enough to win the confidence of service providers and end-users. It also has unique and unmet challenges to overcome, relative to its OS-integrated, software-only model.

4. Developing Android applications with the SE

ABI Research indicates that a total of 345m NFC-enabled devices were shipped in 2013[5]. Those that are supported by Android OS utilise a mobile application to provide a rich user interface and easy deployment options for the management of SE applications. This application is hosted on the smart phone and provides a powerful way to enhance the end-user's service experience, while the SE protects the user's and the service provider's confidential data.

4.1 The Open Mobile API

To embrace the potential of the Android operating system and the certified security of the SE, in 2011 SIMalliance defined the Open Mobile API. By using the Open Mobile API the application development community can deliver applications on mobile operating systems supporting the API, including Android OS with rich user interfaces which interact with secure element based applications. The Open Mobile API is utilised in more than 150 different models of Android devices all around the world.

SIMalliance assessment:

SIMalliance encourages the integration of the Open Mobile API with all future mobile devices in order to provide a proven and standardised way for mobile applications to access the SE.

5. HCE: functional drawbacks relative to the SE

From an end-user perspective HCE and other 'cloud-based' transaction solutions have several drawbacks when compared to an equivalent SE-based deployment.

5.1 Low power mode

'What happens if my battery runs out?' This is often one of the first questions an end-user asks when they are given the opportunity to transfer their payment card functionality to a mobile device. When referring to HCE or other cloud-based transactions, the answer, invariably, is 'the payment cannot be made'. Under these circumstances, an application on the device is managing the transaction and requires battery power to successfully manage the task. This is not the case with an application running on a SE. This solution can utilise power transferred to it by the contactless reader or POS terminal and successfully complete a transaction even when the smart phone is switched-off, or its battery is drained. This SE functionality, known as 'low power mode', means that a user can still rely on their device as a payment instrument even when it is otherwise un-useable. This feature has clear and far reaching implications for end-user convenience.

5.2 Roaming and no data connectivity scenarios

'What if I have no mobile network reception or wi-fi coverage?' Under these circumstances, when the user has disabled data connectivity to avoid roaming charges[6], for example, has bad coverage in a subway, or is in a building with thick walls, HCE or cloud-based transactions may be inhibited depending on the implementation. Even if a cloud-based credential management solution is employed, after a predefined number of transactions has been exceeded the payment application must establish a remote connection in

[5] 'ABI: Smartphones accounted for 80% of NFC devices shipped in 2013' *NFC World, 08.01.14*

[6] 'European visitors 'turn phones off' to avoid charges', BBC News 17.02.14

order to download more tokens if it is to continue to support transactions. This means that an end-user may have performed few or no transactions before their NFC smart phone is refused by a POS terminal. This inconvenience is not experienced when the NFC application is securely running in a SE, as the credentials to pay are always, regardless of whether the device is connected or in coverage of the mobile network.

5.3 Transaction speed

The user experience for most NFC transactions demands a rapid response time. This is certainly the case for ticketing and transportation, where end-users are required to flow through busy turnstiles during a commuting rush hour. Payment transactions also require a quick response although the threshold may be somewhat lower (e.g. 400ms). HCE and cloud-based NFC transactions face a considerable challenge here when compared to SE-based solutions; they must not only contend with the latency of the controller and the application reactivity within the SE, but also the mobile network latency required to communicate with the cloud-based agent that will validate the transaction (if credentials are not pre-stored in the device, e.g. in the secure element). Over LTE, network latency can be as low as 20ms but for a 3G or 2G network it can frequently exceed 100ms and even 300ms; a delay that would jeopardise the NFC user experience should a solution requiring a direct connection to the cloud be used. The result can be long transaction times, or worse, a transaction rejection caused by a 'time out'.

SIMalliance assessment:

In its current form, HCE is best suited to lower value applications where stringent security requirements are not mandatory. Cloud-based solutions are best suited to apps which have no high reliability, performance/throughput constraints and where network connectivity is not required.

In Figure 1, below, SIMalliance plots a variety of NFC services in accordance with their prevailing requirements to access a SE.

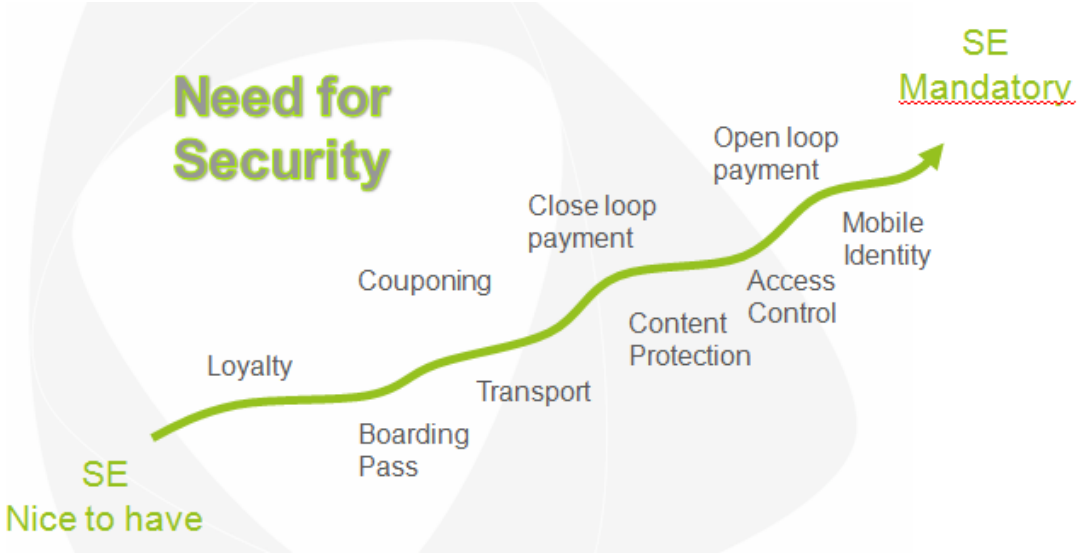

Figure 1: Prevailing SE security requirements by NFC use case

5.4 SE and HCE characteristics compared

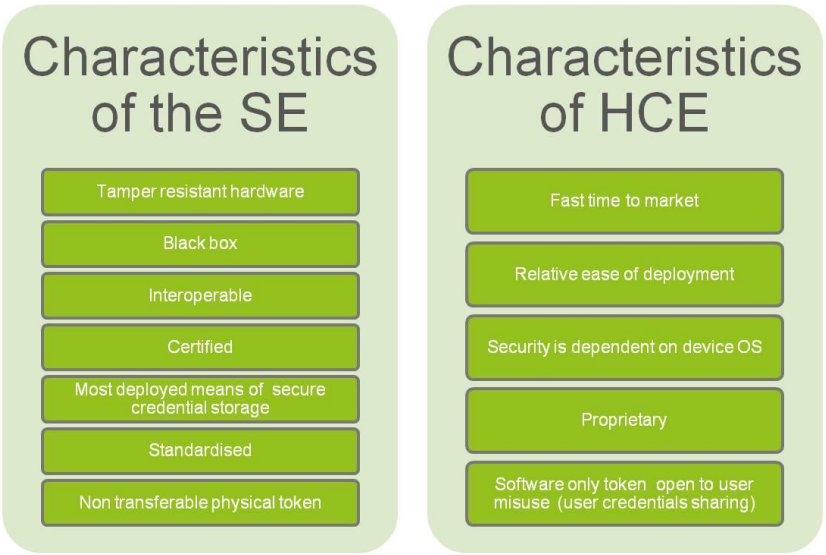

Figure 2: HCE and SE characteristics

6. HCE in today's context: current NFC use cases

In order to facilitate greater understanding, SIMalliance has outlined some of HCE's interoperability challenges in the context of one of today's biggest contactless technology deployments, together with an exploration of the issues relating to after-market backwards compatibility.

6.1 QR code replacement

SIMalliance considers HCE to be most appropriate to low value non-critical application deployment. This is a sector that is widely served by QR codes today (e.g. coupons and boarding passes), which deliver a low convenience, awkward user experience due to the time it takes to align the barcode with the reader. HCE therefore may prove to be a valuable replacement for QR code utilisation. It has the potential to deliver similar service through a substantially enhanced user experience.

6.2 Transport

More than 30 countries around the world have deployed MIFARE© technology in their transport ticketing systems. This technology was developed and initially deployed in plastic cards that only served a single transport application. As a result, when the ticket is validated by a turnstile there is no requirement for the application to be selected by an application identifier (AID). The MIFARE technology, therefore, does not use AIDs in classic implementations, nor in some of its DESFire implementations. This is important because HCE solutions rely on the AID selection command to route the command and locate and trigger the appropriate NFC application in order to complete the transaction. This routing mechanism in HCE, which is based on an 'EXPLICIT' selection by an AID, therefore renders most MIFARE technology around the world as unusable by HCE solutions. In these circumstances, end-users would have to rely on a paper/plastic ticket instead.

Should this technical challenge be overcome in later versions of the Android OS, then usage of MIFARE would require a license agreement from NXP.

6.3 Access control

MIFARE technology is also widely used in the access control market. For the same reasons, the end-user will be able to transfer the functionality of his corporate or domestic access card to his NFC smart phone.

6.4 Backward compatibility with SE based NFC services

HCE transactions are entering the market at a time when a significant number of NFC SE-based solutions have already been deployed. This means that backward compatibility is required in order for these NFC SEs to operate in HCE-enabled smart phones. When an end-user changes their device and inserts an NFC UICC into an HCE enabled handset, a smooth transitional experience should be delivered, together with the continued operation of the NFC services that they previously used. This may be a challenge to achieve; there may be other applications in addition to MIFARE, which will need to be retrospectively adapted in the Android routing table mechanism in order to ensure their continued trouble-free operation.

7. Security of Android OS

7.1 Independent reports

In its current form, the security of HCE is dependent on the security of the underlying Android OS. In a recent report on digital security threats[7], the research arm of global security solutions provider McAfee, McAfee Labs, reported the following:

"To speak of malware that infects mobile devices is to speak of Android malware. Threats against other mobile operating systems, including Apple's iOS, are insignificant compared with malicious Android apps. This quarter [Q3/2013] *our count of Android malware grew by one-third, to more than 680,000 samples."*

As mobile attacks from hackers targeting the Android OS continue to increase, so does the likelihood that more vulnerabilities in the Android OS will be discovered, enabling data within the HCE application to be accessed, replicated or manipulated in such a way that it can be utilised for fraudulent activities.

Cisco's latest 2013 security report[8] reports that Android was the most attacked of all mobile platforms, with 99 per cent of all malicious software aimed at devices running Google's OS.

SIMalliance assessment:

SIMalliance encourages developers to store sensitive user credentials on the SE, not in an HCE NFC application.

7.2 Example technical vulnerabilities

Devices with root access (or those that are subject to a zero-day attack gaining root access) do not provide any substantial security mechanisms at all. Depending on the scenario, the user could themselves act as an attacker or, worse, remote attackers or other installed malware applications could gain access to information stored in applications using HCE.

Even in an un-rooted scenario, malicious HCE applications could try to reserve AID ranges of known payment applications in order to provoke Denial of Service (DoS) attacks. See Figure 2 below for more details on AID routing.

[7] McAfee Labs Quarterly Threats Report, Third Quarter 2013
[8] Cisco 2013 Annual Security Report

Cloud backup and storage services could contain critical credentials of HCE applications and could be a valuable target for attackers. Likewise, the credentials stored in an Android application which are used to gain access to a cloud backup or storage service could be subject to compromise. A SE-based system would not expose any credential data to such backup servers.

7.3 CLF Routing of AIDs

Figure 3: Examples of Implicit and Explicit AID applications in NFC

Aside from transport applications such as MIFARE or Felica most NFC applications are addressed by their AID. Until Android 4.4 was introduced with HCE, all NFC applications on the SE could communicate using contactless technology, since the contactless front-end (CLF), which acts as a gateway between the NFC antenna and the SE, would forward all communication to the SE directly without any host OS intervention.

In Android devices supporting HCE, however, the application selection command is first evaluated by the CLF. As a result, the CLF needs to parse a routing table in order to decide if the requested application is residing on the SE or on the Android host system.

If no entry is found in the CLF's routing table the HCE Android documentation defines a "default" routing, which is to the HCE-based application. This default routing is problematic for the SE as it contradicts the architecture proposed by GlobalPlatform, which also foresees NFC applets that are accessible via NFC right after download to the SE. With Android's HCE, all individual card services must be known and their AIDs must be declared to the operating system at the time of the wallet application's installation, which is not always possible given that (for example) payment cards could be added to a wallet on the fly.

The SIMalliance therefore requires mobile devices to use the SE as the "default" route in order to be compatible with the full variety of NFC applets which are already on the market.

8. Key technical recommendations

From this initial analysis of Android v4.4 and its support for HCE, SIMalliance offers the following technical recommendations:

- **Test thoroughly:** MNOs and service providers should thoroughly test both the coexistence of their own present and future NFC services and wallets together with HCE-based services (such as Google Wallet), to ensure there are no conflicts or misbehaviours.

- MNOs should request OEMs to implement default NFC routing to the SE.

SIMalliance assessment:

In order to distribute and manage valuable and/or sensitive credentials (payment, transport, identity, access) a secure component is necessary in the device as well as a secure management solution for the provisioning and management of such a secure component. This secure component and its corresponding management solution should be interoperable and agnostic to mobile OS platforms.