ABOUT CONSULT HYPERION

“Thought leaders in digital money and digital identity”

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

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

For more information, visit www.chyp.com

ABOUT THE GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors such as financial services and transport. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

The GSMA’s Digital Commerce programme works with mobile operators, merchants, banks, payment networks, transport operators and services providers to support the deployment of mobile commerce services. Alongside the mobile ecosystem, the programmes encourages collaboration, develops specifications and guidelines for technical implementations, and builds value propositions for adjacent sectors.

For more information, visit www.gsma.com/digitalcommerce
Executive summary

This paper is the latest in a series aiming to help interested organisations understand the opportunities and challenges represented by different mobile contactless payments options and supporting deployment models. The key deployment models are secure element (SE) based (handset-embedded or SIM-centric) and host card emulation (HCE). In the six months or so since the last paper, contactless payments have continued to mature in a number of markets and have been accompanied by several announcements that have impacted the deployment models for mobile contactless payments. The announcements and deployment models are explored in the paper.

Mobile contactless payments deployments cover all approaches

While Apple Pay has grabbed the headlines for near field communications (NFC), SIM-centric deployments continue to increase. Globally, there are now 67 live commercial services deployed that use the SIM for the secure element in mobile contactless. In several markets, mobile operators and banks are working collaboratively to bring a consistent set of services to market.

There are still limited HCE deployments, with most services limited scale pilots or trials. Notable exceptions are Australia, where two bands have live services, and Spain, where one bank has a live service. Banks in other markets are expected to follow later this year.

As with any emerging payment technologies, it takes time for a new approach to have a significant effect on spending. The infrastructure for the acceptance of payments needs to coincide with the wide-scale deployment of the means for making a payment. For contactless cards, this is starting to happen in lead markets, such as Australia, Canada, UK, France and Poland. For mobile contactless, evidence of significant transaction volumes is expected soon.

Like Apple and Android Pay, card scheme tokenisation services can be used with SIM-centric deployments

With the rollout of Apple Pay in the US at the end of 2014, Apple chose a traditional secure element and trusted third-party approach, using the card schemes’ token service providers (TSPs) in the role of the service provider trusted service manager (TSM). The scheme TSP model was followed by Google when announcing Android Pay in May 2015, although this uses HCE instead of a secure element to provide the payment application to NFC interface on the handset.

Android Pay is Google’s latest attempt to monetise retailer relationships through related loyalty and couponing functions in the new wallet. Apple is following the same route, extending Apple Pay to include non-payment retail functions.

In the mobile operator community, the SIM-centric approach of using the SIM as the secure element and a trusted third-party through a TSM hub or card scheme TSP seems to have been validated by the choices of Apple and Google. Through mobile operator collaboration, integration of the international card scheme TSPs has potential for a consistent global approach. SIM-centric deployments are continuing to grow in number and are particularly successful when the relationship between mobile operators and banks is a partnership (such as in Canada).

On Android, HCE remains a flexible choice for issuers

When bringing the Android Pay proposition to market, Google did not shut down other NFC solutions using HCE or secure elements in Android. Card issuing banks continue to have the option to implement their own HCE solution for mobile contactless payments that does not rely on Android Pay.
Being directly under issuer control, the HCE approach has limited commercial challenges and gives issuers complete control over user experience. This flexibility has significant implementation risks associated with what is likely to be a bespoke integration for their own environment. If an issuer has a mature mBanking application and internal expertise, then risks may be understood and mitigated. Without this experience, good integration partners will be required.

Issuing bank HCE solutions do not require scheme tokenisation. The market requirement for scheme tokenisation combined with HCE is unproven, as tokenisation is becoming part of the issuer domain for HCE. This is leading to some tension between the large issuers and the card schemes over the use of tokenisation for HCE and other use cases such as remote payments for e-commerce. It is expected that issuer tokenisation services will co-exist with scheme tokenisation and that some issuer TSPs will join handset vendor mobile contactless offerings.

**HCE does not address all payment scenarios**

HCE is still not fully defined for all payment scenarios for all schemes, such as offline transactions or in-app payments. In contrast to HCE, by using the secure element the SIM-centric approach offers a mature and well understood risk model providing support for the standard contactless transaction types and can be extended to support in-app payments. Unlike Apple, different SIM-centric deployments give issuers different controls over the wallet, branding and user experience, with the successes having a collaborative or partnership approach.

**Securely binding users to their device is essential for all approaches**

Fundamental to all approaches is the strength of the binding of the user to the device. The user must be the actual cardholder of the card and the owner of the device onto which payment credentials are loaded, regardless of whether the credential is stored on a secure element or in a host app. Early issuers of Apple Pay have seen significant fraud due to a lack of focus on strong procedures in this area.

As mobile operators are also customer-focused service providers, issuers with mobile operator partnerships can use these relationships to implement stronger authentication processes for HCE, with potential richer data relating to the mobile service subscriber. For example, mobile operators are extending the use of the SIM for more than payments, such as authentication with Mobile Connect.

**Mobile payments are not just NFC card payments**

In many markets, choices are also emerging within the broader mobile payments space that affect the attractiveness of mobile contactless on a given platform. Issuers are increasingly having a choice as to whether to offer contactless card payments for point-of-sale terminals, follow an in-app strategy from one or multiple digital wallet offerings, or, depending on the market, offer direct to bank account mobile payments.

These pressures mean that, even with the controls imposed by the handset manufacturers and card schemes, issuers have increasing discretion as to the type of service to offer their customers. Providers need to be realistic and not necessarily expect to build a strong business case from the payments use case alone.

**Assess the total cost to meet reach, risk and usability needs**

Each of the solutions has merits. This paper considers the similarities and differences in the deployment models and summarises the key features of each approach for side-by-side comparison. The choice for an issuer is dependent on the local market landscape, and its own capabilities and relationships. As with any new service driven by new technologies, it is important that all options are considered and that the total cost of meeting risk and usability requirements are comprehensively assessed for each option over the long run.

1 [http://www.mobileconnect.io](http://www.mobileconnect.io)
# 1. Introduction

## 1.1 Background

In July 2014, to help understand the differences in approaches between SIM secure element (SE) and host card emulation (HCE) services, the GSMA commissioned Consult Hyperion to produce a guide, “HCE and SIM Secure Element: It’s not Black and White”\(^2\). The guide was endorsed by MasterCard, UK Cards Association and the Mobey Forum. Following the publication of this guide, organisations asked for more information regarding the use of HCE and the discussion paper “HCE and Tokenisation for Payment Services”\(^3\) was released in November 2014. This provided a deeper analysis for banks and mobile network operators investigating the use of HCE and tokenisation within a mobile payment service.

Since November 2014, mobile contactless payments have matured in multiple markets and several developments have impacted deployments. The most notable of these developments are introduced and discussed in this paper, bringing the debate about HCE, tokenisation and related issues up to date, and illustrating the strengths and weaknesses of specific deployment options.

The remainder of this section provides a brief introduction to the terms used in this document.

## 1.2 Card emulation and host card emulation

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

Card emulation is the functionality to make an NFC equipped mobile phone act like a smart card. Prior to HCE, an actual smart card device (e.g. a secure element such as a SIM) was required to be accessible to the mobile phone and was used to store the card payment application. This is called “card emulation”. The payment app in the secure element provides transaction and risk logic such that the payment application itself is involved in the process of approving or declining a transaction. In this way, critical data is managed in the tamper-resistant environment of the secure element.

---

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

### 1.3 Credential management

HCE allows payment applications residing on the handset to emulate cards on the NFC interface. What HCE does not provide is the way to secure these applications in the absence of a hardware secure element. Since the security of payment data cannot be relied on in the same way as traditional card products or a secure element, alternative approaches to security are needed. These involve provisioning limited-use payment credentials into the app prior to each transaction for use in a single or controlled number of transactions.

Typically, payment credentials are the cryptographic keys linked to the card funding account that secure the payment transaction. Limited-use payment credentials are a particular type of payment keys (called session keys) which are only valid for a single transaction, as allowed for within the existing EMV payment specifications.

The mechanism to distribute payment credentials to mobile payment applications is called credential management. The organisation performing credential management may be the card issuer or an external service organisation.

### 1.4 Tokenisation

Tokenisation is the process of substituting the personal account number (PAN) with a single-use or limited-use “token PAN”, where use can be limited by the consumer device, channel or merchant. This reduces the impact of data breaches significantly—for example, the capture of PANs from the systems at one merchant would not impact any others. The aim is to make sure that if a token PAN is captured it will have little or possibly no value.

An organisation providing tokenisation services is called a token service provider (TSP). This can be a card scheme (such as Visa, MasterCard or American Express), an independent service organisation (such as a transaction processor) or a card issuing bank.

Tokenisation can be used for mobile contactless payments either when using secure element card emulation or when using HCE. Although recommended, tokenisation does not have to be used for these payments at all. For secure elements, PANs can be used directly in some models, while for HCE an issuer is free use their own security scheme that does not rely on external tokenisation providers (although the card schemes require the use of a dedicated PAN).
1.5 TSM hubs

A trusted service manager (TSM) securely provisions and manages payment applications and data onto secure elements. The TSM acts as the link between service providers and secure element owners. TSMs come in two flavours: service provider TSMs (SP TSM) that manage the payment application and data for card issuers, and secure element manager TSMs that manage the secure element. If each card issuer needs to create and operate its own SP TSM, costs may be prohibitive, especially for smaller issuers.

To simplify the provisioning of NFC payment applications and reduce costs, the concept of the TSM hub was created. The TSM hub acts as a common TSM available for issuers to connect to operators in a given market. The GSMA’s previous discussion paper “HCE and Tokenisation for Payment Services” looked at the approach in more detail.

For more detailed information on the technicalities of tokenisation and payment credential session keys for HCE, please see the GSMA discussion paper “HCE and Tokenisation for Payment Services”.

The remainder of this paper considers notable developments in different markets related to mobile contactless payments, describes current models for deployment options, and provides a high level comparison of the feature set and market needs of the choices available to issuers.
2. Market Developments

This section discusses notable market developments since the last paper and introduces the key themes resulting from recent market activity.

2.1 Secure element deployments continue

While Apple Pay has grabbed the headlines for NFC, SIM-centric deployments are increasing in number. There are now 67 live commercial services around the world that use the SIM for the secure element in mobile contactless. Among them, Vodafone Wallet⁴, Deutsche Telekom MyWallet⁵ and Orange Money⁶ are mobile operator-led examples that service a number of countries.

In several markets, mobile operators and banks are working collaboratively to bring a consistent set of services to market. Notable collaborative deployments include Enstream in Canada and Valyou in Norway.

Valyou is a mobile operator and bank collaboration that provides application provisioning services and a mobile wallet serving the Norwegian market. Valyou offers both a mobile wallet and TSM services for card issuers and mobile operators.

Enstream is a hub to provision mobile contactless payments. It has a flexible architectural model, splitting secure element management (SE TSM) from application management (SP TSM), and providing options for the subscriber user interface. Card issuers can deploy their own wallets or can use one of the wallet providers enabled by Enstream. Currently, there are two wallet providers – Suretap and Ugo. Suretap was created by Rogers and is now⁷ a separate company, promoted and supported by multiple mobile operators.

2.2 Scheme tokenisation has become real

Apple, which uses an embedded secure element (eSE) to secure the payment credentials, and the SIM-centric deployment models suggest the secure element and trusted third-party model holds as the ideal. This balances security and usability by using secure hardware to control payment credentials, thereby providing a risk model the same as contactless cards.

Deployments are simplifying the provisioning of applications by using hubs, either as collaborative TSMs for SIM-centric deployments (as previously mentioned) or via scheme TSPs in the case of Apple Pay (and the same is expected for Samsung Pay) where the TSP acts as an equivalent role to the SP TSM.

The commercial model for TSPs is causing some tension between schemes and issuers, as the issuers look to control costs of tokenisation over the medium term. To recover their costs, the scheme TSPs have fees associated with the provisioning and lifecycle management of tokens, or bundle these in with other services. For example, one cost component is a monthly fee per managed token.

If issuers operate the TSP in-house, then they can avoid this as an external cost. For larger issuers, taking the TSP in-house may generate a saving over outsourcing to the scheme. For small issuers, it may be cost effective to use the scheme TSP rather than develop their own. Although not allowed currently, commentators expect that mobile contactless deployments using the scheme TSP approach will allow issuer TSPs from the larger card issuers to be integrated into the service in the near future.

2.3 HCE using scheme TSPs

With the announcement of Android Pay at the end of May 2015, Google has followed the card scheme tokenisation route and is applying it to HCE. With Android Pay, a user registers a card, authenticates the request with the issuer in an issuer app and receives a tokenised card in an Android Pay cloud service against which payment credentials can be downloaded for POS use through HCE. Android Pay also enables in-app payments.

Although Android Pay is expected to gain some traction, issuers can still follow their own approach and deploy their own HCE mobile contactless payment solution (or join with an SE initiative).

There are a few live commercial HCE deployments, the most notable being in Australia where two banks have deployed solutions. This is expected to change in the second half of 2015 when banks in other leading contactless markets deploy solutions.

Probably the most interesting example is in Poland, where there are two potential collaborations: Visa and a group of banks have announced they are intending to bring an HCE solution to market later in the year and, probably more importantly, the mBanking venture Blik have announced their intention to support HCE at-POS payments in their apps. Blik is a successful mobile payments platform supporting payment online, in-store and P2P using the national inter-bank payment network to process transactions, rather than international card schemes.

2.4 Authentication is a challenge

Device and user authentication are the foundations of the security of all deployment models. Banks that have deployed second generation mBanking solutions have spent considerable effort achieving strong authentication of the device and user, while maintaining good usability. There is little standardisation of approaches across or within markets that do not have a history of collaboration. In these markets, banks can see customer authentication as a competitive issue and will want to control the process as much as possible.

If not addressed correctly, errors in the initial authentication of users can lead to significant fraud issues for banks. For example, fraud9 for Apple Pay has been associated with registration problems10 through the ‘yellow path’ process where banks processes are not suitably strong to stop attackers registering cards.

Once initial user registration and authentication is achieved, verification of users during a transaction is required. The convenience provided by an on-device user verification method using a biometric is playing an increasing role in mobile payment applications, not limited to Apple (for example, Google announced support for fingerprint in Android M), and also not just for fingerprint (for example, USAA Bank is successfully using face recognition for its mBanking logon, which is particularly popular with older demographics).

---

2.5 Usage data is not published

As transaction data is not advertised, current use of HCE, SIM-centric and Apple Pay services can be assumed to be relatively low. This is typical for new retail payment products, which need several years of growth to register a significant number of transactions.

While acceptance remains patchy and as consumers start to learn how to make payments using contactless cards, mobile contactless usage will likely remain low.

---

**TABLE 1: MOBILE CONTACTLESS ROLLOUT IN SELECTED MARKETS**

<table>
<thead>
<tr>
<th>Country</th>
<th>Contactless Infrastructure Rollout</th>
<th>Notable Mobile Contactless Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>POS: 40% (Q1 2015)</td>
<td>SIM: Cash by Optus</td>
</tr>
<tr>
<td></td>
<td>Cards: 48% (Q1 2015, 70% of population with card)</td>
<td>HCE: AMP bank, Commonwealth Bank of Australia</td>
</tr>
<tr>
<td>Canada</td>
<td>POS: 75% (2014)</td>
<td>SIM: Enstream, enabling Suretap, Ugo and Issuer wallets</td>
</tr>
<tr>
<td></td>
<td>Cards: 25% (2014)</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>POS: 30% (2014)</td>
<td>SIM: China Telecom, China Mobile, China Unicom</td>
</tr>
<tr>
<td></td>
<td>Cards: unknown</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>POS: 20% (Q1 2015)</td>
<td>SIM: Orange Cash</td>
</tr>
<tr>
<td></td>
<td>Cards: 30% (Q1 2015)</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>POS: 20% (2014)</td>
<td>SIM: NTT Docomo, SoftBank Mobile, KDDI Mobile</td>
</tr>
<tr>
<td></td>
<td>Cards: unknown</td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td>POS: 80% (Q1 2015)</td>
<td>SIM: DT MyBank, Orange Cash</td>
</tr>
<tr>
<td></td>
<td>Cards: 70% Visa cards (Q1 2015)</td>
<td>HCE: Visa and group of banks announce intention to trial in 2015, Blik (owned by six banks) announce intention to trial</td>
</tr>
<tr>
<td>South Korea</td>
<td>POS: 6% (2014)</td>
<td>SIM: KT Moca Mobile Wallet</td>
</tr>
<tr>
<td></td>
<td>Cards: unknown</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>POS: 39% (Q1 2015)</td>
<td>SIM: Orange Cash, Vodafone SmartPass</td>
</tr>
<tr>
<td></td>
<td>Cards: unknown</td>
<td>HCE: Bankinter, BBVA</td>
</tr>
<tr>
<td></td>
<td>Cards: 10% (2014)</td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>POS: 35% (Q1 2015)</td>
<td>SIM: EE Cash on Tap, Vodafone SmartPass</td>
</tr>
<tr>
<td></td>
<td>Cards: 33% (Q1 2015)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cards: unknown</td>
<td></td>
</tr>
</tbody>
</table>

---

11. http://9to5mac.com/2015/05/19/latest-apple-pay-banks-may/
3. Deployment models

This section illustrates each of the main deployment models for mobile contactless payments that use HCE or secure elements for the payment application. The models illustrate roles rather than specific technical interfaces. The information presented is from publicly available sources.

The key deployment models available today are:

- Android Pay – the approach adopted by Google for the recently announced Android Pay
- Issuer HCE – issuer implemented payment application using HCE
- Apple Pay – the approach used by Apple for its NFC services
- SIM-centric – typical approach for a mobile operator partnership mobile contactless payment deployment.

The Apple Pay model is expected to apply to other embedded secure element approaches offered by other handset manufacturers (for example, the Samsung Pay approach when it launches later this year).

To help to compare different approaches, deployment models are described within the context of the four-corner model of card payments to illustrate the roles in the ecosystem. The issuer maintains its relationship with a card scheme for the payment product issued. The card scheme runs the payment network providing the transaction acceptance relationships with merchants through acquirers (and transaction processors). The payment ecosystem model is common across all mobile contactless deployments for card payments. Other payment products (such as direct to bank account payments) or transactional products (such as for retail vouchers or transit tickets) would have a different ecosystem. However, as card payments are the major deployment for mobile contactless payments to date, the four-corner model is used.
3.1 Provisioning

Initially only available in the US, Android Pay\(^{13}\) is Google’s latest approach to support mobile contactless payments. Approximately one year ago, Google changed its original NFC service, Google Wallet, from using an embedded secure element to using HCE. Android Pay continues with the use of HCE for at-POS payments and provides a set of services to support the registration, management and use of payment credentials from partner card issuers. Android Pay also supports in-app payments directly from merchant apps.

In summary, Android Pay consists of:

- a handset user interface wallet app
- a set of cloud services to administer HCE payment card details, with associated APIs to expose Android Pay services to partners
- integration with card schemes’ TSPs to receive tokenised card details and perform lifecycle management (such as issuer cardholder identification and verification [ID&V] on registration)
- Google Play Services APIs on the handset, to expose Android Pay services to third party apps.

The Google Play Services for Android Pay are to be mandated in Android M, and made available for Android K. Cloud services are expected to be part of Google Play.

A card issuer (e.g. bank) joins Android Pay via a scheme (as per Apple Pay). Any transaction using Android Pay – in-app or POS – will be subject to the commercial terms between Google and the card issuer. The initial release of Android Pay includes loyalty and rewards integration with ‘select retailers’, continuing the existing Google Wallet relationships.

A cardholder registers a card with Android Pay, authenticates to the issuer via the scheme TSP, and gains a tokenised card in the Google cloud provided by the card scheme. This is then used to drive in-app payments and provision limited-use credentials for use through HCE at POS. Google is expected to provide payment credential management.

The anticipated deployment model for Android Pay is illustrated in Figure 1.

Limited details are available for the exact processes to support at-POS payments using NFC. While press releases state that Android Pay services include HCE NFC components for use at contactless POS, no details are available on the developer website\(^{14}\) specifically for POS. The following is a description of the expected processes.

Limited-use payment credentials are expected to be loaded into the Android Pay HCE components, and are generated for the cloud tokenised card. The security scheme used to secure transactions using these credentials is agreed by Google and the card scheme TSPs.

Like any HCE app, Android Pay will use an NFC/HCE API that is part of the operating system (available from Android 4.4 KitKat onwards). This is separate to the Android Pay itself, which is provided through Google Play Services API.

User verification in Android Pay will be able to use fingerprint sensors if available on the device (APIs for fingerprint sensors are to be built into the Android M operating system). When not available, user verification will require password or PIN entry. This means the user experience is not consistent across all devices. It is also worth noting that, although biometrics adds convenience, from a security point of view, biometrics are relatively weak on mobile devices.
(as they are tuned to favour usability) and the security for apps will continue to depend on the strength of the device authentication.

A bank can continue to issue HCE credentials in their own apps: these can be used via NFC at contactless POS without Android Pay involved, but the credentials cannot be used for Android Pay in-app. Similarly, secure element models (e.g. SIM-centric or Samsung Pay) are also outside Android Pay.

From a merchant point of view, a normal contactless card payment transaction is processed. This is unless the merchant is a ‘select retailer’ who has integrated their POS systems with the Google loyalty scheme. In this case, the approach (at least in the US) is to provide a one-tap experience to pay and update/redeem loyalty points. Demonstrations made by Google and Coca Cola showed that this requires a long tap that may cause usability issues.

Embedded into the device OS with the Google Play Service layer, Android Pay is likely to have a significant impact over time. It looks like it will add convenience, especially for remote in-app payments for non-virtual goods. Mirroring Apple Pay, Android Pay uses card scheme tokenisation as the link to bank products. However, the solution does not appear to be fully specified. At the time of writing, there is no detailed information available about POS payments on the Android Pay website, other than indicating they will be supported.
3.2 Issuer HCE

For an issuer HCE deployment, the issuer is responsible for all aspects of the solution—from application development through to limited-use payment credential management. The issuer is responsible for choosing the security scheme to be used in its HCE apps, within the requirements defined in the card scheme specifications, and the use of EMV tokenisation is optional. For more information on implementation approaches for HCE, see the GSMA paper “HCE and Tokenisation for Payment Services”.

The deployment model for issuer HCE is illustrated in Figure 2.

HCE NFC transactions accepted by merchants are directly equivalent to contactless card transactions, meaning issuers and acquirers have the same liability rules as cards (as defined by the card scheme) and merchants are offered the same settlement terms. In agreement with the scheme rules, issuers have to ensure that the card-present liability model matches their risk management policy for HCE transactions. Currently, offline transactions are not supported by card schemes. As it uses HCE at POS, these restrictions apply to Android Pay as well.

Customers download HCE payment apps to their devices from an app store in the same way as for any other app. Issuers must implement means to ensure the security and integrity of apps and payment credentials through the use of software hardening techniques. Third-party tools and services may be used to strengthen device and software authentication. Whatever methods issuers choose to harden apps, it is important that they make allowances for and undertake comprehensive testing, including security code reviews and penetration testing. Mechanisms will also be needed for regular app updates to adapt to new security threats.

Solutions are required to be certified by the scheme whose brand is associated with the app. Each deployment will have to be individually approved by the scheme. For HCE the approvals process is not yet clearly defined and mature. As such, for HCE it is likely to be subject to change for a while and the timescale for maturity for the approach is still several years.
3.3 Apple Pay

With Apple Pay, issuers are offered a packaged approach from Apple, via the card schemes’ tokenisation services. The ecosystem and user experience are managed and defined by Apple.

The deployment model for Apple Pay is illustrated in Figure 3.

The approach for mobile contactless payments has not changed markedly since launch and is as described in the discussion paper “HCE and Tokenisation for Mobile Payment Services”. The issuer joins Apple Pay through the card scheme but has a contractual relationship with Apple that defines the commercial terms (i.e. Apple’s transaction fee) and Apple’s audit entitlements.

The provisioning model is a static tokenised card, installed on the secure element in the handset. Apple manages the secure element. The card schemes provide the TSP and processing for tokenised transaction, before forwarding to the issuer.

The issuer does not have a choice for the user interface. The user registers cards and manages transactions through the Apple Wallet (the new name for Passbook), with user verification being required for all transactions regardless of value. User verification is achieved using on-device fingerprint with Touch ID. This is for convenience rather than security; the security for Touch ID falls back to PIN code entry.

Following Google’s lead, Apple has recently extended Apple Pay to include non-payment merchant transactions for loyalty and couponing.
3.4 SIM-centric

Using the SIM as the secure element is the typical mobile operator approach. A number of deployment models are available for SIM-centric depending on the partnerships and relationships that have developed in particular markets. The models allow direct provisioning of issuer payment applications onto the SIM through TSMs or a new approach using tokenised card credentials.

The direct provisioning method can be simplified using a TSM hub (as discussed in the first section). The TSM hub allows a bank to have a single connection to a TSM that serves multiple operators. The GSMA’s previous discussion paper “HCE and Tokenisation for Payment Services” considered the model for using TSM hubs.

While TSM hubs have started to be deployed in some markets, card scheme tokenisation service providers (TSPs) acting in the SP TSM role, have also emerged as a viable trusted service for card issuer payment credential management. For NFC, the initial suggestion from the card schemes as a simple mapping service that linked an issuer PAN to a virtual PAN stored on the secure element payment application. This developed into the more rounded concept of the tokenisation service provider where issuer PANs are converted to token PANs for use as the payment credential in the secure element payment application.

Tokenisation allows a more generic approach to protecting payment credentials to be applied to mobile contactless payments. It is worth noting that scheme tokenisation services apply to more than just the mobile contactless payments use case and will be used to improve the security of e-commerce and digital wallet transactions generally.

The SIM-centric model allows for scheme tokenisation in much the same way as for embedded secure element deployments, such as Apple Pay. This is illustrated in Figure 4. This model illustrates the use of scheme tokenisation. Other tokenisation service providers may exist, depending on the market.

The use of static tokenisation with the SIM-centric approach, making Apple Pay and the SIM-centric similar, can be seen as a logical step. The approach aims to:

- simplify the mobile card lifecycle management, especially for issuers that outsource these functions for physical cards
- allow issuers to connect to operators through the same tokenisation platforms (today proposed by the card schemes, but competitors are emerging) as other services.

Both models for SIM-centric provisioning (TSM hubs and scheme tokenisation) are valid and act to simplify, and thereby aim to reduce the cost of the provisioning process for issuers. The advantage of these types of collaborative approaches is the extended reach of the service to the customers of multiple operators, for payment applications that fit with the standard acceptance infrastructure, and offer a known and well understood security model.
3.5 Deployment model figures

**Android Pay NFC Payment Deployment Model**

**Apple Pay NFC Payment Deployment Model**

**SIM Centric with Scheme TPS NFC Payment Deployment Model**

**HCE NFC Payment Deployment Model**
4. Comparison

This section provides a comparison of the different approaches for mobile contactless payments introduced in section 3. It gives a high-level view and highlights the key differences between the options, covering aspects such as costs, usability, risk management and card issuer control.

4.1 Solution features

The fundamental solution component, and the key differentiator between mobile contactless solutions, is how payment credentials are managed over the life of the payment application for funding card account. A mobile contactless transaction uses a payment credential to perform a payment. In an HCE solution (either Android Pay or issuer HCE), credentials are dynamic, and normally require a unique credential (such as a session key) for each transaction to be stored on the handset prior to the transaction. With secure element mobile contactless payments, a static credential is installed once on the secure hardware in the secure element for the life of the payment application. The differences in these approaches have implications for usability.

However, although done at different frequencies, both of the aforementioned approaches require equally strong identification and authentication of the user and strong authentication of the device and application for when the credential is stored. The combination of these authenticated elements is referred to as binding. The mechanisms available to perform binding depend on the approach. The options available for Android Pay and Apple Pay are specified by Google, Apple and their schemes’ TSPs. These may not be as flexible or as strong as an issuer would choose for its own solutions. A SIM-centric approach offers a secure hardware token as part of the authentication, and may allow additional mobile operator subscriber data for verification to be used.

The different storage locations for payment credentials have influenced the card schemes in their risk management selections for the allowable transaction types. The current card scheme specifications for HCE do not allow for offline transactions and do not specify what the options are available for point of sale transactions. Transit transaction with HCE will require specific certificates to be installed at transit terminals.

The key features when comparing solutions are:

- Binding – who controls user, device and app binding
- Credential provisioning – how frequently does a credential need to downloaded, how often is the user authenticated
- Wallet – who provides the user interface to authenticate the user
- Transaction types – what types of contactless payment transactions are available
- Lifecycle management – who provides customer support for lifecycle events, such as lost and stolen devices
- Additional service – what additional non-payment services are provided and by who.

These aspects are summarised in Table 2 for each of the mobile contactless approaches considered in this paper.
Apart from the fact that it is the only solution on iPhones, one of the main attractions of Apple Pay is that the issuer has a defined integration point with card schemes’ TSPs. This has made for a relatively straightforward integration for issuers. As such, the approach has been adopted by Google for Android Pay, using scheme TSPs as the interface to issuers. A similar approach is available with SIM-centric deployments that use TSM hubs or scheme TSPs to simplify the integration required.

The drawback of this defined integration approach is a potential lack of flexibility, leading to poorly implemented processes or ‘locked-in’ solutions with vendors and scheme TSPs. For example, the fraud experienced with ‘yellow path’ customer authentication on Apple Pay (section 2.4) is down to poorly implemented procedures and systems.

So, while providing flexibility and protection against lock-in, the most complex approach is for an issuer to implement their own HCE solution. However, even with a relatively long list of vendors offering specific components in the solutions, with some claiming to offer end-to-end solutions, any deployment is likely to be a significant development and integration exercise. Implementation complexity increases the likelihood of budget and timescale overruns.

HCE (both Android Pay and issuer HCE) is not fully defined for all payment transaction types for all schemes. For example, offline transactions are not supported, support for open-loop transit is yet to be deployed and, in offline PIN markets, the process for cardholder verification for higher value transactions is not standardised across schemes. These features are discussed further in the GSMA paper “HCE and Tokenisation for Payment Services”.

### TABLE 2: MOBILE CONTACTLESS PAYMENTS SOLUTION FEATURE COMPARISON

<table>
<thead>
<tr>
<th></th>
<th>ANDROID PAY HCE</th>
<th>ISSUER HCE</th>
<th>APPLE PAY ESE</th>
<th>SIM-CENTRIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding</td>
<td>Google Play</td>
<td>Issuer specific (e.g. mBanking, if available)</td>
<td>Apple iTunes</td>
<td>Mobile operator SIM. Can link to mobile operator subscriber data.</td>
</tr>
<tr>
<td>Payment credential provisioning</td>
<td>Tokenised PAN and dynamic payment credentials</td>
<td>Alias PAN and dynamic payment credentials</td>
<td>Static tokenised PAN</td>
<td>Real PAN or static tokenised PAN</td>
</tr>
<tr>
<td>Wallet</td>
<td>Android Wallet from Google</td>
<td>Issuer Wallet (mBanking app)</td>
<td>Apple Pay Wallet (Passbook) from Apple</td>
<td>Wallet from mobile operator or from issuer (depends on deployment)</td>
</tr>
<tr>
<td>Transaction types</td>
<td>Online only, open-loop transit yet to be standardised</td>
<td>Online only, open-loop transit yet to be standardised</td>
<td>All EMV contactless</td>
<td>All EMV contactless</td>
</tr>
<tr>
<td>Lifecycle management</td>
<td>Android device manager</td>
<td>Issuer controlled</td>
<td>Apple iCloud service</td>
<td>Linked to mobile operator service support</td>
</tr>
<tr>
<td>Additional services</td>
<td>In-app payments, Google retailer loyalty and couponing</td>
<td>Integrated with mBanking</td>
<td>In-app payments, Apple retailer loyalty and couponing</td>
<td>Mobile operator partner services (in-app payments and retailer services)</td>
</tr>
</tbody>
</table>
As mentioned, problems do occur during the lifecycle of payment products, and as such a solution must include suitable customer support. This is particularly important for issuers, as they are the only organisation accepting financial liability for the payment products deployed.

Arguably, the most sophisticated approach for customer support can be achieved in the SIM-centric approach by issuers and mobile operators working in partnership. As service providers, mobile operators are geared up to support customers through integrated call centres. Unlike vendors, whose customer channel continues to be via Internet self-service web forms. Linked call centre support can be important for customers who have general purpose payment products funded from their bank accounts.

### 4.2 User experience

Google and Apple prescribe the user experience, within the constraints of the card schemes, as they mandate the user interface (wallets). This leaves little scope for issuers to control how the cardholder interfaces with their products. The user experience aspects of each solution can be summarised as in Table 3.

#### Table 3: Payment User Experience Comparison

<table>
<thead>
<tr>
<th></th>
<th>Android Pay HCE</th>
<th>Issuer HCE</th>
<th>Apple Pay ESE</th>
<th>SIM-Centric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction start</td>
<td>Unlock phone, app on by default</td>
<td>Unlock phone, start app running</td>
<td>Double-click homescreen to wake, app on by default</td>
<td>No interaction if default application, may need to unlock and start wallet app running if CVM required</td>
</tr>
<tr>
<td>Transaction control</td>
<td>Google</td>
<td>Under issuer control</td>
<td>Apple</td>
<td>Issuer specified within mobile operator wallet</td>
</tr>
<tr>
<td>Transaction CVM</td>
<td>CVM entered in Android Pay user interface, fingerprint to be available in Android M depending on device</td>
<td>No CVM, online PIN at POS, on-device CVM (if available) or specific online cryptogram</td>
<td>Apple CVM - Touch ID all transactions, can be pre-entered</td>
<td>Standard EMV contactless options (No CVM, online PIN at POS or consumer device CVM)</td>
</tr>
</tbody>
</table>

In terms of usability, the offerings are quite similar. The main difference is the availability of the EMV cardholder verification methods (CVMs) for the payment transaction. The full set of EMV features is available using a secure element (e.g. local verification of passcode or m-PIN) but not with HCE. The options were discussed in more detail in the GSMA paper “HCE and Tokenisation for Payment Services”.

Both the secure element and HCE approaches can allow for the ‘no CVM’ option for lower value payments (as per a contactless card). In contrast, Apple Pay does not allow the no CVM option for any value of transaction, requiring the use of fingerprint verification for all transactions. This caused transactions to be very slow (approximately one second) in the first instance, leading to Apple updating its approach in the latest iOS to allow the fingerprint to be verified prior to the transaction.
4.3 Needs analysis

In addition to the types of features that must be supported by a mobile contactless payments solution, a card issuer needs to have a compelling business case. For most participants in the transaction value chain, including many card issuers, a business case for a payment product is based on having a large number of transactions, as the margin on each transaction is very low.

For mobile contactless payments, a compelling business case has best chance of being delivered when the card issuer can:

- reach a significant proportion of its customer base
- best promote its brand to be the customers’ choice for transactions
- understand and control the risks associated directly with transactions
- integrate the technology solution with a low impact on its own systems
- control the costs of the service as it develops over time
- make allowance for the implementation risks resulting from the lower levels of maturity of new technology or a new implementation approach.

These aspects are summarised in the Table 4 for each of the mobile contactless approaches looked at in this paper.

### TABLE 4: COMPARISON OF MEETING ISSUER NEEDS

<table>
<thead>
<tr>
<th></th>
<th>ANDROID PAY HCE</th>
<th>ISSUER HCE</th>
<th>APPLE PAY eSE</th>
<th>SIM-CENTRIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reach</td>
<td>Integrated into Play APIs for Android M. Made available for Android K</td>
<td>NFC handsets from Android 4.4 upwards</td>
<td>Single handset. Currently, limited to iPhone 6/6+. Penetration market dependent</td>
<td>NFC compliant (non-Apple) handsets</td>
</tr>
<tr>
<td>User Experience Control</td>
<td>Google</td>
<td>Issuer</td>
<td>Apple</td>
<td>Mobile operator or issuer</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Dynamic limited-use credential</td>
<td>Dynamic limited-use credential</td>
<td>Local payment keys on SE</td>
<td>Local payment keys on SE</td>
</tr>
<tr>
<td>Ease of Issuer Integration</td>
<td>APIs to scheme TSP and Android Pay</td>
<td>Issuer implemented</td>
<td>APIs to scheme TSP</td>
<td>APIs to TSM hubs or APIs to scheme TSP</td>
</tr>
<tr>
<td>Cost</td>
<td>TSP fees, credential Management fees, Google transaction fees (currently zero)</td>
<td>Credential management fees</td>
<td>TSP fees, Apple transaction fees</td>
<td>TSM fees, mobile operator fees</td>
</tr>
<tr>
<td>Maturity</td>
<td>Currently being defined, yet to rollout. Initially, only US</td>
<td>Limited live services, mostly experimentation</td>
<td>Standard TSM/SE model with scheme tokenisation, expanding out from the US</td>
<td>Standard TSM/SE model, live in many markets</td>
</tr>
</tbody>
</table>
Card scheme specifications for HCE remain immature. As stable certification and approvals for HCE apps is some way off, the secure element remains a better understood platform for mobile contactless.

No solution provides complete coverage for an issuer’s customer base. Issuers have to decide which of the options they will support, basing their choice on the services that meet their requirements best. Mutually beneficial relationships can play a key part here.

Issuers control over their brand is best achieved through an issuer’s own HCE offer. However, HCE is likely to require significant new technology integration and internal expertise. Many issuers will not be in a position to undertake such an integration and will look to outsource as much as possible. In this case, integration with mobile operators and TSM hubs, or handset vendor offerings and scheme TSPs (e.g. Android Pay, Apple Pay) are likely to offer the easiest approach.

In most industries, having a number of deployment choices leads to more competitive pricing. To an increasing extent this is the case for mobile contactless, where there are now a number of options for issuers on the Android platform. To promote Android Pay and establish traction in the market, TSP services from some of the card schemes do not currently carry any charges (if transactions are processed through the scheme) and in the initial US release Google is reported not to be including an issuer transaction fee for participants. This is noticeably different to Apple Pay which has widely reported issuer fees in the US. The Google approach may have a knock-on effect on Apple Pay, with some industry commentators suggesting that the current issuer transaction fee will not last.

The underlying business model for Apple and Google is not payment service related. The revenue from Apple Pay is significant in as much as it may cover the costs involved (through fees and potential savings), but Apple’s focus appears to be to make their handsets more functional and desirable, to continue to have significant handset sales. As with their other services, Google’s focus for Android Pay appears to be on monetising data through advertising. This allows them to launch without transaction fees. In contrast, card scheme revenue is directly related to transactions and becoming leading TSPs should enable them to add significant revenue to their network services over time.

In many markets, choices are also emerging within the broader mobile payments space that impacts on the attractiveness of a mobile contactless platform. More issuing banks are needing to choose whether to offer contactless card payments at POS, use an in-app strategy from one of the digital wallets, or offer direct to bank account mobile payments, depending on their market. These developments suggest that it is not just directly comparable approaches for NFC that will affect future pricing of services.

Probably, the most significant new cost element for issuers of HCE solutions is the provision of dynamic limited-use payment credentials. These need new systems if issuers are to manage this themselves or adds new costs (often charged on a per-seat basis) from credential management service providers. The lifetime costs of providing this service across all users (both the very active and less active) need to be carefully considered by issuers. As live services are very thin on the ground currently, cost metrics are unclear. Therefore, it is not obvious that this approach has advantages over the traditional method of static credential download to a secure element.

The pressures described mean that issuers have increasing discretion as to the type of service to offer its customers. For the incumbent card issuers who offer bank accounts, the mobile contactless payments use case is unlikely to be the killer service that results in significant churn if not offered. Providers need to be realistic in their pricing and consider more than just payment for the business use case.

4. Conclusions

While the pace of change for mobile payments is seen to be increasing in many markets, it has taken time for emerging payment technologies to have a significant effect on spending. For example, in the UK contactless cards and terminals started rolling out in 2007, and it is only in the last year that a significant number of transactions have been achieved. The same is true in more successful markets such as Canada and Australia. The infrastructure for the acceptance of payments needs to coincide with the wide-scale deployment of making a payment.

Like Apple and Android Pay, scheme tokenisation services can be used with SIM-centric deployments

The rollout of Apple Pay in the US at the end of 2014 refocused interest on mobile contactless payments. Apple chose a traditional secure element and trusted third party approach using the card schemes' TSPs. The model of using scheme TSPs was followed by Google when announcing Android Pay in May 2015, although this uses HCE instead of a secure element to provide the payment application to the NFC interface on the handset.

Android Pay is Google's latest attempt to monetise retailer relationships through related loyalty and couponing functions in the new wallet. Apple is following the same route extending Apple Pay to include non-payment retail functions.

In the mobile operator community, the SIM-centric approach of using the SIM as the secure element and a trusted third party through a TSM hub or card scheme TSP seems to have been validated by the choices by Apple and Google. Through mobile operator collaboration, integration of the international card scheme TSPs has potential for a consistent global approach. SIM-centric deployments are continuing to grow in number and are particularly having success where mobile operators and banks are partners.

HCE on Android remains a flexible choice for issuers

When bringing the Android Pay proposition to market, Google did not stop other NFC solutions using HCE or secure elements in Android. Card issuers still have the option to implement their own HCE solution that does not rely on Android Pay.

Under issuer control, the HCE approach offers limited commercial challenges and gives issuers complete control over user experience. Alongside this flexibility is the significant risk associated with a bespoke integration into their environment. If an issuer has a mature mBanking application and internal expertise, then risks may be understood and mitigated. Without this, quality integration partners will be required.

Scheme tokenisation is not required for issuer HCE and the market requirement for scheme tokenisation combined with HCE is unproven. Tokenisation is becoming part of the issuer domain for HCE which is leading to some tension between the large issuers and the card schemes for HCE and other use cases, such as e-commerce payments. It is expected that issuer tokenisation services will co-exist with scheme tokenisation and that some issuer TSPs will join handset vendor mobile contactless offerings.

HCE does not address all payment scenarios

HCE is not fully defined for all payment scenarios for all schemes, such as offline transactions or in-app payments. Unlike HCE, by using the secure element, the SIM
centric approach offers a mature and well understood risk model provide support for the standard contactless transaction types and can be extended to support in-app payments. In contrast to Apple, different SIM-centric deployments give issuers different controls over the wallet, branding and user experience, with the successes having a collaborative or partnership approach.

Securely binding users to their device is essential

Fundamental to each approach is the strength of the binding of the user to the device. Users must be the cardholder and the owner of the device into which payment credentials are loaded, regardless of whether the credentials are stored on an SE or in a host app. Initial issuers offering Apple Pay have experienced significant fraud due to a lack suitable procedures.

As mobile operators are also customer-focused service providers, issuers with mobile operator partnerships can use these relationships to implement stronger authentication processes for HCE, with potential richer data relating to the mobile service subscriber. For example, mobile operators are extending the use of the SIM for a wider set of applications than just payments through Mobile Connect.

Not just NFC card payments

Choices are also emerging within the broader mobile payments space in many markets that affect the attractiveness of mobile contactless on a given platform. Issuers are increasingly having a choice as to whether to offer contactless card payments for POS, or whether to follow an in-app strategy from one or multiple digital wallet offerings or, depending on the market, offer direct to bank account mobile payments. These pressures mean that, even with the controls imposed by the handset manufacturers and card schemes, issuers have increasing discretion as to the type of service to offer their customers. Providers should not count on a strong business case from the payments use case.

Review the total cost to meet reach, risk and usability needs

Each solution covered in this paper has merit. The paper considered the similarities and differences in the deployment models and summarised the key features of each approach for side-by-side comparison. The issuer’s choice is dependent on the local market landscape, and its own capabilities and relationships. All options should be considered and the total cost of meeting risk and usability requirements should be comprehensively assessed for the long-term, as with any new technologies.