The future of contactless mobile payment: with or without Secure Element?

By Sylvain Godbert, mobile payment and security expert at Nextendis

By Jean-Philippe Amiel, director of Nextendis

February, 2015

Introduction

POS terminals accepting contactless payment are being extensively deployed across Europe. In 2014, contactless cards can be used at 2 million merchant locations worldwide[1]. The number of contactless transactions across Europe more than tripled between 2013 and 2014[1].

Today most of the latest smartphones have NFC (contactless) capabilities and can therefore offer contactless payment services. According to the latest research by Strategy Analytics[2], contactless mobile payments by NFC-enabled mobile handsets are expected to account for $130 Billion in worldwide consumer retail spending by 2020.

It seems today that there is no obstacle to the massive rollout of contactless mobile payment services. However, despite the numerous pilots that have been launched in the last years, the payment industry is still searching the way forward toward large scale deployments across the globe.

This white paper analyses the evolution of the contactless payment ecosystem over the last decade and investigates possible developments for its future. After a first generation of contactless mobile payment using the Universal Integrated Circuit Card (UICC) as a Secure Element (SE), distinct trends appeared recently and are gaining strong momentum: Google's Android OS proposing a Host Card Emulation (HCE) architecture without SE and Apple pushing Apple Pay, its mobile payment service relying on an embedded SE in the mobile phone. So, will the future of the contactless mobile payment be with or without SE?

[1] Source : http://newsroom.mastercard.com/press-releases/european-contactless-momentum
[2] Source: https://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5628

The emergence of the UICC-based model

The first contactless mobile experiments started in the mid-2000s and led to the inclusion of an NFC controller chip and an RF antenna inside mobile phones, providing contactless communication and connection to a chip-based Secure Element (SE) hosting contactless applications.

From there, several architecture options were developed to emulate a payment card in a mobile phone. All these approaches were based on a chip-based SE, able to provide a tamper-resistant environment to host the Mobile Payment Application (MPA) and its sensitive data.

The main telecoms and payment industry actors joined forces and defined an open and standardized SE architecture, through the GlobalPlatform Card specifications. Additionally, GlobalPlatform Messaging specifications were also developed to connect, through standardized interfaces, the back-office systems, the mobile phones and the SE, for the deployment of NFC services in a mobile phone environment.

Three types of SE implementations have been used so far, based on:

- Universal Integrated Circuit Card (UICC) under Mobile Network Operator (MNO) control.
- Embedded Secure Element (eSE) under handset manufacturer control.
- Secure Memory Card (SMC) with or without NFC controller under Service Provider (SP) control.

While these three implementations provide a similar environment for hosting the MPA from a functional and a security standpoint, they involve different organizations and lead to different business models. For instance, deploying the MPA onto the UICC requires issuing banks (Issuers) to work collaboratively with MNOs. Alternatively, deploying the MPA onto the eSE, requires agreements between Issuers and mobile phone manufacturers.

Supported by important MNO investments, the UICC-based model quickly became the most widespread implementation in the last decade. This model gave to MNOs a key position in the contactless mobile payment ecosystem: as UICC owners they were the inevitable entry point for "Over-The-Air" (OTA) management of the UICC and the applications hosted in the UICC. This situation led to the introduction of two new roles:

- The SEI[3] TSM (called here MNO TSM) manages, on behalf of the MNO, the UICC contents and installation of UICC applications.
- The SP TSM handles, on behalf of the Issuer, the secure and confidential personalization of the MPA into the UICC.

In the UICC-based model, the contactless MPA emulates a contactless payment card. Hence, like contactless payment cards, MPA implementations are payment scheme specific and support Mag Stripe Data (MSD) transactions only (in the US market) or both EMV and MSD transactions (in the rest of the world).

Some MNOs have developed mobile wallets which support all the mobile contactless applications and in some cases with an already present prepaid card: Vodafone's SmartPass™, Deutsche Telekom's MyWallet, etc.

[3] SEI : Secure Element Issuer

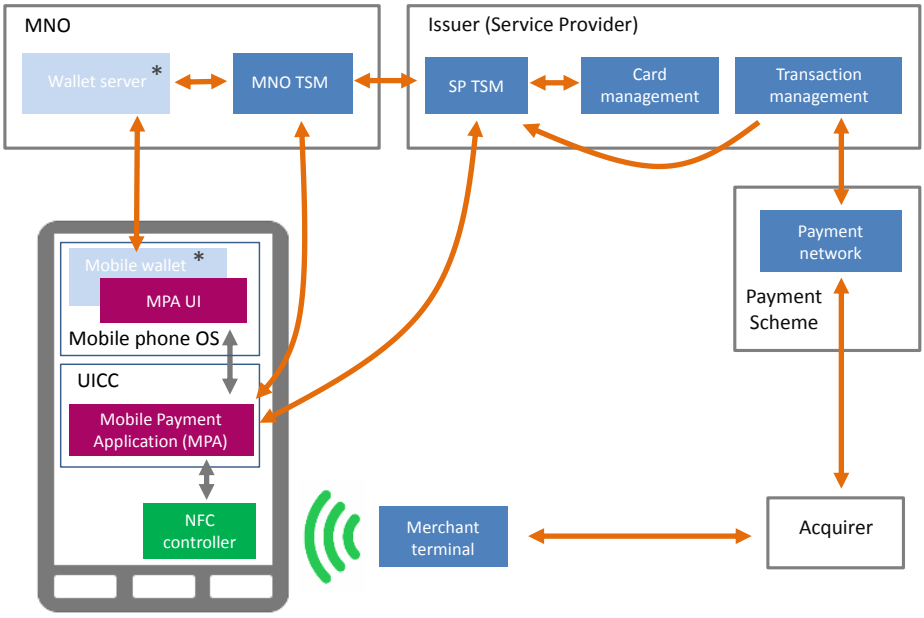

Figure 1 : Overall architecture of the UICC-based model for contactless payment transactions

(*) MNOs do not necessarily need to implement a wallet for contactless applications.

This model requires strong collaboration between different types of actors of the ecosystem at technical, commercial and branding levels: MNOs (and TSM providers), Issuers (and payment schemes), handset manufacturers (and mobile OS providers). For the Issuer, deploying UICC-based contactless payment services requires commercial agreements for the use of the UICC with each MNO. In addition, the Issuer usually contracts TSM services from a 3rd party (as OTA technology is only mastered by few companies, such as SIM vendors).

Google HCE and EMV Tokenization initiatives: moving to a cloud-based payment model without SE

Google announced in October 2013 the support of “Host Card Emulation” (HCE) functionality in Android v4.4 KitKat, allowing an Android application to emulate a contactless card and to communicate directly with a contactless reader.

The release of HCE paved the way to a new approach for developing contactless services. This new architecture removed the dependencies that were created in the SE-based model as any service provider was able to roll out independently contactless mobile services, without requiring the usage of a SE and a TSM platform. This was seen as a new opportunity by some services providers for which security was not of a paramount importance (e.g. retailer loyalty programs and coupon distribution).

One might have thought that payment services would not embrace this architecture as the MPA is no longer hosted in a tamper-resistant chip-based SE, but in the mobile operating system, a more vulnerable environment. Nonetheless, in an interesting turn of events, major payment schemes (VISA, MasterCard and American Express) announced in February 2014 their support for "cloud-based payment" on HCE mobile phones through the release of new specifications and subsequent trials. However, in order to provide an acceptable level of security and usability, the payment industry had to rethink the entire mobile payment transaction flow.

For cloud-based payment on HCE mobile phones, payment transactions were amended to integrate cloud-based security mechanisms and a new type of token-based transactions was specified, valid both for contactless and remote payment transactions.

> ***Cloud-based payment*** *is an approach in which the payment credentials used to perform transactions are provided by a remote server (in the cloud) to the mobile application and are dynamically provisioned into the MPA before each transaction (or set of transactions).*

In order to offer an improved protection of the cardholder account data located on the mobile phone against counterfeit and account misuse, the payment industry also developed the concept of Payment Tokenisation.

> ***Payment Tokenisation*** *is a mechanism standardized in EMVCo’s “Payment Tokenisation Specification”. It allows replacement of the cardholder’s Primary Account Number (PAN) by a surrogate value (named a Payment Token), which is used in place of the PAN in payment transactions.*

Payment Token is restricted to a particular domain of use and can be generated for a dedicated payment channel, consumer device or merchant. Nonetheless, Payment Token is not unique to one transaction. Usage of Payment Tokens prevents the risk of the cross-contamination of fraud between payment channels, consumer devices and/or merchants.

Transaction security is ensured by a Token Cryptogram, which is a transaction-unique cryptogram generated by the MPA using the Payment Token and additional transaction data. The Token Cryptogram is sent with the Payment Token in an authorization message instead of the Application Cryptogram used in EMV transactions, or instead of the dynamic Card Verification Value (CVV) used in MSD transactions.

Token-based transactions require a new actor, the Token Service Provider (TSP), to carry the following roles:

- **Token-PAN mapping management**: ensures the tokenization/de-tokenization of PANs/Tokens during authorization, clearing and chargeback.
- **Transaction management**: verifies the Token Cryptograms during online authorization requests.

- **Account management**: handles the enrolment of the user to the cloud-based services, including an Identification & Verification (ID&V) process and the assignment of Payment Tokens in place of the cardholder PAN.
- **Credential management**: provisions the MPA with Payment Tokens and other limited or single use cryptographic keys used to generate Token Cryptograms.

Payment networks have naturally positioned themselves as the TSP but other providers will likely emerge and propose these services (or part of them). The main payment schemes have announced they will waive token service fees until the end of 2015. It is however predictable that a business model based on transaction fees will be proposed to finance TSP services in the near future.

For contactless payment, token-based transactions can be executed without requiring updates on the existing contactless merchant POS infrastructure. Integration effort for Issuers is required primarily for interfacing with the TSP.

It is important to note that offline authorizations are not supported, as the cloud-based payment model requires a systematic check of the Token Cryptogram by the TSP at each payment transaction. Payments transactions shall therefore always be authorised online.

Cloud-based payment also simplifies the provisioning process of the MPA that can be initiated simply from the cardholder account data.

> ***Card Digitization*** *is the process of creating a virtual card - Digitized Card - from an existing plastic/chip credit/debit card into a Digital Wallet. On HCE mobile phones, Card Digitization leads to the provisioning of cardholder account data and cryptographic keys into the MPA, enabling both contactless and remote payment transactions.*

In the cloud-based payment architecture, Card Digitization is usually performed by the Wallet Service Provider in association with the TSP and the Issuer. The Digitized Card data (i.e. cardholder account data, Payment Token, cryptographic keys, etc.) are provisioned into the Credential management system of the TSP and the noncritical elements are downloaded into the MPA. The payment schemes and group of Issuers are developing propositions where they hold the role of Wallet Service Provider.

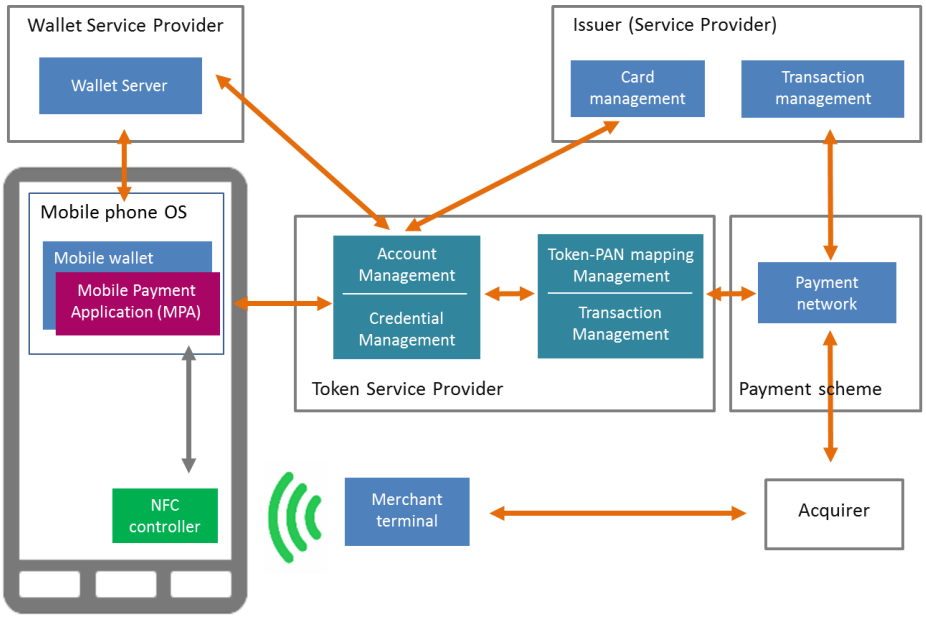

Figure 2 : Overall architecture of the cloud-based model for contactless payment transactions

The Apple Pay initiative: Combining tokenization and SE-based model

This panorama would be incomplete without mentioning the recent Apple Pay initiative, which launched in the US in October 2014, with discussions on-going for a service launch in many countries in Europe.

This new services allows Apple's devices owners to get a Digitized Card into their Apple's Passbook for performing in-app and contactless payments at participating merchants. The services is currently supported on iPhone 6 and iPhone6 Plus, and should be extended later on to iPad Air 2, iPad mini 3 and Apple Watch.

As one can expect, this new service is well integrated into the Apple ecosystem, providing a simplified onboarding process for cardholders and for Issuers.

Users can enrol by themselves to the Apple Pay service by adding one or more credit/debit cards into Passbook, Apple's wallet application. Payment Tokens are used making the Card Digitization process quite simple: the user can either select the credit/debit cards already in his/her iTunes account or add another credit/debit card by taking a picture of the card or manually entering his/her cardholder account data. This selected card must be an eligible card issued by a bank that contracted to Apple Pay services. Apple has announced so far partnerships with American Express, MasterCard, Visa and some major US Issuers.

For Issuers, contracting with Apple Pay means that, in exchange for transaction exchange fees paid to Apple and once connected to the Apple platform, all their cardholders owning a compatible Apple device can create a digitized version of their payment card and use it for in-app and contactless payments at participating merchants.

For in-app payments, this requires e-commerce merchant apps to integrate Apple Pay's check-out process. For in-store contactless payments, Apple Pay is expected to work at any merchant terminal equipped with contactless POS terminals.

Each payment transaction requires a systematic user authentication using Apple's fingerprint authentication mechanism (Touch ID).

The solution architecture relies upon an eSE-based architecture associated with the Payment Tokenization framework:

- The MPA is hosted on an eSE.
- A SEI TSM allows the provisioning of the MPA into the eSE.
- The Account Management platform interfaces the different Issuers with the Apple Pay platform and enables the Card Digitization process.

In the US, where the service has been launched, Apple Pay is known to support only online transactions. No public announcement has been made regarding the future support for offline-authorized transactions in Europe. While this restriction is not an issue in the US (online transaction is the rule in the US market), it could generate acceptance glitches in some countries in Europe where some merchants may still have offline-only capable terminals.

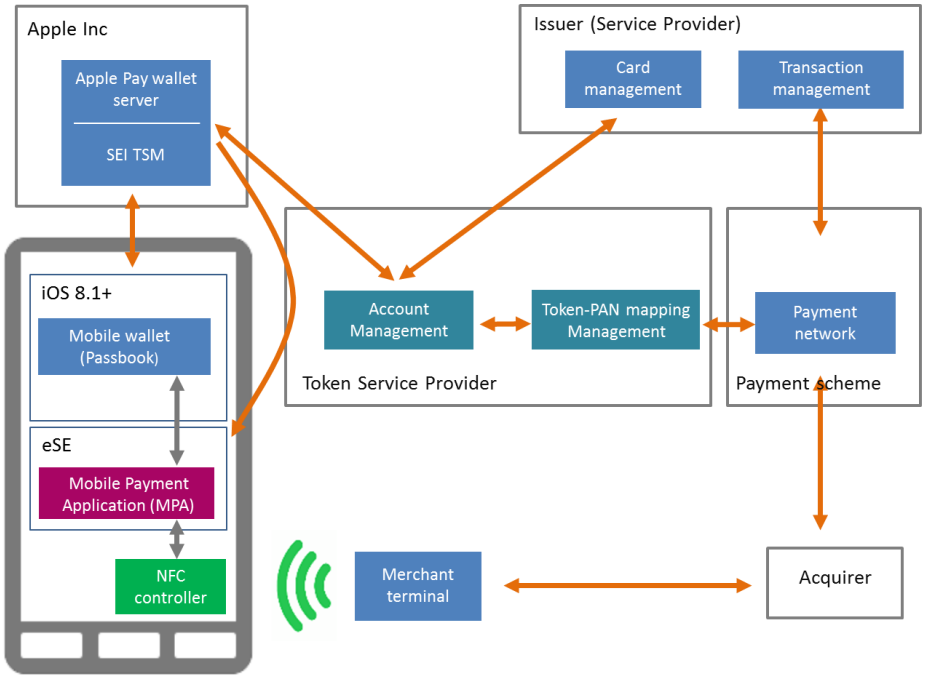

Figure 3 : Overall architecture of the Apple Pay model for contactless payment transactions

Comparison summary of the security framework of the 3 architecture models

The following table lists the main security characteristics for each model.

		UICC-based model	Cloud-based model on HCE devices	Apple Pay's eSE-based model
MPA hosting		In the UICC	In the mobile OS (optionally with white box cryptography)	In the embedded SE
Sensitive data & keys hosting	**Inside the mobile phone**	In the MPA : • PAN + cardholder account data • EMV & MSD cryptographic keys • Mobile PIN	In the MPA : • Tokenized PAN + cardholder account data • Single use or limited use cryptographic keys	In the MPA : • Tokenized PAN + cardholder account data • Single use or limited use cryptographic keys In a "secure device area" • Fingerprint pattern
	In the cloud (*)	Online PIN (Issuer)	Mobile PIN (TSP) PAN (TSP) Single use or limited use cryptographic keys (TSP)	PAN (TSP) Single use or limited use cryptographic keys (TSP)
Cardholder Authentication		Optional: no CVM for transaction below a certain limit	Mandatory: CVM for every transaction)	Mandatory: CVM for every transaction
Supported CVM		Online PIN (verified by Issuer) or Mobile PIN (verified by MPA)	Mobile PIN (verified by TSP)	Fingerprints (Touch ID)
Authorization cryptogram		Application cryptogram (verified by Issuer)	Token Cryptogram (verified by TSP)	Token Cryptogram (verified by TSP)
Supported authorizations		Offline & online authorizations	Online authorization only	Online authorization
Supported channels		Contactless payments	Contactless & remote payments (in-app, mobile web)	Contactless & in-app payments

(*) This table lists only new elements managed in the cloud, i.e. in Issuer or TSP back-office systems.

What contactless mobile payment might look like in the future?

Payment Tokenization is here to stay

Payment tokenization is a logical evolution for payment transactions. Not only does it provide obvious security benefits, but it also offers clear advantages for Issuers and Merchants. By reducing PAN exposure to unauthorized use, while preserving transactions compatibility with legacy payment terminals, Payment Tokenization has already convinced some major payment actors, should they be the payment schemes for HCE cloud-based payment or Apple for its new Apple Pay services.

For Issuers, Payment Tokenization simplifies the issuance and life-cycle of Digitized Cards in Digital Wallets (should they be mobile or internet wallets):

- Fraud risk is better contained by limiting the domain of use of a Token to a specific mobile phone or merchant,
- Digitized Card life-cycle can be managed more easily and independently from the associated physical card. For instance, if a mobile phone is stolen, its token may be revoked without incidence on the cardholder physical card.

For Merchants, Payment Tokenization relieves them from the burden of storing sensitive information in a PCI DSS certified environment.

A few months after the release of the EMVCo tokenization specifications, Visa and MasterCard announced the deployment of their tokenization platforms, thus taking the role of TSP. In addition, payment processors and domestic schemes may also propose their own tokenization platform in the future.

There is little doubt that the technology will gradually spread in the payment industry and even that token-based payment transactions may soon become the de-facto standard for payment transactions not performed from a chip card.

Will the simplification of the UICC-based model be sufficient to make it mass market?

Simplification initiatives are under progress

Despite the maturity of this model, the UICC-based model still suffers from a significant complexity and inherent MNO fragmentation, which slow down its massive deployment.

To simplify this ecosystem, different initiatives have been launched recently. GlobalPlatform is currently working on an “End-to-End Simplified Service Management Framework” aiming at simplifying the deployment of contactless mobile services by limiting the possible options for a given type of SE and type of applications. This initiative gives simpler end-to-end configuration templates, specific to each sector, and contactless payment is the first targeted sector.

In parallel, TSM Hubs have been set up in some domestic markets to simplify the onboarding process for Issuers. The goal of these hubs is to provide a unique access point for an Issuer to connect to all the MNOs while providing SP-TSM functionalities.

Despite these two initiatives, rolling out a UICC-based payment service still requires heavy up-front investment and operational costs for Issuers. These investments may appear even more daunting as

the UICC-based architecture is not supported on iPhones, whose market share account for 42% in the UK, 21% in Germany and 21% in France[4].

Should more disruptive approaches be considered?

The Issuers enthusiasm to join HCE trials clearly showed that there is still an appetite from the banks to propose mobile contactless services to their cardholders. With Apple Pay and the on-going HCE-based initiatives, the competition is becoming fiercer for the UICC-based model. Having said that, there are also lessons to be learnt from these new competitors.

Firstly, Payment Tokenization could be considered and integrated in the UICC-based model, as successfully done so far in the US with Apple Pay. The Payment Tokenization framework offers a global way of onboarding new Issuers - through the TSP - which may offer MNO an opportunity to go one step beyond the current one-by-one Issuer onboarding process.

Secondly, extending UICC-based MPA capability to support in-app payments is clearly another way forward. Payment schemes have published specifications for remote mobile payments and they could be amended for the UICC-based model. This would however require building up a mobile wallet proposition, sufficiently global and business-friendly to arouse e-merchants interest and to gain both Issuers and MNOs support.

Finally, cardholder authentication methods could be enriched to benefit from the popular mobile phone authentication methods (fingerprints, mobile screen patterns, etc.) and there is the possibility to move from application authentication to wallet authentication, offering a single sign-on process that may be lacking to some wallets.

With the possibility to support token-based transaction and hence to offer to Issuers a TSP-based rather than MNO-based onboarding process, the UICC-based model could have the potential to achieve the goal of becoming a mainstream approach in the mobile payment market.

The cloud-based model: a high-potential competitor?

How far from commercial deployments?

The HCE-based architecture is attractive as it simplifies the UICC-based ecosystem, making Issuers able to develop independently new mobile payment services for their cardholders, without requiring to contract services from MNOs and TSM providers. Regarding the Wallet Service Provider role, Issuers may even decide to provide their own mobile wallets, increasing their branding exposure. However, wallet propositions from payment schemes also exist and these propositions cover also remote payments, making it more appealing to e-merchants than an Issuer-centric remote payments offer.

It shall also be noted that the cloud-based model requires specific fraud and risk management processes on the Issuer side. This inevitably leads to extra investment cost for the Issuer, which should not be under-estimated.

HCE technology is still at an early stage regarding the simultaneous support of host-based and SE-based contactless apps on the same mobile phone. Besides, some security issues are still only partly answered.

[4] Source : Kantar worldpanel statistics (http://www.kantarworldpanel.com/global)

There is no doubt that the next releases of Google's Android OS will gain maturity on the management of contactless services from UICC-based and host-based apps - now that these approaches have been trialed simultaneously in the field.

In regard to HCE security aspects, due to the fact that the MPA - hosted in the mobile OS - is not able to protect its key and account data against logical and physical attacks, cloning could occur. To mitigate cloning risk, two mechanisms shall be set up in parallel:

- Keys and data shall be made as non-sensitive as possible using Payment Tokenization and usage of single use or limited use keys.
- User authentication shall be made mandatory for each transaction to prove user acknowledgment of the transaction.

In consequence, user authentication on a mobile phone becomes a key element in the HCE security framework and current user authentication on mobile device may need improvement. At least two initiatives are exploring a way forward to address this security challenge and can offer solutions applicable to HCE mobile phones:

- GlobalPlatform with the publication of Trusted Execution Environment (TEE) device specifications and API,
- The Fast IDentity Online (FIDO) Alliance with the recent release of specifications for standardizing strong authentication methods for online transactions.

The future will tell us whether HCE mobile phones shall evolve and embed a SE, a TEE zone or another form of tamper-proof mechanism for user authentication …

A model with powerful sponsors

Soon after the release of the HCE technology in 2014, Google abandoned the support for SE-based contactless payment for Google Wallet. Since then, HCE is now the sole supported technology for "Tap and Pay" by Google Wallet.

At the time of writing, Google's long-term strategy is still unclear. The recent release of HCE, associated with the support from payment schemes, may indicate that they will invest further in that architecture. On the other hand, the current discussions to acquire the company SoftCard and the recent rumors about a Google MVNO in the US market, could predict a change of strategy to the UICC-based model.

In the short-term, it is very likely that Google will invest further in the deployment of its HCE-based Google Wallet. The very high penetration rates of Android phones in Europe (50% in the UK, 70% in Germany, 68% in France)[5], makes Google a very powerful actor in this competitive market.

Payment schemes are also active promoters of the HCE cloud-based model: this ecosystem, through the Payment Tokenization and the Card Digitization process, gives them a central position. This central position also facilitates payment wallets proposal from the payment schemes addressing both contactless and remote payments.

At this stage, it is difficult to predict if there is still a long way to go until large scale deployments based on HCE cloud-based payment model. However, with the current engagement from major actors such as payment schemes and Google, it seems very likely that large scale cloud-based payment offers will emerge on HCE mobile phones in the coming years.

[5] Source : Kantar worldpanel statistics (http://www.kantarworldpanel.com/global)

A new momentum for the eSE-based model?

Indisputably, Apple with Apple Pay has showcased a secure, user-friendly solution with seamless integration for Issuers that may create attention and trigger similar ambition from other large phone manufacturers to set up their own mobile payment service.

There is still for Apple an important milestone to achieve with the launch of Apple Pay outside US to install for good their solution as the obvious answer to mobile payment in the Apple universe.

Nonetheless, Samsung is already rumored to soon propose contactless payment services based on a similar eSE architecture.

Apple has been influential enough to convince cardholders, Issuers and e-merchants (especially for in-app payment) to enroll in the Apple Pay service, mainly as the owner of a huge existing user community. Besides, most of the users have their credit/debit card details stored in their iTunes account. The path may be more challenging for other smartphone manufacturers that do not hold such community. In addition, manufacturers using Android OS (such as Samsung) will be fighting on a very competitive ground. Firstly, because Google will presumably invest further in its mobile payment services (available to all Android users). Secondly, because MNOs and SIM vendors are already proposing UICC-based solution available on these smartphones.

So, even if the eSE architecture has proven to be a good ground for building both secure and user-friendly mobile payment services, a model in which handset manufacturers act as Wallet Service Providers may not develop very widely beyond few tier-one handset manufacturers.

About Nextendis

Nextendis is an independent consultancy focused on digital technologies for telecoms, payment and public transport areas. With both technology and domain expertise, Nextendis consultants are providing support during your project life cycle from inception to implementation.

Our involvement with banking and retail industry mostly concerns the following practices:

- *Card issuance & payment transactions*
- *e-Commerce & m-Commerce*
- *Loyalty and couponing on cards and mobile devices*
- *Acquiring solutions : Payment terminal and mobile POS (mPOS)*

For more information, visit us at: www.nextendis.com