HCE, Apple Pay…

The shock of simplifying the NFC?

WHITE PAPER

Galitt

Contents

ABOUT THIS DOCUMENT

This document provides the vision of Galitt about the HCE technology for NFC mobile payment. It is based on various studies conducted by Galitt for major European players in the payment industry.

Galitt completed their first HCE payment in their R&D laboratory in May 2013.

The first version of this document was published in France on September 30th, 2014.

ABOUT GALITT

In the field of electronic payments and electronic transactions, Galitt is the leader in France and throughout the world for its testing tools and expertise in innovative technologies.

In 2013, Galitt achieved a turnover of 28 million euros and employed 240 people. To learn more about Galitt, please visit our website:
www.galitt.com

Contact Etudes :

Mr. Rémi Gitzinger
Directeur - Conseil
+33 1 77 70 28 59
r.gitzinger@galitt.com

Introduction

The enthusiasm for HCE created a renewed interest this year in mobile NFC payment from the many players in the payment ecosystem. This topic today is essential for banks, international payment networks *(such as Visa and MasterCard®)*, mobile network operators, manufacturers of smartphones, PSPs, TSM solution providers, tokenization solution providers and large retailers.

The materialization of this general interest in mobile NFC payment to provide services is based on three main prerequisites :

- The massive deployment by banks of payment terminals accepting NFC payments,
- The high rate of mobile subscribers using NFC-compliant smartphones,
- The widespread increase in digital wallet offers.

The deployment of mobile contactless payment solutions raises some questions, particularly with respect to the business case, the end-user experience, the customer adoption and the sensitive issue of the security of data and transactions.

This white paper sheds light on the changes resulting from the introduction of HCE technology on the contactless payment value chain and its impact on the positioning of the various players in this ecosystem. This document also presents implementation scenarios and associated issues - in particular, the security concerns resulting from this new architecture.

1. The landscape of mobile NFC payment

NFC[1] is a technology derived from RFID[2] technology, initially launched by Sony and Philips *(now named NXP)*, allowing the exchange of data in the near field *(within a few centimeters)* between a card and a contactless reader or between two NFC chips.

This technology has become widespread in the field of transit, where paper tickets have been replaced by NFC smart cards, particularly in Brussels, London and Paris.

For several years, NFC has been a hot topic globally and its extension to the field of payments is expected to be a real innovation, paving the way for mobile contactless payments. However, an *"NFC revolution"* has yet to materialize and usage has changed little, despite the fact that the number of NFC mobile devices is increasing significantly *(there were almost 300 million NFC smart phones worldwide in late 2013 and over 500 million expected by the end of 2014 - Source: ABI Research study)*. The number of contactless transactions is progressing slowly *(at a volume of less than 1% in Europe, except in the United Kingdom and Poland, with 2% and 4% of contactless payment transactions in 2014 respectively - Source: EPCA)*.

One reason of the slow mass adoption is due to the complexity of the ecosystem of NFC mobile payments. Indeed, the interaction of many players involved results in a complex process for the customer to subscribe to the service.

Among the deployed solutions - for instance, on the *"SIM-centric"* model launched in France - the subscription process requires the **Customer** to have an NFC **smartphone** and a compatible SIM card - **SE**[3], a subscription with a mobile operator - **MNO**[4], and to be a customer of a **bank** that offers contactless payment service with this particular MNO *(Bank-MNO contractual agreement)*.

The MNO, as the owner of the SIM card, checks the eligibility of the customer for the requested NFC service and must have a commercial agreement with the Bank to enable the administration of the payment service on the SIM card.

The Bank can then have access to a security domain on the customer's SIM card to deliver the mobile payment service to its client.

1 - Near Field Communication
2 - Radio Frequency IDentification
3 - Secure Element
4 - Mobile Network Operator

This "*SIM-centric*" model imposes a new player, the **TSM**[5], which is in charge of remote management of a secure area within the SIM card, which contains the payment application and the bank data required for the mobile contactless payment. The TSM, therefore, creates a technical link between the Bank, the MNO and the **smartphone** *(the **SE**)* of the **Customer**.

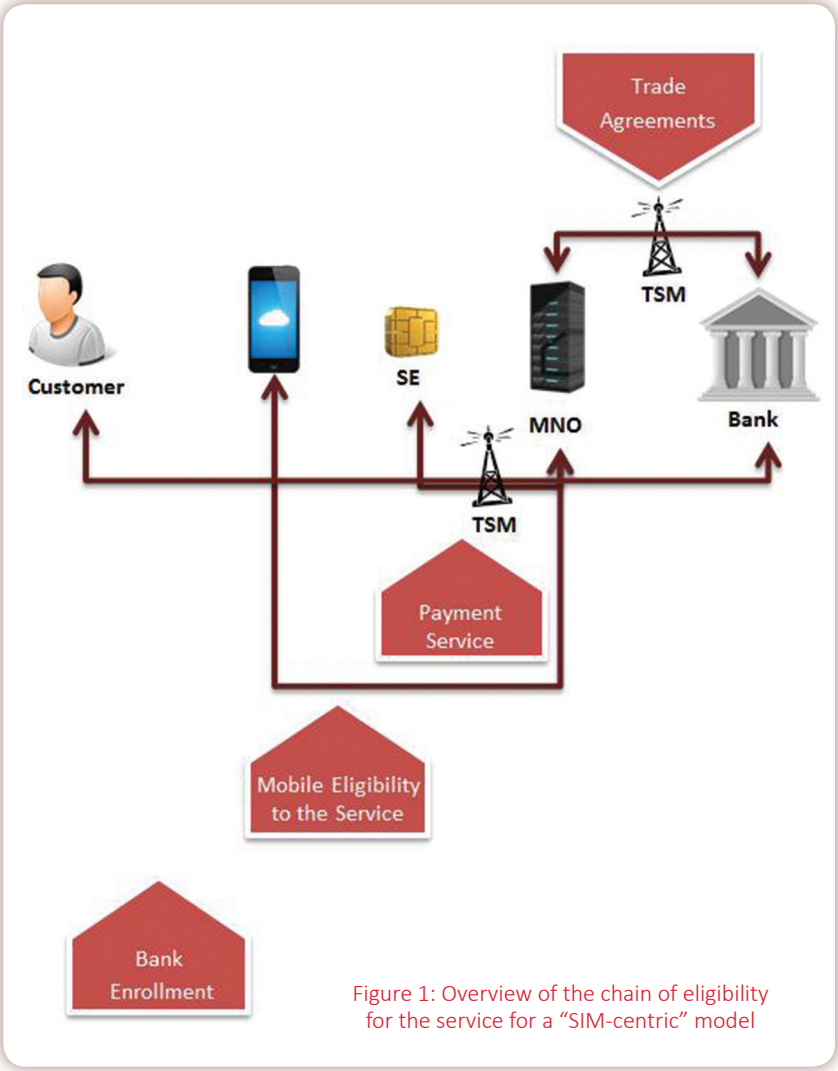

Figure 1: Overview of the chain of eligibility for the service for a "SIM-centric" model

5 - Trusted Service Manager

The customer subscription and activation processes and the organization of the different eligibility verifications are improving, but remain complex.

Moreover, these actors are facing interoperability issues in the field. Standardization bodies have defined exchange standards between involved systems, but their implementations are often subject to interpretation. To make them fully effective, these standards will eventually be supplemented by a dedicated certification program. The development and the implementation of this program might be long as it will be the result of the contributions of all the players directly interested in the generalization of this model of service administration for mobile devices *(MNOs, TSMs, and service providers)*.

In addition, smartphone manufacturers are also moving forward without synergy on contactless technology.

With the launch of the iPhone 6, which integrates NFC technology and a dedicated SE, and the Apple Pay[6] service, Apple has redefined the contours of the ecosystem by deploying an innovative "*SE-based-like*" architecture allowing a simplification of the customer experience to subscribe and use the service.

Apple is positioning itself as a facilitator of payments, with Apple Pay being a payment method, not a new form of payment.

The architecture of this service helps to harmonize the ecosystem by clarifying the value chain - the roles of each player - for the construction of a new business model for the payment industry.

Moreover, the deployment of NFC payment terminals and contactless EMV cards continues steadily in Europe and Asia and is accelerating in the United States with its liability shift towards EMV technology entering into effect in October 2015.

6 - Apple Pay has been first launched on October 2014.

2. HCE, the second breath of NFC

The difficulties in harmonizing the value chain *(business model)* and the slow convergence of solutions to a proven standard framework *(use cases and customer processes)* are major obstacles to the widespread adoption of NFC mobile payments.

Since the evolution of its Android operating system by the end of 2013, Google is acting as a catalyst with its HCE - Host Card Emulation - technology, which pushes the limits of the model and stimulates the introduction of new new mobile NFC services *(dematerialisation of restaurant vouchers, gift cards, value-added services using geolocation, etc.)*

2.1. What is HCE ?

HCE is defined as a service integrated into the operating system of a mobile device, allowing software applications installed in the mobile to interact directly, via dedicated interfaces *(APIs[7])*, with the NFC interface. With this service, an application can emulate a virtual card in the mobile device to communicate with a contactless reader.

Unlike the NFC mobile payment solutions currently deployed *(e.g."SIM-centric" model)*, HCE does not require the use of a Secure Element[8] ***(SE)*** in the mobile to host a payment application and sensitive data.

In terms of architecture, an *"SE-centric"* type of solution positions the SE as a central component through which passes any NFC communication *(using SWP[9] protocol between the NFC component of the mobile and the SE)* - in particular, a contactless payment transaction.

7 - Application Programming Interface (programming interface at the application level).
8 -There are 3 types of SE : UICC ("the SIM card"), Embedded SE and Secure Memory Card (removable card, type µSD).
9 -Single Wire Protocol

HCE technology allows routing of NFC communication - e.g., a contactless payment transaction - directly from the NFC component to an application installed in the mobile and supporting the exchanged application commands *(e.g. a payment application – Figure 2)*.

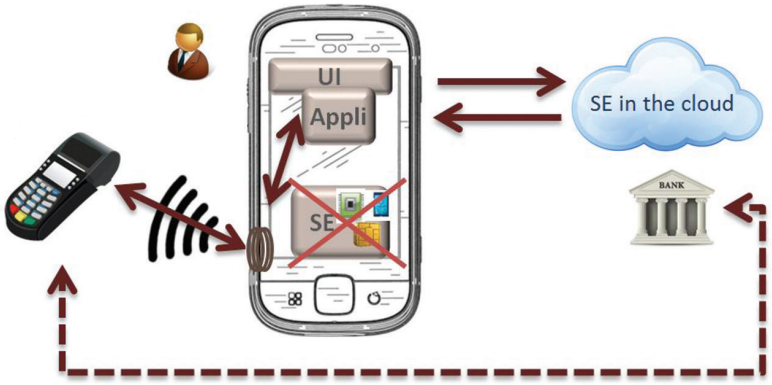

Figure 2: Example – Use case of the HCE technology without Secure Element

Since an SE is not required, the HCE service offers more flexibility for hosting sensitive data associated with the payment application. Four options are available:

1. 1.In the payment application itself,
2. 2.In an SE[10],
3. 3.In a secure environment in the mobile *(e.g. TEE)*,
4. 4.In the cloud *(a solution called "SE in the cloud" – Figure 2)*.

It is important to note that the two technologies - "SE-centric" and HCE - can coexist in the same mobile environment. Indeed, Android defines a routing table that allows the NFC component to identify the preferred channel for a particular transaction; Android writes in this table the list of applications hosted in the SE.

Already supported by RIM on the Blackberry - based on the original idea to move the ownership of the SE from the mobile to the cloud - Google's introduction of HCE service on the KitKat version 4.4 of Android since

10 - Conceptually, a HCE application can be limited to a routing function of commands executable by an application hosted in the SE (in this case the SE hosts the application and data).

November 2013 opens up the NFC to a wider range of mobile devices. Google subsequently materialized this progress, by abandoning as of April 2014 the *"SE-based"* version of its Google Wallet™ in favor of an HCE *"SE in the Cloud"* solution.

The launch of Apple Pay in October 2014 confirms the trend of manufacturers to propose a card emulation service for NFC applications natively in mobile devices, even if *(contrary to the development done on Android) the Apple service will remain initially dedicated exclusively for Apple Pay (payment service only)* and will be accessible only from the *"PassBook"* wallet.

HCE technology has aroused great interest from various players within the payment industry, especially from international payment networks such as Visa and MasterCard®.

In February 2014, Visa published specifications and a framework of requirements[11] for the development of NFC mobile payment solutions based on HCE technology in mobile devices. This approach takes advantage of the HCE architecture by providing an implementation scenario using the *"SE in the Cloud"* model *(Figure 2)*.

Similarly, but in accordance with its own development process, MasterCard® has launched several pilots early in 2014 implementing the HCE[12] technology to test this solution before editing a set of specifications, taking into account the pilot results.

11 - Visa Cloud-Based Payments Contactless Specifications v1.0.
12 - "MasterCard® to Use Host Card Emulation (HCE) for NFC-Based Mobile Payments", MasterCard® press release, Feb. 19, 2014.

2.2. Main impacts of HCE on the NFC ecosystem

The opportunity provided by HCE architecture to avoid the use of an SE as a central unit modifies the model imposed so far by the SE-centric architectures, especially that of *"SIM-centric"* solutions *(Figure 3)*.

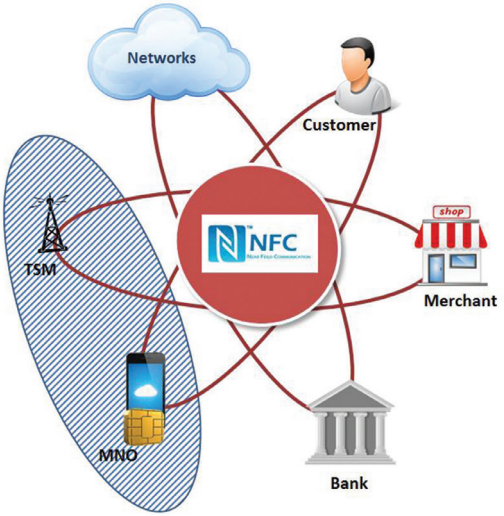

Figure 3: NFC payment ecosystem associated with a "SIM-centric" architecture

The role of the MNO, then, is limited to its fundamental job of providing and managing channels of data communication with a mobile device.

The role of the TSM depends on the selected solution to host sensitive data in the payment application. If the solution involves the use of an SE or a TEE service, the TSM keeps control of the keys and data management. However, the TSM is no longer necessary in the case of an *"SE in the Cloud"* scenario, where the management of sensitive credentials data is directly supported by a solution specified by each payment network[13].

For the customer, the ecosystem evolution will create new user experiences and will provide the opportunity to simplify the subscription process, allowing less fragmented management of the NFC payment service.

It will be based ultimately on the Visa and MasterCard® frameworks redefined in 2014 to allow the operation of the Visa Mobile payWave™ and MasterCard® Mobile PayPass™ solution in the HCE *"SE in the Cloud"* mode.

Therefore, the HCE technology directly impacts the mobile payment ecosystem as it resolves the dependencies of NFC services with the SE and the TSM and hence the associated need to enter into multiple contractual agreements between stakeholders.

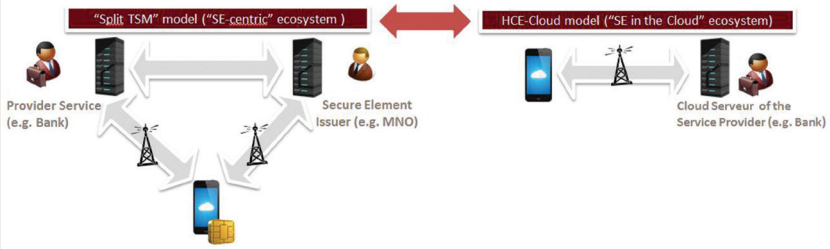

Figure 4: Comparison of a "SE-centric" ecosystem and HCE "SE in the Cloud"

13 -Visa Cloud-Based Payments Platform or MasterCard® Crendentials Management System.

2.3. Case of implementation of the HCE

While the number of players involved int the processing chain is reduced, it would be naive to believe in a technical simplification of NFC mobile payments with the arrival of HCE. Indeed, bypassing the use of an SE in the NFC mobile payment solution forces the implementation of additional security options or compensatory measures to mitigate the security risks introduced by HCE compared to "*SE-centric*" solutions.

The subscription process *(enrollment)* and the payment process itself are critical customer experiences on Internet in general, and even more so on mobile devices.

Possible kinematics depend on the choice of the implementation scenario.

2.3.1. Payment flow of an "SE in the Cloud" solution

In the case of a HCE "*SE in the Cloud*" solution, the payment execution process takes into account the network coverage to execute the transaction. Depending on the environment, the transaction can either be executed online or offline.

In online mode, the transaction is processed synchronously with the "*SE in the Cloud*" server *(Figure 5)*. The data required to perform an EMV transaction are retrieved in real time from the cloud server.

In order to harmonize the user experience regardless of the environment, it is necessary to implement a process which also operates in offline mode.

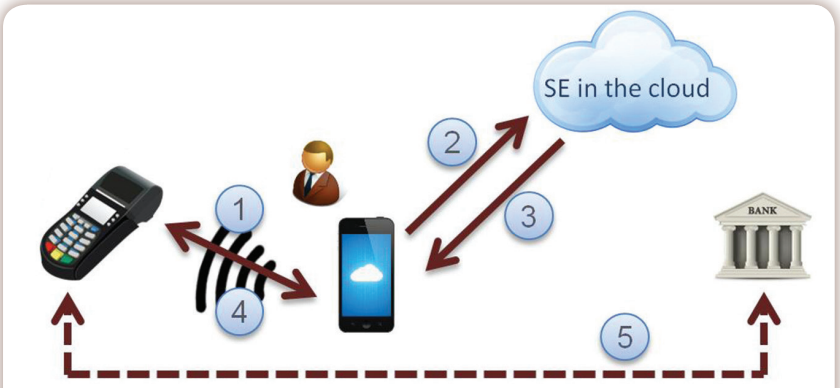

Figure 5: HCE "SE in the Cloud" flow - payment in online mode

The solution consists of desynchronizing the phase of collecting the NFC payment application data *(conducted in online mode, Figure 6)* from the phase of executing the actual NFC payment transaction using the previously collected data *(conducted in offline mode, Figure 7)*. During the transaction, the NFC transaction data previously loaded on the mobile device is used, and network coverage is no longer required.

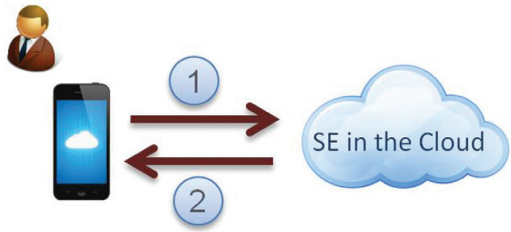

Figure 6: HCE "SE in the Cloud" flow - Collection of payment data

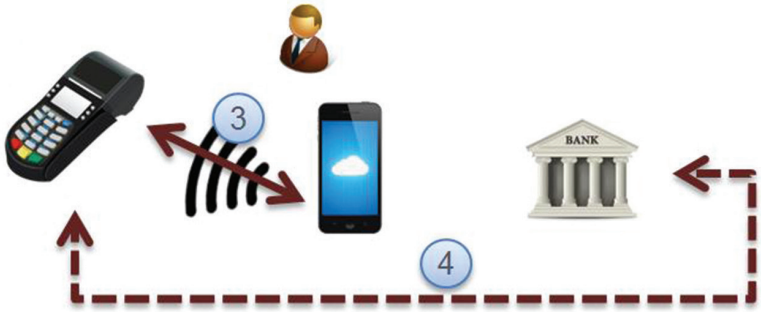

Figure 7: HCE "SE in the Cloud" flow - Payment in offline mode

Since there is no secure data storage area in the mobile device, it is necessary to limit the lifetime of the data pre-loaded in the mobile. To avoid lowering the security level of the payment, transaction execution in offline mode must be operated according to the framework of requirements and recommendations set by Visa and MasterCard®.

Also, for performance reasons, both Visa and MasterCard® define as their preferred process payments in offline mode with an online authorization to the issuer.

2.3.2. Payment kinematics of a "SE-based" solution

As mentioned above *(chapter 2.1)*, there are different possibilities in implementing an HCE architecture. One of them is to use an SE to store sensitive data of NFC payment applications.

This scenario allows using *"traditional"* payment process without having to consider operating in offine or online mode, since the mobile has all the elements necessary to complete a transaction (*application, data and cryptographic keys)*.

The Apple Pay service that is embedded in the environment of the iOS system allows the execution of an *"SE-based"* NFC payment transaction; i.e., it uses the data from the NFC payment application and the cryptographic functions hosted in the SE of the mobile to compute the transaction. Conceptually, the NFC exchanges being routed directly to the *"host"* that runs the transaction, the Apple Pay service is probably based on an *"SE-based"* HCE architecture.

This architecture is probably more pragmatic in the current context. Indeed, it is preferable to rely as much as possible on existing standards and already field-tested technical options. This includes in particular the use of an SE to store sensitive data, the respect of the existing standardized roles and functions of the TSM and using a payment execution process independent of the network coverage. A payment service must be built step by step, based on proven track record successes in the field.

Apple's approach is part of a scalable, evolutive, industrial approach. It is indeed likely that the hardware architecture of the iPhone 6 has enough flexibility to allow in the near future for the coexistence of NFC services managed in the *"SE-centric"* mode with other services managed in the HCE mode. Furthermore, assuming HCE solutions *(hosting sensitive data in the cloud)* could become widespread, the current Apple architecture for NFC payment would ultimately allow a migration towards an *"SE in the Cloud"* approach.

3. Security considerations

3.1. Security – a key issue

The increase in the use of HCE technology in mobile device operating systems will accelerate the deployment of NFC mobile payment solutions. Indeed, the use of this type of solution will take advantage of the NFC acceptance infrastructure already largely deployed following the migration of EMV smart cards to dual-interface contactless cards and of the large trials of mobile NFC payment conducted using *"SE-centric"* architecture.

The deployment of HCE *"SE in the Cloud"* solutions will have to meet strict performance requirements to avoid lowering the completion time of a contactless transaction *(in the case of mobile payment in online mode)*.

Ultimately, successful mass adoption will require offering a friendly user experience, simple customer subscription and activation processes and a high level of security of the transactions and of sensitive data, a key issue often overlooked by the general public and generally misunderstood.

This aspect deserves clarification to better understand the *"backstage infrastructure"* which enables mobile NFC payment, especially as HCE technology positions security considerations on the front of the stage, in particular for solutions that do not use SE.

The goal for the bank is to control the risk of fraud and to be in a position to mitigate the risks associated to smartphone theft, identity theft *(during enrollment)* and fraudulent transaction executed without the knowledge of the smartphone owner. This requires authentication of the mobile *(serial number, OS settings, etc.)* and verification of the smartphone owner, avoiding static PIN and preferring non-replay methods such as one-time password, biometrics, secret sharing, etc.. These methods may require network coverage at the time of execution of the transaction.

The Apple Pay service uses biometrics to authenticate the smartphone owner, with the reference biometric template being stored encrypted in a secure environment in the mobile. The authentication of the holder is done within the smartphone, simultaneously with the execution of the NFC mobile payment and not before, as in the case of NFC payment solutions requiring entry of a personal code prior to executing the transaction.

Any method of risk management implemented by the issuer based on the recommendations of international payment networks will help strengthen the overall security of the payment system. In particular, the method aiming at limiting the categorie of merchants to which acceptance of NFC mobile payment transactions is authorized is a step in this direction.

The implementation of these security measures may be done by using parameters in the NFC payment application such as requiring systematic authorization, and setting upper limits in transactions cumulated amounts and numbers. Similarly, the management of the card[14] number, the implementation of a mechanism for tokenization *(see next section)* or the use of a virtual PAN *(to be used once or to be limited in time)* are the types of mechanisms which should usually be considered with the implementation of the HCE technology.

3.2. Convergence towards tokenization

There is a general misconception that tokenization, and specifically tokenization for EMV payment, only meets the need for anonymity of the PAN. Tokenization is about the replacement, during a reversible process, of the PAN by a Payment Token *(role of the Token Service Provider - TSP, Figure 8)*, keeping the same format and the same properties as a classical PAN.

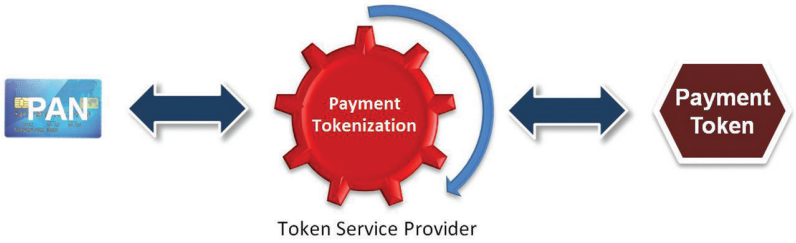

Figure 8: Tokenization and de-tokenization process by a TSP

The benefit of this tokenization mechanism is to minimize impacts in existing payment transactions processes while enabling the execution of a payment transaction using a token uniquely derived from the PAN. Adding attributes to the Payment Token allows to limit its use to a particular domain *(partitioning of use)*. A Token Payment may be limited to a transaction channel - for example, only for NFC mobile payment - and to a single device, or by assigning a security level during its issuance and its storage.

14 -E.g.: Limitation of the use of a banking payment application on a single channel (contactless proximity payment from a mobile).

The impacts of implementing tokenization on issuing and acquiring front end and back end processing are more or less important depending on whether the tokenization solution will be internalized or outsourced. Tokenisation may, in fact, complicate the mobile NFC payment solution implementation, especially for the processes of enrollment, authorization processing or charge back management.

Therefore, an issuer must choose, according to its own system and its internal security requirements, the most effective solution to implement tokenization, taking into account requirements associated with real-time processing. However, issuers should follow the requirements developed by international networks to standardize tokenization functions such as token generation, issuance and management of Payment Tokens, cryptographic mechanisms and exchange protocols for the authorization and clearing *(this induces a necessary upgrade of the IT system of the issuer)*.

Publishing a detailed technical framework[15], EMVCo has indeed announced in March 2014 the preparation of specifications for payment tokenization.

These should probably capitalize on the experiences of Visa and MasterCard®, which have each commercialized their own tokenization service in September 2014[16] and whose first client was none other than Apple, for Apple Pay service.

Focused on presenting its latest products, Apple may have overlooked the fact that the Apple Pay service represented a major change in the ecosystem of payment and transaction processing in industrializing at a large scale tokenization services designed by international payment networks - Visa and MasterCard® being, in this case, positioned as TSPs.

Therefore, tokenization enables Apple to implement its own payment system. More generally, it allows a player to set up its own payment system without involving the card issuer. This is a key concept of tokenization that yet remains essentially presented in terms of a single security function. Actually, tokenization is part of the adjustment of the mobile payment ecosystem and thus participates fully in the simplification of the customer experience, as sought by the vendors of "*SE-centric*" solutions.

The HCE solutions from Google and the Apple Pay service are similar as they tend to make tokenization a key standard for payment services on connected devices.

15 - EMV - Payment Tokenisation Specification - Technical Framework, Version 1.0 (March 2014).
16 - Visa Token Service (VTS) et MasterCard Digital Enablement Service (MDES).

Galitt

Conclusion

Mobile payment solutions using HCE technology and based on tokenization services should be considered as an element helping the convergence of the e-commerce and proximity payment channels. The relevance of this approach depends on the willingness of the major players to unify their payment solutions by offering a single means of payment through a digital wallet, regardless of the acceptance channel.

This is what Google is doing with the integration of the HCE technology to its Google Wallet™. Some service providers also offer a digital wallet based on HCE technology, including the Apple Pay service that addresses not only NFC proximity but also e-commerce payment *(the Apple Pay service can be integrated into mobile e-commerce applications), incorporating the latest security tools (such as biometric authentication and tokenization)* and significantly enhancing the security level of this payment channel.

Security remains a central issue that must be considered for each use-case *(especially during the enrollment stage)* so that there is no reduction in the overall security level and so that these solutions are trusted by users. In particular, the security of the mobile environment must be consistent with the choice of local or remote hosting of sensitive data.

The main challenge of HCE technology is to meet the expectations of simplification following the customer's feedback from the deployments of *"SIM-centric"* NFC mobile payment solutions in the field.

The choices of implementation and the overall usability of the Apple Pay service reach this goal and succeed in improving the user experience while ensuring high security standards.

The adjustment in the security environment of these solutions, especially of the payment protocols, may require banks or PSPs to make the necessary adjustments on their IT systems.

HCE appears as the lever to generalize the uses of NFC. The end user could then be the winner thanks to the convergence of payment systems: a unique end-user experience regardless of the payment channel used, an easier payment execution process and the opportunity to benefit from additional services.

HCE has all the assets to favorably change the ecosystem of NFC mobile payment, assuming that the risks associated to the introduction of these new technologies are carefully evaluated. This challenge can be detrimental in terms of profitability for the different actors if the technologies used are not completely under control.

ABOUT THE AUTHORS

Alexandre Martin
Senior Consultant

As an expert in NFC payment solutions since 2006, Alexandre relied on his experience as a consultant, functional auditor, head of a working group of the International Standardization Organization (GlobalPlatform) and project coordinator, working on numerous studies and projects ("Payez Mobile", Softcard/Isis, Google Wallet™), to offer his perspective on the major trends presented in this paper.

Stéphane Dubois
Senior Consultant

In support of project management, Stéphane has worked on major projects to redesign electronic banking platform on the acquiring and issuing sides. More recently, Stéphane worked as a consultant on studies related to the HCE and the EMV tokenization, leveraging his experience to contribute to this white paper.

Also contributing:
Hervé Ammeux *(Project Director),*
Olivier Brizai *(Consultant),*
Thomas Bouttin *(Consultant)*

Galitt

www.galitt.com

17 route de la Reine - 92100 Boulogne - France
Tél. : +33 177 702 800
Fax : +33 177 702 823
contact@galitt.com

Galitt

Graphic design : Jean-Charles Dart - j.c.dart@sfr.fr