Executive summary

In recent months, the mobile payment ecosystem has experienced significant changes as major internet and technology players have each launched their own ‘digital wallets’ (including Apple Pay, Android Pay and Samsung Pay). These models, combined with existing payment mechanisms from mobile network operators and financial institutions, introduce new operating models and technologies, such as the use of embedded Secure Elements (eSE), tokenization, Host Card Emulation (HCE) and Magnetic Secure Transmission (MST).

To understand the impact of such initiatives and anticipate further developments in this ecosystem, during 2Q 2015 EY surveyed approximately 30 companies involved in this field, including financial institutions, payment schemes, manufacturers of point-of-sale (PoS) hardware, payment card manufacturers and mobile network operators. Our eight key findings were:

1. Card-based mobile payment solutions, which leverage existing payment infrastructure and offer faster go-to-market, are gaining traction. In the medium term, the payment cards are likely to continue to dominate mobile payments.

2. NFC (Near Field Communication) has become the dominant mobile payment communication technology. It is being more widely adopted despite limited penetration of NFC-enabled PoS machines. However, on-going equipment renewal, which accelerated in the US with the on-going migration to EMV chip-and-pin cards, should remove this brake over the next five years. As contactless payment cards come into wider use, customer behavior is likely to change.

3. Magnetic Secure Transmission (MST) enables users to make contactless payments with existing cards and PoS devices, but raises several concerns over security and user-experience; it is seen as a transition technology on the path to NFC.

4. The advantages of the telephone operator’s SIM (Subscriber Identity Module) as a security element are challenged by the launch of eSE-based and HCE-based solutions, which benefit from a simpler go-to-market route and allow device manufacturers and services providers to reduce their dependency upon mobile network operators.

5. HCE (Host Card Emulation) is seen as a promising solution, especially if combined with tokenization. In particular it is seen as a flexible and scalable solution for banks.

6. Tokenization is seen as an effective way to increase transaction security, or at least limit fraud, because the primary account number (PAN) is replaced by a token. Its use for payments other than mobile is being considered.

7. Technology fragmentation adds to complexity and is a problem that is likely to force ecosystem players to collaborate. No clear leader has yet emerged in this market, since no solution looks universal.

8. Mobile payment business models are likely to evolve, with transaction fees stable or falling as the value chain becomes more complex as new players arrive.
The consumer payment and mobile payment industry is broad, encompassing multiple systems with limited overlap. This study focuses upon the mobile payment ecosystem, as described in the illustration below which covers card-based, consumer to merchant payment systems in countries where a significant proportion of the population have bank accounts.

Initiatives targeting unbanked customers (such as mobile money solutions in emerging markets) or peer-to-peer (P2P) based solutions (Facebook, Snapcash) or account-based solutions (MCX or Zapp) are not considered in this study as they are designed for use in different circumstances and regions.

Within the chosen ecosystem, EY performed about 30 interviews with financial institutions, payment processors, card manufacturers and PoS manufacturers in Europe, the Americas and Asia to better understand the dynamics of mobile payment initiatives.
For the purpose of this survey, mobile payment initiatives have been examined in terms of three characteristics:

- **Security**: How are payment credentials on the mobile phone made secure? With a secure element embedded into the mobile phone (embedded Secure Element), with a NFC SIM card (SIM as a secure element - the model already promoted by mobile network operators) or with a software-based secure element (Host Card Emulation - a software architecture that provides exact virtual representation of the secure element)?

- **Use of tokenization**: Is tokenization (see explanation on the next page) used in the mobile payment solution or not?

- **Transmission**: What is the communication technology used between the mobile phone and the PoS terminal? Is it Near Field Communication (NFC), Magnetic Secure Transmission (MST - a technology which emits a magnetic signal that mimics the magnetic strip on a traditional payment card) or QR Code (a matrix barcode)?
What is tokenization?

Tokenization involves substituting a number, called a token, for the Primary Account Number (PAN) on the customer's card. The token cannot be reversed or de-tokenized except by the trusted tokenization system. This trusted tokenization system is normally a company in the payment value chain (such as a payment scheme operator or payment card manufacturer).

The main advantage of tokenization is that no payment information is stored in the secure element (physical or cloud). It is replaced by the PAN which can only be decrypted by the token service provider.

The three main global card brands, Visa, MasterCard and American Express, agreed a framework for a global tokenization standard in 2013. This is now widely used in mobile payment solutions and is being considered for use for other, non-mobile payments.

How the tokenization process works:

- A set-up is needed. This enables the customer bank to authenticate the payment card and authorize the token service provider to generate a PAN-like token, which is then sent securely to the mobile device (step #1 in the illustration below).

- During each transaction, the tokenized PAN is de-tokenized by the token service provider, allowing the transaction to be processed by the usual payment ecosystem (steps 2, 3 and 4 in the illustration below).

The tokenization model

1. Loads token into mobile phone
2. Initiates payment transaction
3. Routes PAN-like token to usual payment network
4. Receives and de-tokenizes token

Sources: EY analysis and interviews
Survey outputs – Key findings

Our interviews generated eight key insights:

1. Card-based mobile payments are likely to prove the preferred mobile payment solution. That’s because issuance and purchasing systems are well-developed, the route to market is easy, and customers already use them. So payment cards are not threatened by mobile payment solutions in the medium term.

2. NFC penetration in the PoS installed base has grown steadily since 2012 but remains weak (approximately 15% of PoS terminals worldwide are NFC equipped, rising to 30% in the US in 2014). However, the number of NFC-equipped terminals in the US has risen sharply since 2013 as adoption of EMV cards is accompanied by equipment renewal and because the development of contactless payment cards encourages holders to use them more often.

Comparison of mobile payment initiative communication models

<table>
<thead>
<tr>
<th>Near Field Communication (NFC)</th>
<th>Magnetic Secure Transmission (MST)</th>
<th>QR Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>![NFC Symbol]</td>
<td>![MST Symbol]</td>
<td>![QR Code Symbol]</td>
</tr>
<tr>
<td><strong>Phone requirement</strong></td>
<td>Almost half of smartphone shipments in 2015</td>
<td>All Samsung smartphones from Samsung Galaxy 6</td>
</tr>
<tr>
<td><strong>PoS requirement</strong></td>
<td>15% of PoS terminals worldwide in 2014</td>
<td>All PoS which are compatible with magstripe payment</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Apple Pay, Android Pay</td>
<td>Samsung Pay</td>
</tr>
<tr>
<td>![NFC Symbol]</td>
<td>![MST Symbol]</td>
<td>![QR Code Symbol]</td>
</tr>
<tr>
<td>Level of technological penetration</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Sources: EY analysis and interviews

---

**Mobile payment: war of the wallets**
3. Magnetic Secure Transmission (MST) is a technology used by Samsung Pay which emulates a magnetic field and is compatible with standard magnetic PoS terminal, so merchants don't need to upgrade their terminals. This makes MST a more easily accessible technology whilst NFC PoS penetration remains low. However, when magnetic stripe terminals are located behind the counter, the purchaser has to pass the mobile device to the cashier, (which customers don't like doing) and there are also security concerns. So MST is seen as a transition technology prior to wider NFC adoption.

4. The appeal of SIMs as a secure element pale after the launch of eSE and HCE-based solutions, which benefit from a simpler go-to-market model and allow device manufacturers and services providers to reduce their dependency upon mobile network operators. But SIM-based payment systems are still being launched nonetheless to leverage the brands and reach of mobile network operators and other ecosystem players.

---

Comparison of security models of mobile payment initiatives

<table>
<thead>
<tr>
<th>SIM as a Secure Element (SaaS E)</th>
<th>Embedded Secure Element (eSE)</th>
<th>Host Card Emulation (HCE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Cooperation between MNO &amp; banks</td>
<td>Cooperation between OEM &amp; banks</td>
</tr>
<tr>
<td>Secure element</td>
<td>Physical</td>
<td>Physical</td>
</tr>
<tr>
<td>Example</td>
<td>MyWallet by Deutsche Telekom</td>
<td>Apple Pay</td>
</tr>
<tr>
<td></td>
<td>Orange Cash by Orange</td>
<td>Android Pay</td>
</tr>
</tbody>
</table>

Sources: EY analysis and interviews
5. Host Card Emulation (HCE) is seen as a promising solution, especially if combined with tokenization. Instead of a security device, it has a software-based secure element, making it easy to market, deliver, and scale-up. It is easier for Google or Microsoft who provide operating systems to promote the use of a dematerialized secure element than to push users or manufacturers into adding hardware to their phone. However, the absence of a physical security device could deter take-up, as customers often see the cloud as less secure. The HCE pricing model has yet to be clearly defined.

6. Tokenization is perceived as an effective way to achieve secure transactions, or at least limit fraud, through the use of a tokenized PAN. The tokenized PAN is stored in the embedded secure element in place of the credit card information. This however requires a set-up process and requires other players to let the token service provider play a central role during the transaction (tokenized PAN generation during set-up and PAN-de-tokenization during payments). Because the token service provider is at the heart of the transaction, many tokenization solutions have been launched. Payment schemes or card tokenization can be combined with all-mobile payment solutions (SIM-based, eSE and HCE) and is used by pivotal players such as Apple and Google in their payment solutions.
Technology fragmentation is seen as a problem and forces actors in the ecosystems to collaborate on a wide variety of solutions developed by numerous players (manufacturers vs. operating systems) and at this stage, there is no clear leader emerging from this market, as no solution can be perceived as universal. For example, Apple Pay is based on NFC, eSE and tokenization, Google chose NFC and HCE potentially combined with tokenization and Samsung Pay is based on MST/NFC technology. On the long term, market fragmentation and customer adoption ramp-up should notably depend on dominant technology:

- If the SE is in the phone, SE manufacturers will have to address a more concentrated market (~8 major worldwide device manufacturers vs. ~800 MNOs worldwide) which will create a “winner-takes-all” model.

- If the SE is dematerialized (HCE), it will generate a business threat for SE manufacturers but the ramp-up of these initiatives should remain low on a short-term perspective.

Mobile Payment business model is expected to evolve with player remuneration as a key stake: while value chain is gaining in complexity (potentially up to 4 more players – mobile manufacturer, secure element manufacturer, trusted execution environment and token service provider), transactions fees are expected to be flat if not to decline. Combined with market fragmentation, non-definitive business models are a key factor of complexity for banks.

The established value chain – and how it might look in the future

**Established and new payment/M-payment value chains**

<table>
<thead>
<tr>
<th>Customer</th>
<th>EMV card production and personalization</th>
<th>Issuer</th>
<th>Payment scheme</th>
<th>Acquirer</th>
<th>PoS manuf.</th>
<th>Merchant</th>
</tr>
</thead>
</table>

- **NFC SIM**
  - Customer
  - Mobile operator
  - NFC SIM manufacturer
  - Trusted Service Manager
  - Issuer
  - Token Service Provider
  - Payment scheme
  - Acquirer
  - PoS manuf.
  - Merchant

- **eSE**
  - Customer
  - Mobile manufacturer
  - eSE manufacturer
  - eSE provisioning manager
  - Issuer
  - Token Service Provider
  - Payment scheme
  - Acquirer
  - PoS manuf.
  - Merchant

- **HCE**
  - Customer
  - Mobile manufacturer
  - HCE
  - TEE
  - Issuer
  - Token Service Provider
  - Payment scheme
  - Acquirer
  - PoS manuf.
  - Merchant

Source: EY analysis
Glossary

eSE: Embedded Secure Element
HCE: Host Card Emulation
NFC: Near Field Communication
MNO: Mobile Network Operator
MST: Magnetic Secure Transmission
M2M: machine-to-machine
OEM: original equipment manufacturer
PAN: Primary Account Number
SIM: Subscriber Identity Module
TSM: Trusted Service Manager
TSP: Token Service Provider
TEE: Trusted Execution Environment
PoS: point of sale
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2015 Ernst & Young Advisory.
All rights reserved.
Studio EY France - 1511SG322
SCORE France N° 15-057

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts

Etienne Costes
Partner, Ernst & Young Advisory
etienne.costes@fr.ey.com

Thibaud Chabrelié
Senior Manager, Ernst & Young Advisory
thibaud.chabrelie@fr.ey.com

Charles Viennot
Ernst & Young Advisory
charles.viennot@fr.ey.com

Louisa Melbouci
TMT Marketing manager
louisa.melbouci@fr.ey.com