Mobile Payments
Update on HCE, Tokenization and Security

GSMA
23 July 2015
Market Developments

Rapid changes in a fragmented market

• Scheme tokenization has become real
  • Apple Pay
  • HCE
  • Samsung Pay
  • Android Pay

• SIM Centric Deployments continue
  • 67 live commercial services deployed that use the SIM for the secure element in mobile contactless

• Authentication and Binding is a challenge:
  • Apple Pay yellow path issues

• Usage Data isn’t published:
  • So is assumed to be low ... For now
Deployment Models – Apple Pay

- Apple Pay:
  - Secure element, Apple wallet, scheme controlled tokenization, static payment credentials, online or offline EMV
Deployment Models – Android Pay

- **Apple Pay:**
  - Secure element, Apple wallet, scheme controlled tokenization, static payment credentials, online or offline EMV

- **Android Pay**
  - HCE, Android wallet (possibly Issuer option), scheme or issuer controlled tokenization, dynamic HCE payment credentials, online EMV only plus Google dynamic tokens (for in-app payments)
Deployment Models – Issuer HCE

- **Apple Pay:**
  - Secure element, Apple wallet, scheme controlled tokenization, static payment credentials, online or offline EMV

- **Android Pay**
  - HCE, Android wallet (possibly Issuer option), scheme or issuer controlled tokenization, dynamic HCE payment credentials, online EMV only plus Google dynamic tokens (for in-app payments)

- **Issuer HCE**
  - HCE, Issuer Banking App, Alias PAN or scheme tokenization, dynamic payment credentials, online EMV only, unclear about in-app payment
Deployment Models – SIM Centric

- **Apple Pay:**
  - Secure element, Apple wallet, scheme controlled tokenization, static payment credentials, online or offline EMV

- **Android Pay**
  - HCE, Android wallet (possibly Issuer option), scheme or issuer controlled tokenization, dynamic HCE payment credentials, online EMV only plus Google dynamic tokens (for in-app payments)

- **Issuer HCE**
  - HCE, Issuer Banking App, Alias PAN or scheme tokenization, dynamic payment credentials, online EMV only, unclear about in-app payment

- **SIM Centric secure element**
  - Secure element, Mobile operator wallet, tokenized PAN, online or offline EMV
The Authentication Challenge

Who controls user, device and app binding?

- Problems with Apple Pay in the US are not problems with underlying technology
  - *Fraudsters downloading other peoples’ cards to their phones*
  - *Lack of focus on strong procedures in this area*

- Identification is the critical weak link in the chain, which can be used as the entry point for payment app providers:
  - *The MNO (via the SIM and mobile operator subscriber data)*
  - *An issuer (e.g. mobile banking apps)*
  - *The handset manufacturer (iTunes, Google Play)?*

- Identification can be part of an integrated payment app service or a separate service to third-parties
  - *E.g. MNOs offering identity verification to third-party payment app providers*
Card Issuer Drivers

Card issuer needs to:

- Reach a significant proportion of its customer base (customer choice is key)
- 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, and
- Make allowance for the implementation risks from the maturity of new technology or a new implementation approach

- But payment is not the killer app: it’s the last leg of the experience
  - Value added services are critical; loyalty, couponing, etc
  - Need to add real value to the customer’s life, not simply provide another payment method
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 (customer choice is key)
- 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, and
- Make allowance for the implementation risks from the maturity of new technology or a new implementation approach

- But payment is not the killer app: it’s the last leg of the experience
  - Value added services are critical; loyalty, couponing, etc
  - Need to add real value to the customer’s life, not simply provide another payment method
Conclusions

In conclusion ...

- Like Apple and Android Pay, scheme TSPs can be used with SIM centric deployments.
- On Android, HCE remains a flexible choice for issuers:
  - *Card issuers continue to have the option for mobile contactless payments to implement their own HCE solution that does not rely on Android Pay.*
- HCE does not address all payment scenarios:
  - *Offline and in-app payment support is still unclear*
- Securely binding users to their device is essential for all approaches:
  - *Authentication services are the current weak point in deployments*
- Mobile payments are not just NFC card payments:
  - *But issuers have increasing discretion as to the type of service to offer its 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.
Contact

Browse [www.chyp.com](http://www.chyp.com)
Follow [@chyppings](https://twitter.com/chyppings)
Mail [info@chyp.com](mailto:info@chyp.com)
Comment [http://www.chyp.com/media/blog/](http://www.chyp.com/media/blog/)
Listen [http://www.chyp.com/media/podcasts/](http://www.chyp.com/media/podcasts/)

Consult Hyperion UK
Tweed House, 12 The Mount
Guildford, Surrey GU24HN, UK.
+44 1483 301793

Consult Hyperion USA
535 Madison Avenue, 19th Floor
New York, NY 10022, USA.
+1 888 835 6124