Session 2: “Understanding the payment ecosystem and the issues” – Visa Europe

Agnes Revel Martineau
VP, Head of Product Specifications, Standards and Industry Liaison

ETSI
01st, July, 2014
Agenda

• You said mobile payment…

• What is the mobile environment? How to approach it?

• In detail….
  What has been done?

• What next?
You said mobile payment...

- Vision
- What is mobile payment?
- Standard maturity
Vision - Focused on consumer choice

Any

Handset  Network  Technology  Issuer  Wallet  Payment product
What is mobile payment?

‘Mobile payment’ is a fabulously generic term which means different things to different people

If I use:

– the browser on my phone to purchase an item from a web site
– an application to make an in game purchase
– my bank’s application to move money from my internet bank portal
– a person to person payment using one of many different solutions
– a contactless payment at Point of Sale
– a mobile to accept card payments (as a terminal)

All these (and quite a few others) will probably be considered by consumers as mobile payments

One device
Anywhere, anytime
Richer consumer experience
Mature Standards
What is the mobile environment? How to approach it?

- Mobile - an Untrusted environment
- SE based approaches
- Stickers Approaches
- Cloud based Approaches

Understanding the payment ecosystem and the issues

01st July 2014
Mobile is an untrusted environment

- Mobile phones are easy to steal/lose - 9 million mobile devices are lost annually.

- Mobile phones have limited input capabilities - long or complicated passwords don’t work.

- Mobiles are designed as portable devices, so use with a second device (two factor) is painful.

- Malware on mobile phones is rising fast; causing a drop in new computer-related malware.

- But users tend not to worry about malware on mobile phones, and have limited options to deal effectively with it.
Mobile Payment Application - SE based

Mobile equivalent of the payment application that runs in the chip on a contact or contactless chip payment card.

Different options for SE (Visa Compliant): Protect **keys** that generate the Transaction Authentication credential used during the payment

- **Sim Centric**: Secure element in the SIM
- **Mobile Centric**: Secure element embedded on handset
- **Accessory Centric**: Secure element embedded in the accessory (e.g., dongle, skin)
- **Micro SD Memory Card**: Secure element on the micro-SD card
- **Micro SD Memory Card with NFC antenna**: Secure element and NFC antenna both on the micro-SD card

---

**Payment App**
- Allows consumer to select card, wave and pay

**Account Data**
- Physically hosted on a secure chip embedded in the device

**NFC Controller**
- Transmits payment information to the terminal

**Contactless Payment Terminal**

---

Understanding the payment ecosystem and the issues | 01st July 2014
Mobile Payment Application - Sticker

Non-integrated mobile equivalent of the payment application that runs in the chip on a contact or contactless chip payment card

- Self-adhesive Tags, can be attached conveniently to any mobile device
- Help habituate consumers towards making mobile payments
- Can be combined with a companion app to provide a ‘near-NFC’ experience
- Contain an embedded chip and antenna
Mobile Payment Application – Cloud Based approach for contactless payment using NFC HCE

“In the cloud” equivalent of the payment application that runs in the chip on a contact or contactless chip payment card.

Cannot store long term Keys in mobile app/OS so need a different approach to Transaction Authentication: Limited use Transaction Authentication credentials (Time or Domain).

- The Secure Server performs core functions that provision and manage consumer accounts and transaction authentication credentials according to predefined preferences
- The mobile application provides an interface to the user.
- Messages as securely exchanged between the Secure Server and the mobile application
- Enforce use of dynamic data / keys (account parameters) and limited validity (time to live, maximum number of transactions)
- Reduced integration effort and cost
  - Reduced numbers of actors
In detail…
What has been done

• Enforcing security and Authentication
• Privacy
Enforcing Security and Authentication in an untrusted environment?

• Multiple layers of security protect Visa mobile payments:
  – Array of security methods used within Mobile device
  – Advanced security technology to uniquely identify each contactless transaction against counterfeit fraud
  – Real time analysis of transaction by processing network against potential fraud

• As we evolve to Cloud Based Payment:
  – Shift of security from the front-end (mobile) to the back end (secure server)
  – Increase use of Fraud detecting / behavioral engines
  – Evolution in Cardholder verifications methods
  – Limitation in time and domain of Data and Keys
  – Risk Based authentication and “Defence in layer”
Privacy

• Privacy by design
  – All product development ensure that careful consideration is given to consumer privacy
  – Clear analysis of risks is carried
    • How to mitigate risk?
    • What is the residual risk? Is it acceptable?
  – Continuous enhancements during lifecycle of the product

• Active participation to Privacy Impact Assessment (RFID mandate)
  – Driving the industry effort on single European template for the financial sector

• Tokenisation
  – Introduce yet another layer of privacy by replacing a consumer PAN by a surrogate token, making it form factor specific, channel specific and/or merchant specific
What next?
As we evolve to the next generation of Mobile payment

• Simplifying and cutting cost of integration

• We can expect emergence of new technologies and methods to carry out mobile payment
  – We should be agnostic to those rails and support innovation

• We can expect increased Malware
  – We should reinforce Consumer education and information on the risks associated with the use of mobiles and how to protect themselves
    • Rooting / jailbreak phone
    • App Downloading from untrusted sources
  – We should have stronger rules in place on OS and App stores to ensure
    • App store verification of App codes and origin of the application
    • Intrusion detection by OS or security application
  – We should enforce best practices for application developer
    • Clearer messaging of permissions requested by given application
    • Reduce set of permissions to only the necessary ones
Thank you