Mobile/NFC Security Fundamentals

Anatomy of a Mobile Device: Security Architecture and Secure Provisioning

- Smart Card Alliance and GlobalPlatform Webinar
- March 5, 2013
Introductions

- Randy Vanderhoof
- Executive Director
- Smart Card Alliance
The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.
Mobile & NFC Council

- Raise awareness and accelerate the adoption of all applications using NFC
  - Access control, identity, loyalty, marketing, payments, peer-to-peer, promotion/coupons/offers, transit, ...
- Accelerate the practical application of NFC, providing a bridge between technology development/specifications and the applications that can deliver business benefits to industry stakeholders.
Today’s Webinar Topics & Speakers

- **Introduction:** Randy Vanderhoof, Executive Director, Smart Card Alliance
- **Introduction to GlobalPlatform:** Kevin Gillick, Executive Director, GlobalPlatform
- **Anatomy of a Mobile Device:** Philip Hoyer, Director, Strategic Solutions, HID Global
- **Security Interfaces and Secure Provisioning:** Gil Bernabeu, Technical Director, GlobalPlatform
- **Q&A:** Randy Vanderhoof, Smart Card Alliance
Contactless and NFC Payments Continues to Spread

- Form factors
- Applications
NFC Security Webinar Series #1 – Anatomy of a Mobile Device

- Kevin Gillick
- Executive Director
- GlobalPlatform
GlobalPlatform is the standard for managing applications on secure chip technology.

Across several market sectors and in converging sectors:
What is the output of GlobalPlatform?

- Specifications – technical industry guidelines
- Configurations – applying the guidelines to different market sectors
- Security Certifications – streamlining security requirements & testing
- Industry Compliance Program – confirming a product’s functionality aligns to GlobalPlatform technology
- Educating the Industry – white papers & technical documents
- Workshops – specification training & educational
Mobile Task Force (MTF)

Established in 2007 to actively contribute to the development of mobile telecommunications standards worldwide.

Overview:

- The task force provides input to the technical committees, concerning the specific and emerging requirements of the mobile sector, in order that the GlobalPlatform Card, Device and Systems Specifications can be expanded and updated to suit market needs.

The primary objectives is to:

- collect business requirements
- facilitate new market opportunities between the mobile sector and other industries
- highlight that differentiation of products and services can be achieved through multiple applications
- demonstrate that various business models can be applied within one implementation
- communicate that a neutral and scalable infrastructure can protect current investments relative to future technology evolutions
Anatomy of a Mobile Device

- Philip Hoyer
- Director, Strategic Solutions
- HID Global
Definition of Mobile

- Smartphone
- Phablet
- Tablet
Anatomy

Handset

UI / Keyboard

Application #1

OS

Applet

Secure Element

Contactless Frontend (CLF)
Anatomy – 2 -

Handset

UI / Keyboard

Application #1
Application #2

Secure Element Access

Contactless Frontend (CLF)

Applet #1
Applet #2
UICC/SIM

Applet #3
Applet #4
Embedded SE

Applet #5
Smart micro SD
Secure Elements

On Phone:
- Embedded SE

Removable
- UICC / SIM
- Smart micro SD

Attached
- Phone Sleeves (ex. iCarte for Apple phones) (still harbours micro SD)
- Attached reader inserting ISO smart card
- Stickers
Security Continuum

Security

Complexity

Phone OS

Software Based Solution

Trusted Execution Environment (TEE)

Secure Element (SE)

SE + TEE combination
Interfaces

Handset

UI / Keyboard

Application #1
Application #2

Crypto Middleware

Secure Element Access

OS

Trusted UI / Keyboard

TEE

Contactless Frontend (CLF)

Applet #1
Applet #2
Applet #3
Applet #4
Applet #5

UICC/SIM
Embedded SE

Smart Micro SD
Security Interfaces and Secure Provisioning

- Gil Bernabeu
- Technical Director
- GlobalPlatform
Interfaces - standardisation

Handset

- Trusted UI / Keyboard
- Application #1
- Application #2
- TEE Client API
- PKCS #11
- Open Mobile API
- Secure Element Access
- OS
- Applet #1
- Applet #2
- Applet #3
- Applet #4
- Applet #5
- UICC/SIM
- Embedded SE
- Smart micro SD

Crypto Middleware

OS

UI / Keyboard

Trusted App

Contactless Frontend (CLF)
**Being Worked On**

- Secure Element Access Control: which application has access to which Applets

- Routing of NFC Services from CLF to multiple secure elements
Hosting multiple services

- **Bank Security Domain**
- **Office Security Domain**
- **Transit Security Domain**
- **Store Security Domain**

- **Applet #1**
- **Applet #2**
- **Applet #3**
- **Applet #4**

- Bank
- Office
- Transit
- Store
Secure Provisioning

Handset

UI / Keyboard

Application #1
Application #2

Crypto Middleware

Secure Element Access

Remote Admin Agent

OS

TEE

Contactless Frontend (CLF)

Applet #1
Applet #2
UICC/SIM

Applet #3
Embedded SE

Applet #4
Smart Micro SD

Applet #5

GlobalPlatform SE OTA

SIM OTA
Provisioning - TSM

GlobalPlatform Mobile Messaging

Bank
- Payment card issuer
Transit
- Transit card issuer
Store
- Issues coupons and loyalty cards
Office
- Issues access cards to employees
TSM-SP
- Connects SP and SEI
TSM-3rd Party
- Control SE usage
SE Issuer TSM
- Stores credentials securely

Credentials
- NFC SE
- NFC antenna
- NFC chip

Reader infrastructure
- NFC phone
- Wallet

MNO
- SIM OTA
- SE OTA
Mobile & NFC Security Webinar Series

- **Mobile/NFC Security Fundamentals: Secure Elements 101**
  - March 28, 2013, 1pm ET/10am PT
  - *Speakers*: Brent Bowen, INSIDE Secure; Greg Coogan, Morpho Cards; Sanjiv Rawat, Giesecke & Devrient; Sree Swaminathan, First Data

- **Mobile/NFC Security Fundamentals: NFC Forum Tags and Security Considerations**
  - April 18, 2013, 1pm ET/10am PT
  - *Speakers*: Tony Rosati, NFC Forum/Blackberry; Joe Tassone, Identive; Randy Vanderhoof, Smart Card Alliance; Mike Zercher, NXP Semiconductors; Rob Zivney, Identification Technology Partners

- **Mobile/NFC Security Fundamentals: NFC Application Use Cases – Security Perspectives**
  - May 9, 2013, 1pm ET/10am PT
  - *Speakers*: Rene Bastien, SecureKey Technologies; Jonathan Main, NFC Forum/MasterCard; Steve Rogers, IQ Devices; Tony Sabetti, Isis; Randy Vanderhoof, Smart Card Alliance
NFC Solutions Summit 2013