What UICC Security Means for NFC

Jean-Francois RUBON
SIMalliance representative
NFC Solutions Summit
SIMalliance: Who we are

SIMalliance members represent 86% of the global SIM market and deliver the most widely distributed secure application delivery platform in the world (UICC/SIM/USIM).
What we do...

SIMalliance is the global, non-profit industry association which simplifies secure element (SE) implementation to drive the creation, deployment and management of secure mobile services.

SIMalliance:

> Promotes the **essential role of the SE** in delivering secure mobile applications and services across all devices that can access wireless networks

> Identifies and addresses SE-related technical issues, and **clarifies** and recommends existing technical standards relevant to the SE implementation

> Promotes an **open SE ecosystem** to facilitate and accelerate delivery of secure mobile applications globally

> Monitors the **market** and produces market data reports

*Security, Identity, Mobility*
SIMalliance Latest Deliverables

> Secure Element Deployment & Host Card Emulation v1.0
  > Introduction to Android's Host Card Emulation (HCE) and explores its value to the NFC ecosystem relative to the SE

> UICC LTE Profile
  > A collection of requirements for optimal support of LTE/EPS networks by UICC.
  > Widely utilized by North American MNOs.

> UICC Device Implementation Guidelines
  > Outline fundamental and optional UICC features device vendors need to support to optimize UICC interoperability in future devices.

> Stepping Stones Documents
  > Best practices for development of interoperable applications (USIM, NFC, SE).

> General SIM Security Guidelines
  > Ensure that a SIM's security levels are optimally maintained.
SIMalliance: Creating Opportunities for Market Growth

> Open Mobile API

- Standardized way to connect mobile apps with all SEs on a device (SE form factor neutral) including a service layer to provide a more intuitive interface and increasingly powerful functionality.
- Enables delivery of highly secure business and consumer mobile applications across all SE form factors.
- Referenced by GSMA (NFC Handset & APIs Requirements and Test Book) as a mandatory feature.
- Open Source implementation available (Seek-for-Android).
- Implemented in more than 150 models of Android NFC smartphones
An SE for Each Business Model

> An SE is a tamper resistant component which is used in a device to provide the security, confidentiality, and multiple application environments required to support various business models

> An SE resides in extremely secure chips and may exist in a variety of form factors

> The SE should provide separate memory for each application without interactions between them

> SIMalliance considers true SEs to be a combination between software and dedicated hardware

**UICC (SIM)**
> Includes the application that authenticates the user in the network
> Controlled by the mobile network operator (MNO)

**Embedded SE (eSE)**
> SE embedded in the mobile at the time of manufacturing
> Controlled by the device maker (OEM)

**Secure MicroSD**
> SE embedded in µSD form factor and featuring large memory
> Controlled by the service provider (SP)
Strong NFC Foundation in Place for Use by Service Providers

In 2013: 78m NFC SIM shipped (SIMalliance): +159%

- Japan/Korea: 37m
- North America: 24m
- Europe: 14m

124m NFC SIM shipments in 3 years

2014: 416m NFC phones to be shipped*

2017: 53% of NFC-ready PoS globally*

*Forecast
What About HCE?

> Ultimately, SIMalliance thinks HCE will be good for the NFC ecosystem as a whole. It will:
  - Increase the breadth and number of NFC services available to end users
  - Drive wider adoption and utilization of NFC
  - Increase end-user familiarity with what NFC is, together with how it is used
  - Stimulate market innovation by encouraging new developers into the market

> BUT the technology remains immature, un-standardized and, relative to SE-based deployments, vulnerable to malicious attack. It is:
  - Yet to be standardized. As a result it is not yet interoperable
  - Exposed to a variety of potentially significant security vulnerabilities
  - Dependent on numerous variables for its operational continuity
Appropriate Utilization

**In its current form, HCE is best suited to:**

- QR-code replacement services
- Use cases where the user’s stored credentials are of low value and guaranteed security is not mandatory
- Use cases where the emulated NFC application is not based on a current and pre-existing card application
SIMalliance Assessment

> In order to distribute and manage valuable and/or sensitive credentials (payment, transport, identity, access), a secure component is necessary in the device as well as a secure solution for the provisioning and management of this component.

> This component and its corresponding management solution should be interoperable and agnostic to mobile operating system platforms.

> It is necessary to have the secure component and management system certified, following extensive security testing procedures conducted by several recognized third-party laboratories. This ensures the secure NFC ecosystem is audited using the latest generation of known attack path techniques.

At the moment, these pre-requisites are not met by HCE.
Take Away

> **MNOs:**
  - Request OEMs to implement OMAPI and default NFC routing to the SE
  - Accelerate the deployments of SE-NFC infrastructure
  - Maximize the efforts to defragment the market
    - Be more cooperative and open with each other (uniform wallet approaches) and with NFC service providers to enable easier access to the SE and encourage more partnership applications

> **NFC service providers:**
  - SE-NFC is worth the effort
    - It remains the sensible business choice:
      - SE-NFC is bulletproof, ready to go, certified, ubiquitous
      - MNO supporting infrastructure is huge
      - UICC alternatives, supporting non MNO-centric business models already exist
‘Secure Element Deployment and Host Card Emulation v1.0’ white paper is freely available to download from the SIMalliance website

Thanks!

Visit www.simalliance.org for more information