Applying the NFC Secure Element in Mobile Identity Apps

RANDY VANDERHOOF
Executive Director

Smart Card Alliance

Session ID: MBS - 403
Session Classification: Mobile Security

RSA CONFERENCE 2012

Agenda

- Agenda topics
  - NFC basics: functionality and security
  - NFC ecosystem for payments and identity/security
  - Challenges for a mobile identity apps using NFC

Near Field Communication (NFC)

- **Near Field Communication (NFC) is a short-range wireless connectivity technology** (also ISO/IEC 18092) Communication occurs when two NFC-compatible devices are brought within four centimeters of one another. **NFC operates at 13.56 MHz** and transfers data at up to 424 Kbits/second.

- The primary uses of NFC are to:
  - **Peer-to-Peer:** Exchange data or connect devices, such as wireless components in a home office system or a headset with a mobile phone
  - **Reader/Writer:** Access digital content, using a wireless device such as a cell phone to read a “smart” poster embedded with an RF tag
  - **Card Emulation:** Make contactless transactions, including those for payment, offer redemption, access, and ticketing

Mobile Application Security

- No Security – limited or no protection of data stored on mobile device
  - Ex. Facebook profile, shopper rewards number

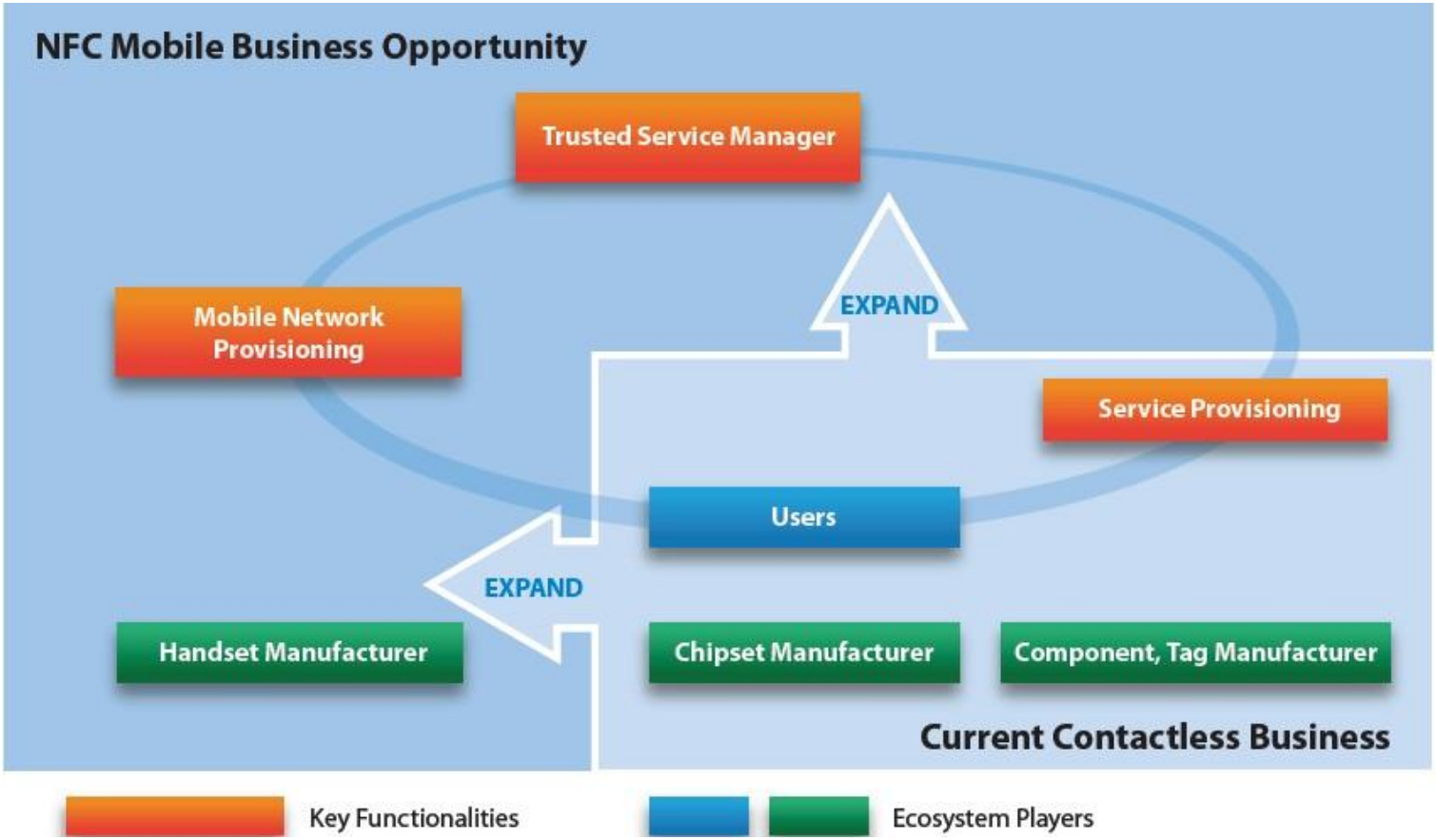
- Basic Security – data can not be accessed or duplicated easily, economically impractical to use protected data
  - Ex. Gift cards, transit pass, low value prepaid

- Hardened Security – encrypted, many security levels, stored in secure element
  - Ex. Bank cards, drivers license, log-in data, high value prepaid

NFC and Application Security

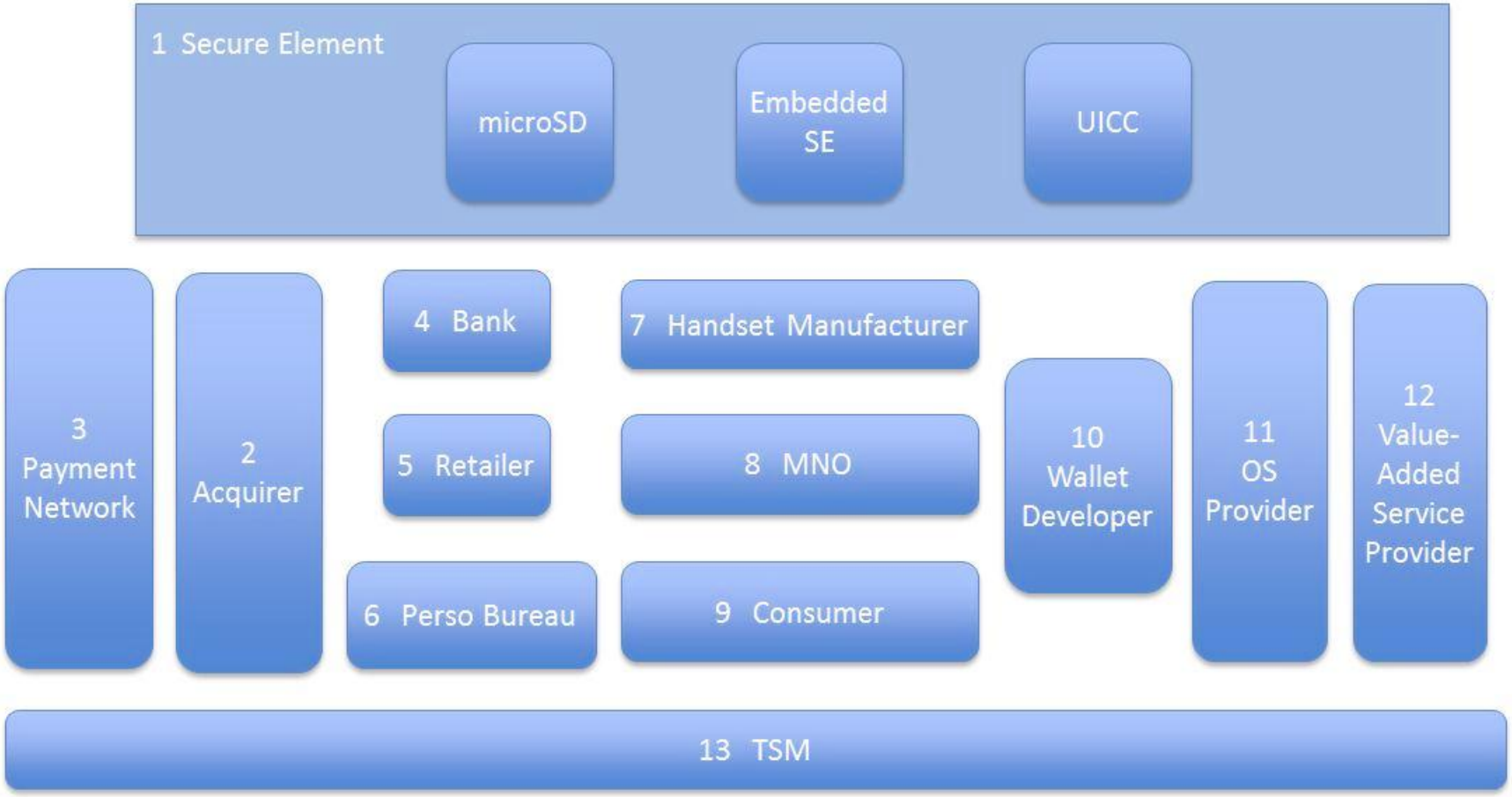
- Several secure architectures are available to implement NFC applications:
- Removable elements:
  - UICC (SIM) based secure element communicating using the Single Wire Protocol (SWP) with the NFC controller
  - SD card-based secure element uses the SD card format to provide the security features required by the applications
- Non-removable elements
  - Embedded hardware secure element uses a non-removable SIM-type element that is part of the mobile phone
  - Secure element features in the mobile device as part of the baseband processor

What the NFC Ecosystem Looks Like

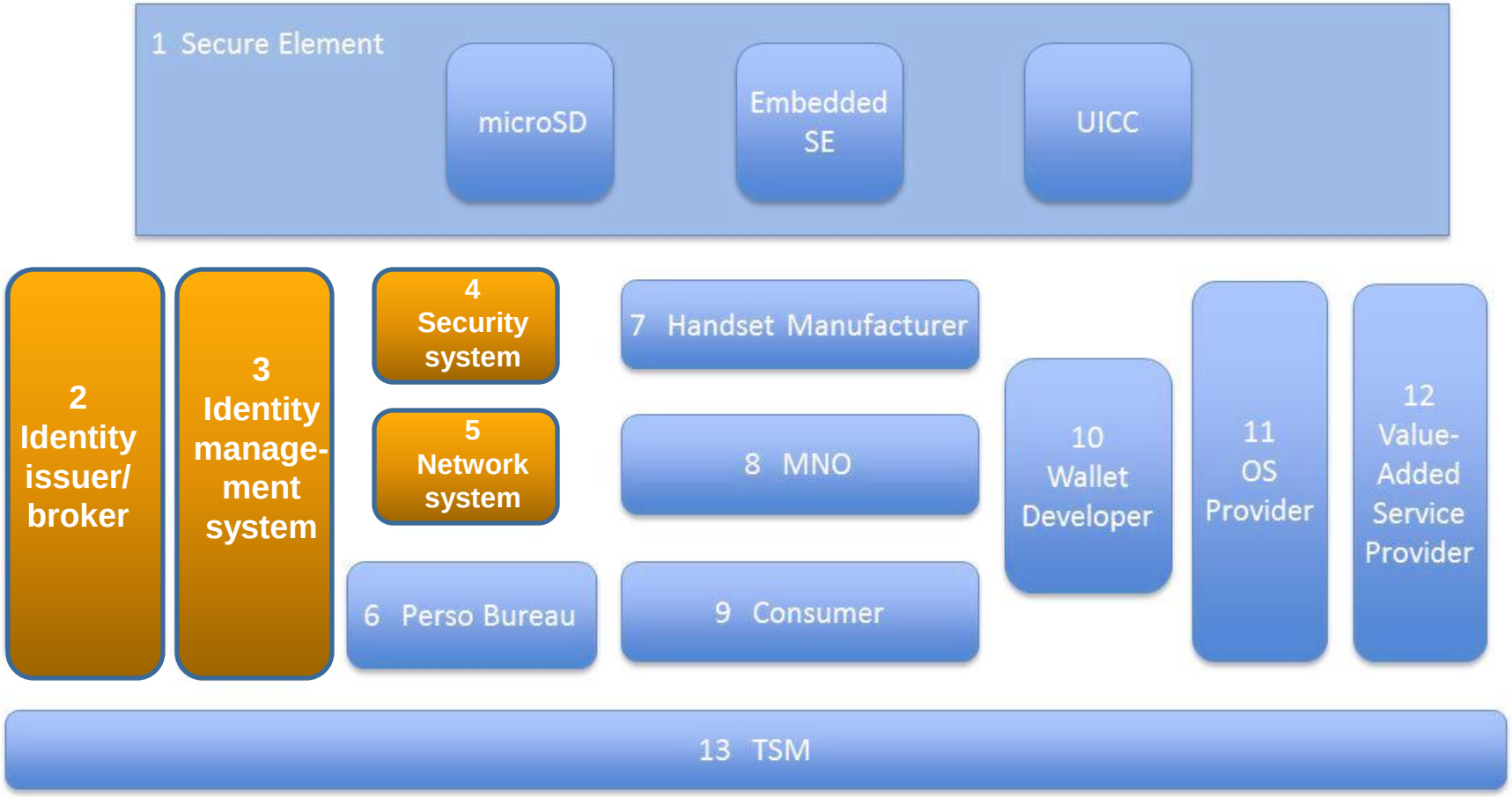


The Trusted Service Manager (TSM) provides a contact point between service providers and NFC mobile phones. Service providers can provide NFC mobile phones with remote multi-application management functionality through the TSM

What the NFC Payments Ecosystem Looks Like Using Mobile Devices?



What the NFC Identity/Access Ecosystem Looks Like Using Mobile Devices?



Trusted Channels of Communications

Identity Credentials on a Mobile Device

Challenges

- Private Keys/ non-repudiation
  - Private keys currently generated on card and not exportable/ clonable under FIPS 201 to other tokens (but NIST examining it)
- Who owns and manages Secure Element?
  - MNOs?
  - Handset Maker/ OS-apps-cloud services provider?
  - End-user/ Employer or gov't agency (MicroSD)?
- Mobile credentials delivery
  - Reading existing FIPS validated PIV card using 14443 protocol
  - MicroSD as a separate token issued and managed by end user
  - CMS to mobile device manager to mobile device with embedded secure element – full credential with cryptographic signing keys

Alternatives to NFC for Payments

- Identity/Access alternatives are similar but the availability has not fully matured

	Integrated NFC	MicroSD	Stickers, Fobs	Bar Codes	Payments in the Cloud	SMS
Reliability	●	◐	◕	◔	◕	◔
Transaction Speed	●	●	●	◕	◐	◕
Security	●	●	◕	◔	◐	◐
Ease-of-Use	●	◕	◕	◕	◐	◐
Wallet Functionality	●	●	○	○	●	○
Acceptance	◔	◔	◔	◔	○	○
Device Availability	○	◕	◕	●	●	●
Additional Value Add Applications	●	◕	○	◐	●	○

Legend: Worst ○ ◔ ◐ ◕ ● Best

What Is Left To Be Done?

Knowledge Gap Surrounding NFC technology

- Technical:
  - How NFC services work on multiple brands and models
  - NFC security models (USIM, MicroSD cards, Embedded SE)
- Payments and Access Security:
  - Understanding end-to-end security
- Consumer Awareness and Acceptance Training
  - How does it work?
  - When & where to use it or
  - Where will end-user applications come from?

Will NFC accelerate contactless reader and digital credentials acceptance?

Satisfy regulators, media, security professionals about data protections and security methods

How to Apply What You Learned Today

- How to Apply It
  - Apply mobile payments lessons learned to identity apps
  - Extend existing security architecture to include mobile issuance and transactions
  - Use state of the art digital credentials on mobile devices to leapfrog existing technology shortcomings

Thank You ……

…….Questions?

Randy Vanderhoof
Executive Director
Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
(800) 556-6828
rvanderhoof@smartcardalliance.org

www.smartcardalliance.org