Mobile/NFC Security Fundamentals

Secure Elements 101

- Smart Card Alliance Webinar
- March 28, 2013

Introductions

- Brent Bowen, INSIDE Secure
- Chair, Mobile & NFC Council, Smart Card Alliance

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

- **Introductions:** INSIDE Secure & Chair, Smart Card Alliance Mobile & NFC Council
- **Secure Element Fundamentals:** Sridher (Sree) Swaminathan, Director Product Development - TSM and Chip Solutions, First Data
- **Types of Secure Elements**: Sanjiv Rawat, NFC Technical Account Manager, Mobile Security, Giesecke & Devrient
- **Secure Elements in Action**: Greg Coogan, Field Marketing North America, Morpho
- **Q&A:** Randy Vanderhoof, Smart Card Alliance

Secure Elements 101

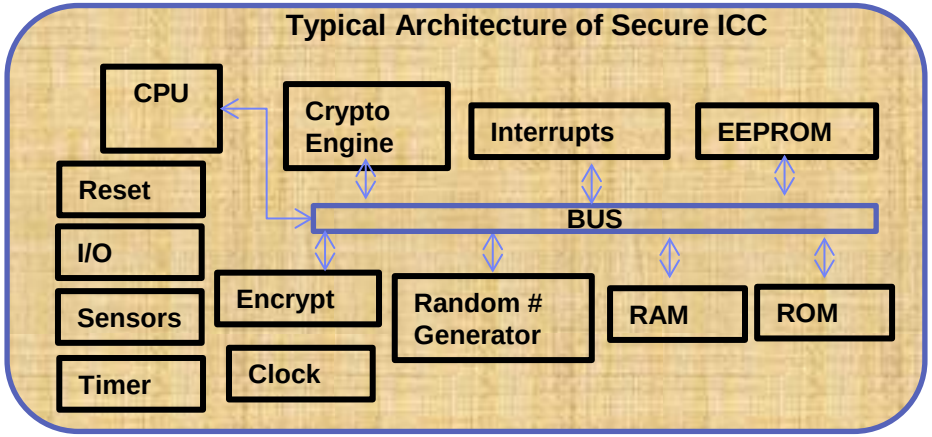
- Sridher (Sree) Swaminathan
- Director, Product Development -TSM & Chip Solutions
- First Data

What Is a Secure Element

- Secure Element
  - A tamper resistant Smart Card chip that facilitates the secure storage and transaction of payment and other sensitive credentials. Secure Elements are used in multi-application environment and can be available in multiple form factors like Plastic SmartCard, UICC(SIM), eSE, micro SD etc.

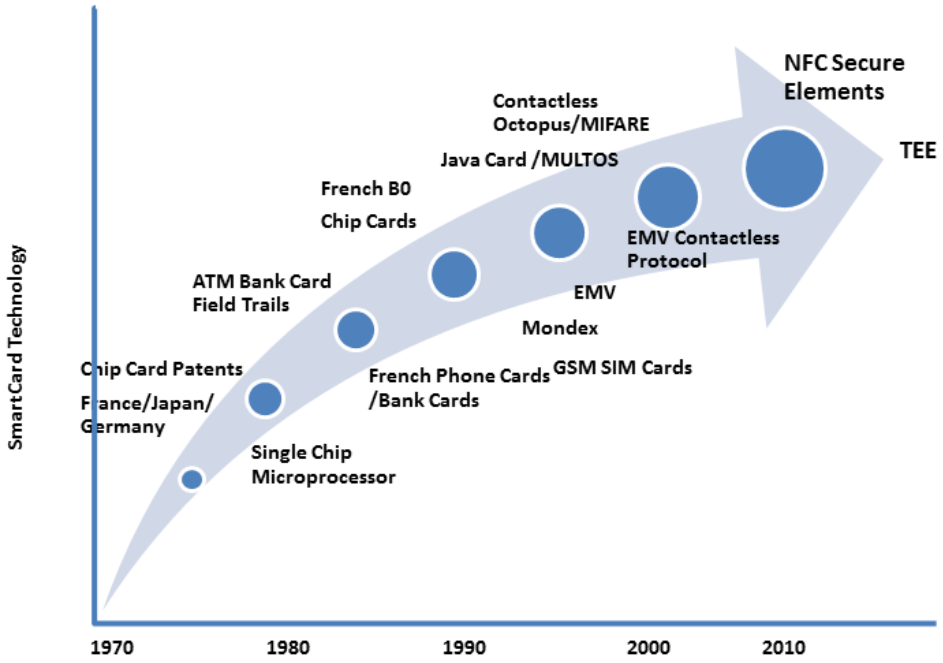
What Is a Secure Element

- **Secure Elements = Secure ICC Cards (Smart Cards)**
  - Secure Microcontrollers
  - CPU
  - Operating System
  - Memory
    - Immutable(ROM), Mutable(EEPROM) and Volatile(RAM)
  - Crypto Engines
  - Sensors, Timers, RNG
  - Communication Ports
  - FIPS, CC Certifications



Evolution of Smart Cards

- From the ‘70s to date…



Types of Smart Cards

Smart Card types

- Contact
  - ICC Cards with contacts for external communications. Card is inserted into a reader/POS terminal for transactions to occur. Follows ISO-7816 standards.
- Contactless
  - ICC Cards with no visible contacts. Communicates using Radio Frequency with 13.56 MHz through antennas. Card is tapped at a distance of up to 4 cm. for read/write. Follows ISO-14443 standards.
- Hybrid
  - Combines the features of contact and contactless cards with 2 separate chips used for contact and contactless interfaces
- Dual Interface
  - Same chip is used for both contact and contactless interfaces

Mobile NFC

- **Near Field Communication (NFC) is a technology in smartphones that can enable contactless transactions and other data exchange with variety devices.**
  - RF Wireless Technology
  - ISO/IEC 14443, 18092, MIFARE, FeliCa etc.
  - Payment, Ticketing, Access, Loyalty & Coupons, etc.
  - Secure Elements help store payment credentials
  - Used in conjunction with Mobile UI(e.g. Wallets)
  - E.g. Google Wallet, ISIS Wallet

Mobile NFC

NFC Forum Specifications

Reader/Writer mode

- Device can read/write any NFC Forum supported tag types.
- ISO 14443 and FeliCa schemes

Peer-to-Peer

- Two NFC devices can exchange data between themselves.
- ISO/IEC 18092 standard

Card Emulation

- NFC device (phone) acts as a contactless card

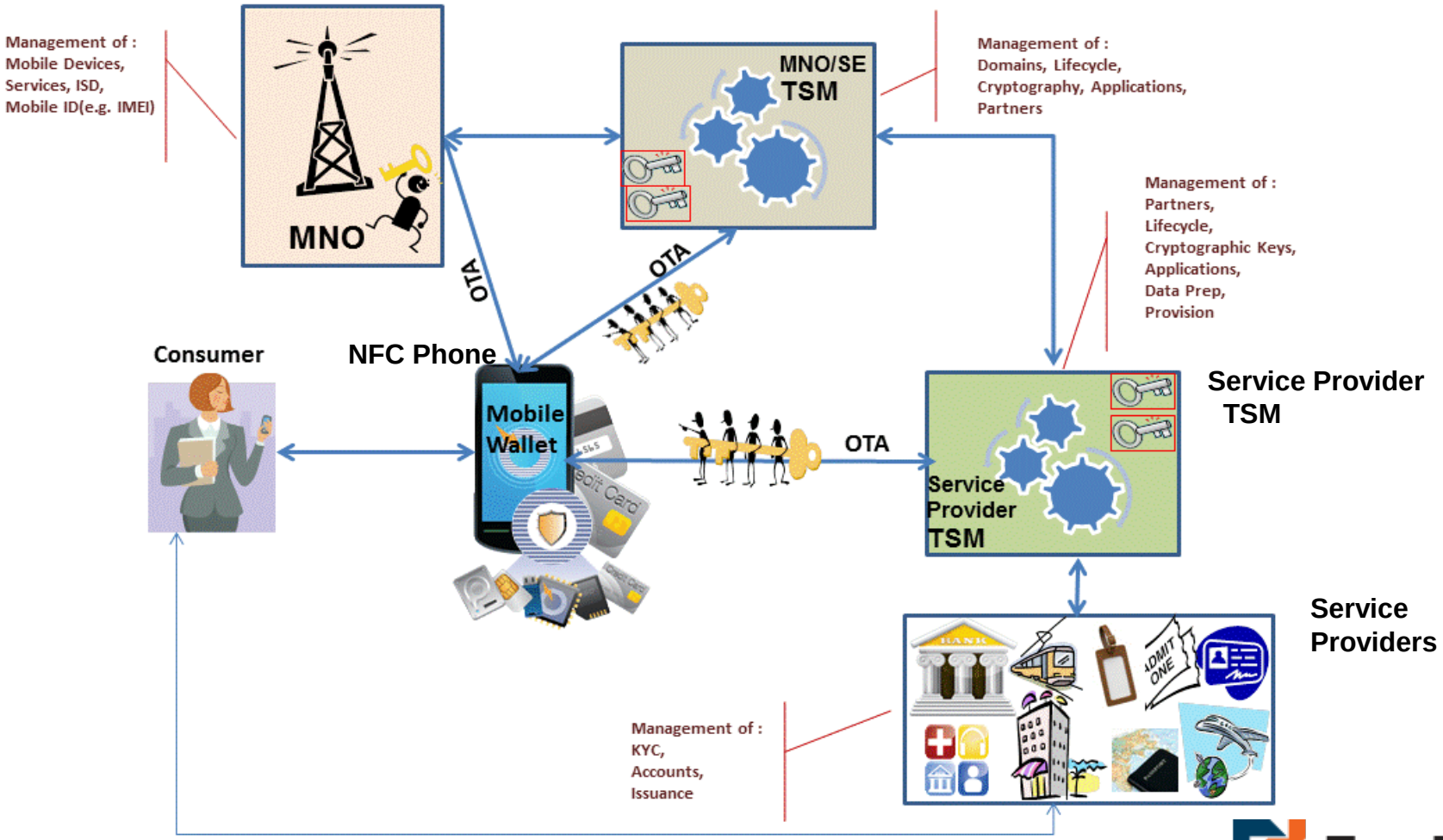
Trusted Service Managers(TSM)

- **TSM is a 'Trusted Third Party' that brings the service providers together for the provisioning and life cycle management of Payment, Access, Transit and other Secure Element related credentials in a secure manner.**

  E.g. - First Data, G&D, Gemalto etc.,

- **TSM Functions**
  - Provision/Deletion
  - Key Management/Data Prep
  - Post Issuance Life Cycle Management
  - OTA(Over-The-Air)
- **TSM Models**
  - MNO / SE TSM
  - Service Provider(SP) TSM

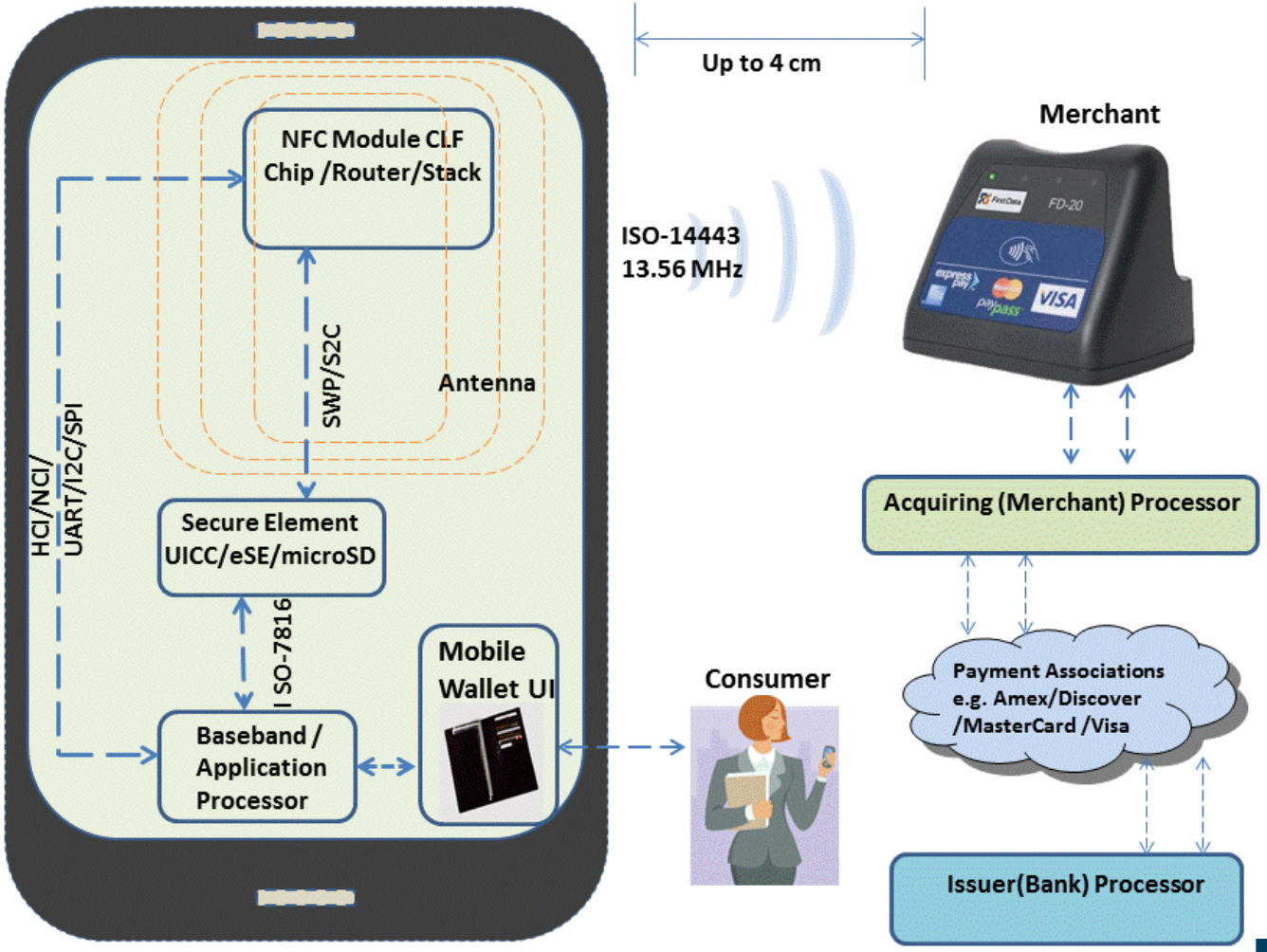
Trusted Service Managers(TSM)



Secure Element & NFC

- **Components of a typical mobile NFC phone**
  - Secure Element(SE)
    - UICC, Embedded SE, micro SD
  - NFC Controller
    - NFC Chip, Stack, CLF
  - Mobile Wallet
    - UI Application for consumer interaction
  - Communication Protocols/Interfaces
    - ISO-7816, ISO-14443, SWP,UART,I2C,SPI
  - Smart OS
    - Android, iOS, BlackBerry OS, Windows Phone
  - SE OS
    - Java, Multos, Proprietary

NFC Phone Architecture



How Does a Secure Element Work?

- **How does a Secure Element work?**
  - Contains an OS –Java, Multos
  - Multiple systems Interaction – MNOs, TSMs, Data Prep systems, POS Transactions
  - GlobalPlatform Specification for Interoperability
  - Communication – Secure Channel, APDUs
  - Multi-Applications – Applets, Security Domains
    - E.g. Payment brands, PPSE, Access, Transit
  - Security
    - Cryptographic Keys – Symmetric, Asymmetric

GlobalPlatform & Secure Element

GlobalPlatform

- Cross industry, international, nonprofit organization which identifies, develops and publishes specifications for a secure and interoperable environment for the chip technology.

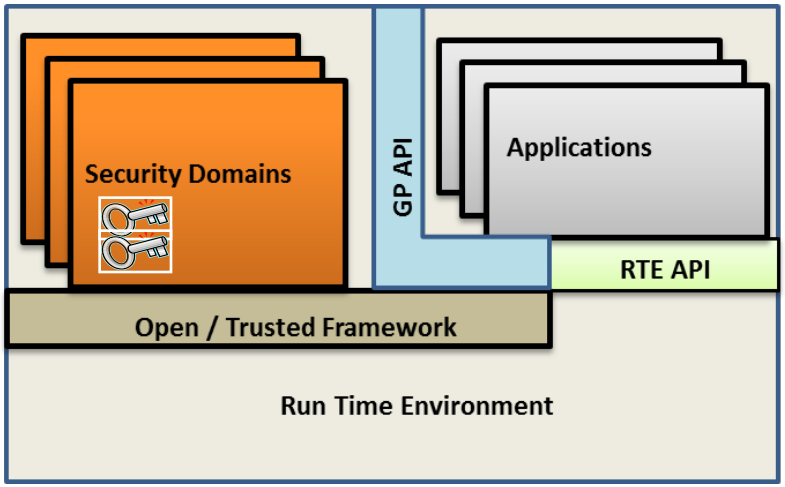
GlobalPlatform Specifications

- Card Specification
- Device Specification
- Systems Specifications

GlobalPlatform & Secure Element

Security Domains

- Area of ownership for entities within the chip
- Issuers
- Controlling authorities
- Application providers



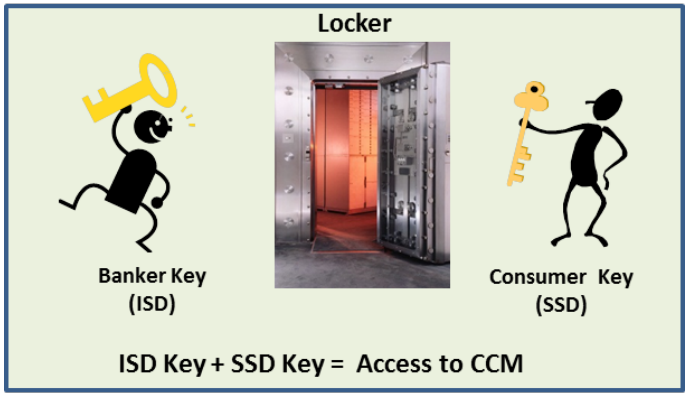
Communication

- APDU
- Secure Channel
- Applications - Installation, Extradition, Provision and Deletion
- AIDs

Security Domains Hierarchy

Security Domains

- Issuer Security Domain
- Supplementary Security Domain
  - CASD
  - TSD
  - APSD

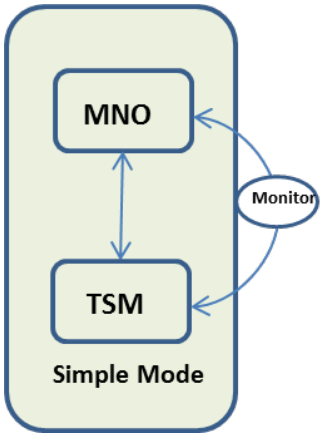


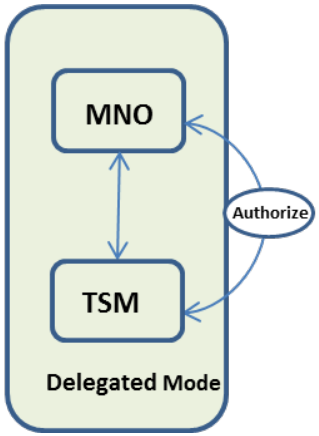
NFC Deployment Models

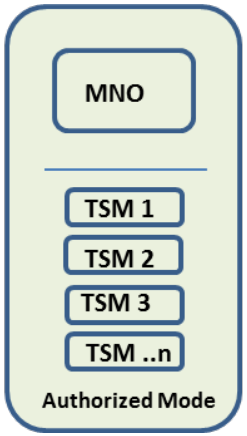
- Simple Mode
- Delegated Mode
- Authorized Mode

TSM Deployment Models

- **Simple Mode**
  - Card Content Management is done by the MNO can be monitored by the TSM.
- **Delegated Mode**
  - Card Content Management is delegated to a TSM with preauthorization
- **Authorized Mode**
  - Card Content Management is fully delegated to a TSM







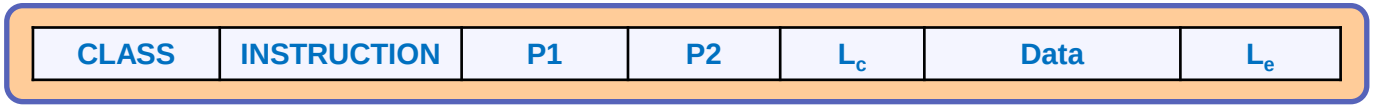
Secure Element Communication

Card Content Management (CCM)

- Loading, Installation, Perso, Extradition, Deletion

APDU -

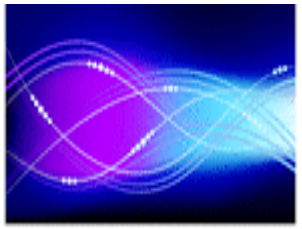
- Application Protocol Data Unit
- Command APDU



- Response APDU

Secure Element Communication

- **Secure Channels**
  - Secure Communication between card and off-card entity
  - SCP02 - Symmetric secure channel protocol
  - SCP03 - Asymmetric secure channel protocol
  - SCP80 - OTA secure channel protocol(ETSI)



- **Keys & Diversification**
  - Master Keys
  - Card Keys
  - Session Keys

- **Provision**
  - Store Data commands – Stores credentials
  - Data Grouping Identifiers – Groups data for storage

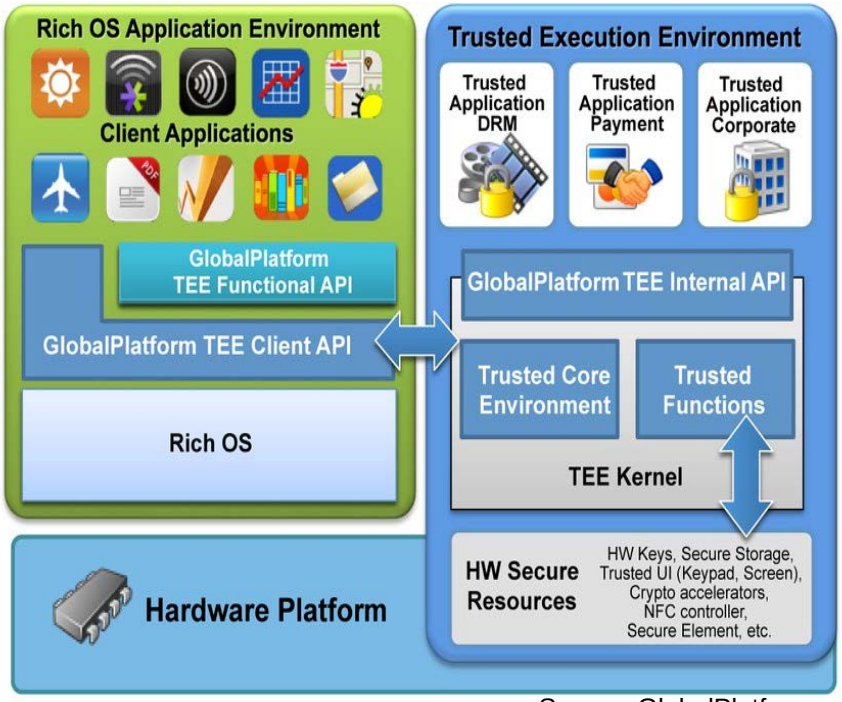
Trusted Execution Environment

- **Challenges in Mobile Device Environment**
  - Malware and Viruses
  - Privacy
  - Financial Fraud
  - Content Protection
  - Enterprise Data
  - Secure Space
- **Solution: Trusted Execution Environment (TEE)**
  - Framework for mobile device security
  - Layer between Rich OS and SE
  - Protection against malware and viruses

Trusted Execution Environment

TEE Architecture

- Environment isolation
  - Rich OS
  - Trusted Applications
  - Secure Element
- TEE Internal API
- TEE Client API
- TEE Functional API

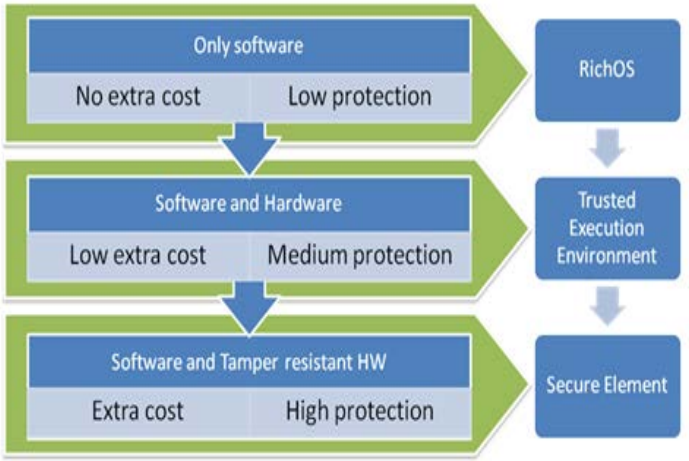


Source: GlobalPlatform

Trusted Execution Environment

Cost vs. Protection

- Higher protection = Higher costs



Source: GlobalPlatform

Potential Use Cases for TEE

- Mobile Payment
- DRM –Content Management
- Corporate Access –Email, Intranet

Standards for SE & NFC

Standards	Purpose
EMVCo http://www.emvco.com/	Global standard for credit and debit payment cards based on chip card(ICC) technology
ETSI http://www.etsi.org/	European Telecommunications Standards Institute is a standardization organization in the telecommunications industry
GlobalPlatform http://www.globalplatform.org/	Organization provides specifications for a secure and interoperable environment for the chip technology
GSMA http://www.gsma.com/	Association of mobile operators for supporting the standardizing and deployment of the GSM mobile system
ISO http://www.iso.org/	International Organization for Standardization. Provides standards for contact(ISO-7816), Contactless(ISO-14443) chip technologies
NFC Forum http://www.nfc-forum.org	Industry association that promotes the specification and use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs.
Payment Schemes	Provides specifications for contact and contactless payments. (Amex, Discover, MasterCard, Visa)
PCI https://www.pcisecuritystandards.org	PCI Security Standards Council provides Payment Card Industry Security Standards -Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS)
FIPS https://csrc.nist.gov	U.S. government computer security standard describes Security requirements and standards for cryptography modules
Common Criteria http://www.commoncriteriaportal.org/	Common Criteria is an international standard for computer security certification. Provides evaluations of Information Technology products and protection profiles

First Data.

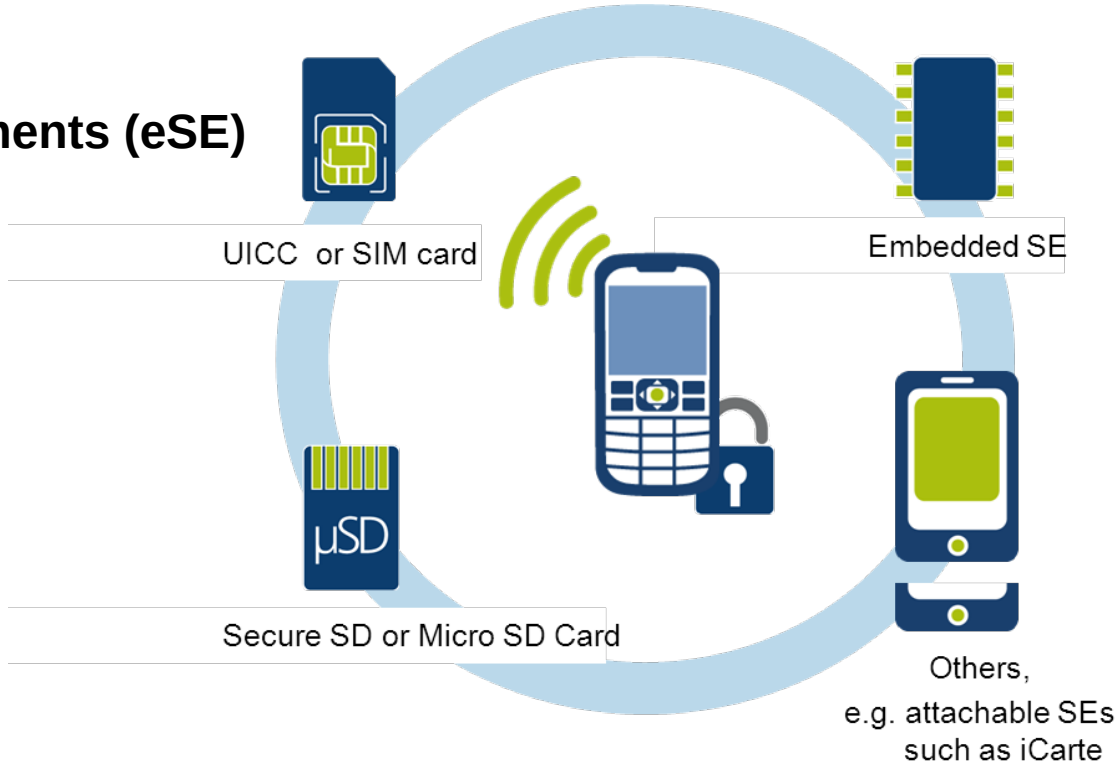
Smart Card Alliance

Types of Secure Elements (SE)

- Sanjiv Rawat
- Technical Account Manager
- Giesecke & Devrient

Types of Secure Elements

- UICC
- Embedded Secure Elements (eSE)
- MicroSD
- Stickers (Not a SE)



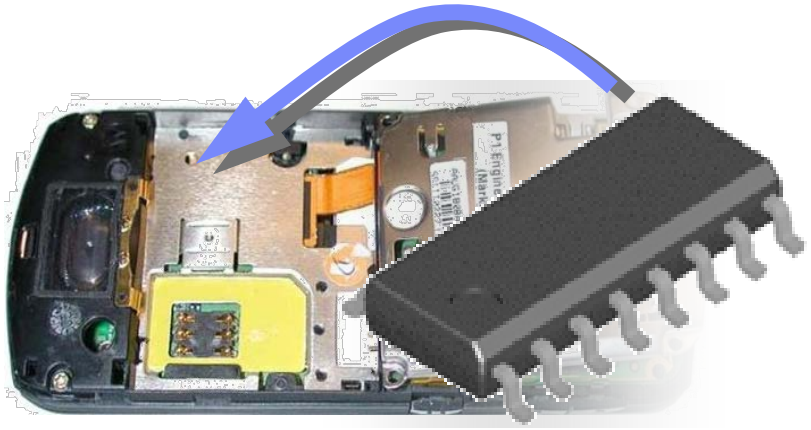
Different types of SEs

UICC

- **Mandatory in GSM and LTE standards**
- **UICC already used as SE for storing network information**
  - Applications residing the UICC can include USIM, CSIM, and ISIM
- **Variety of memory sizes available from 256K to 1.2M and beyond, along with a variety of form factors (2FF, 3FF, 4FF)**
- **Built on Java card and GlobalPlatform standards allowing**
- **GP security standards allow for security domains (SD) where 3rd parties can manage their own applications on the UICC**
  - Banks, retailers, and transit authorities for their secure applications based on GP Specs
  - 3rd parties are granted access to SDs by the issuing MNO
  - MNO provides each 3rd party with a unique security key to access its SD
- **UICC communicates with the NFC controller in the handset through a Single Wire Protocol (SWP)**
- **The UICC plus an NFC-enabled device creates the framework for secure transactions in an NFC environment, while storing secure credentials on the UICC**

Embedded Secure Element (eSE)

- **Similar to a UICC, but in another form factor**
- **Built into mobile devices during the manufacturing process by Original Equipment Manufacturer (OEM)**
- **Cannot be removed from the mobile device**
- **Does not require the same level of standardization as the removable type**
  - Follows GP standards vs. telecommunication standards
- **Issued and managed by either the OEM or MNO**



MicroSD

- **Changes any mobile phone to an NFC phone**
  - Was considered a bridging technology, now a third option where the SP owns and manages the SE
- **MicroSD SE: With or Without an embedded Antenna**
  - MicroSD with the NFC capabilities and built-in antenna
  - MicroSD without the antenna that requires an external NFC capabilities (i.e.: sleeves or antenna connection)
- **MicroSD issued & owned by a 3rd party (banks, etc.)**
  - No MNO or OEM manufacturer involvement
- **Most handsets have a built in MicroSD slot**
  - Slot position will impact the NFC strength – there is no standard placement of the slots within a mobile device, thus placement can greatly impact the read range and effectiveness
- **Security, issuance and distribution remains completely in the hands of the SP**

Stickers/NFC tags

Bank or Transit Stickers:

- Bridging or companion products for a contactless card emulation
- Stickers are self-adhesive contactless cards designed to be attached to the back of handsets
- Issued by banks as a companion card or as a different form factor cards for contactless applications
- Typically a single application
- No OTA post-issuance life cycle management of applications
- No direct connection to the mobile device

NFC Tags:

- Secure reading smart tags (sharing and pairing of information)
- NFC tags can be easily incorporated into promotional marketing media, such as posters, retail displays, product packaging, direct mail and numerous other print options
- Less secure than Secure Elements

2 Types of Stickers:

- Passive RFID – relies on RF energy transferred from the reader to the tag to power the tag (example: posters, product info, etc.)
- Active RFID – uses an internal power source (battery) within the tag to continuously power the tag and its RF communication (example: toll-gate pass)

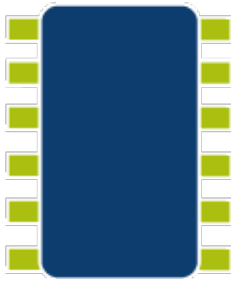
Secure Elements

UICC

- Promoted by MNOs
- New SWP, HCI protocols
- First NFC UICC products available in 2012, many new handset models expected

Embedded SE

- Type and model specified by handset vendor
- Security chip directly embedded into the mobile device
- Technology is available (e.g. Blackberry, Nokia, Samsung)
- Mainly MNO independent



MicroSD

- 3rd party products that are independent of the MNO
- Many handsets today have µSD slots, although RF performance critical
- Combination with m-banking (OTP, PKI), m-commerce

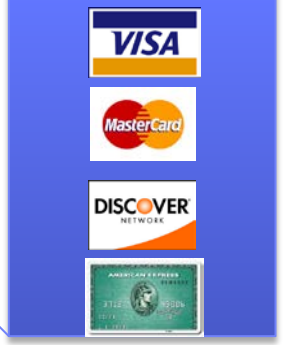
SE Secure Element
SIM Subscriber Identity Module
SWP Single Wire Protocol

The Secure Element in Action

- Greg Coogan
- Field Marketing North America
- Morpho

ISIS Style Deployment of Secure Element

Wallet App



Isis App

NFC Enabled SIM

NFC Enabled Merchant

Mobile Network Operator

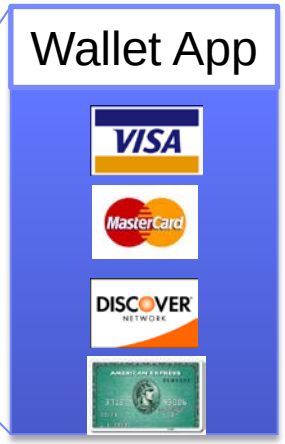
ISIS Consortium

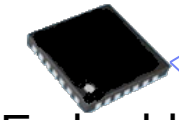
Credit Card Issuers

Merchant Acquirers

Trusted Service Manager

Google Wallet Style Deployment of Secure Element





Google Applet

Embedded NFC Chip

NFC Enabled Merchant

Mobile Network Operator

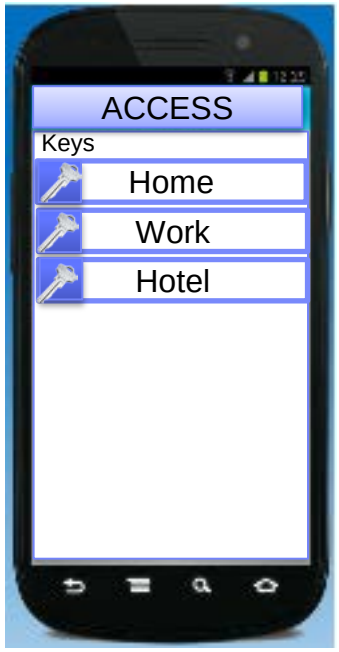
Google Wallet

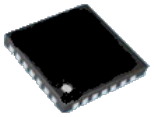
Credit Card Issuers

Merchant Acquirers

Trusted Service Manager

Secure Elements for Access





Access Company

Trusted Service Manager

Hotels
Corporations
Government

Secure Elements in Transit

Controlling Authority

Trusted Service Manager

Payment Provider

Mobile payments platforms may also support transit

Smart Card Alliance

Questions & Answers

Mobile & NFC Security Webinar Series

- **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 Technlogies; Jonathan Main, NFC Forum/MasterCard; Steve Rogers, IQ Devices; Tony Sabetti, Isis; Randy Vanderhoof, Smart Card Alliance

NFC Solutions Summit 2013

NFC SOLUTIONS SUMMIT 2013

SMART SECURE MOBILE PAYMENTS AND NON-FINANCIAL NFC APPS

May 15-16 | Hyatt Regency San Francisco Airport | Burlingame, California

NFC Forum Smart Card Alliance

- **Brent Bowen, bbowen@insidefr.com**
- **Sridher (Sree) Swaminathan, FirstData.com**
- **Sanjiv Rawat, sanjiv.rawat@gi-de.com**
- **Greg Coogan, greg.coogan@morpho.com**
- **Randy Vanderhoof, rvanderhoof@smartcardalliance.org**

Smart Card Alliance

191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828

www.smartcardalliance.org