Smart Card Alliance

# Secure Elements 101

Sree Swaminathan
Director Product Development, First Data

First Data

# Secure Elements

- Secure Element is 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 UICC(SIM), eSE, micro SD etc.

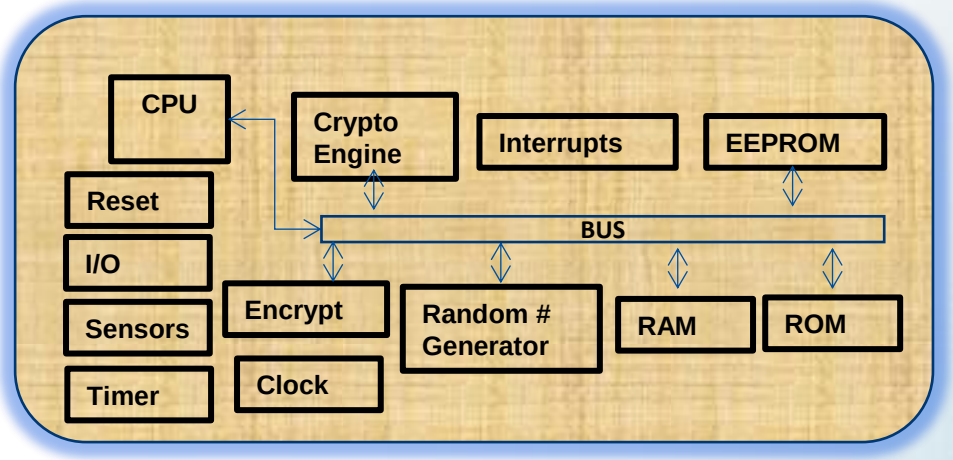

Smart Card Alliance

First Data

# Inside a Secure Element / SmartCard

Secure Elements are similar to Secure ICC Cards (Smart Cards)

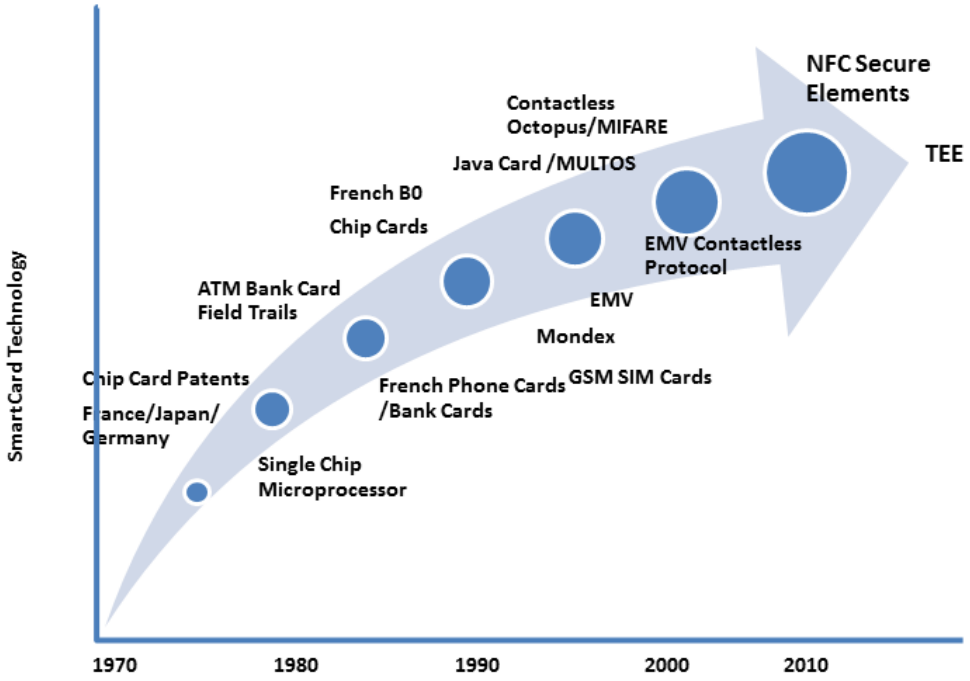
- Secure Microcontrollers
- CPU
- Operating System
- Memory Types
  - Immutable(ROM), Mutable(EEPROM) and Volatile(RAM)
- Crypto Engines
- Sensors, Timers, RNG
- Communication Ports
- FIPS, CC Certifications




Smart Card Alliance

First Data

# SmartCard History



# 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 separate chips used for contact and contactless interfaces
- Dual Interface
  - Same chip is used for both contact and contactless interfaces

Smart Card Alliance

First Data

# Secure Element and 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 etc.

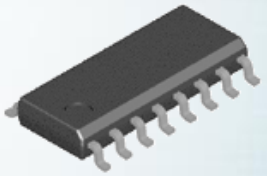

Smart Card Alliance

First Data

# Types of Secure Elements

- UICC or SIM
  - MNO Centric Secure Element
  - UICC modified to include
  - Removable and uses SWP
  - MNO TSMs manage the security and space
  - E.g. ISIS TSM

- Embedded Secure Elements (eSE)
  - OEM or SEI owned
  - Built inside the device mother board
  - E.g. Sprint , Google model




- MicroSD /Dongles
  - Issuer or Consumer centric models
  - Removable

Smart Card Alliance

First Data

# Modes Of NFC Transactions

- 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  acts as a contactless card

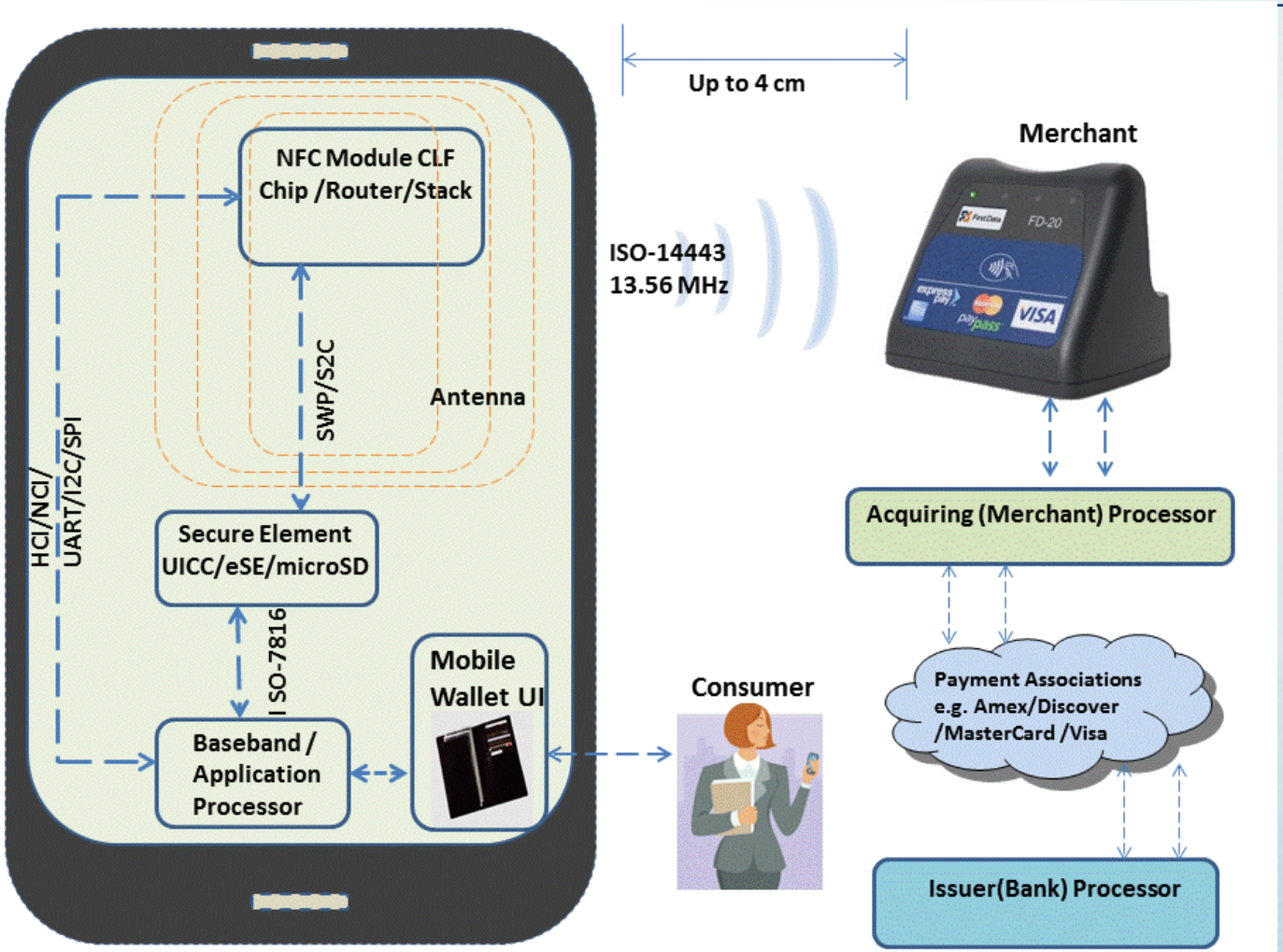

Smart Card Alliance

First Data

# 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

# Secure Element & NFC



# 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.,

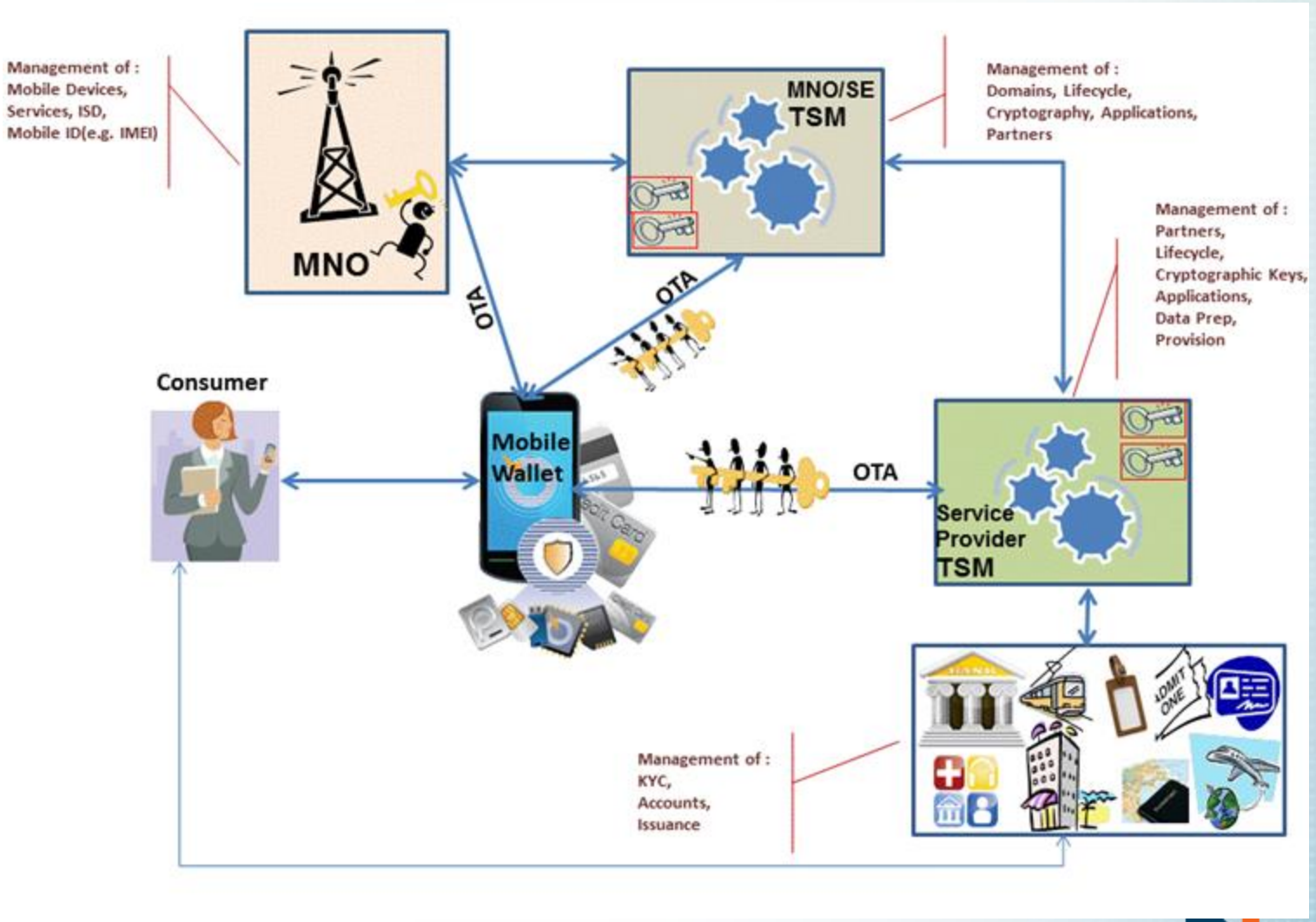
- TSM Functions
  - Provision/Deletion
  - Key Management/Data Prep
  - Post Issuance
  - Life Cycle Management
  - OTA(Over-The-Air)

- TSM Models
  - MNO / SE TSM
  - Service Provider(SP) TSM

Smart Card Alliance

First Data

# Trusted Service Managers(TSM)




Smart Card Alliance

First Data

# Standard organizations for 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

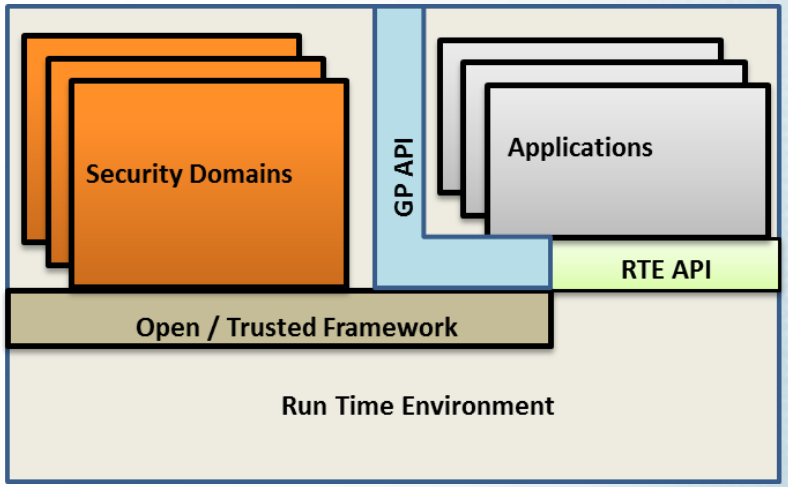
Smart Card Alliance

First Data

# GlobalPlatform & Secure Element

## Security Domains

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




## Communication

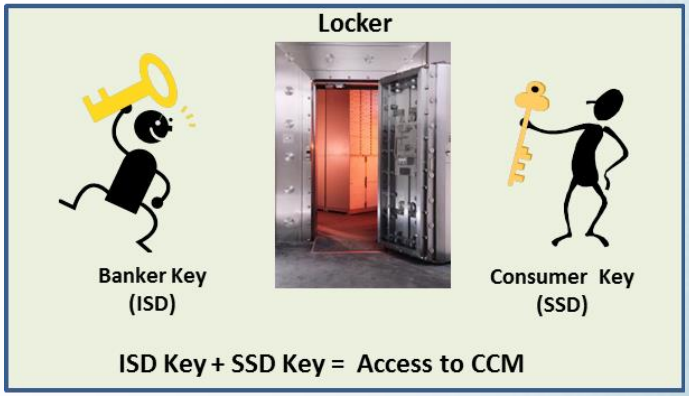
- APDU
- File Structures
- Secure Channel protocols
- Applications - Installation, Extradition, Provision and Deletion
- AIDs

Smart Card Alliance

First Data

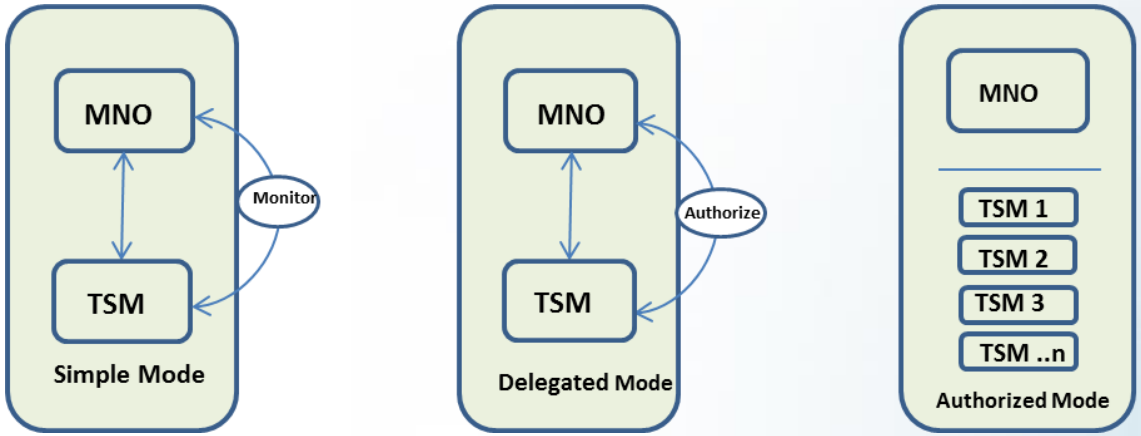
# Security Domains Hierarchy

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



# Security Domains Hierarchy

- 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




Smart Card Alliance

First Data

# Cryptography

- Cryptography for:
  - Confidentiality
  - Data integrity
  - Authentication
  - Non-repudiation

- Types of Cryptography
  - Symmetric key cryptography
  - Asymmetric key cryptography

- Symmetric key cryptography : Same key is used both for encryption and decryption

- Asymmetric key cryptography: Different keys are used both for encryption and decryption

Smart Card Alliance

First Data

# 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

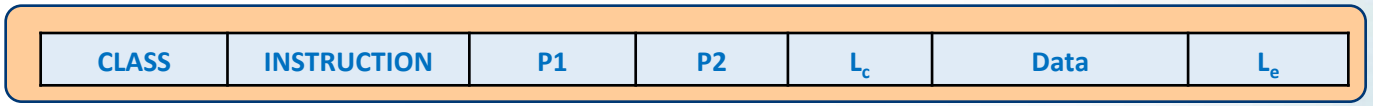
Smart Card Alliance

First Data

# Secure Element Communication

- Card Content Management (CCM)
  - Loading, Installation, Perso, Extradition, Deletion

- APDU
  - Application Protocol Data Unit
  - Command APDU




  - Response APDU

# Deployment and other Considerations

- Credentials Security
- TSM Deployment Model
- Wallet Integration
- Certification
- Lifecycle Management
- Support Model
- Flexibility for changes

Smart Card Alliance

First Data

# Standards for SE & NFC

| Standards | Purpose |
|---|---|
| **EMVCo**<br>http://www.emvco.com/ | Global standard for credit and debit payment cards based on chip card(ICC) technology |
| **ETSI**<br>http://www.etsi.org/ | European Telecommunications Standards Institute is a standardization organization in the telecommunications industry |
| **GlobalPlatform**<br>http://www.globalplatform.org/ | Organization provides specifications for a secure and interoperable environment for the chip technology |
| **GSMA**<br>http://www.gsma.com/ | Association of mobile operators for supporting the standardizing and deployment of the GSM mobile system |
| **ISO**<br>http://www.iso.org/ | International Organization for Standardization. Provides standards for contact(ISO-7816), Contactless(ISO-14443) chip technologies |
| **NFC Forum**<br>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**<br>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**<br>https://csrc.nist.gov | U.S. government computer security standard describes Security requirements and standards for cryptography modules |
| **Common Criteria**<br>http://www.commoncriteriaportal.org/ | Common Criteria is an international standard for computer security certification. Provides evaluations of Information Technology products and protection profiles |

Smart Card Alliance

First Data

Sree Swaminathan
First Data
Sridher.Swaminathan@FirstData.com