Smart Cards and Standards: What Makes Them Secure

Presented by
Gilles Lisimaque, Sr VP and Co-Founder

Gemplus

Co-Chair - Smart Card Alliance Educational Institute
June 4, 2002
Agenda

- Primary standards & specifications:
  - ISO 7816, PCSC, X509
  - Open Card platforms (Javacard & Multos)
- Security standards and their challenges
  - FIPS 140, Common Criteria
- Specifications for interoperability
  - Global Platform
  - GSA specification
- Industry Specifications
  - GSM (presented in another EI201 Session)
  - EMV
- References for use with RFPs
Where do these standards apply

ISO 7816
- Interface between the card & the terminal

PC/SC
- Common driver interface for all smart card readers connected under Windows

X509
- Digital Signature format & associated certificates

Open OS
- In the smart card only, allows a common application development platform for in-card applications

FIPS 140
- Tamper resistance of a cryptographic device

Common Criteria
- Threat evaluations and secure application protections

GSA specification
- Common way to find data files in cards & common application structures for US Government applications

Global Platform
- Card application management and issuance in the card as well as in the back-end

EMV
- Hardware specifications for smart cards and terminals
- Multi application selection for smart cards
- Credit & Debit: commands and related transaction flow
ISO 7816 – The Card Tool Box

- Consists of 12 parts, all full of options allowing nearly all cards to claim they are in compliance
- Designed to be used as building material by each industry (or even a given application) to select what one wants for its cards and terminals
- ISO 7816 does not promote or even suggests any kind of interoperability
ISO 7816 – The philosophy

• “ Defines the card as seen at the interface”
• Does not define what is inside the card but only the “logical view” of the commands and data structures when they cross the card interface
• Does not define or propose any card application functions and does not link commands in coherent procedures
ISO 7816 – What to reference (1/2)

- **Parts 1 & 2**: The card physical form factor and the location of the contacts is to be observed.
- **Part 3**: The answer to reset and the transmission protocol is to be chosen from a list of options.
- **Part 4, 8 & 9**: A standard command format is available, some basic commands can be chosen (e.g. Select) but the data structure is to be defined by each application (Files and/or data elements and/or data objects or even relational data base SQL like). It is up to each application (or industry) to pick up its own subset from all the available options.
ISO 7816 – What to reference (2/2)

- **Part 5**: Application names in the card should comply with the international naming registration to avoid collisions. Backward compatible with Credit/Debit cards.
- **Part 6**: If the application uses data elements their tag structure and values should comply with this part.

- **Part 7**: is for Relational data bases in cards (SQL)
- **Part 10**: is for non microprocessor cards (memory)
- **Part 11**: will define card biometric commands
- **Part 15**: will define PKCS#15 cryptographic data structures & commands
Personal Computers and Smart Cards

- PC/SC allows applications to be independent of the smart card reader (Windows drivers structure for hardware)
- Microsoft Crypto API allows applications to use crypto services of various crypto devices
- Do not address (yet) a standard mechanism to launch an application when a given smart card is inserted in reader PC
Component relationship

Smart Card Base Components

- Service Providers
- Driver
- Reader
- Smart Card

Part of Windows

Each card requires at least one service provider

Each reader requires a device driver

"Interface"

PC/SC

Smart Card and Standards
Smart Card Crypto Provider

1. Application calls Smart Card Base Provider using CryptoAPI

2. Smart Card Base Provider verifies signature of SCCP before loading it

3. SCCP calls the Resource Manager to establish a connection to a card and reader

PC/SC
Digital Certificates – X509 standard

- Electronically certifies a digital information (equivalent to a public notary signature)
- Signed by a trusted authority (CA)
- Digitally binds the owner of the public key

The following Public Key
5E F8 87 32 AF 7E C9 7A 76 1E 49
belongs to John Doe at John@Doe.com
Signed: Real Trust Certification Authority
Valid until January 1st, 2003
What are certificates for?

- They bind a “user” or an “information” to a key pair (public-private)
- Helps to:
  - prevent spoofing
  - distribute public keys
  - establish trust
- Are used as electronic identifications for
  - people
  - Devices
  - Data elements
- Provide means to verify in an off-line environment the authenticity of a piece of data (similar to a public notary certificate for papers)
  - Biometric template reference
  - Identification number
CA the CApstone ...... Of PKI

CA
Digital
Certificates

Public Key
Technology

Digital Signature

Public Key
Private Key

Protocols

IPSEC SET SSL x509 S/MIME

Applications

Browsers
E-Mail

Customers and Market

X509
JavaCard & Multos – Open OS

- The proprietary smart card Operating Systems of the nineties are being replaced by open specifications using Virtual Machines such as JavaCard and Multos.
- It allows card and application Issuers to be more independent of the card manufacturers (Open offer)
- It allows application developers to hit the market faster by deploying software only and not the cards
- When used in conjunction with a secure card application management it allows true multi issuers
- The use of an interpreter in the card allows a secure firewall between applets coming from different sources
JavaCard Architecture - On-Card components

Card/Reader interface

In card API

- Card application management
- WG10
- Applet xyz
- GSM

Virtual Machine

Native Functions & System Resources

Hardware

Matches the application in the terminal (and the network)

Open Card OS
MULTOS Architecture - On-Card components

Card/Reader interface

In card API

- Applet Management
- EMV MC
- MONDEX
- GSM

Virtual Machine

Security Manager

ICC Processor Facilities

Processor

Matches the application in the terminal (and the network)

MEL Language JAVA Translator

Open Card OS

Smart Card and Standards
Comparison JavaCard & MULTOS

- JavaCard: a standard, flexible tool box
- A known language and an easy tool for applet developers in cards
- Requires the addition of Global Platform (or similar) to manage the card and its applets

- MULTOS: a turn key system
- Comes as a complete package for cards issuers, with its certification authority, language, tools and personalization process
- Global platform is possible
Split VM Architecture for development

- The converter (off-card)
  - Class loading, linking and name resolution
  - Verification
  - Bytecode optimization and conversion
- The interpreter (on-card)
  - Bytecode execution and security enforcement
Requirements for Issuers

• Java Card in itself is not sufficient
  – It defines interoperability at the developer level (API in card but not at the interface)
  – It does not help the card issuer to really manage the applications in the card

• Issuers have specific requirements
  – Interoperable application management
  – Clear definition of life cycles for open cards
  – Issuer application domains enforced on the card
  – Multiple application providers on a single card

Global Platform addresses these issues
FIPS 140

- Specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system

- Requirements
  - Cryptographic modules
  - Module interfaces
  - Roles & Service
  - Finite state machines
  - Physical Security
  - Software Security
  - Cryptographic Key Management
  - Cryptographic algorithms
  - EMI/EMC
  - Self-tests
Four Incremental Security Levels

- “Formal models” and “proofs”
- Strong physical security (intrusion detection, tamper resistant coating, environmental fluctuations)
- Identity based Authentication
- Enhanced physical security (critical security parameter I/O, zero-ization of sensitive data on intrusion detection)
- Device authentication
- Improved physical security (e.g. tamper evident coating)
- No Physical Security Mechanism
- Basic requirements for a cryptographic module (e.g. the encryption algorithm must be approved by FIPS)
FIPS 140 & Smart Cards

- Smart Cards are more than just a cryptographic device and they compare more to portable computers security for many applications.

- FIPS 140 addresses ONLY cryptographic devices and it is not easy to isolate the cryptographic hardware & functions of a smart card.
Common Criteria Security Standards

- Common Criteria for Information Technology Security Evaluation
- ISO Standard 15408 (version 2.1)
- Single (common) IT product/system security criteria
- Mutual recognition of product evaluations
- Better availability of IT security-capable products
Common Criteria Model

- Not a “to do” list as FIPS 140 but uses a threat/vulnerabilities/countermeasure model
  - Requires more work from the application

- An industry establishes a list of threats
- The application addresses its vulnerabilities
- The product shows its countermeasures

- The product shoots for a “Security Target” in the “Protection Profile” of its application field.
Common Criteria Security Standards

- **Description of requirements**
  - Protection profile and security target
  - Catalog of security functional requirements
- **Evaluation of security features**
  - Catalog of assurance requirements
  - Seven Evaluation Assurance Levels (EAL)
    - EAL1 to EAL7 increasing security
    - EAL 5 and over is not “cross border” equivalent
    - Closely related to TCSEC Orange Book
Protection Profiles for Smart Cards

- **SCSUG Smart Card Protection Profile V3.0 (US)**
  - Work from the 6 major payment associations
  - Addresses 23 threats most of which are oriented towards the card issuer & the end-user

- **European Protection Profiles for Smart Cards:**
  (a Russian doll approach)
  - PP/9806 - Smartcard Integrated Circuit Protection Profile v2.0
  - PP/9810 - Smartcard Embedded Software Protection Profile v1.2
  - CPP/9911 - Smart Card Integrated Circuit with Embedded Software v2.0

- Information at: http://csrc.nist.gov/cc/
What does the SCUG PP address?

- Defines the smart card life cycle phases
- Identifies the phases associated with the IC manufacturers and with other authorities in the life cycle
- Identifies the needs of the phases
- Identifies the Security Administrators and Users for each phase in the life cycle
Smart Card Life Cycle

1. Embedded software development
2. IC development
3. IC manufacturing and testing
4. IC Packaging and testing
5. Smart card product finishing process
6. Smart card initialization & personalization
7. Smart card issuance and use
Conclusion on Security Standards

- FIPS 140 gives a generic level of security insurance for a given cryptographic product but with no guarantee the application will use it correctly and will globally be secure in any way.

- Common Criteria forces the application to work on its specific risk assessment and define the level of security required in all aspects of its system.
GSA Specification
Smart Card Interoperability Spec

• Provides Solutions to Interoperability Issues
  – Client Applications and Smart Card Communication
  – Tight Coupling between Client Application and SC APDU Sets
  – Evolving “Card Edge” Interface and Card Data Structure
  – Works for Both File System and Virtual Machine Cards

• Defines Architectural Model for Interoperability
  – Basic Services Interface (BSI) for Client Applications
  – Virtual “Card Edge” Interface (VCEI) as Interoperability Mechanism for incompatible existing cards
  – Common Data Model (CDM) Structure with Card Capability Container (CCC) in SCIS Compliant Smart Card
GSA - SCIS Implementation

- Implemented in the client (PC) by Smart Card Service Provider Modules (SCSPM)
  - Basic Services Interface (BSI)
    - API for applications that call SCSPM
  - Virtual Card Edge Interface (VCEI)
    - API for SCSPM to communicate with cards

- Implemented in the card by
  - Common Data Model (CDM)
  - Card Capabilities Container (CCC)
GSA – SCIS Card model

• Common Data Model (CDM) Structure
  – General Information coded using TLV objects
  – Includes a Card Capabilities Container (CCC)
  – Protected Personal and Card Information such as Biometric and Digital Signature Certificates
  – Data structures for Login & Access control applications

• Card Capability Container (CCC)
  – Mechanism for translating APDU sets
  – Describes how a given card differs from Virtual Card Edge Interface (VCEI)
  – Maps: card APDUs <-> Virtual APDUs
  – Grammar for translation rules (CCG)
Global Platform

- Global Platform specifications define a standard for Card Issuers to create multi-application chip card systems. It defines card components, command interfaces, transaction sequences, and interfaces, which can be common across many different industries.

- The Global Platform gives Card Issuers the power to manage and change the content of their cards while also offering the ultimate in flexibility by enabling them to share control of some of their card space with business partners. The ultimate control always rests with the Card Issuer, but through the Global Platform, the business partners of a Card Issuer can be allowed to manage their own applications on the Card Issuer’s cards as appropriate.

Extracted from Open Platform Card Specification 2.0.1 – April 2000
Global Platform Features

• Complete Card Life Cycle Management
  – defines requirements and roles of every party involved with cards and applications
  – separates application management
• Defines Smart Card Management System (SCMS) and its functions
• Provides a Secure Install mechanism
  – applet delivery controlled by the Card Issuer
  – applet delivery performed by an Applet Provider: well adapted to Internet
• Velocity Checking Security mechanism
  – refines the security policies
Global Platform Card Domain

• Provides card global services:
  – management of applets (life cycle, install, etc)
  – access and management of global card data (ICC Serial number, personalization information, etc)
  – management of card life cycle (blocking, auditing, ..)
  – management of the of a mapping between security domains and applets

Acts as the security domain manager.
The card registry is controlled by the card issuer
Global Platform Application life cycle

- INSTALLED
- SELECTABLE
- PERSONALIZED
- LOGICALLY DELETED
- BLOCKED
- LOCKED

Global Platform
Smart Card and Standards
EMV – Europay Mastercard Visa

- First publication in 1996
- Current version: EMV 2000 version 4.0
- Four volumes
  - Physical and electrical characteristics of the card
  - Organization of applications within the card and the set of commands
  - Transaction flow allowing a purchase process
  - Terminal Specification

- [http://www.emvco.com](http://www.emvco.com)
EMV Specification

ISO 7816 – 1/2/3

EMV Part 1
Physical Characteristics
Electrical Characteristics
Communication Protocol

EMV Part 2
ISO 7816-4 to 9
Command Set

EMV Part 3/4
Transaction Process
What is EMV for?

- Allows to design world wide accepted Credit and Debit applications in smart cards
- Three layers of interoperability
  - Basic common layer between payment systems
  - Same payment system between card & terminal
  - Same financial institution for card & terminal
- Allows multiple application cards to be used in multi-application terminals (standard selection mechanism)
EMV Context Risk Management

- Issuer Specific
- Payment Association Specific: Europay or MasterCard or Visa
- EMV Core or Common Specifications
- Card Operating System

**Merchant**

- Same Financial Institution than the card’s Issuer
- Same Payment Association than the card’s Issuer’s
- Any Payment Association back end system compliant with EMV
EMV Risk Management:

• Unlike the magnetic stripe card, the *smart card* takes decision to: - Accept, -Deny, or -Ask for an on-line authorization to the card Issuer bank.

• Decision taken according to
  – the "Risk Management" rules stored within the card at personalization stage by the Issuer
  – The level of knowledge the card issuer and the merchant financial institution have about each other (e.g. revocation lists)

• Parameter of decision can be:
  – Purchase amount
  – Cumulative amount
  – Number of consecutive off-line transactions
  – Random security check
The card, and the terminal decide if it is worth the time and the cost of going online.

The risk management rules are defined by each issuer and managed by the card.

1. Do you accept this 30$ Transaction?
   - No, please ask my bank issuer (amount of 30$m is higher than the limit).
2. Give me the signature.
3. Do you accept $30 Transaction?
   - Yes, I accept it.
4. EMV Terminal
5. Digital Signature
6. EMV
Conclusion: What about Interoperability?

- There are different aspects to interoperability
- Solutions available
  - Development in the cards have been simplified thanks to Java
  - Hardware terminal specifications are clarified with EMV
  - Multi application selection is possible for cards and applications compatible with the EMV Selection mechanism
  - Multi application management with Global Platform
- Issues still pending
  - No standard way for a PC to find (or launch) an application on the network by looking at the card inserted
  - No browser equivalent in smart cards. Card application element (applet) tied tightly with the applications in the terminal as well as the back end systems
Specifications & application layers

Global Platform

Card Manager
  - Card Configuration
  - Personalization
  - Applet Download
  - Card/Application Maintenance

SC Reader

GP Card Manager
  - GP API
  - Applets
  - Run Time Env (RTE)

GSA - SCIS

Applications
  - BSI
  - XSI
  - SPS
    - Virtual Card Edge Interface
    - Reader Driver

SC Reader

CDM	CCC

PC/SC

Applications
  - SCSP
  - CSP
  - Resource Manager
  - Reader Driver

SC Reader

Smart Card
References to Standards and Specifications for RFPs

- Primary standards & specifications:
  - ISO 7816 ANSI or ISO
  - PC/SC Microsoft
  - PKCS RSA Labs
  - X509 ANSI/NCITS

- Industry Specifications
  - GSM ETSI
  - EMV EMVCO
References to Standards and Specifications for RFPs

• Card Operating Systems
  – Proprietary
  – JAVACard
  – MULTOS
  Card vendors
  Javacard forum
  MASCO

• Specifications for interoperability
  – Global platform
  – GSA specification
  GSA/NIST

• Security standards
  – PKCS
  – FIPS 140
  – Common Criteria
  RSA Labs
  NIST
  ISO/NIST
Contact Information

Jim F. “Jim” Russell
Director
MasterCard International
Http://www.Mastercardintl.com
James_russell@mastercard.com

Gilles M. Lisimaque
Senior Vice President
Gemplus Corporation
Http://www.Gemplus.com
Gilles.Lisimaque@Gemplus.com