Smart Card Technology Capabilities

Won J. Jun

Giesecke & Devrient (G&D)

July 8, 2003
Table of Contents

• Smart Card Basics
• Current Technology
• Requirements and Standards
• Next Steps
Smart Card Basics

- Definition
- Components
- Different Types
- Standards and Specifications
- Applications
Definition

• What is a smart card?
  – A plastic card with an embedded microprocessor chip.

• What is the essence of a smart card?
  – Authentication
  – Data storage
  – Validation
  – Self-lock mechanism
The Dimensions

Smart Card according to ISO/IEC 7810 and ISO/IEC 7816-2

- Magnetic Stripe: 19 mm x 29 mm x 54 mm
- Embossing: 10 mm x 85.6 mm x 0.76 mm

Smart Card Technology Capabilities
The Contacts

Contacts of the Smart Card Module according ISO/IEC 7816-2

- VCC  Power Supply Voltage
- RST  Reset
- CLK  Clock
- RFU  Reserved for Future Use
- GND  Ground
- VPP  Programming Voltage
- I/O  Input/Output
The Module

Cross-Section of a Smart Card Module

Adhesive Area
Bond Wire
Globe Top Covering
Epoxy Tape

Chip/Dye
Contact Plate/ Metallization (Au/Ni/Cu)

12 - 14 mm
0.2 mm
0.6 mm
The Chip

- Features:
  - 32 kByte ROM
  - 16 kByte EEPROM
  - 1.3 kByte RAM
  - Crypto Unit ACE

- Chip size:
  - Area = 21.23 mm$^2$
  - $x = 4.28$ mm, $y = 4.96$
Different Types

Contact

Contactless

Hybrid

Dual-Interface (Combi)
How Smart?

• Simple Memory Card
  – No Security

• Intelligent Memory Cards
  – Access Control Conditions for defined areas
  – Dedicated functionality (e.g., Telephone-Chip Card)

• Microprocessor Card
  – Microcomputer / Microcontroller

• Super Smart Card
  – Microcomputer, Keypad, Display, Battery, etc.
Relevant Standards and Specs

- ISO 7810
- ISO 7816
- ISO 14443 Types A and B
- Java Card 2.1.1 and 2.2
- Global Platform Card Specification 2.0.1’ and 2.1
- GSCIS v2.1 (draft)
Types of Usage

- Identification and authentication
- Encryption and digital signature (RSA 1024/2048 bit; on-card key-pair generation)
- Biometric (on-card matching)
- Secure Data storage
- Single Sign-on
Assessing the Current Technology

Areas to Assess:
• Card Operating System (COS)
• Protocol
• Memory capacity
• Functionality
There are Pro’s and Con’s for both types of COS’s. Both can be made secure and flexible. It is analogous to comparing Unix and Windows®™ operating systems. The philosophical arguments can be made for file-structure-based or Java-based card.

However……Java Cards are in fashion!
File-Structure Based Smart Cards
Purpose of a Smart Card OS

- Secure Messaging
- RSA Signature
- Data Structures ISO 7816-4
- Dynamic Installation
- Transmission T=1, T=0
- Encryption
- Multi-Application
- State Machine Concept
- Access Control
- Multi-Purpose Command Set
- International Standards
- ISO

Smart Card Technology Capabilities
• Security is provided by the JCVM, Firewalls and Security Domains
Java Card Basics

• A multi-application smart card
  – Several applications can be loaded on to the same card
  – “Firewall” between applications
  – Sharing between applications
  – ISO-7816/4 compliant application selection.

• Smart card interoperable--
  – at the source code level
  – at the load file level
  – at the loader level.
Protocol

- T=0 : Byte transfer. Developed by the French
- T=1 : Block transfer. Developed by the Germans
- USB : Based on existing USB v.1.1+ Specs.
Memory Capacity

• 16 KB
• 32 KB *
• 64 KB
• 128 KB

* Currently most popular
Functionality

Highlights:
• RSA 1024/2048 bit algorithms
• Triple-DES, SHA-1
• On-card key-pair generation
• On-card Biometrics matching engine
Biometrics On-card Matching

• **Main advantages:**
  - Sensor independent

• **Latest developments:**
  - Fingerprint on-card matching
  - Iris on-card matching
  - On-card matching Java applet
Basics of On-card Matching

– The actual data is preprocessed in the background system and sent to the card
– Biometric verification takes place on the chip card
– Reference data does not leave the card
– The card itself changes the security status (e.g., unblocks itself) after a successful verification.
Other Form Factors

- Smart chip with USB interface.
  - Same Chip Operating System as on smart card.
  - Connectivity through USB port. Smart card reader not necessary.

- Three features in one single USB device:
  - Multiapplication smart card operating system
  - Fingerprint sensor
  - Image processing software
Current Trends

- Java Card 2.1
- Global Platform 2.0.1’
- 32 to 64K EEPROM
- On-card key-pair generation (RSA 1024-bit)
- Biometric on-card matching (fingerprint)
- Hybrid and composite card bodies (ISO 14443)
- FIPS 140-2, Level 2 or 3
Current Trends
## Requirements and Standards

<table>
<thead>
<tr>
<th>CAC Release 2.0 ICC Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Java Support</strong></td>
</tr>
<tr>
<td>➢ Java Card 2.1</td>
</tr>
<tr>
<td><strong>Standards:</strong></td>
</tr>
<tr>
<td>➢ ISO 7816, parts 1-7</td>
</tr>
<tr>
<td>➢ T=0</td>
</tr>
<tr>
<td>➢ EMV.</td>
</tr>
<tr>
<td>➢ Global Platform 2.0.1.</td>
</tr>
<tr>
<td>➢ DAP verification</td>
</tr>
<tr>
<td>➢ Delegated management and services</td>
</tr>
<tr>
<td>➢ ISO 10373 Parts 1-3</td>
</tr>
<tr>
<td>➢ ISO 7810</td>
</tr>
<tr>
<td>➢ GSCIS 2.0</td>
</tr>
<tr>
<td><strong>Micro-controller/Processor:</strong></td>
</tr>
<tr>
<td>➢ 32KB EEPROM</td>
</tr>
<tr>
<td>➢ 8-bit processor.</td>
</tr>
<tr>
<td>➢ Crypto co-processor</td>
</tr>
</tbody>
</table>
## Requirements and Standards

<table>
<thead>
<tr>
<th>CAC Release 2.0 ICC Specification (Cont’d)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crypto Algorithms:</strong></td>
</tr>
<tr>
<td>• Triple DES</td>
</tr>
<tr>
<td>• SHA-1</td>
</tr>
<tr>
<td>• RSA</td>
</tr>
<tr>
<td>• RSA (1024-bit key length)</td>
</tr>
<tr>
<td>• FIPS PUB 180-1 Secure Hash Standard</td>
</tr>
<tr>
<td>• FIPS PUB 186-1 Digital Signature Standard</td>
</tr>
<tr>
<td><strong>On-Card Key Generation</strong></td>
</tr>
<tr>
<td>• 30 seconds or less</td>
</tr>
<tr>
<td><strong>Security:</strong></td>
</tr>
<tr>
<td>• FIPS 140, Level 2 or 3 validation</td>
</tr>
<tr>
<td>• Countermeasures for Differential Power Analysis and Simple Power Analysis Attacks</td>
</tr>
</tbody>
</table>
Requirements and Standards

Requirements on the horizon:

- \(\geq 2048\)-bit key length
- On-card Biometric Verification
- Contactless PKI
- Hybrid and Dual-interface cards
- Super Smart Cards
Next Steps

• Standards are needed to address the coming requirements.
• Existing standards may need to be updated to accommodate the changing technology.
• Validations are needed to test conformance.