Introduction to Smart Cards

JEAN-LUC Giraud
MacCrypto’01
Outline

■ What are Smart Cards?

■ How do we make them?

■ How do they work?

■ How can you program them?

■ What can you do with them?
What is a Smart Card?

A piece of silicon and a plastic body
A Closer Look (1)
A Closer Look (2)

Contactless Smart Card

Card Body (Front)

Chip

Antenna

Card Body (Back)
Outline

- What are Smart Cards?
- How do we make them?
- How do they work?
- How can you program them?
- What can you do with them?
Manufacturing: Cutting
Manufacturing: Gluing
Manufacturing: Bonding
Manufacturing: Encapsulation
Manufacturing: Finished Modules
Manufacturing: Module on Body

Electrical Initialisation
Manufacturing: Personalisation

Electrical and Physical Personalisation
Outline

- What are Smart Cards?
- How do we make them?
- How do they work?
- How can you program them?
- What can you do with them?
Card Families

Memory

Microprocessor
Memory Cards

- Bitmap, synchronous access
  - R/W
  - R/Erase only

```
1011011011
0011101111
1011011111
```

```
0000000000
0000000000
0000001111
```
Enhanced Memory Cards

- Onboard hardwired crypto engine
  - Card Authentication
  - MAC on balance
Memory Card Application

- Loyalty
- Payphones
Smarter Smart Cards

- Microprocessor based
- Onboard Memory (RAM, ROM and EEPROM/Flash)
- Programmable
- Onboard processing

Security features
- Crypto coprocessor (PK, DES,…)
- Physical sensors (V, freq,…)
- Physical protections (shielding,…)

29/01/2001
Bull Patents
Chip Structure (0.25mm$^2$)
Smart Card Module

- Microprocessor
  - CPU
- Data Bus
- Address Bus
- EEPROM / FLASH
- ROM
- RAM
- Microcontact
- Microchip
- Micromodule
Communications

- One communication channel: serial line

- “Layered” transmission protocol
  - Application: Application Protocol Data Unit
  - Transport: T=0, T=1, T=14
The Application Protocol Data Unit

- An APDU contains:
  - a command message,
  - a response message.
ADPU Syntax

- **APDU Command**
  
  ![Command Diagram]

  - Class (CLA)
  - Parameters (INS)
  - Instruction (P1, P2)
  - Data (Lc)
  - Command Data (Data)
  - Response Length (Le)

- **APDU Response**
  
  ![Response Diagram]

  - Response Data (Data)
  - Status Word (SW)
Example

READ BINARY (P1, P2, Le)

Data, SW

P1, P2 : specify the data to be retrieved
Le : length of data to retrieve

CLA  INS  P1  P2  Lc  Data  Le
A0  B0  xx  xx  0  Le
**Required Infrastructure**

- Personalisation Center
- Issuing Center
- Reader
- Middleware (CDSA)
- Back-end System

http://www.gemplus.com/usb
Middleware (Windows platform)

- PKCS #11
- CAPI
- Token X
- Token Y
- Token Z
- CSP A
- CSP B
- CSP C
- PC/SC
- RS232
- USB
- PCMCIA
- Reader
- GemSAFE
- Hardware
- Software
- PCI
- IBM card
Outline

- What are Smart Cards?
- How do we make them?
- How do they work?
- How can you program them?
- What can you do with them?
Mask your Own Code

Pros:
- Small code footprint
- “Complete” control

Cons:
- Development in C and target assembly language
- Use emulators
- Mask lead time (~2 month)
- Bug fixes
Use Proprietary Cards

What you (usually) get:
- File System
- Fixed set of APDU Commands
  - ✔ Read/Write files
  - ✔ Cryptographic computations

Pros:
- Off the shelf products
- Cheaper

Cons:
- Not extensible
- Bug fixes
Use Open Cards

■ Choice
  ◆ Java
  ◆ Microsoft

■ Standard API
  ◆ Crypto
  ◆ GSM (SMS, Pro active commands... )
Applet Life Cycle

- Write code in Java
- Compile it
- Debug it (simulator)
- Verify and Convert it (specific byte code)
- Load it
  - Personalisation center
  - Point of sale
  - Over the Internet
Outline

- What are Smart Cards?
- How do we make them?
- How do they work?
- How can you program them?
- What can you do with them?
Why use a Smart Card?

Crypto

Theoretical

Practical
Advantages of a Smart Card

- Tamper resistance
  - Storage

- Portability

- Tamper resistance
  - Processing

- Ease of use
- Onboard key generation
Main applications

- Public phone cards (pre-paid)
- Cellular phone GSM cards,
- Banking cards,
- Health cards.
New applications

- Electronic purse,
- Transport,
- Security of information system,
- Identity,
- Loyalty,
- Games,
- Physical access control.
Attacking Smart Cards

- Timing Attacks

- Power Analysis
  - Simple Power Analysis
  - Differential Power Analysis

- Invasive Attacks
  - Probe Stations
  - Focused Ion Beam
Standards: ISO/IEC 7816
Integrated circuits cards with contacts

- ISO/IEC 7816-1: Physical characteristics.
- ISO/IEC 7816-4: Inter-industry commands.
- ISO/IEC 7816-5: Registration system for applications in IC card.
- ISO/IEC 7816-6: Inter-industry data elements.
- ISO/IEC 7816-7: Inter-industry commands for Structured Card Query Language (SCQL).
Resources

On Card development:

- **Java card**: http://www.javacard.org
- **Windows for SC**: http://www.microsoft.com/smartcard/
- **Gemplus**
  - Developer web site: http://www.gemplus.fr/developers/index.htm
  - Developer conference: http://www.key3studios.com/gemplusworld/
  - June 20, 21, Paris.

Middleware:

- **PCSC-Lite**: http://www.linuxnet.com/
- **OCF (java)**: http://www.opencard.org/
- **CDSA**: http://www.opengroup.org/security/l2-cdsa.htm
- **PKCS**: http://www.rsasecurity.com/rsalabs/pkcs/index.html

Questions:

- Jean-Luc.Giraud@gemplus.com
Conclusion

Smart = Personal
Portable
Secure