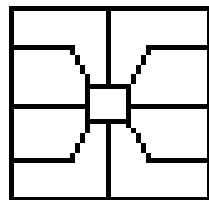


# *Introduction to Smart Cards Technology*



Dr. Vincent GUYOT  
ESIEA / LIP6 – Paris (France)  
vincent.guyot@{esiea,lip6}.fr

# Presentation Outline


- Overview
- Technology Review
- Applications

# Section 1: Overview

# Introduction

- Power of a computer
- Speed and security of electronic data
- Freedom to carry information anywhere
- Computer small to fit inside a plastic card

# Historical Milestones

- 1974, memory card (R. Moreno, Innovatron)
  - 1978, processor "smart" card (M. UGON, BULL)
  - 1980s, France Telecom public phones
  - middle 1980s, banking cards
  - 1990s, mobile telephony security (SIM/USIM)
  - 2000+
- 

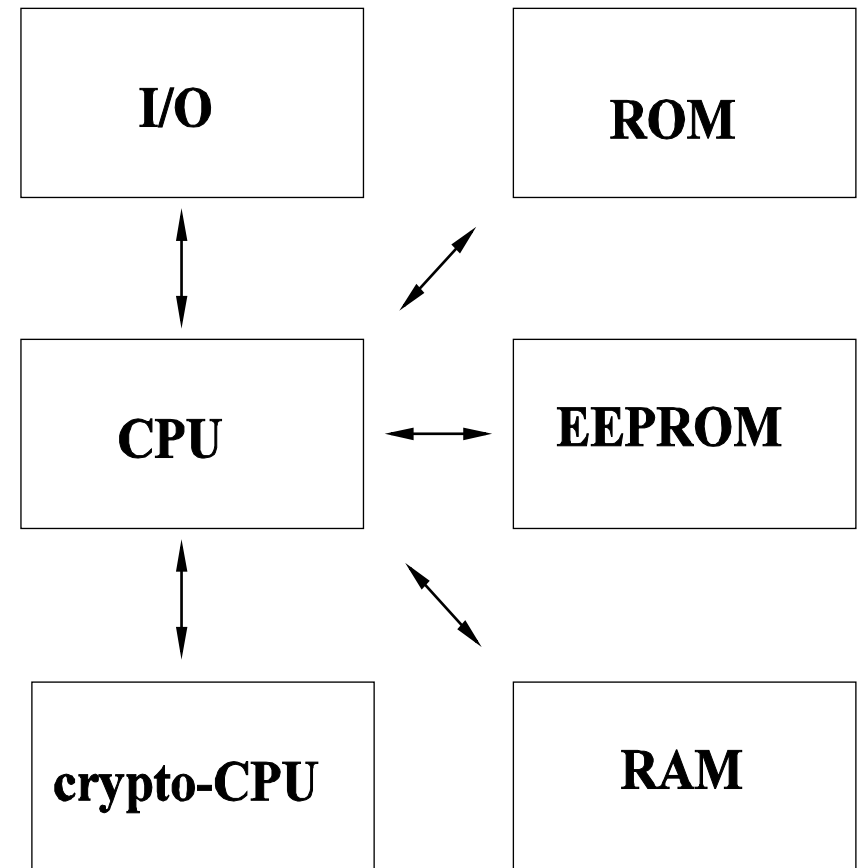


# Smart Card Evolution

- Driving factors of the growing interest in smart cards domain:
  - Declining cost of smart card
  - Growing concern that magnetic cards leak security
  - Smart card technology enables business transactions

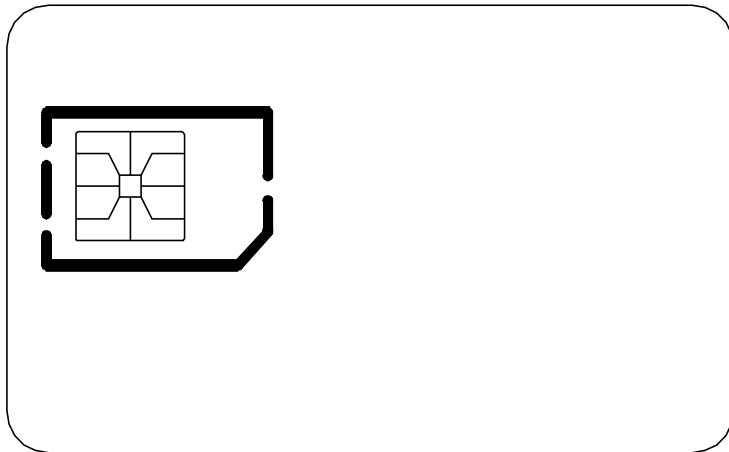
# What is a Smart Card? (1/3)

- Central Processor
- Crypto-processor
- RAM
- Storage memory
- I/O (serial port)

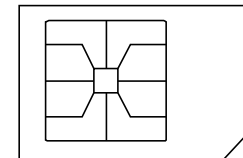


# What is a Smart Card? (2/3)

- Mobile token
- Credit card size
- SIM size



**ID-1**



**ID-000**



# What is a Smart Card? (3/3)

- Look like standard plastic card
- Embeds an Integrated Circuit (IC) chip
- Stores information
- Carry out local processing on the data stored
- Perform complex calculations
- Contact or contactless cards (Radio Frequency)
- Cryptography

# A very secure object

- All-in-one computer
- Non-linear addressing access
- Protection sensors
- Various counter-measures

# How many Cards?

- Billions of card holders worldwide
- More than 90 countries (primarily in Europe)
- Several purposes:
  - Processing point-of-sale transactions
  - Managing records
  - Protecting computers
  - Secure facilities

# Personal Computers facilities

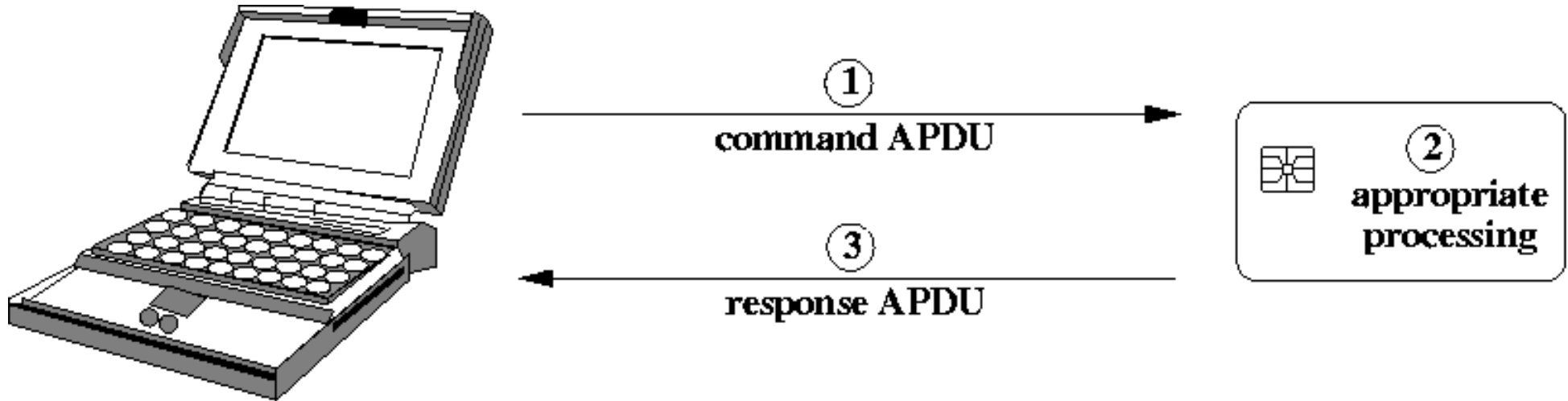
- PC/SC (PC Smart Card) C/C++ dev
- OCF (OpenCard Framework) Java dev
- Windows built-in since win2K (win32/NT add-on)
- UNIX compatibility (MUSCLE project)
- CCID "driver-less" smart card readers
- JavaCard environment → Java card
- Reader-less smart card technology

# Smart Cards Readers

- Serial
- USB
- PC CARD (PCMCIA)
- Keyboard embedded
- Floppy disk form-factor



# Communication process



Mandatory header				Optional part		
CLA	INS	P1	P2	Lc	Data	Le

Command APDU

Optional header		Mandatory part	
Data		SW1	SW2

Response  
APDU

# Section 2: Technology Review

# Section Objectives

- Smart card microchip technology
- Chip Operating System (COS)
- Key features and characteristics
- International standards



# The Micromodule (1/2)

- Smart cards:
  - Credit card-sized
  - Made of flexible plastic
  - Embedded with a micromodule containing a single silicon Integrated Circuit (IC) chip:
    - Memory
    - Processor

# The Micromodule (2/2)

- Eight metallic pads on its surface, designed to international standards:

C1: VCC (power supply voltage)

C2: RST (to reset the microprocessor)

C3: CLK (clock signal)

C4: RFU (reserved for future use)

C5: GND (ground)

C6: VPP (programming voltage)

C7: I/O (serial input/output)

C8: RFU (reserved for future use)

<b>C1</b>	<b>C5</b>
<b>C2</b>	<b>C6</b>
<b>C3</b>	<b>C7</b>
<b>C4</b>	<b>C8</b>

# Micromodule components

- MicroProcessor Unit (MPU): 8 bits to 32 bits RISC up to 32 Mhz
- I/O controller: manage the flow of data between the card and Card Acceptance Device (CAD)
- ROM: where the instructions are permanently burned into memory by the silicon manufacturer
- RAM: temporary storage of results from calculations or I/O communications
- Application memory: EEPROM stores for 10yr+

# What is the COS? (1/2)

- Chip Operating System is a sequence of instructions embedded in the ROM
- Divided into two families:
  - General purpose COS: generic command set
  - Dedicated COS: commands designed for specific applications (example: electronic purse)

# What is the COS? (2/2)

- Management and interchanges with the outside
- Management of the files and data stored
- Access control to information and functions
- Management of card security (cryptography)
- Maintaining reliability (data consistency, sequence interrupts, recovering from an error)
- Management of various phases of the card's life cycle (fabrication, personalization, active time, end of life)

# Key Features and Characteristics (1/2)

- Cost: from \$1 to \$10 (depending of complexity)
- Reliability: 10.000 read/write cycles (ISO: drop, flexing, abrasion, temperature, X-ray, etc.)
- Error Correction: COS performs error checking and sends to the terminal status codes
- Storage capacity: 8K to 4MB (+compression)
- Security: highly secure (temper-resistant, DES, DES3, RSA, ECC, etc.)
- Processing Power: 32 bits RISC / 32 Mhz / 5V

# ISO 7816 Standards (1/3)

- Standards are key to ensure interoperability and compatibility of multiple card and terminal vendors.
- Standardization since 1980's, at national and international levels.
- Standards are established by International Organization for Standardization (70 countries).

# ISO 7816 Standards (2/3)

- 7816-1 governs the physical dimensions of the card: width, length and thickness (credit card)
- 7816-2 governs the dimensions and the locations of the chip contacts
- 7816-3 governs the electric signal and transmission protocol
- 7816-4 governs inter-industry commands and responses



# ISO 7816 Standards (3/3)

- 7816-5 provides a registration system for application identifiers to select an application
- 7816-6 governs data elements for interchange
- 7816-7 governs commands to support a relational database on a card
- 7816-8 governs security related inter-industry commands
- 7816-10 governs synchronous cards

# COS Standards

- Smart cards conform to a set of international standards.
- Currently, no standard Chip Operating System.
- Each smart card vendor provides the market with a distinct product.

# Section 3: Applications

# Section objectives

- Why organizations should consider using smart cards
- The key advantages of smart card technology
- The current obstacles to acceptance of smart card technology
- Examples of where smart cards are used today

# Application areas

- First chip cards: simple pre-paid telephony cards using memory cards
- Now: financial, communications, government programs, information security, physical access security, transportation, retail and loyalty, health care, university identification, etc.

# When consider Smart Cards?

- A portable record is necessary or desirable
- The records are likely to require updating
- The records will interface with several automated systems
- Security and confidentiality of the records are important

# Advantages of Smart Cards

- Capacity provided by the embedded processor and data-capacity for highly secure, off-line processing
- Adherence to international standards
- Established track record in real world applications
- Durability and long expected life span
- COS that support multiple applications and independent secure data storage on one card

# Barriers to Acceptance of Smart Cards

- Higher cost as compared to magnetic cards
- Present lack of infrastructure to support cards
- Lack of standards to ensure interoperability among varying smart card programs
- Unresolved policy and legal issues (privacy and confidentiality)



# Differences with Magnetic Stripe Cards

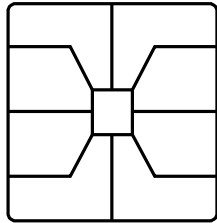
- Increasing complex performance
- Application requirements of today card systems
- Alternative to magnetic stripe cards
- Enhancement to magnetic stripe cards in the form of a hybrid card (micromodule and magnetic stripe)

# Applications areas (1/2)

- Communication applications
  - Secure initiation of calls and identification of caller on GSM phone
  - Activation and subscribing on pay-TV
- Financial applications
  - Electronic purse to replace coins
  - Credit and/or debit accounts
  - Securing payment across the Internet (Electronic Commerce)

# Applications areas (2/2)

- University Identification (variety of applications)
- Health card (containing insurance data)
- Retail and loyalty (card marketed to specific consumer profiles)
- Transportation
  - Drivers licenses
  - Electronic Toll Collection Systems
- Information Security (access card, biometric)



Questions?

`vincent.guyot@{esiea,lip6}.fr`