Smart Card Concepts

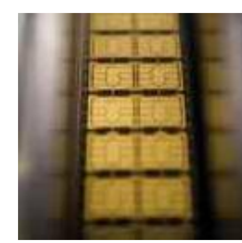
Carte à puce et Java Card

ATAC

2011-2012

Jean-Louis Lanet

Jean-louis.lanet@unilim.fr



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Agenda

- Card Technology
- Standards
- Manufacturing
- Operating system

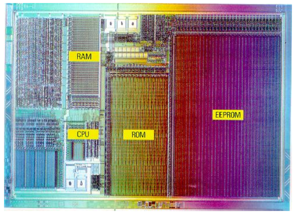
Magnetic-strip cards

- Defined by ISO 7811-2 (properties) -4 (coding) –5 (location of the magnetic stripes)
- Storage capacity 1000 bits

Features	Track 1	Track2	Track 3
Amount of Data	79 char	40 char	107 char
Data Coding	6 bit alpha	4 bit BCD	4 bit BCD
Data density	210 bpi	75 bpi	210 bpi
Writing	Not Allowed	Allowed	Allowed

What is a Smart Card?

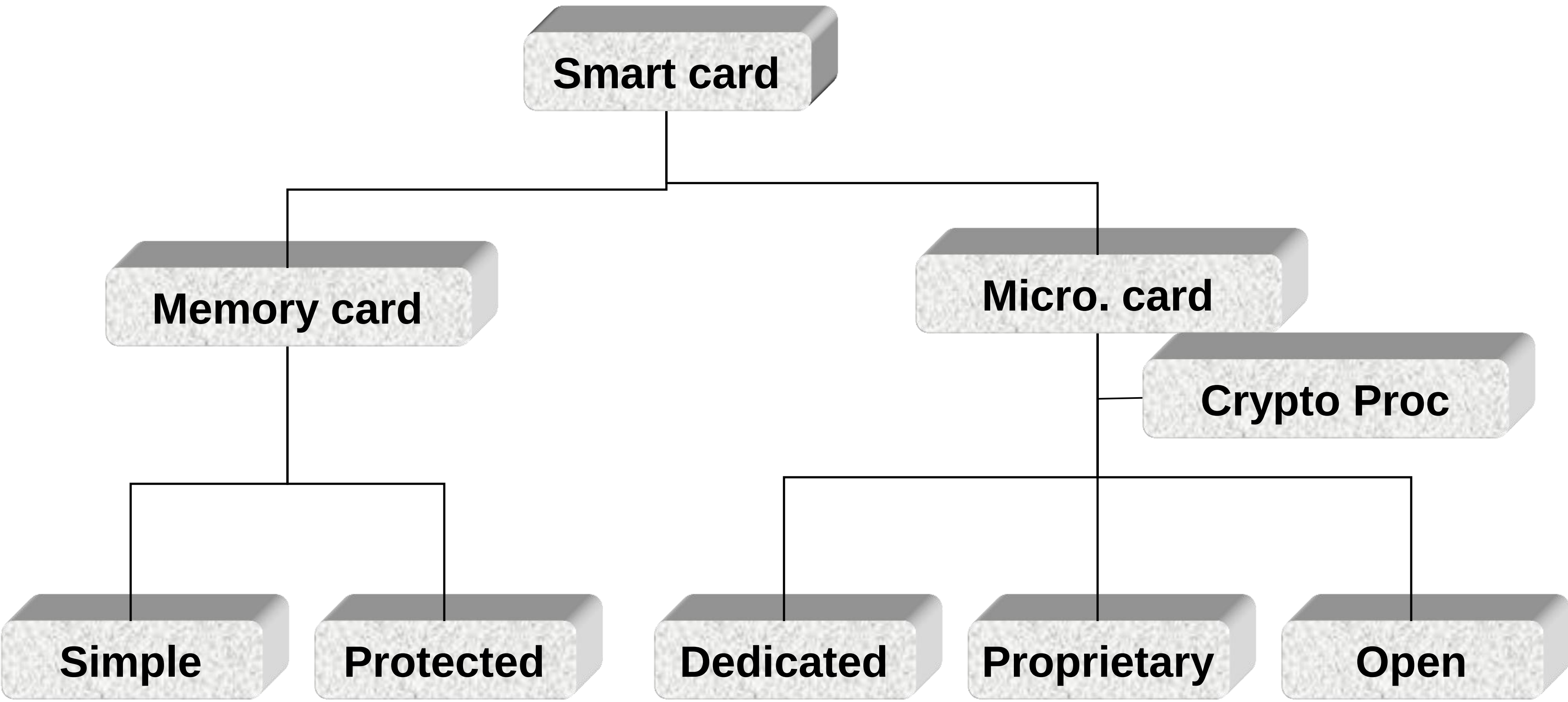
A piece of silicon on a plastic body



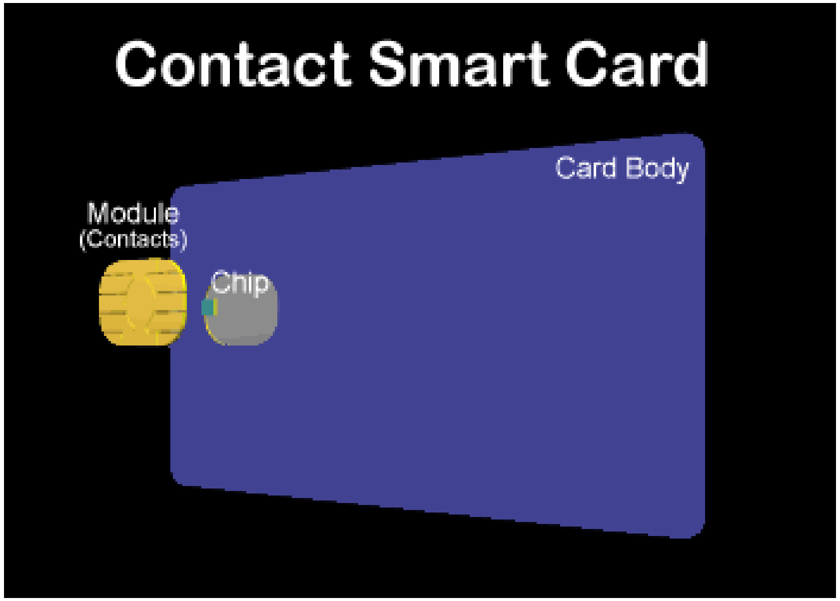
Chip

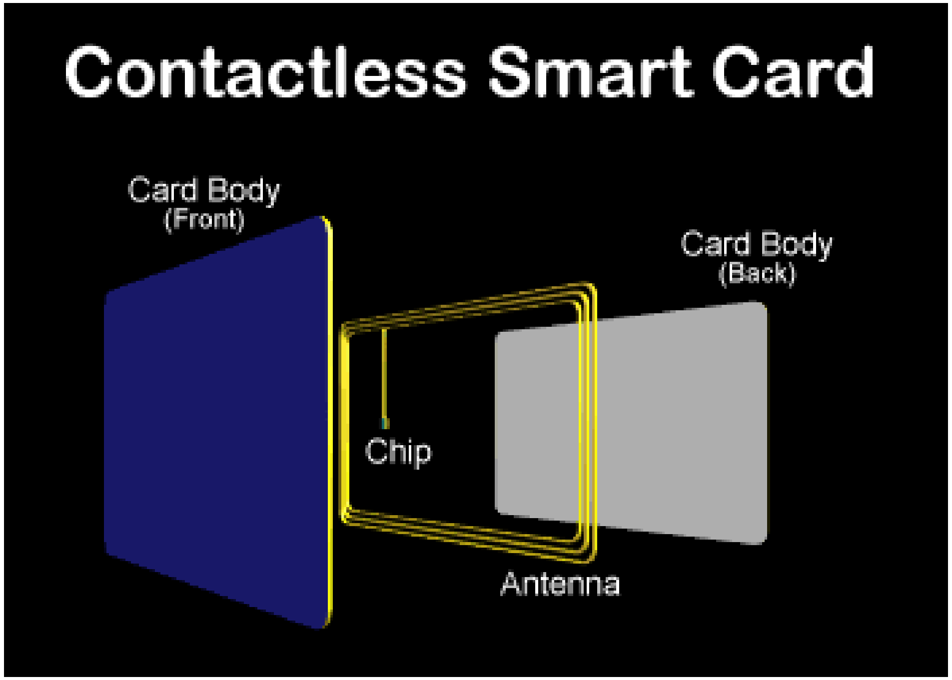
A very secure way of storing a small amount of sensitive data

Smart Cards


Smart card
Memory card
Micro. card
Crypto Proc
Simple
Protected
Dedicated
Proprietary
Open

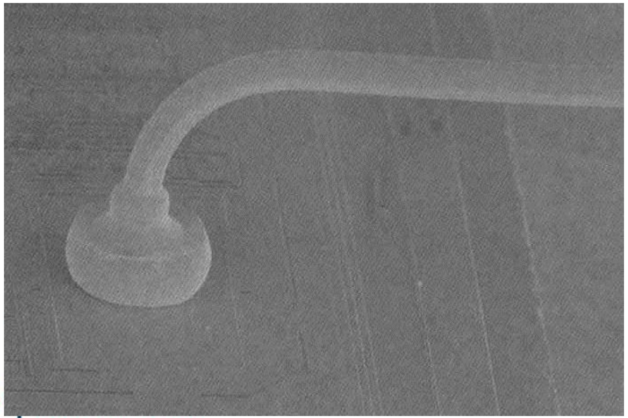
Contact / Contact less

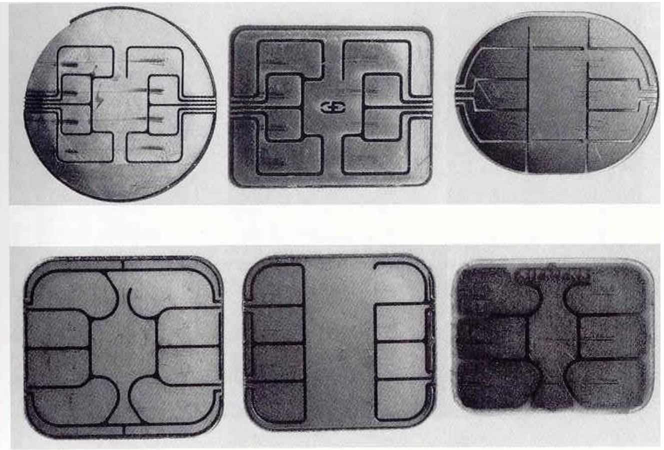




Contact

- Electrical connections between the chip and the module (wire bonding process),
- 8 contacts (C1-C8) but only 6 used (see ISO7816-2),
- C6 used as Vpp while EEPROM where not embedding charge pump,
- Supply voltage 2,7v (SIM) to 5,5v (standard TTL) and clock provided by the reader.





Université de Limoges

Contact less card (NFC)

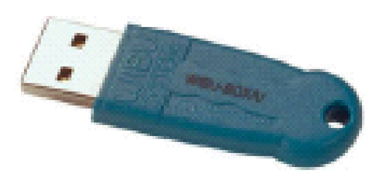
- No electrical connection (*cf.* RFID technology) used of inductive coupling to supply power to the chip,
- Need : modulator, demodulator, anti-collision mechanism, voltage regulator, reset generator and an aerial.
- For data transfer all known digital modulation techniques can be used (ASK, FSK and PSK).
- Standards : close coupling ISO/IEC 10536 (3-5Mhz), proximity cards ISO/IEC 14443 (13,56Mhz) and Hand Free Cards ISO/IEC 15693,
- Used for public transportation, ski pass, access control, payment with GSM…

Form Factor

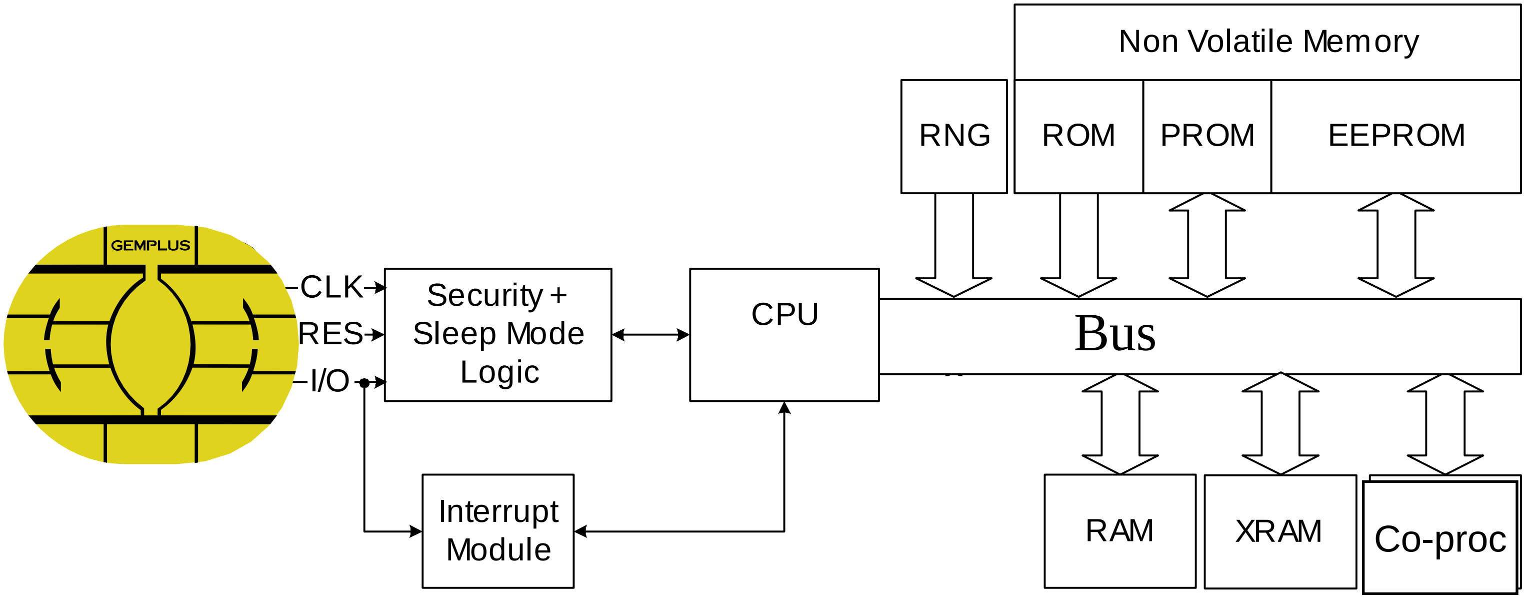
- With contact:
  - ISO 7810, 7816-1,1816-2
  - USB
- Contactless : several standards

- Hybrids
- Buttons
  - iButton (1-wire)
  - JavaRing

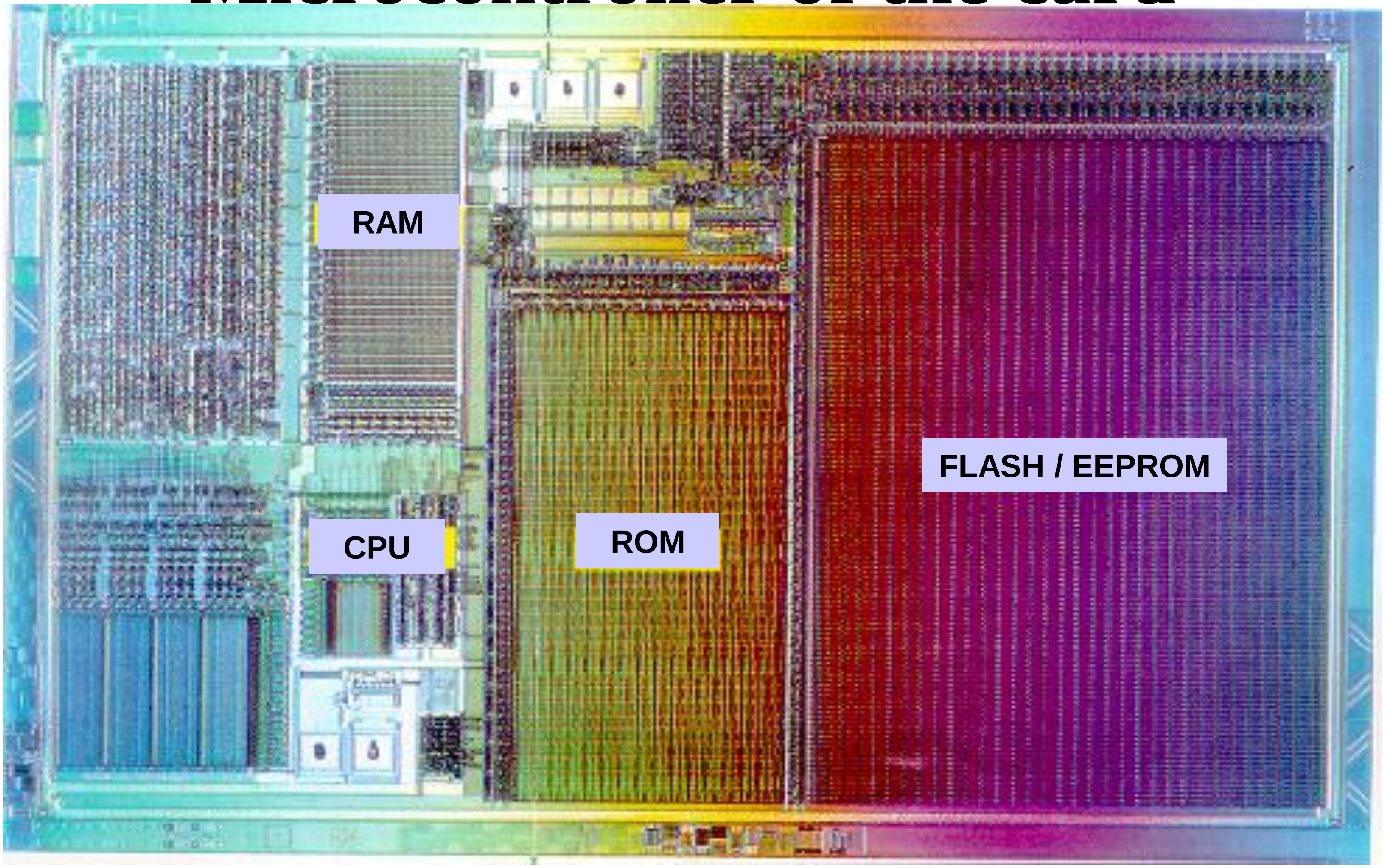
- Dongle (serial, parallel, USB, mmc)



Microprocessor architecture

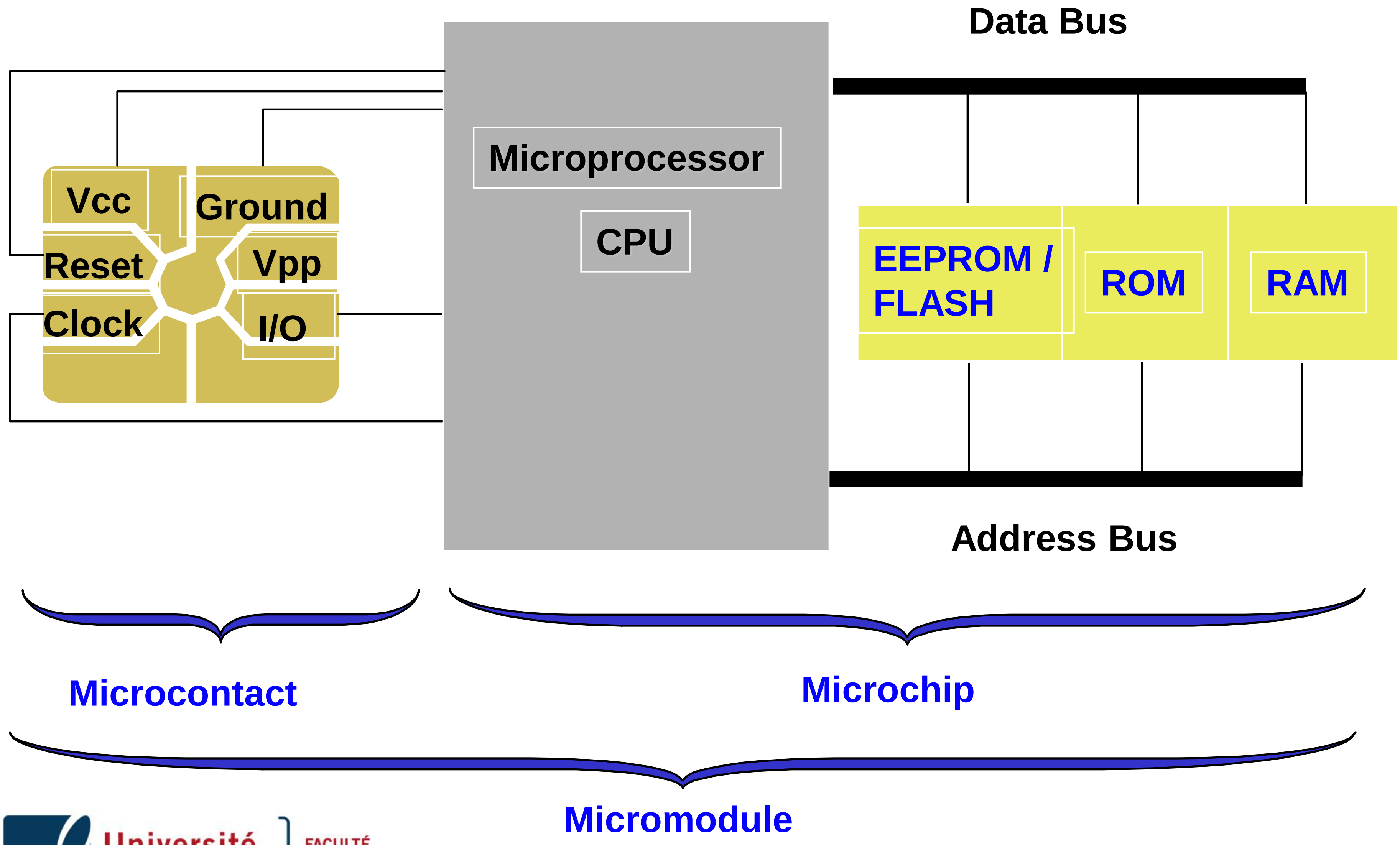


Microcontroller of the card



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Contact card



Different Types of Memory ...

- ROM : CPU only NO ACCESS !
  - used for embedded Operating System
- EPROM : Write once, read FOR EVER !
  - Used for initialization area (eg. Lock bytes)
- EEPROM : Write, erase, read FLEXIBLE !
  - used to store applicative data or added functionalities
- RAM :Write, erase, read TEMPORARY !
  - used during power on sessions only

New Non Volatile Memories

- Flash EEPROM Memory :
  - Advantages :
    - Same memory for Program and Data
    - Time to Market reduced for prototyping
    - Cell size (element to store 1 bit) ratio vs. E^2 : 1/3 smaller
  - Disadvantages :
    - Granularity Data memory : 512*32 comparing with 1-byte access.
    - Erase time more important than E^2 memory
    - Cell size larger than ROM

New Non Volatile Memories

- FeRAM :
  - Advantages :
    - Same memory for Program and Data and computing area (RAM).
    - Same access time for Read, Erase and Write (same as DRAM)
    - Cell size ratio vs. E^2 : 1/3 smaller
  - Disadvantages :
    - Technology under development (new Technology)

Smart Card memories

	RAM	EEPROM	FlashRAM	FéRAM
Persistency	No	Yes	Yes	Yes
Read acc.	0.1µs	0.15µs	0.15µs	0.15µs
Write	0.1µs	10µs	10µs	0.4µs
Erase	-	5ms	100ms	-
Granularity	-	4bytes	64bytes	-
Cycles	Unlimited	10^6	10^5	10^{10}

Comparing Smart Card vs. PC

	Smart Card	PC	Ratio
RAM	1kbyte	128Mbyte	130 000
Storage	64kbyte	6Gbytes	100 000
Baud rate	192 kbits	100Mbits	500
CPU Speed	20 Mips	500Mips	25

Agenda

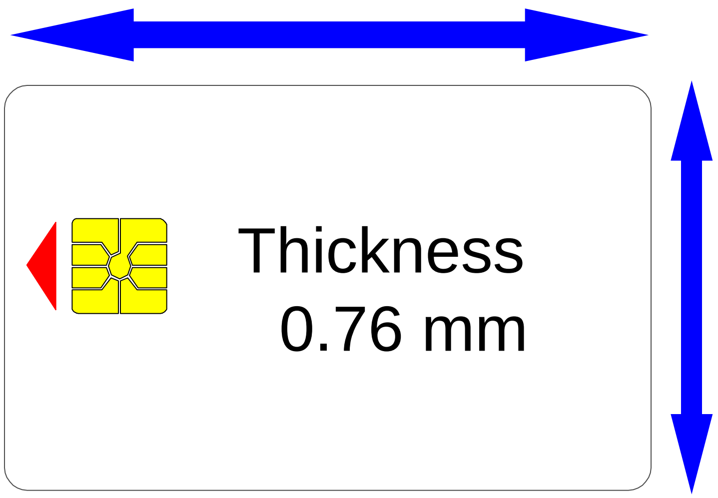
- Card Technology
- Standards
- Manufacturing
- Operating system

ISO/IEC 7816
Integrated circuits cards with contacts

- ISO/IEC 7816-1 : Physical characteristics.
- ISO/IEC 7816-2 : Dimension & location of contacts.
- ISO/IEC 7816-3 : Electronic signals & transmission protocols.
- ISO/IEC 7816-4 : Inter-industry commands and file system.
- 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).
- ISO/IEC 7816-8 : Security architecture and related inter-industry commands.

ISO/IEC 7816-1 (7810)

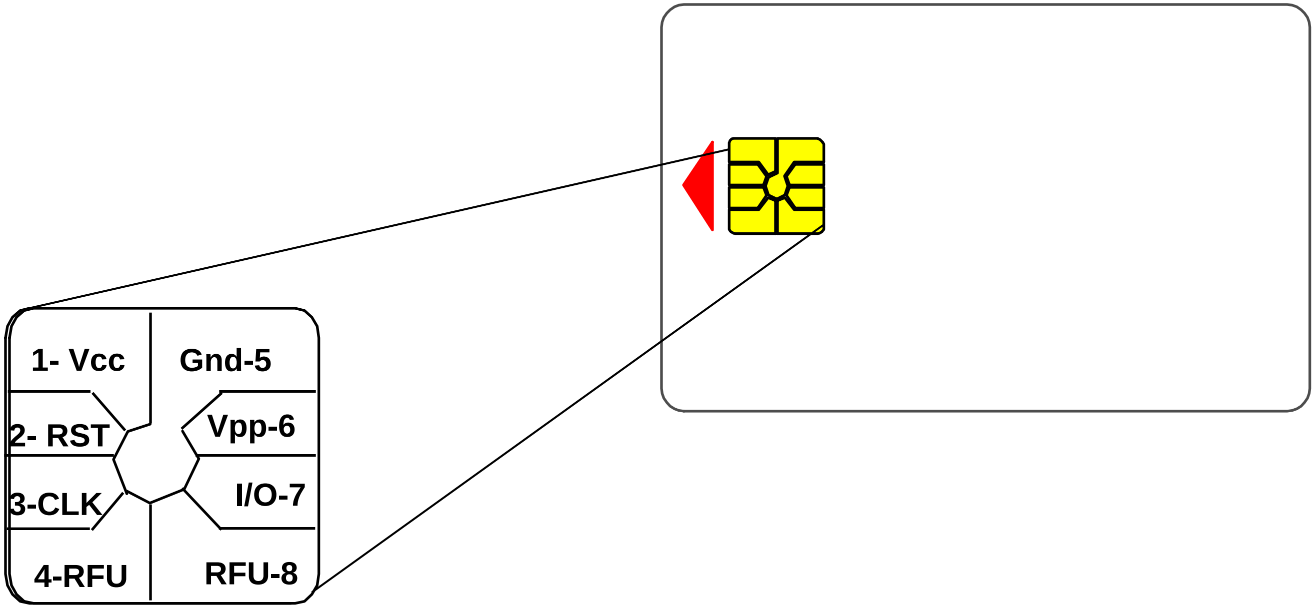
- Governs the physical characteristics of a smart card :



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

ISO/IEC 7816-2

- Governs the dimension and location of the chip contact :



ISO/IEC 7816-3

- Electrical characteristics :
  - clock frequency [1 MHz, 5 MHz],
  - communication speed.
- Transmission protocols :
  - T=0, T=1, T=CL defined,
  - T=14 reserved for proprietary protocols.
- Answer to reset (ATR)
- Protocol type selection (PTS) :
  - If several protocols supported or if parameters need to be adjust
  - Negotiable mode and specific mode

Smart Card Reader exchange

- The card NEVER initiates a communication with the reader

Smart Card introduction

Response to the ATR ←

Protocol negotiation PTS →

Negotiation answer PTS ←

Command APDU →

Answer APDU ←

End of session

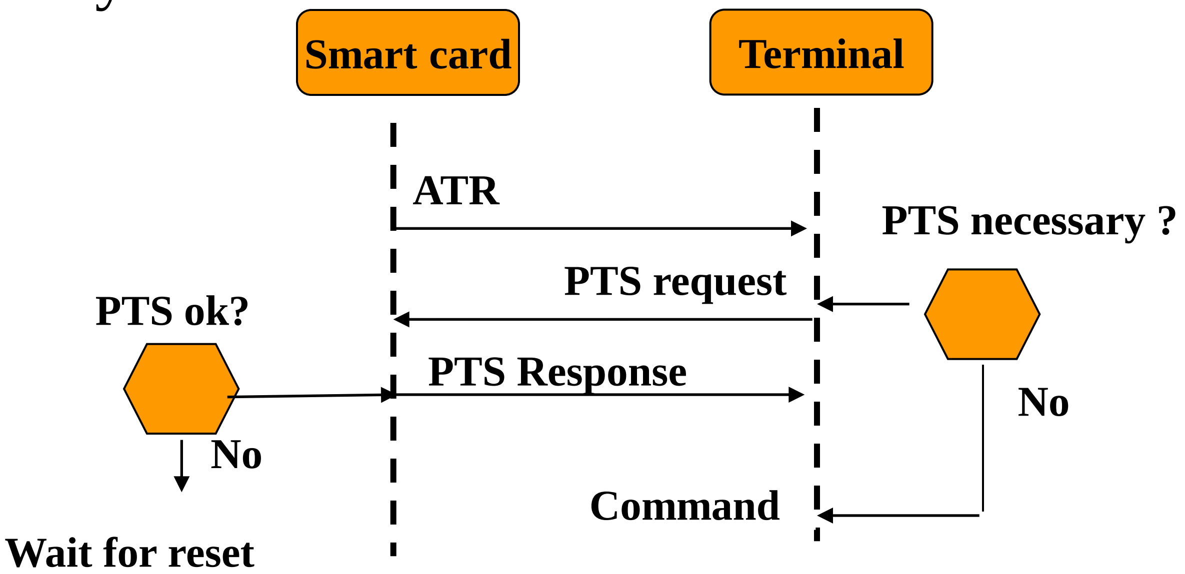
Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Answer To Reset

- Starts the smart card program,
- Data elements TS-T0-Tabcd-T1…k-TCK
  - TS: Byte coding convention (3B direct, 3F inverse)
  - T0 : Format characters
  - Ta,b,c,d : Interface characters,
  - $T1..T_k$: Historical characters to identify OS, version number of the ROM mask, can be omitted.
  - TCK: XOR checksum from T0 to the last byte before TCK.

Protocol Type Selection

- Needed only if the terminal wants to modify parameters,
- If the card agrees, it sends the PTS back to the terminal
- Otherwise the terminal execute a reset (warm => protocol change),
- Only one PTS after the ATR.



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Transmission protocols

- T=0 most widely used (1989), T=1 block oriented
- T=14 Japan and Germany

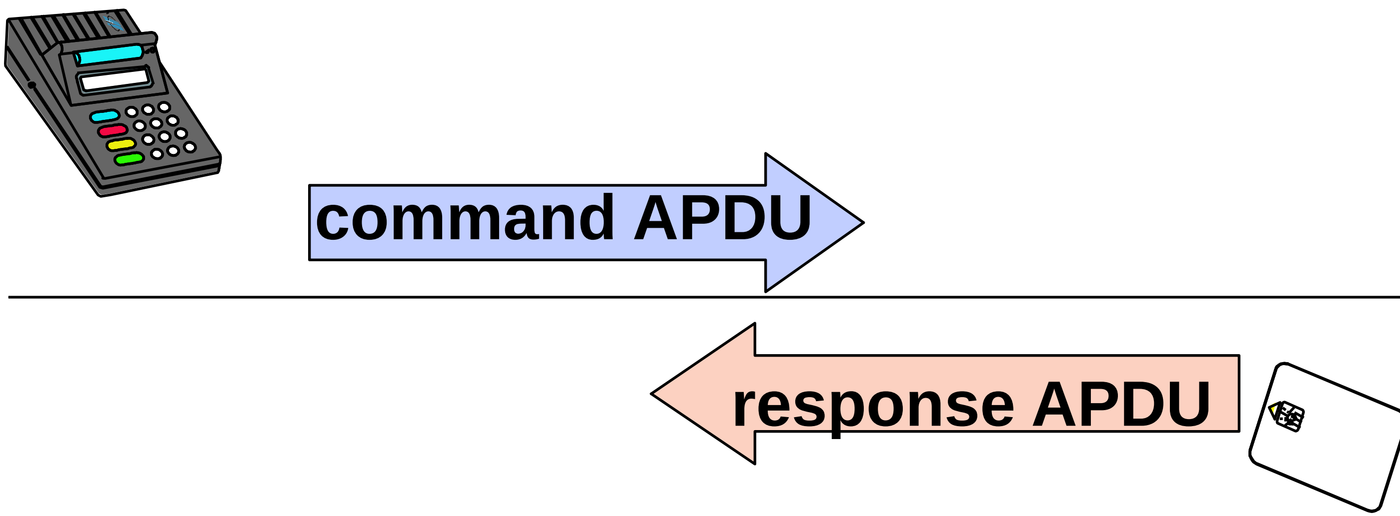
Transmission protocol	Meaning	ISO
T=0	Asynchronous, half duplex, byte oriented	7816-3
T=1	Asynchronous, half duplex, block oriented	7816-3
T=2	Asynchronous, full duplex, block oriented, tbs	10536-4
T=14	National functions	No ISO

Transport protocols

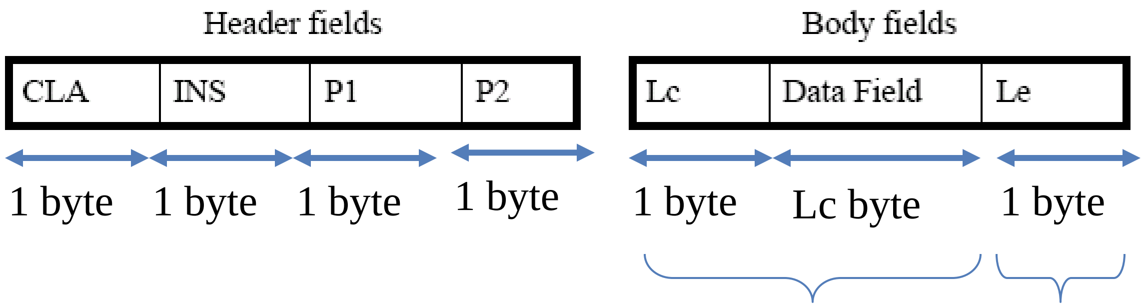
- T=0
  - Byte oriented, Serial transmission (1 start bit, 8 bits data, 1 parity bit, 2 stop bits)
  - Transmission error (parity only) 2 etu mute (“0”)
- T=1
  - Block oriented, Header : NAD, PCB, LEN; data : INF, CRC.
  - NAD 3 bits destination address, 3 bits source address
  - PCB define the kind of block
    - I (#block, more) numbered mod 2, more = 1, another block follow
    - R(#block, error) numbered mod 2, next expected bloc,
    - S specific command (RESYNC, IFS, ABORT, WTX)

The Application Protocol Data Unit

- Independence of application versus low layers
- An APDU contains either :
  - a command message,
  - a response message.

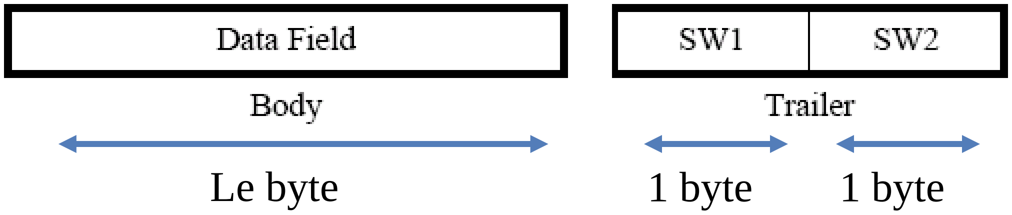


APDU syntax



CLA : class
INS : instruction
P1 : parameter 1
P2 : parameter 2
Lc : length of command data
Le : expected lentgh of the response

Response syntax



Le : length of the expected response
SW1: Status Word 1
SW2: Status Word 2

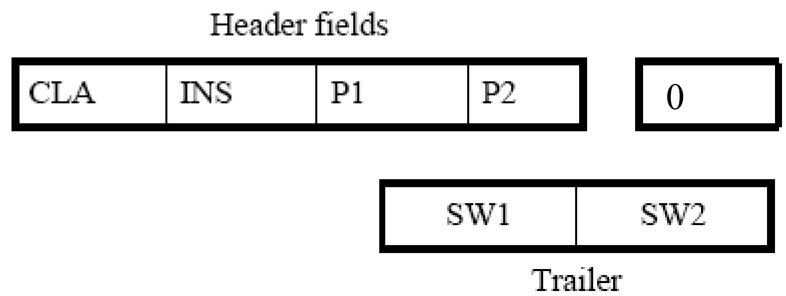
CLA Class byte

b7 to b4	b3	b2	b1	b0	Meaning
			X	X	Logical channel number
	0	0			No secure messaging
	1	0			Secure messaging header not authentic
	1	1			Secure messaging header authentic
‘0’					Structure and coding compliant with 7816-4
‘8’,’9’					User specific codes
‘A’					Structure and code defined in additional document GSM11.11

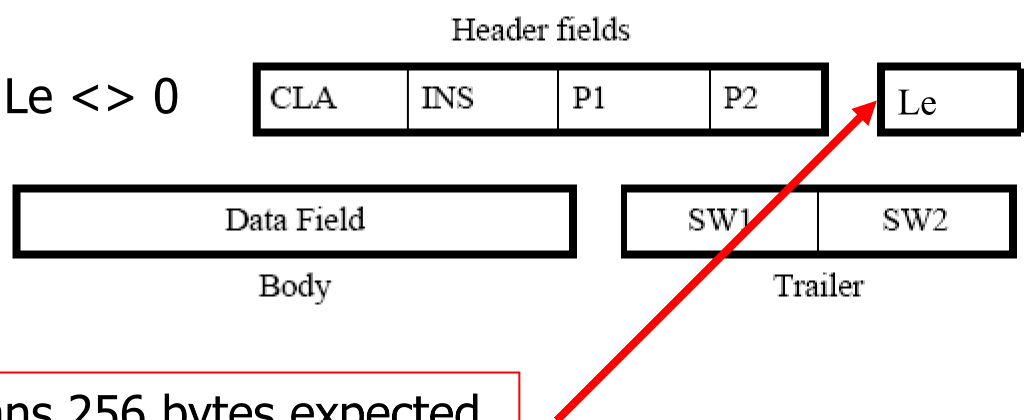
Class	Application
’80’	Electronic purse compliant with EN 1546-3
‘8x’	Credit card compliant with EMV-2
‘A0’	GSM compliant with prETS 300 608/GSM 11.11

Four possibilities

Case 1: Lc = 0 and Le = 0



Case 2: Lc = 0 and Le <> 0



Warning Le = 0 means 256 bytes expected

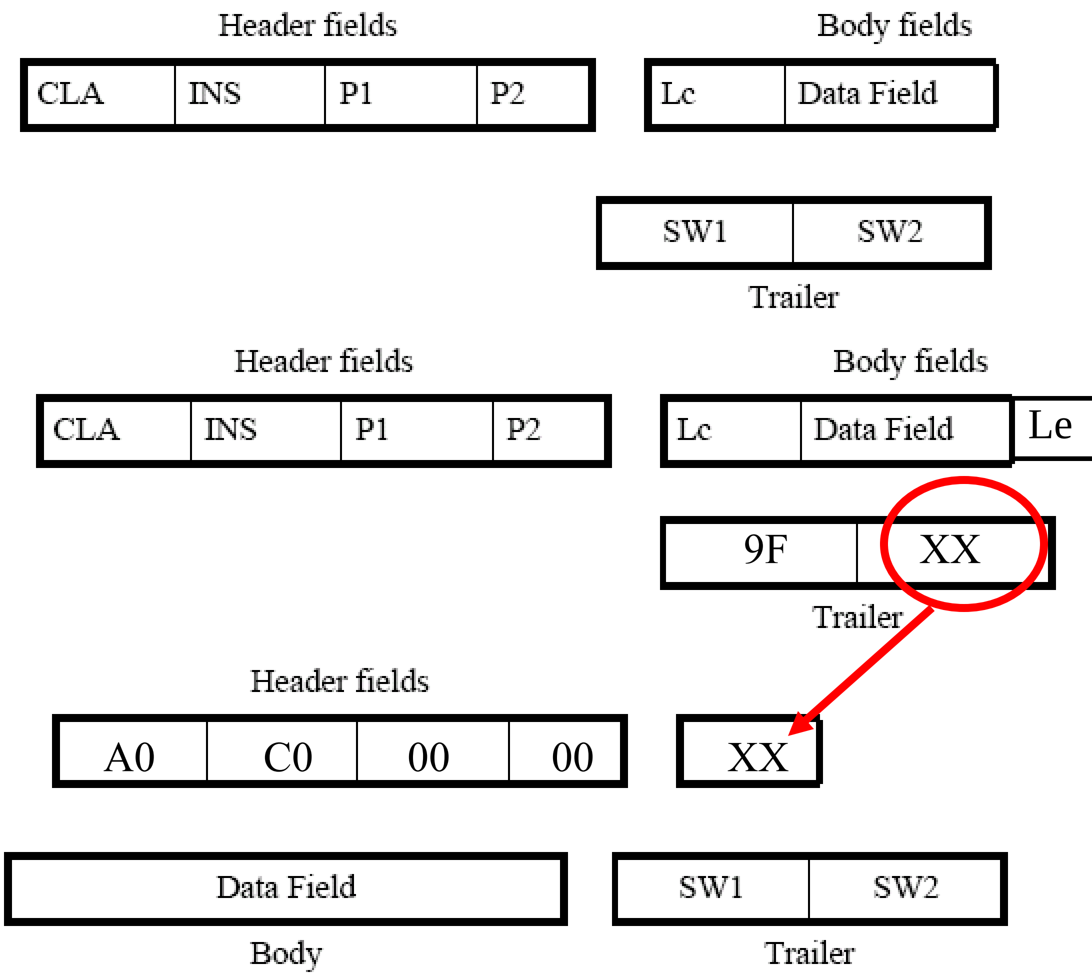
The difference between case one and two is made with the command not at the protocol level !

Four possibilities

Case 3: Lc <> 0 and Le = 0

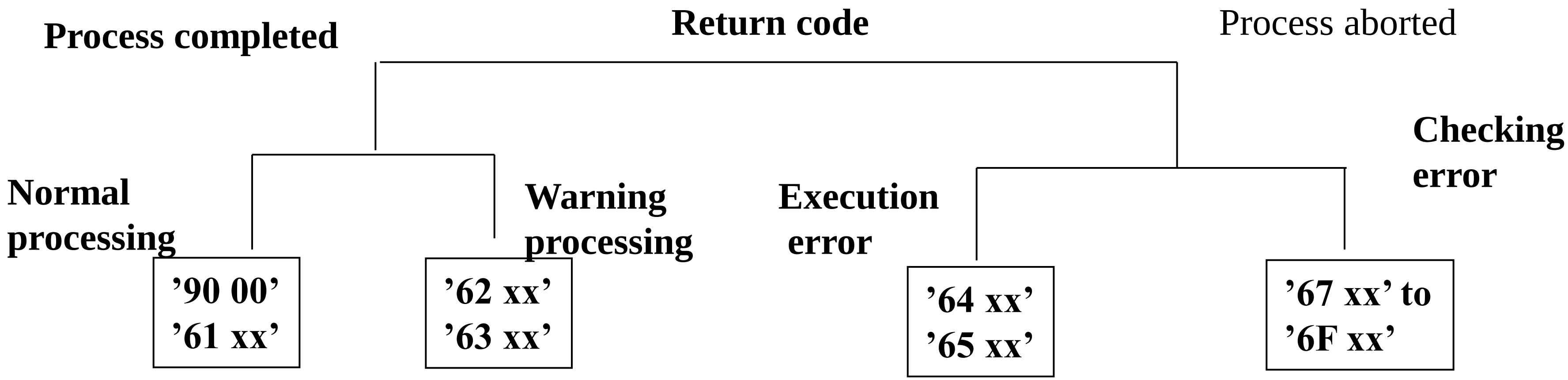
Case 4: Lc <> 0 and Le <> 0

Commande Get Response



Return Codes

- SW1, SW2 = ’90 00’ command successful, ’63xx’ or ’65xx’ means EEprom has been modified,
- More than 50 different return codes defined by standard,
- Often not respected…



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

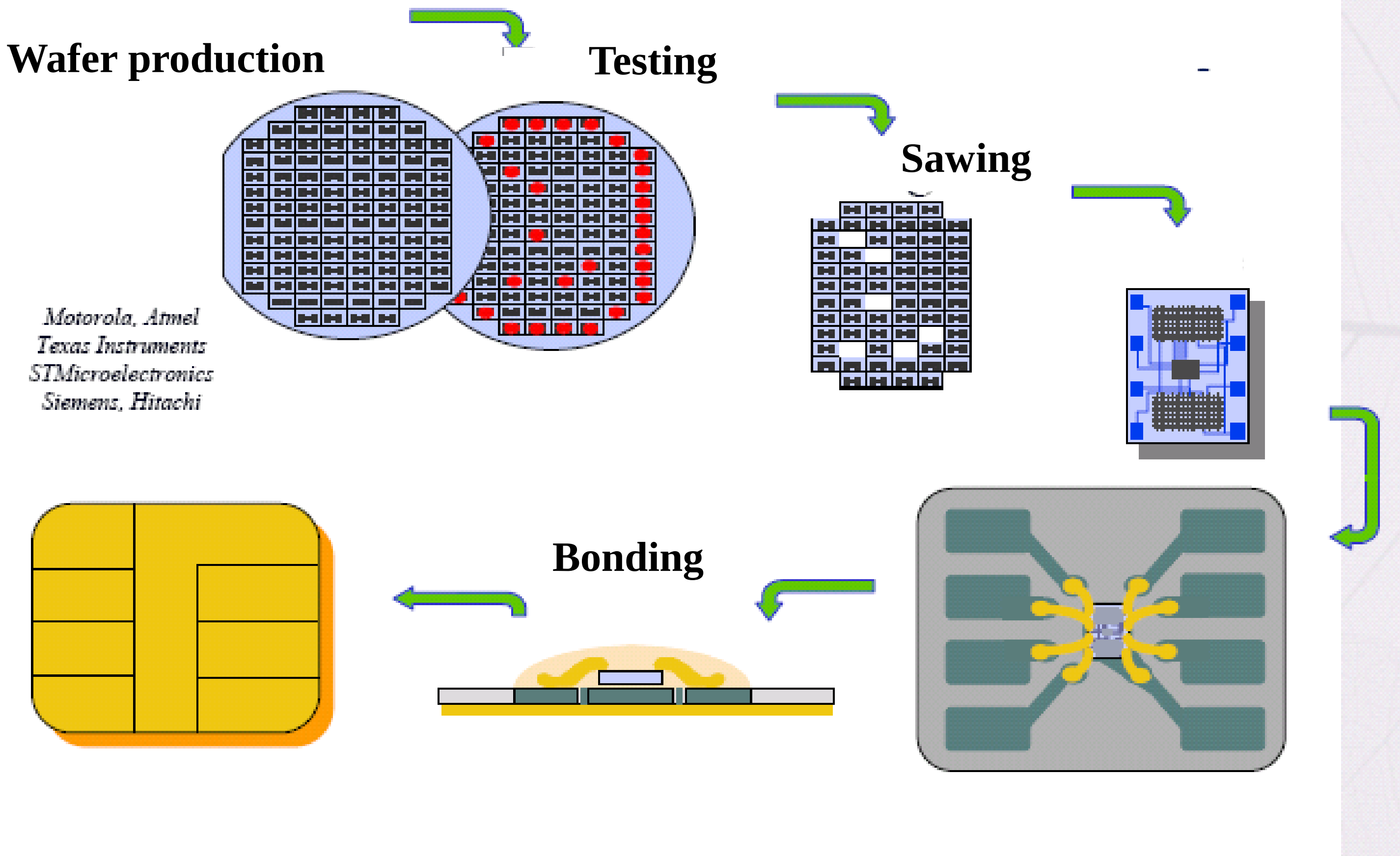
ISO/IEC 7816-4

- There are no user programs, no memory management and no parallelism.
- It just defines the file system
  - Specifies contents of messages (commands, responses).
  - Structure of files and data.
- and the security architecture
  - Access methods to files and data.
  - Methods for secure messaging.
- But also the filter mechanism.

Agenda

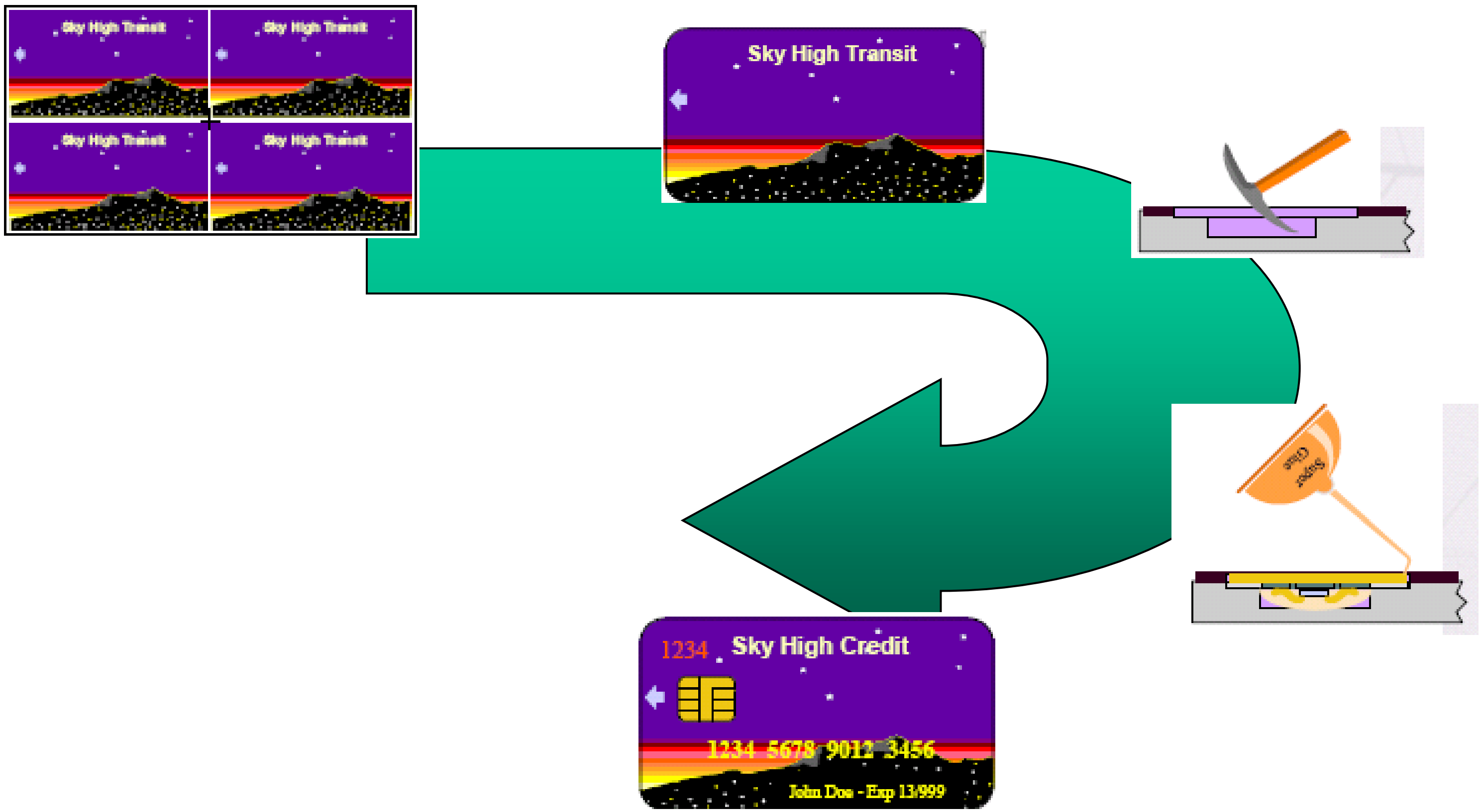
- Card Technology
- Standards
- Manufacturing
- Operating system

Manufacturing cycle (1/3)



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Manufacturing cycle (2/3)



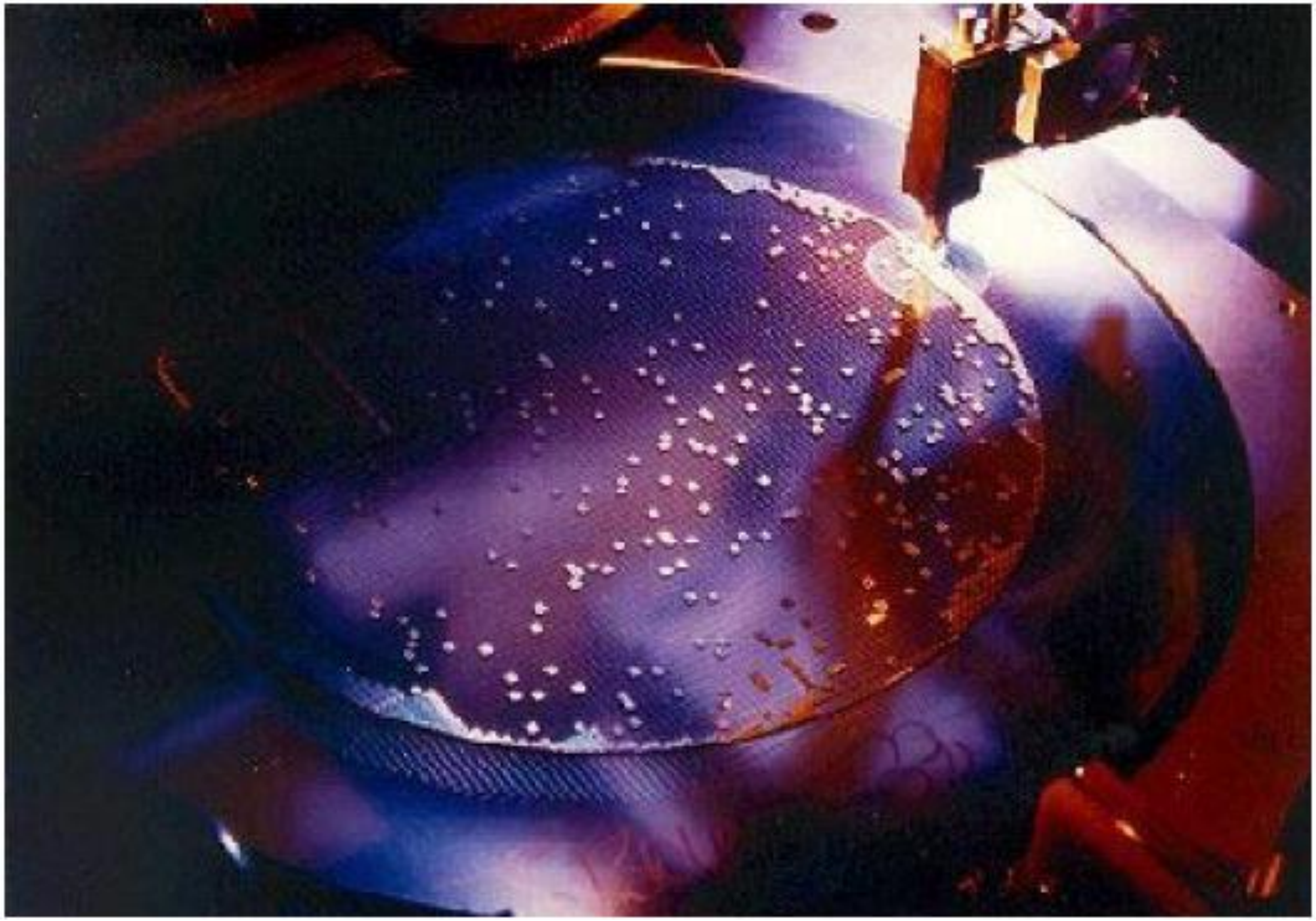
Manufacturing Cycle (3/3)

Manufacturing : Sawing

Cutting silicon wafer into individual chips. During the previous step, electrical test, defective chips are marked with an ink drop.

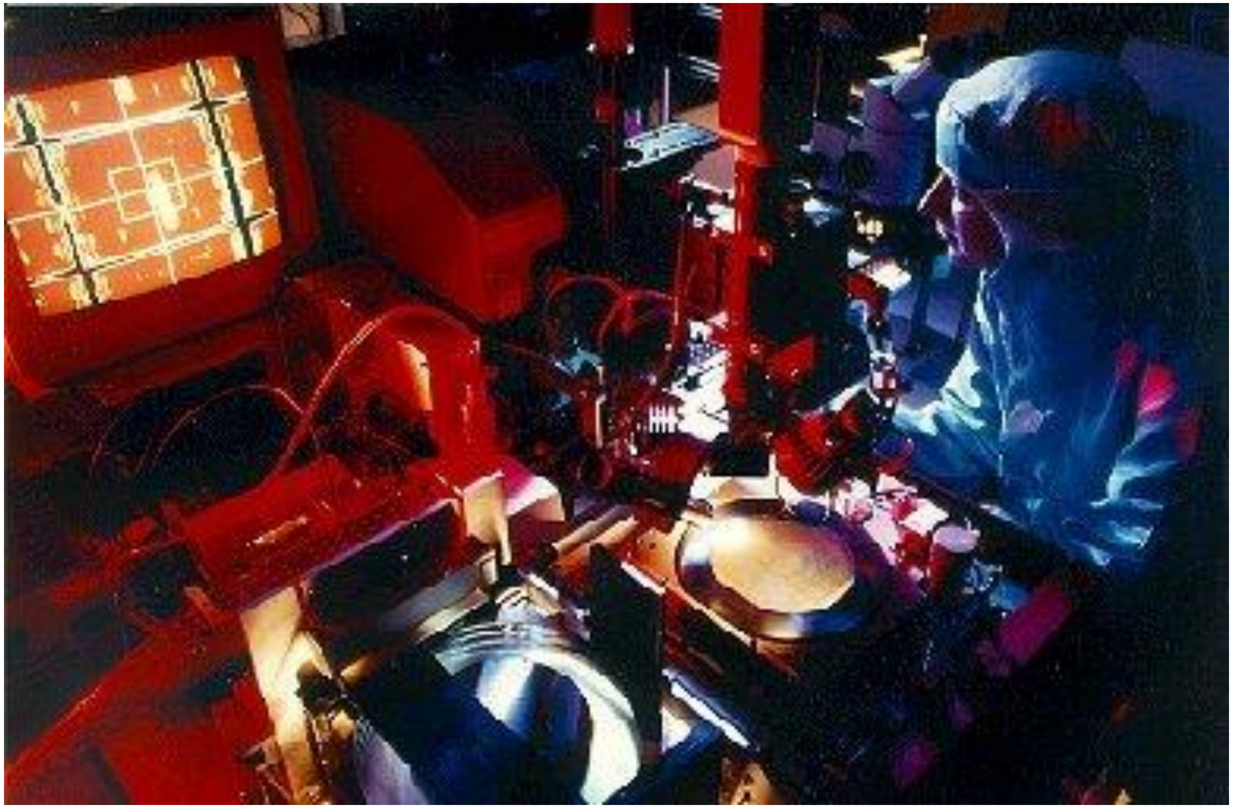
Université de Limoges
FACULTÉ DES SCIENCES ET TECHNIQUES

Manufacturing : Testing



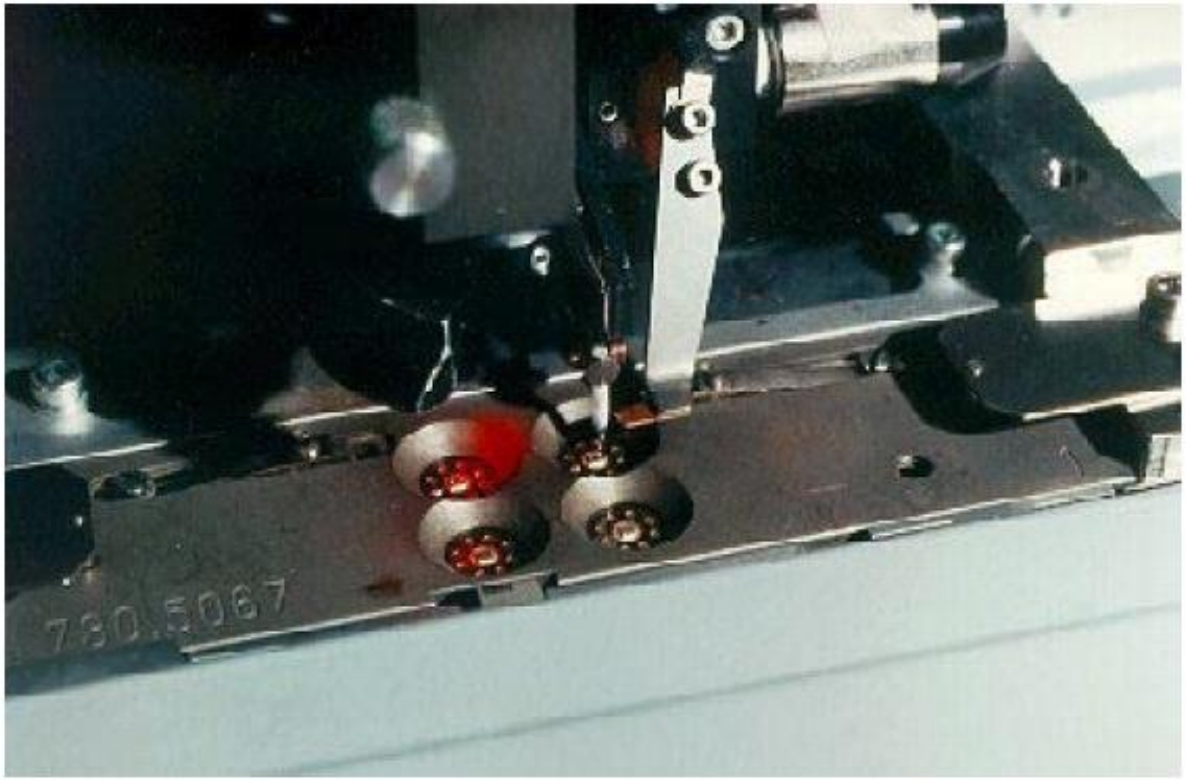
Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Die Bonding



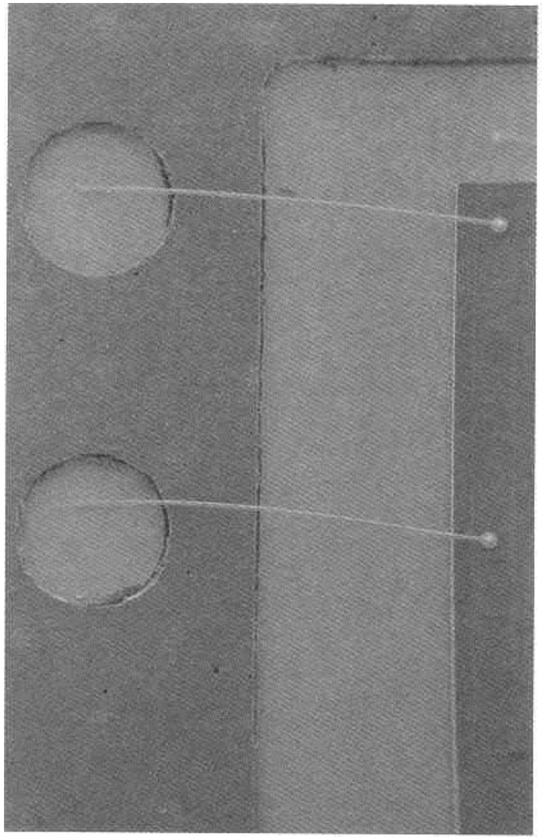
Gluing the chip into the cavity located on the film, ensuring proper physical and electrical connection.

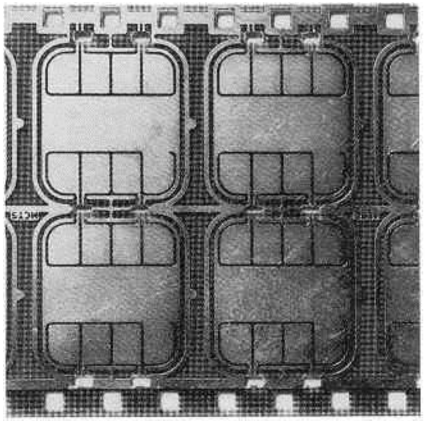
Manufacturing : Bonding

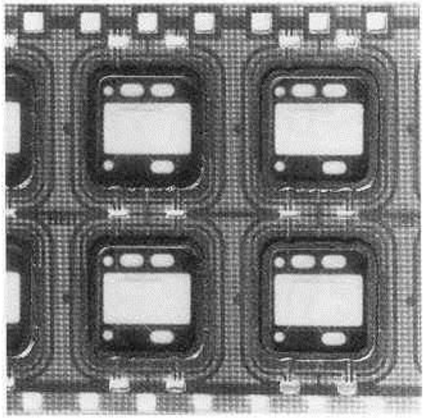


Electrically connecting the chip's bonding pads and the contacts on the micro module using gold wires.

Bonding







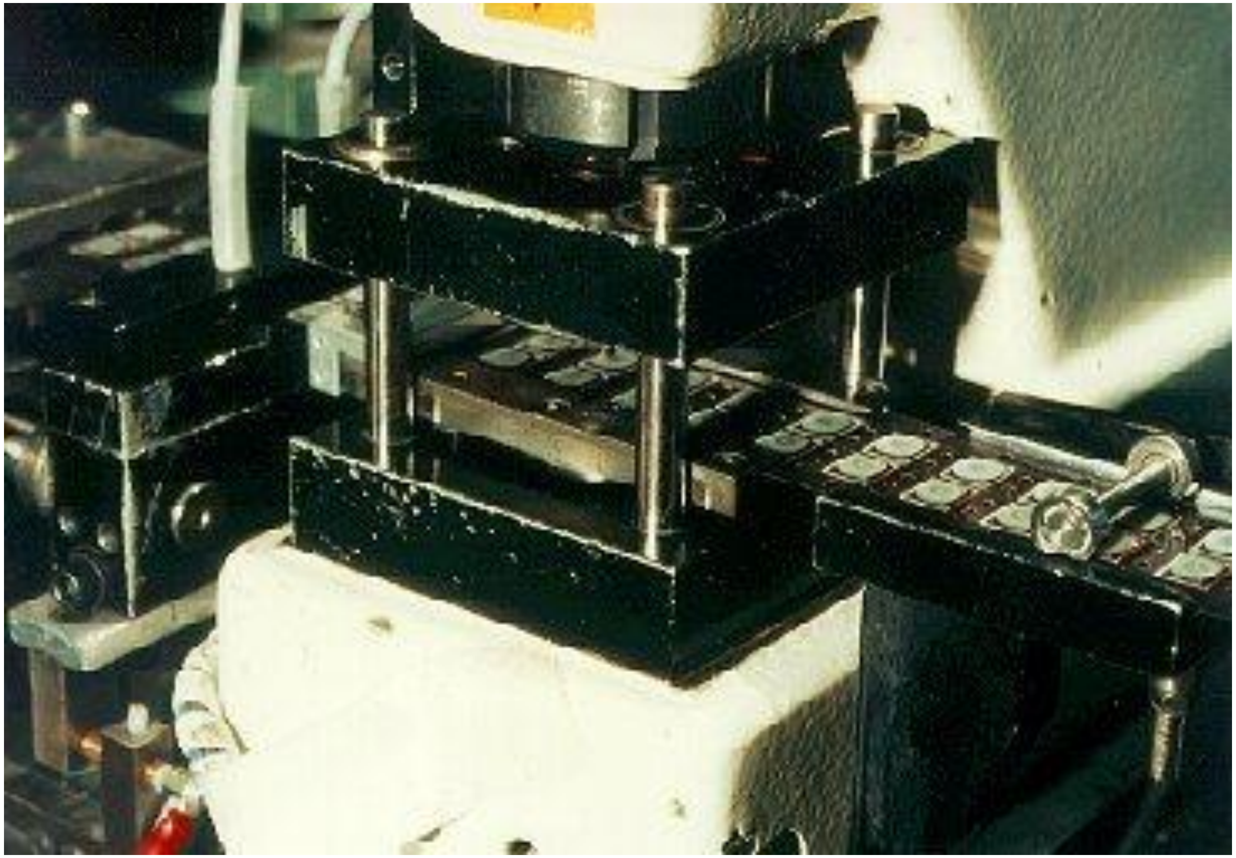
Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Manufacturing : potting

Protecting the chip and wires with a drop of epoxy resin, ensuring the physical durability of the micro module

Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Grinding

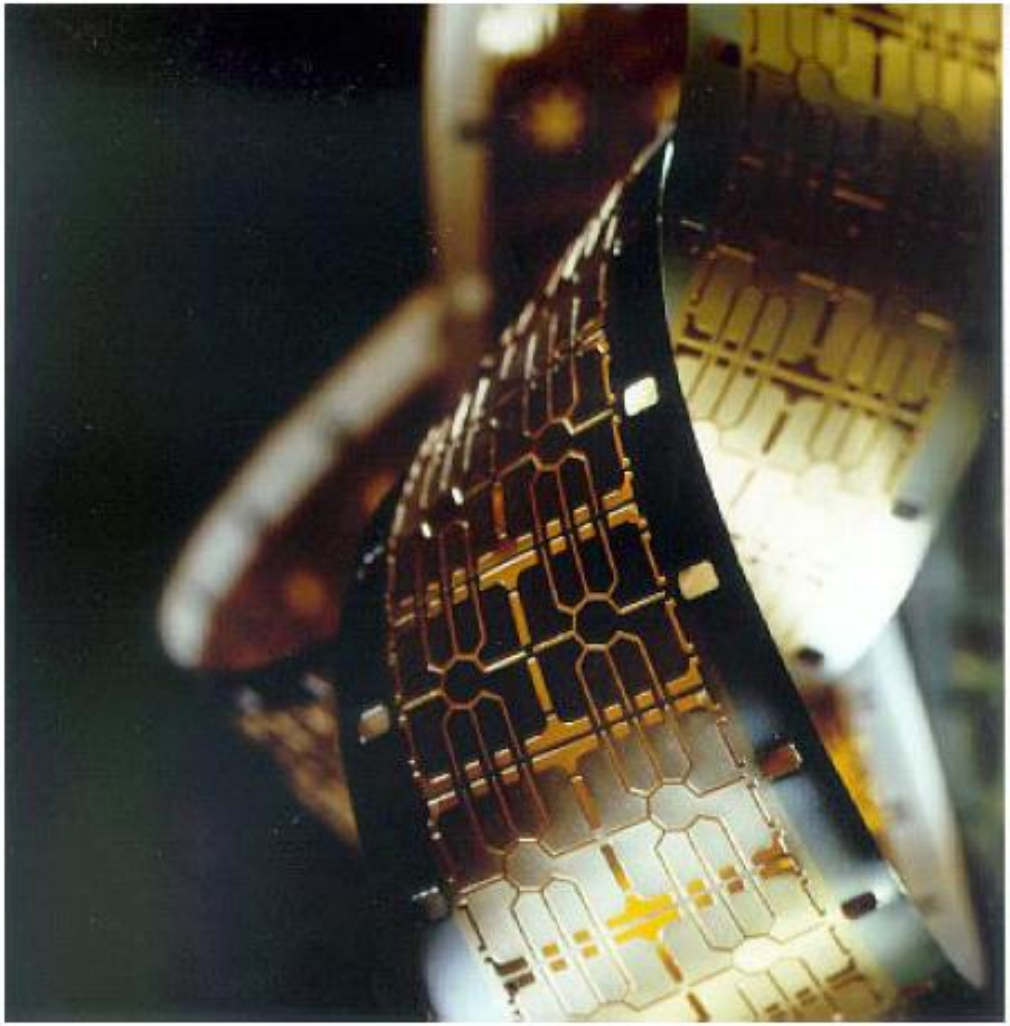


Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Electrical Testing

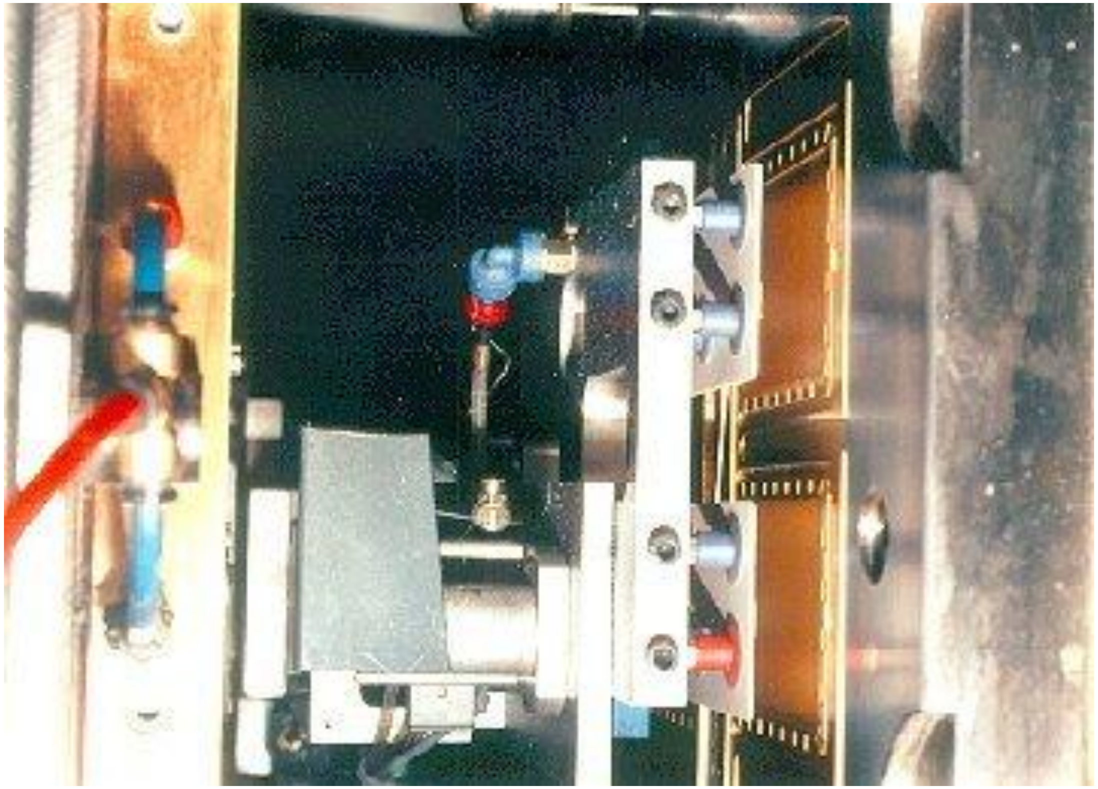
Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Manufacturing: finished modules



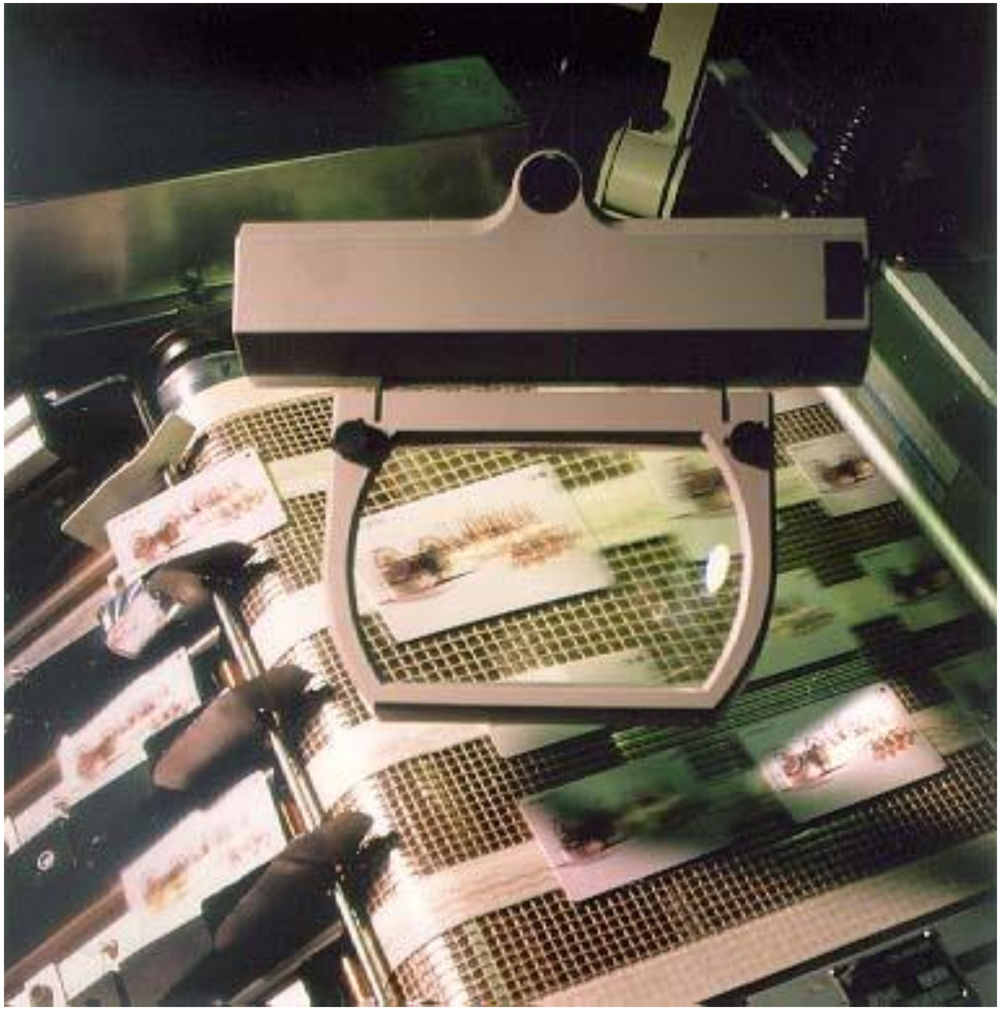
Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Card Moulding



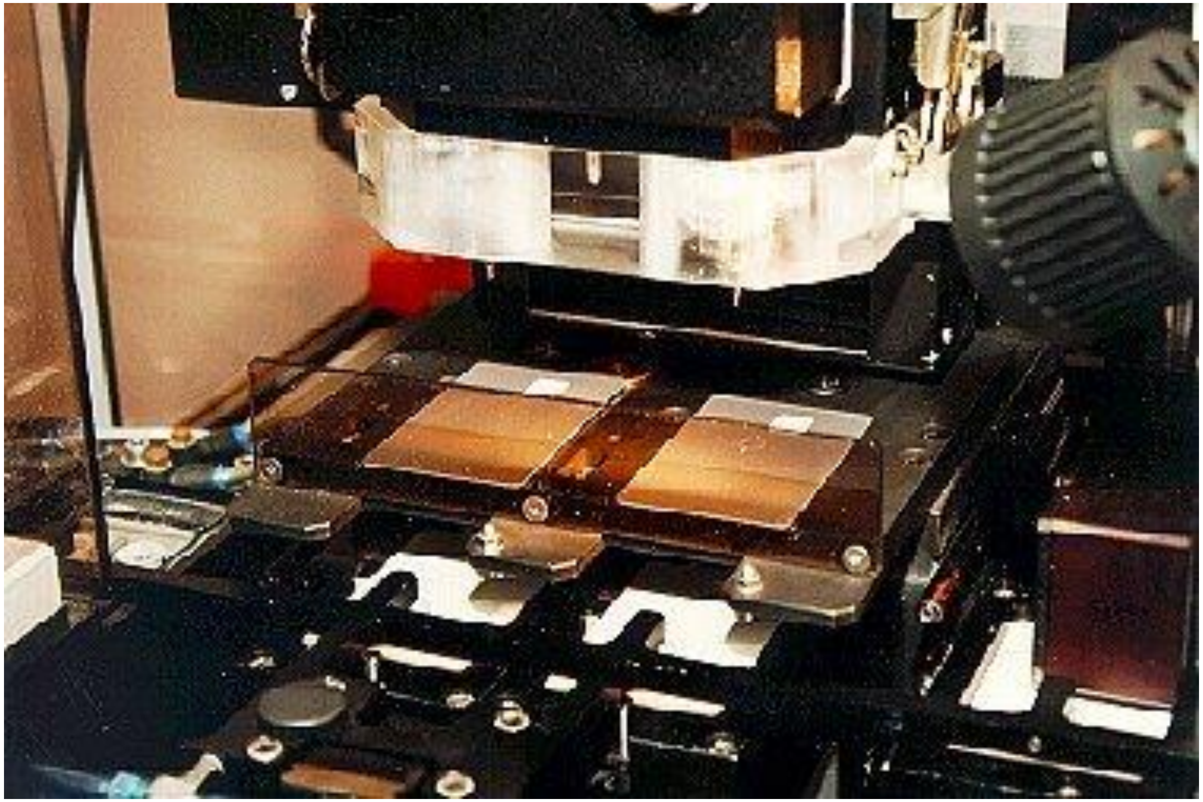
Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Offset Printing



Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Grinding



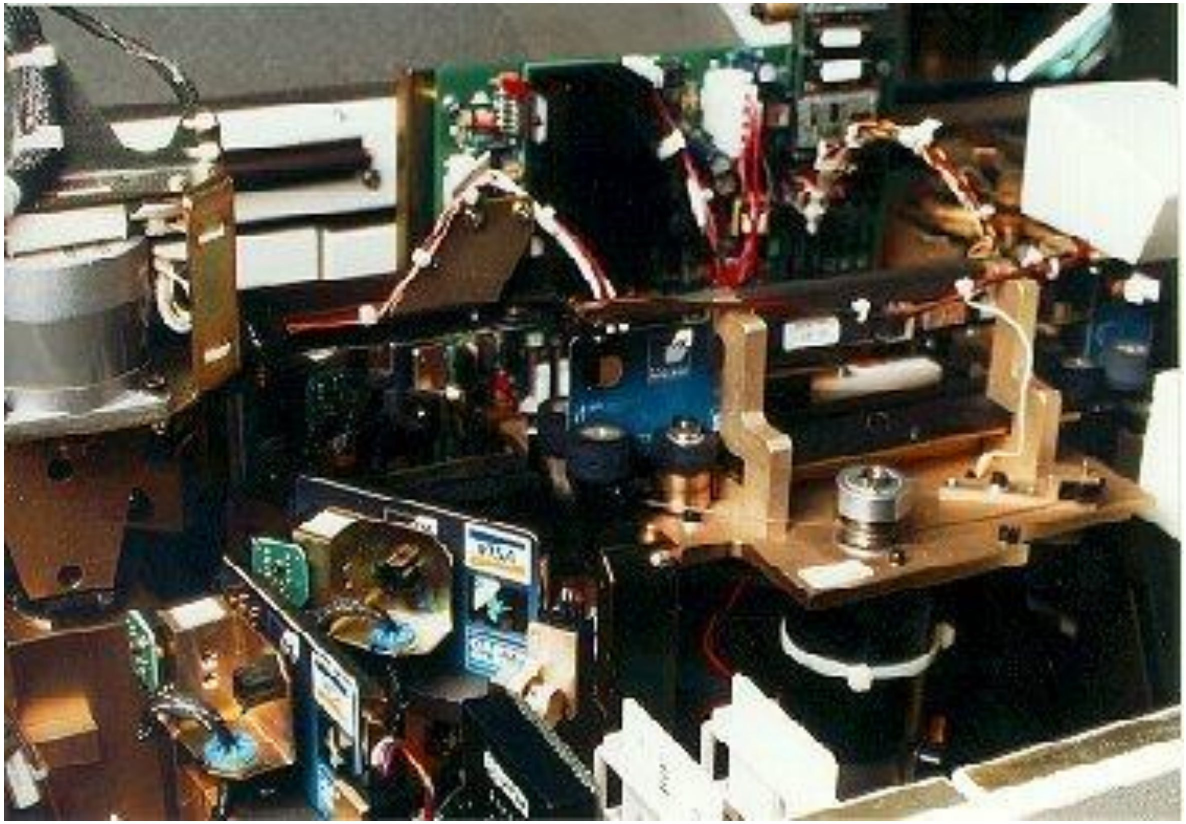
Manufacturing : Embedding & Test

Plug-In

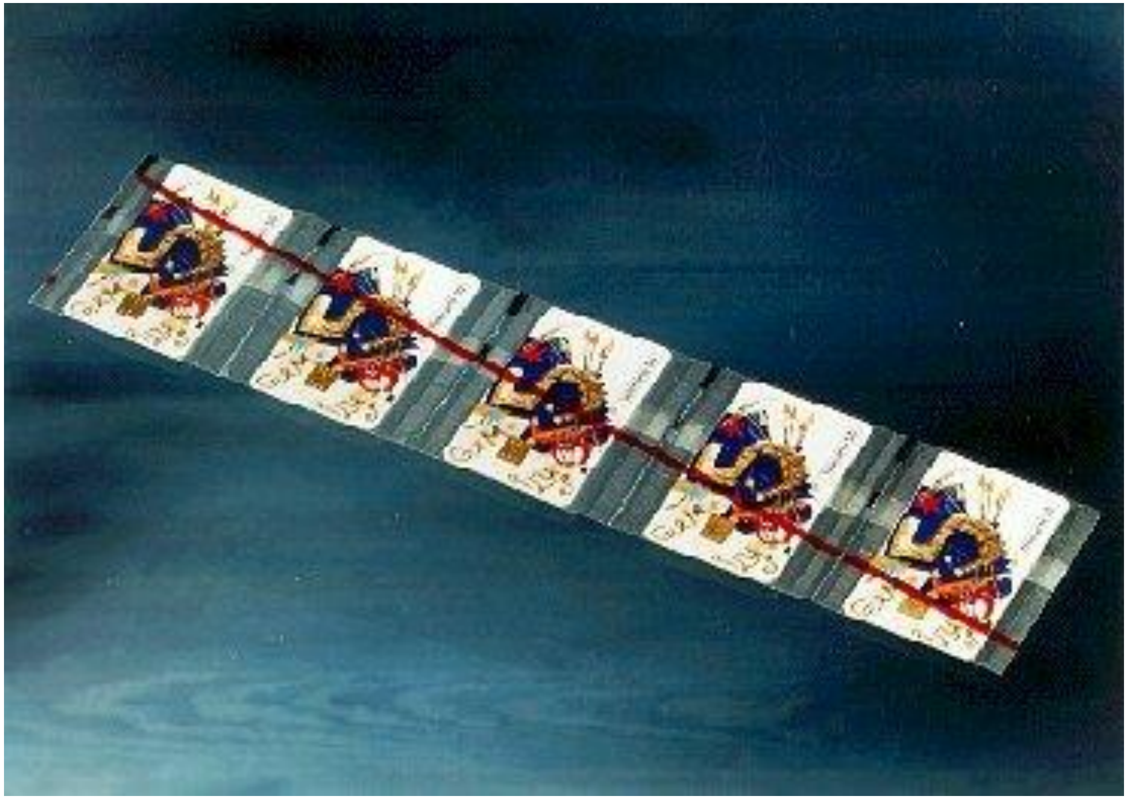
Cutting to plug-in format for mobile phones.

Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Personalization



Packing



Agenda

- Card Technology
- Standards
- Manufacturing
- Operating system

Fundamentals

- Functions : manage the resources
- Program written in ROM code (no self modifying techniques allowed),
- No change are possible once the chip is manufactured
  - quick and dirty programming IS NOT AN OPTION !!!
  - Smart Card OS is reliable and robust,
- Design consideration :
  - Persistence…
  - Closely coupled with the hardware

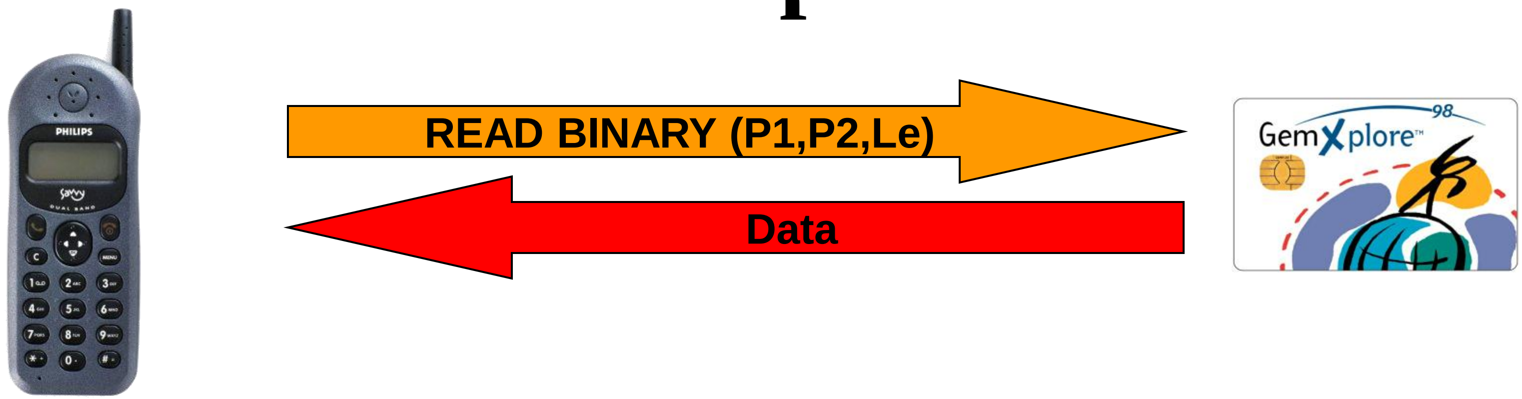
Introduction

- At the beginning no real OS only stand alone applications
- Mask your own code
  - Pros: small footprint, complete control
  - Cons : development in C and target assembly language, use emulators, Mask lead time 2 months, bug fixes.

Development 7816-4

- Use proprietary cards
  - What you get
    - File system
    - Fixed set of APDU commands: read/write files, cryptographic primitives
  - Pros: off the shelf product, cheaper
  - Cons not extensible, bug fixes.

Example



- P1=Offset High,
- P2=Offset low.

Syntax :

CLA	INS	P1	P2	Le
A0	B0	xx	yy	Le

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

7816-4 based OS

- Data are stored in files structures in Eeprom,
- A file must be selected before any action,
- Made of a header and a body,
  - The header stores the access conditions and the structure of the file.
  - For security reasons header and body are stored on different eeprom pages

Soft Masks

- It is an extension of the hard mask
- Often written in C, compiled and linked to the libraries,
- Can be download in Eeprom if the card is not blocked,
- Need ?
  - Bug fixes,
  - Adding new functionalities,
  - A customer needs a rewriting of a command…

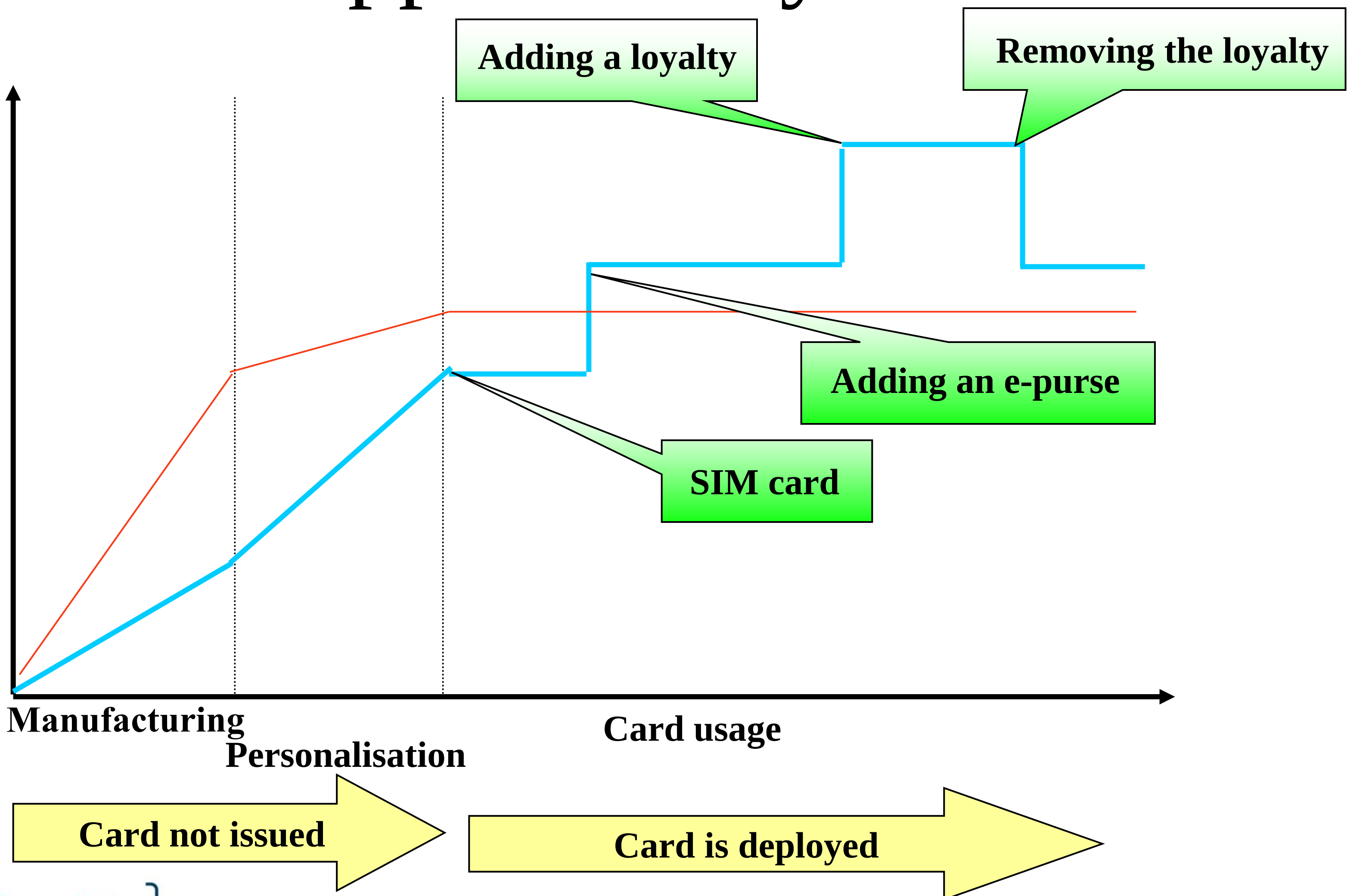
OS based on 7816-4

- Pro
  - Cheap, easy to use
  - Possible to insert new commands
- Cons
  - Unable to execute code
  - Frozen after personalisation phase,
  - Data oriented.

Time to market

- Time between decision and product launch
- Could take as one year if mask need to be redevelop
- Not really adapted to current market :
  - Mobile phone is a highly competitive market,
  - Interoperability is needed,
  - Development cost are too important,
- Smart card manufacturers developed generic smart card: open cards
  - With real operating system
  - Able to download application during their life cycle

Applet life cycle

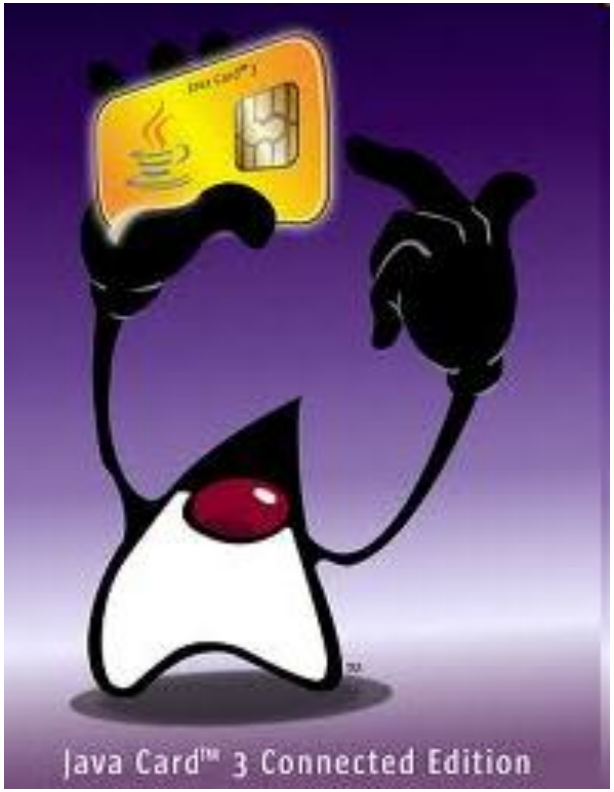


Open cards

- From a developer point of view:
  - Until now, writing an application required a specific knowledge,
  - No need of smart card specialists,
  - Solution : use general purpose programming language (C, Java, Visual Basic…)
  - Much more easier to integrate applications,
  - More tools to test applications,
- From an end-user point of view
  - Several application on a single card,
  - Possibility to load/unload application when needed.

Smartcards of the present days

- Java Card
  - Embedded virtual machine,
  - Open standard (Java Card 2.2),
  - Wide support of the industry
    - IBM, Visa,…
  - Reduction of development time.



Applet development

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

MULTOS

- Based on the MEL (Multos Executable Language) interpreter.
  - Operating system and memory firewalls
  - Virtual Machine layer to provide abstraction
  - Application Programming Interface (API)
  - Application management including secure loading and deleting methods.
- See http://www.multos.com

Basic Card

- Based on the Basic language
  - DOS like file system,
  - P-Code byte code interpreter
- PRO
  - Fit well for a small amount of cards
- CONS
  - Not supported by major smart card manufacturers
  - Proprietary code (http://www.zeitcontrol.de)

Next step ?

- Smart Card Web Server : portable web server,
- Access to the secret stored in the card through your browser,
- Use the USB port, TCP/IP protocol, data security through SSL, multi-threading, full garbage collection… *id est* JC3.0

Any question ?