Smart Cards and their principles

Smart Cards and their principles

Samia Bouzefrane

Associate Professor

CEDRIC –CNAM

samia.bouzefrane@cnam.fr
http://cedric.cnam.fr/~bouzefra

These slides are dedicated to Roland Moreno who was sensitive to my teaching activities on the chip cards
A special thanks to Michel Ugon who provides me some information concerning the history of chip cards

le cnam

Smart card: introduction and Principle

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Smart Cards nowadays

- Today : more than 5 billions of cards
- **Monetics** :
  - banking card : Credit Cards Group, new EMV cards, etc.
  - e-wallet : **Octopus**, **Moneo** in France, **Proton** in Belgium, **Geldkarte** in Germany
- **Identification** :
  eID in Belgium), **E-passports** (from august 2006 in France), Biometric Passport (since June 2009)
- **Education** (student card/restaurant card)
- **Mobile phones** (**SIM** card)
- **Medical domain** (**Vitale** card in France, **SIS** card in Belgium).
- **Transportation** (**Navigo Pass** in Paris, **Oyster** in London)
- **Secure access to buildings** : for authentication the card has a crypto-processor dedicated to cryptographic computation.

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

The example of Passeports in France

Since 2006 in France :
Electronic passport contains a chip that stores personal data of the holder: (name, date of birth, citizenship, passport number, digital photo).

Since June 15th 2009 :
Biometric passport : RFID chip that allows at a low distance to be read – contains the same data as in electronic passport but stores digitalized finger prints (from the age of six) of the holder.

(http://www.prefecture-police-paris.interieur.gouv.fr/demarches/passeport_elec/passeport_2006.htm)

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

Market of contact/contactless smart cards

Worldwide Smart Secure Device shipment – 2012 and 2013 forecasts

(Source : Eurosmart, April 2013)

Eurosmart estimated worldwide Smart Secure Devices (microprocessors)
Millions of Units

	2012	2013 forecast	2013 vs 2012 % growth
Telecom	5.100*	5.350	5%
Financial services	1.200	1.480	23%
Government - Healthcare	310	360	16%
Transport	135	160	19%
Pay TV	135	145	7%
Others	90	100	11%
Total	6.970	7.595	9%

* Source SIMalliance

Worldwide Smart Secure Contactless market figures – 2012 and 2013 forecasts (included in the above forecasts)

(Source : Eurosmart, April 2013)

Eurosmart estimated worldwide Smart Secure Contactless Devices (microprocessor)
Millions of Units

	2012	2013 forecast	2013 vs 2012 % growth
Financial services	295	455	54%
Government - Healthcare	170	210	24%
Transport	135	160	19%
Others	60	70	17%
Total	660	895	36%

Source Eurosmart: http://www.eurosmart.com/index.php/publications/market-overview.html

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

Smart Insights Weekly
#13-19, #13-32, #13-41 and #13-42

According to ABI Research report "Smart Cards in Latin America", smart card shipments within the Latin America's region will increase from 752 million in 2013 to 1.15 billion in 2018, focusing the ID and payment cards.

Ingenico supports US EMV migration. It has already collaborated in the Canadian EMV migration, providing a platform for processors to test EMV transactions.

According to IDC, smartphone shipments in China are expected to reach 450 million units in 2014 compared to expected 360 million in 2013, with Android to continue to be the most used operating system

Gemalto and Zetes will supply parts of the Belgium ePassports program. ePassports are to be introduced in May 2014, and to be provided more than 400,000 ePassports every year, during 5 years.

Santander UK has launched a new Student Smart Card which combines a University undergraduate ID with Visa debit functionality.

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

Smart Insights Weekly
#13-19, #13-32, #13-41 and #13-42

Oberthur Technologies has renewed its partnership with STM (La Société de Transport de Montréal), the transport authority of Montreal in Canada, for four years. The company will continue to issue the CityGo card.

TCRM (Transports en Commun de la Région Messine), the local public transportation network in the Metz urban area in France, inaugurated the new 100% contactless ticketing system.

Opal smart card is now available in the entire Sydney Ferries network; there are 669 card readers across the 40 wharves in Sydney servicing all 8 ferry routes and at 17 train stations across the city.

The Brazilian Senate has approved a bill to regulate mobile payments, by granting Brazil's central bank the power to regulate small financial transactions made through mobile devices.

The number of mobile banking customers of mobile money systems in Bangladesh passed the 6.0 million mark in August with transactions reaching nearly BDT 1.6 billion (EUR 15 million) per day.

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

History – Invention of smart cards

- In 1968, Helmut Gröttrup and Jürgen Dethloff, two ingenieers of a deuch company Giesecke & Devrient, invent an automatic card. They filed a patent on Sept 6, 1976 (granted later on 1982).

- In 1969, the american Halpern, Castrucci, Ellingboe contribute in the information card. They filed a patent in Oct. 1970.

- 1970: Kunitaka Arimura filed a patent in March 1970 in Japan

- The first patent on a chip card (secured memory) is filed on March 1974 by Roland Moreno)

le cnam

Inhibiting means by Roland Moreno

- Means proposed on 1974 and deployed not before 1983

-Internal comparison of a confidential code

- Error counter that causes the self-destruction of the chip if several attempts are failed (a fuse is destroyed)
- Processing means
- Reading is irreversibly impossible for predetermined memory areas (keys, pin
- Writing, modifying, deleting are impossible irreversibly for predetermined memory areas.

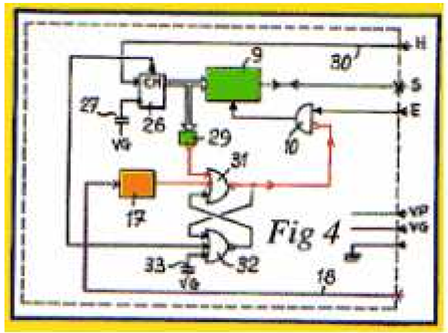


Figure by Roland Moreno in:
http://www.encyclonova.com/index.php/Moyens_inhibiteurs

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

The chip-card inventors

➢In 1975, the Company Honeywell Bull in France filed a patent (in 11 countries) for a portable card with signal processing means. The inventors are: Bernard Badet, François Guillaume, and Karel Kurzweil.

➢In 1977, Dethloff filed a patent for a memory card with inhibiting means integrated within a micro-processor card (the card can be re-programmed thanks to a mask).

➢In August 1977, the french Michel Ugon working with Bull company filed a patent for a micro-processor card called CP8, pour « Circuit Portatif des années 80 », that has been deployed from 1990, another patent on the SPOM (Self Programmable One chip Microprocessor) architecture on April 1978.

Provided by Michel Ugon

First chip card

- **1982: first wired card (with Schlumberger)**
- **1983 first a card with a microprocessor (with Bull CP8)**
  - ✓ Manufactured by Motorola for Bull CP8
  - ✓Uses a processor of type 6805 (micro-controler of 8 bits of Motorola)
  - ✓With a PROM of 1 KB

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

The companies of smart card

In 1978, DGT that becomes France Telecom achieves prototypes, Point of Sales (terminals) and cards and heled in the creation of Groupement d'Intérêt Economique (GIE) called *Carte à Mémoire* gathering 10 french banks.

In 1979, the giant of petroleum services Schlumberger joined Innovatron capital for 23 %, then 34 %, and merges with its concurrent companies : Solaic in 1997 then Bull CP8 in 2001.

In 1983, first deployment of smart cards has been acheived thanks to chip phone (télé-carte) for phone booths.

At the end of 1980, the GIE « *Carte bancaire* » that succeeds the GIE « *Carte à mémoire* », orders 16 millions of CP8 cards.

In 1988, Marc Lassus founds Gemplus in France. Gemplus was number 1 until its merger with (ex Schlumberger) in 2006. More than 6.8 billions of cards have been manufactured from 1980 to 2006. The worldwide market is today Gemalto, followed by Oberthur Card Systems and Giesecke & Devrient.

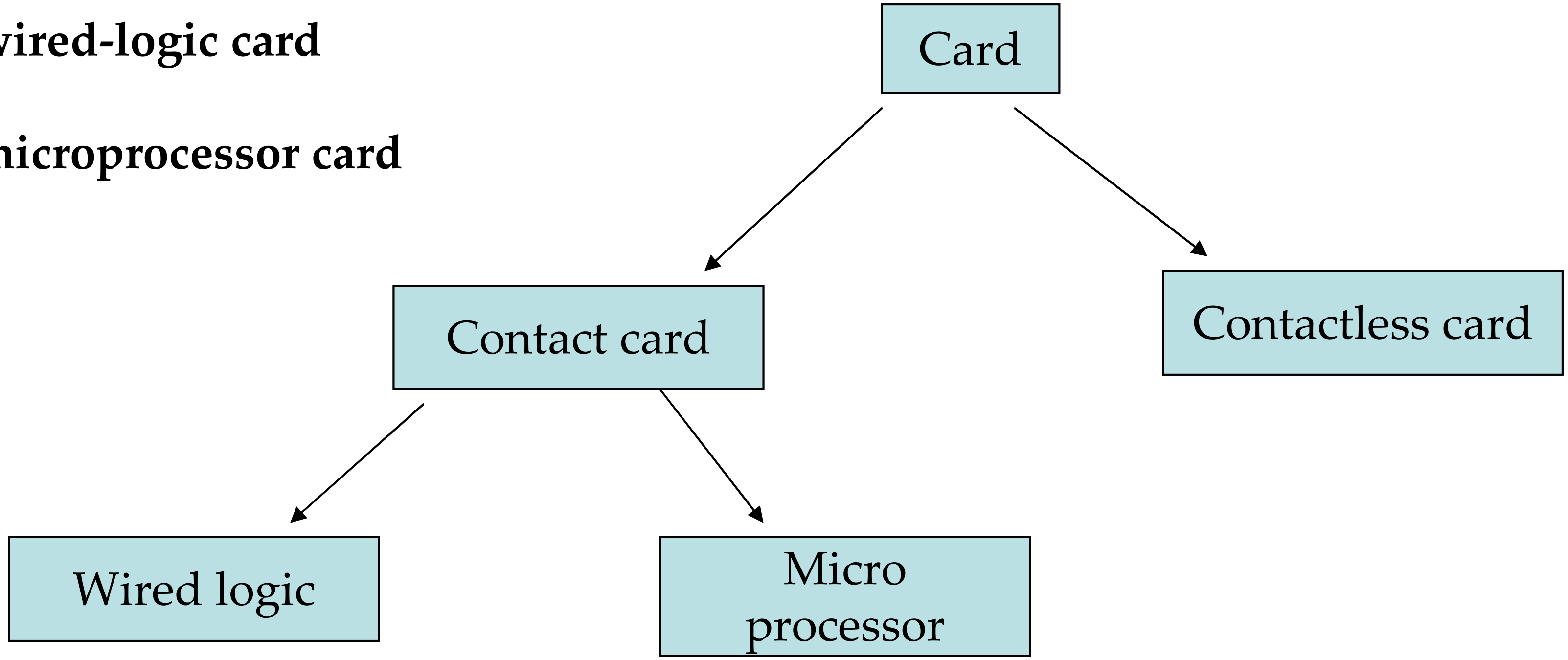
Some dates

Year	Event
1979	First card manufactered by Motorola for Bull CP8
1980-81	First experimentations for payed TV
1983	First phone cards by France Télécom operator
1984	First version of banking card (carte bleue) based on Bull CP8 card
1987	Publication of the standards of ISO 7816
1989	First GSM cards for mobile phones (Gemplus)
1998	First Java Card platforms

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

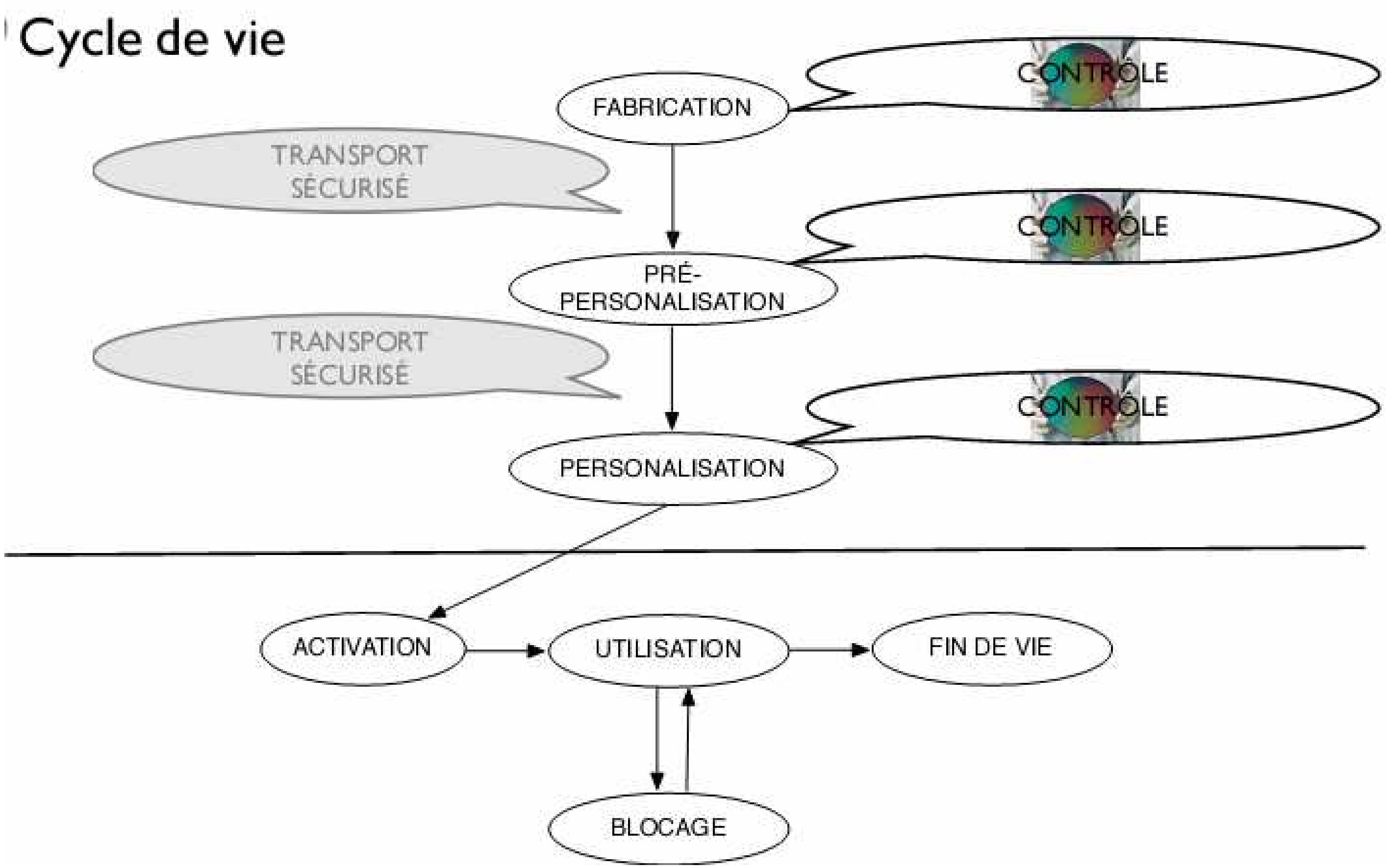
Products

- wired-logic card
- microprocessor card



le cnam

Card life cycle



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Microcontroler card

- Smart cards/chip cards
- Contain a microcontroler :

  - CU
  - PROM
  - RAM
  - EEPROM
  - interface of I/O
  - crypto processor

  } within the same component

- Processor : 16 or 32 bits
- EEPROM : from 1KB to 128 KB (256 KB for Java Card or Basic Card)

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

The principal categories of OS

- **Before 1990:**
  - **Mono-application OS**
  - **- M4, BO, COS,...**

- **Evolution (1990-1995) :**
  - **- MP, MP100, MCOS**
  - **- Multi-application**
  - **- CQL (1993), Basic Card,....**

- **Towards the opening**
  - **- Java Card (since 1996)**
  - **- .Net**

le cnam

Hardware architecture

- **CPU : 8, 16 & 32 bits,**
  - **core 8051, AVR, ARM, MIPS**

- **Memory :**
  - **RAM : 1 to 4 KB**
  - **NVM (EEPROM/Flash) : 16 to 32 KB**
  - **ROM : 32 to 64KB**

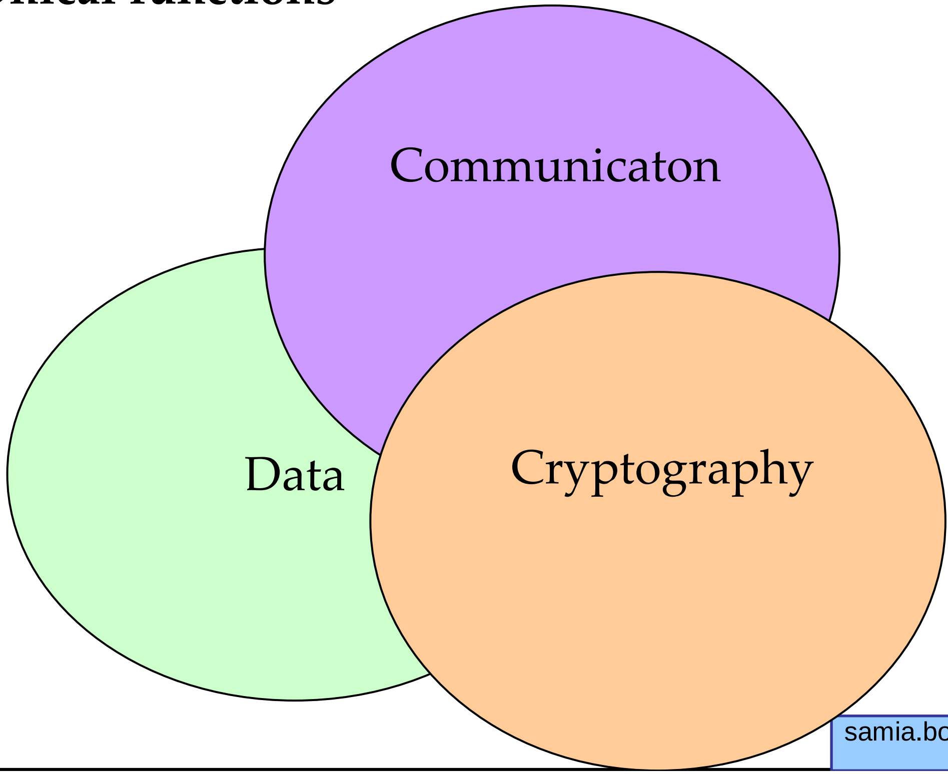
- **Co-processor**
  - **Java Card : execution of the Byte Code of Java Card**

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

Software architecture

- I/O managment
- Memory management
- Cryptographical functions



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Standardization

The standards

The standards in relation with the card:

- **ISO 7816 (contact smart cards) ISO 14443 (contactless smart cards),**
- **ETSI, (telecommunications, GSM)**
- **EMV, (payment cards)**
- **ICAO, (UNO agency, biometry, passport)**
- **Health,**

...

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Standards of AFNOR / ISO

➢ **The position of the contacts**

ISO card

AFNOR card

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Principal standards of contact cards: ISO 7816

➢ **ISO 7816 « Idenfication cards – Integrated circuit cards with contacts »**

✓Published by ISO (International Organisation for Standardisation)

✓The most important standard that defines the features of the smart cards using an electrical contact

✓15 standards are proposed for contact cards.

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Principal standards of contact cards

- The standard ISO 7816-1 defines the physical characteristics of the card
- The standard ISO 7816-2 defines the position of the contacts within the card
- The standard ISO 7816-3 defines the electric signals used to communicate with the card
- The standard ISO 7816-4 defines the basic commands to interact with the smart cards

The standard ISO 7816-1

- **ISO 7816-1 : revised in March 1998**
defines the physical characteristics of the cards
ex : geometry, resistance, contacts, etc.

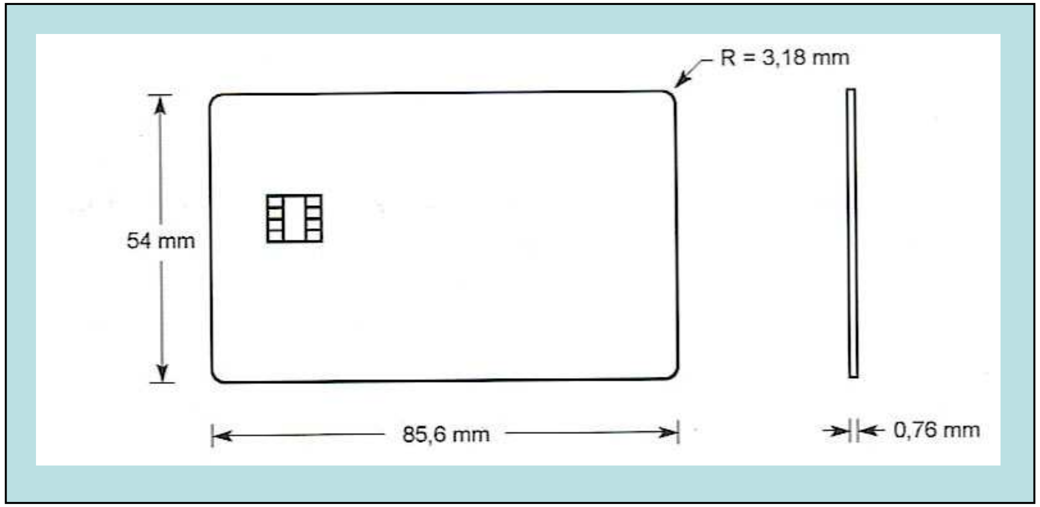
samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Mechanical characteristics of smart cards

- **Even if we know two kinds of chip cards**
  - ✓**The format of the banking card**
  - ✓**The format of the SIM card**

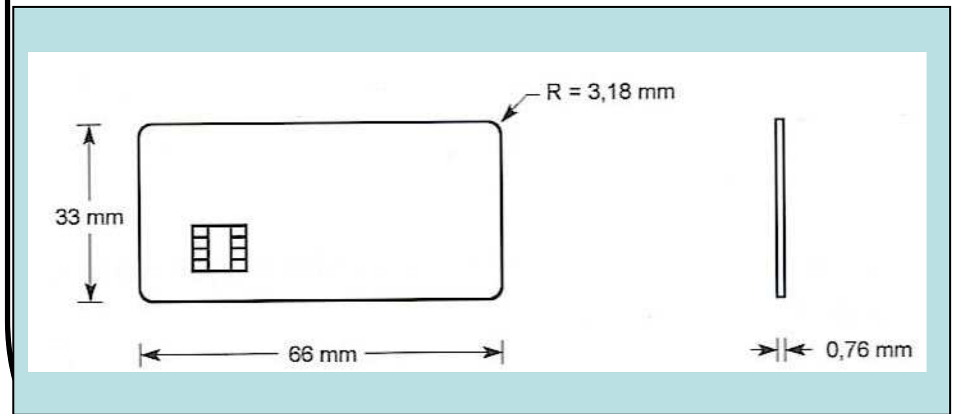
- **3 standardized formats : ID1, ID00 et ID000**

Three Formats

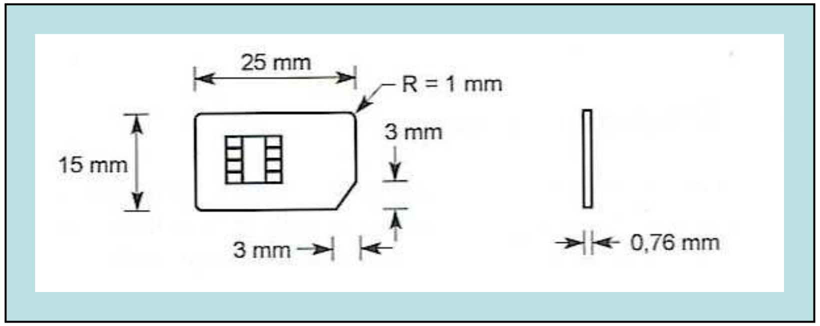


ID 01

ID 00

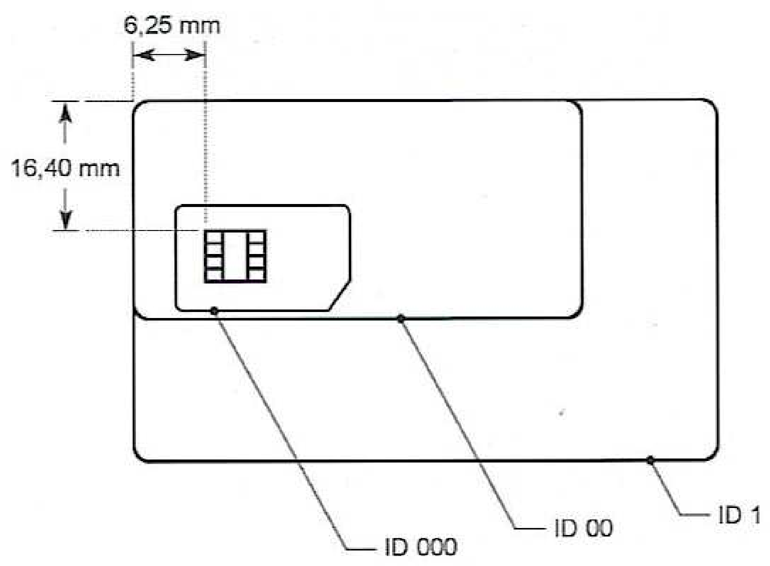


ID 000



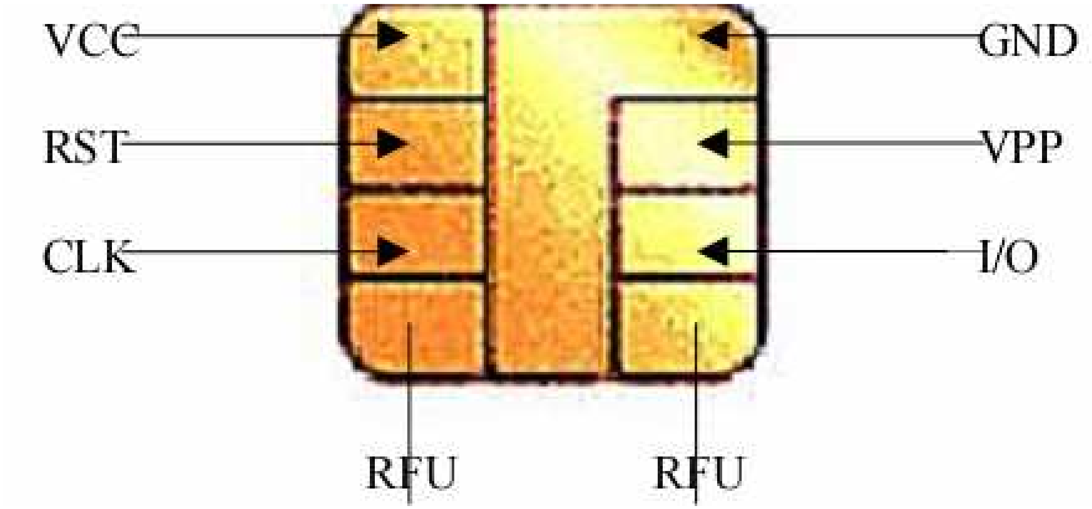
Three Formats

➢The manufacturer provides one size (ID1), the client may reduce the dimension to have the format ID00 or ID000 (ex. SIM card)



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

ISO 7816-2



Vcc: electric power (3 to 5 V)
RST: is the « reset », initializes the microprocessor (warm reset)
cold reset = power off and then power on
CLK: clock signal because there is no clock in the card
GND: ground
Vpp: used in old cards to have a second power necessary for their programming
I/O: used to exchange data and commands with the terminal: half-duplex communication.

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

ISO 7816-3

Defines the electrical interface and the communication protocols :

- ✓**The transmission protocols (TPDU, Transmission Protocol Data Unit)**
  T=0 : byte oriented protocol, T=1 : packet oriented protocol,
  T=14 : reserved for proprietary protocols,

- ✓**Selecting a type of protocol,**

- ✓**The Answer to Reset (ATR) corresponds to the data sent by the card when power on,**

- ✓**The electric signals, like the voltage, the clock frequency and the communication speed.**

When inserting a card into a reader

- **The standard ISO 7816-3 specifies the behavior of the card when powering on/off**
- **In the reader, there is an interface circuit :**
  - ✓ Connection of the card and activation of its contacts by the interface circuit
  - ✓ Reset the card
  - ✓ Response To the Reset (ATR) sent by the card
  - ✓ Dialogue between the card and the terminal
  - ✓ Deactivation of the contacts by the interface circuit
  - ✓ Retrieve the card

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

ATR as defined by ISO 7816-3

- **ATR (Answer To Reset):**
  - **Upon the card is powered on, it sends an answer to a reset (ATR)**
    The size of the ATR can reach 33 bytes. The ATR provides to the terminal some parameters necessary to establish a communication with the card.

  - **Parameters sent by the card:**

    - The transport protocol ;
    - Data transmission rate;
    - Serial number of the chip, etc.

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

ATR

- **ATR is the response to a reset**
- **ATR at least 2 bytes, at most 33 bytes**
- **Transmission is half duplex with asynchronous mode**
- **Clock frequency is between 1 to 5 MHz**
- **Communication is achieved through the I/O contact of the card and the reader**

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

The initial character of the ATR

- **First chracacter of the ATR= TS**
- **TS can take two values: (ZZAAAAAA)[1] ou (ZZAZZZAA)[2]**
- **1: inverse convention :**
  - **low level A = logical « one »**
  - **high level Z = logical « zero »**
  - **ba (bit transmitted first) = bit 7 (the most significant bit)**
  - **bh (bit transmitted at last)=bit 0 (the less significant bit)**

  TS = 0011 1111 (3F, in Hexadecimal)
- **2: direct convention :**
  - **low level A = logical « 0 »**
  - **high level Z = logical « 1 »**
  - **ba (bit transmitted first) = bit 0 (the less significant bit)**
  - **bh (bit transmitted at last)=bit 7 (the most significant bit)**

  TS = 0011 1011 (3B, in Hexadecimal)

TPDU/APDU Protocols

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

ISO 7816-4

- **This standard defines the structure of the messages called APDU (Application Protocol Data Units) exchanged between the reader and the card.**

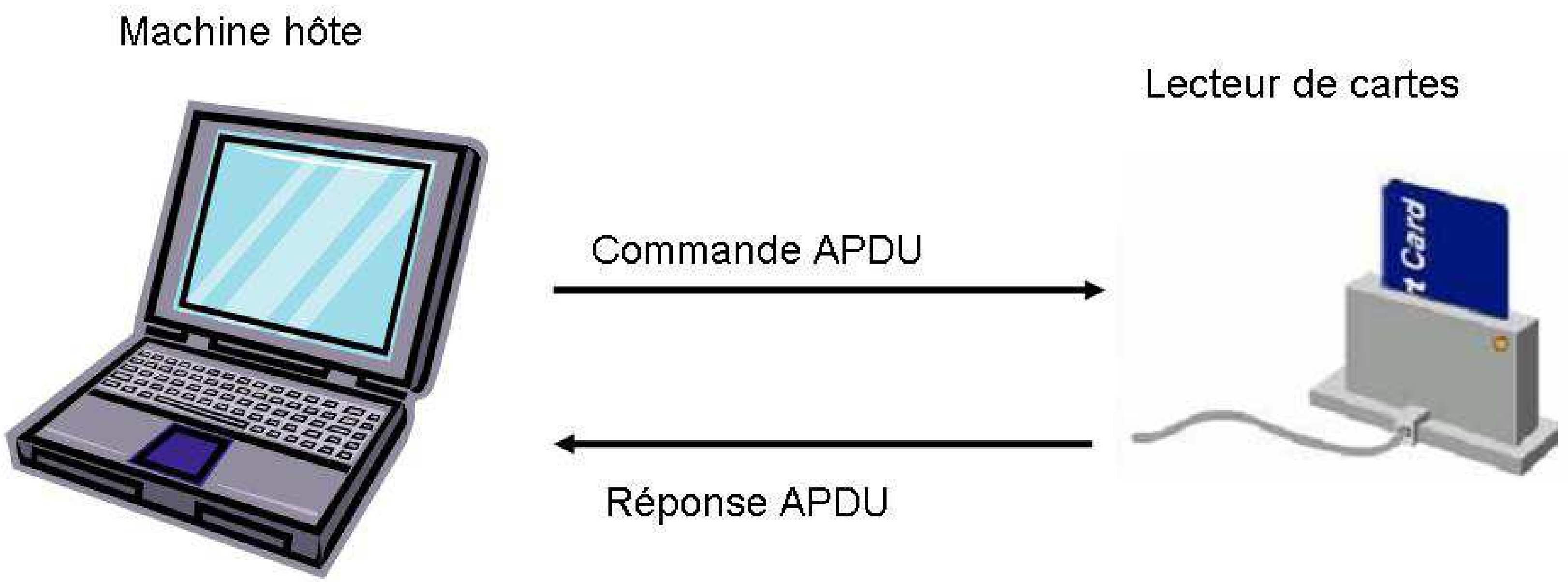
- **The communication is based on Client-Server mode,**

- **The terminal is always the initiator of the communication.**

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

ISO 7816-4 : APDU protocol



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

APDU commands format

APDU command						
Mandatory head				**optional body**		
CLA	**INS**	**P1**	**P2**	**Lc**	**Data field**	**Le**

- CLA (1 byte): instruction class --- dedicated for an application domain
- INS (1 byte): defines the instruction of the command
- P1 (1 byte) and P2 (1 byte): the parameters of the instruction
- Lc (1 byte): data length
- With Le=0, - if a writing command => no useful data
  - if reading command => the command must return 256 bytes of data
- Data field (bytes whose length is the Lc value): a sequence of bytes.

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Response APDU format

APDU Response		
Optional body	**Mandatory part**	
Data field	**SW1**	**SW2**

- Data field (with a variable length): byte sequence
- SW1 (1 byte) and SW2 (1 byte): Status words sent by the card.

SW1 SW2 =		
	0x90 0x00	Success
	0x6E 0x00	CLA error
	0x6D 0x00	INS error
	0x6B 0x00	P1, P2 error
	0x67 0x00	LEN error
	0x98 0x04	Bad PIN
	0x98 0x40	Card blocked

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Examples of cards

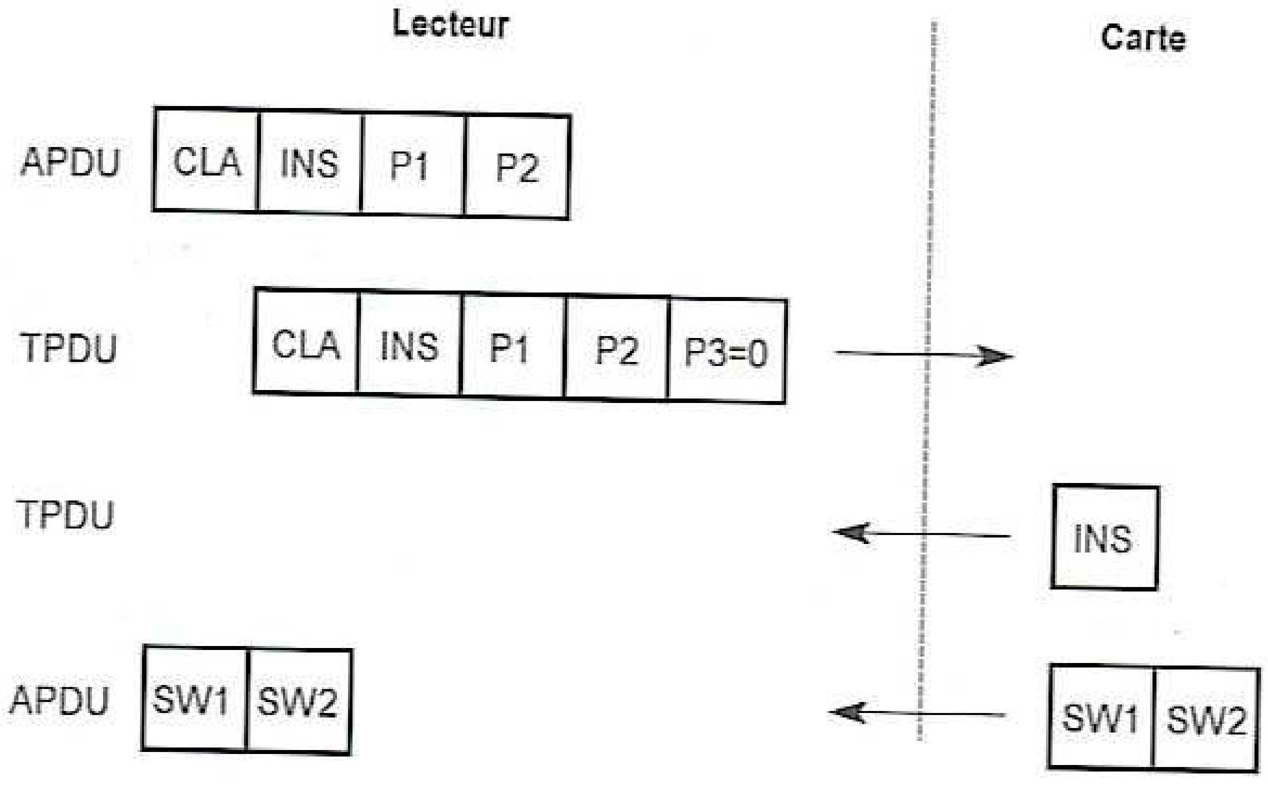
Fields of APDU command	Values
CLA	BC = french credit cards, vitale cards, A0 = SIM cards 00 = Moneo card (e-wallet in France), Mastercard, Visa
INS	20 =PIN code verification, B0 = Binary read B2 = Read record D0 = Binary write DC = Write record A4 = Directory selection C0 = get an anwer
P1, P2	parameters
LC	Length of the data sent by the command
Data	contains LC bytes (PIN code to check)

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

APDU Protocol (ISO 7816-4)

- **The standard tries to be conform to the OSI model of ISO**
- **Application layer (APDU) is not really separated from the transport layer (TPDU)**
- **There 5 types of APDU commands**

Sending a command without useful data

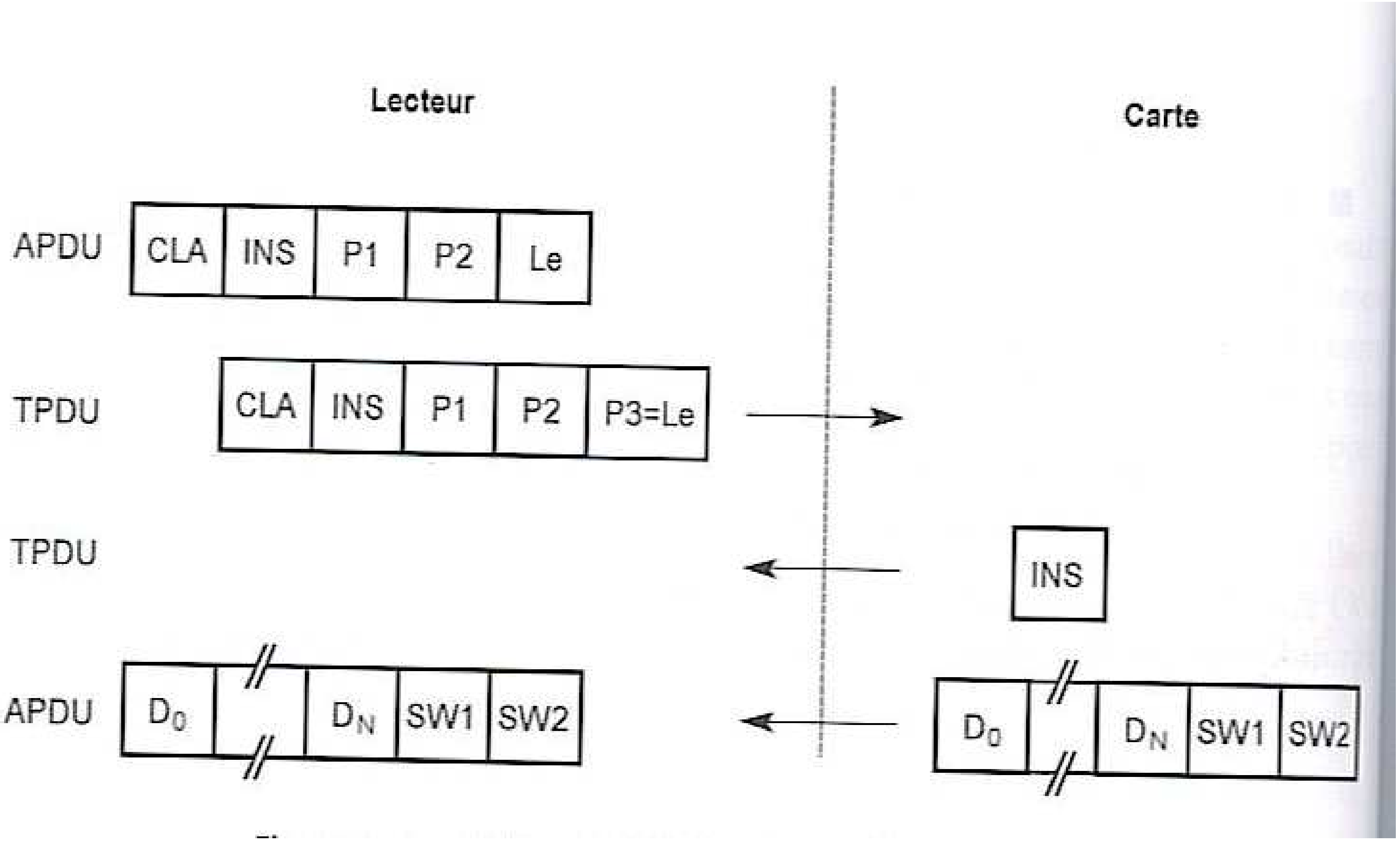


samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

Command with the reception of data from the card

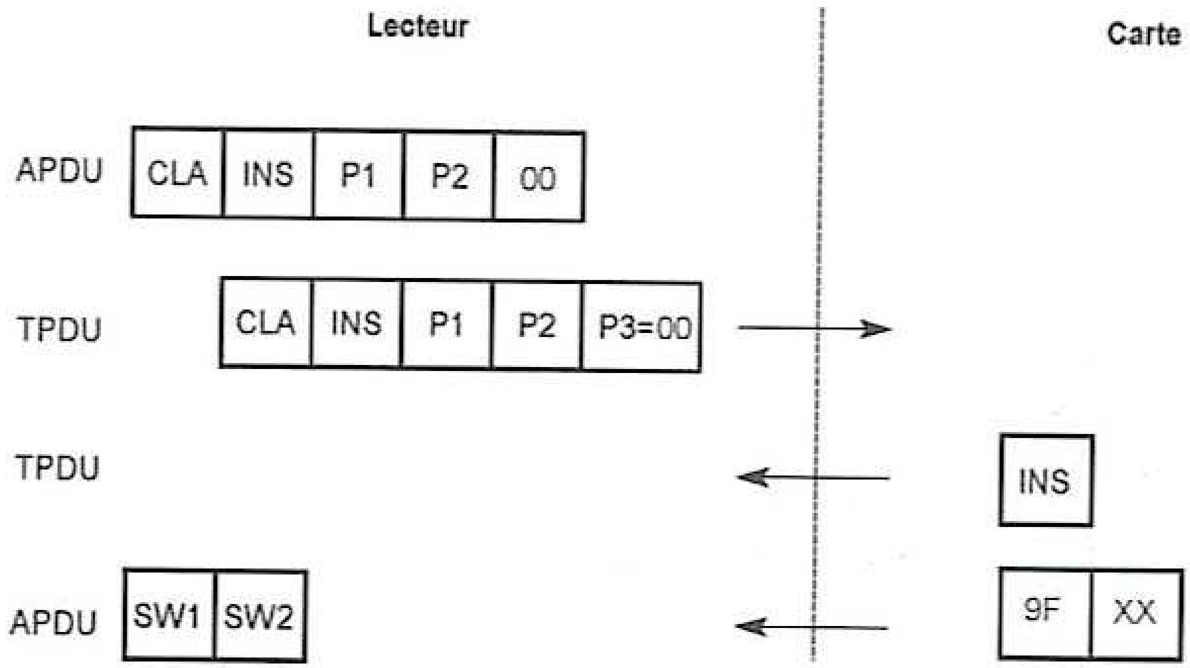
➢ **The number of data sent by the card may be different from *Le***



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Command with an invitation to send data from the card

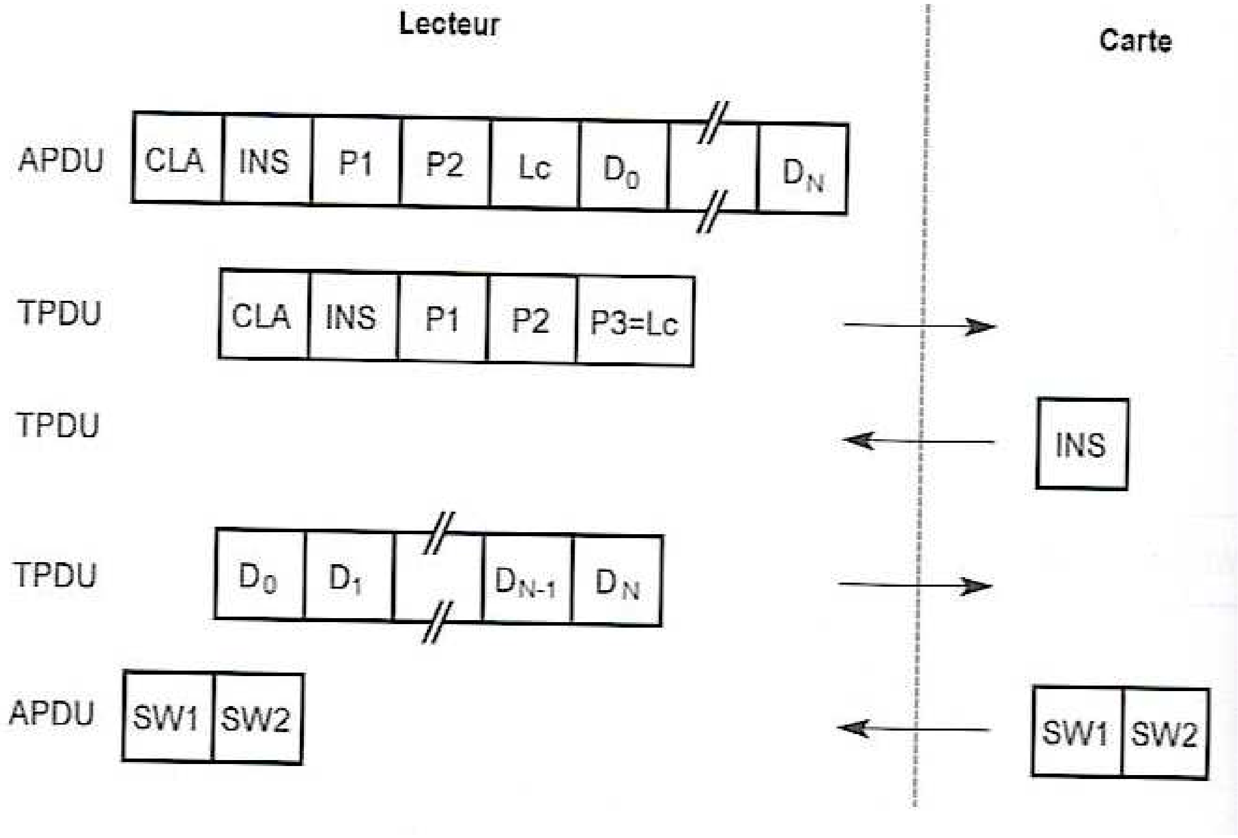
➢*Le=0* because the number of bytes waited for is unknown
➢SW1 SW2 = 9F XX (with XX the number of bytes to be sent by the card
➢The reader must send a command with this number of bytes (GET RESPONSE command)



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Command with data sent to the card

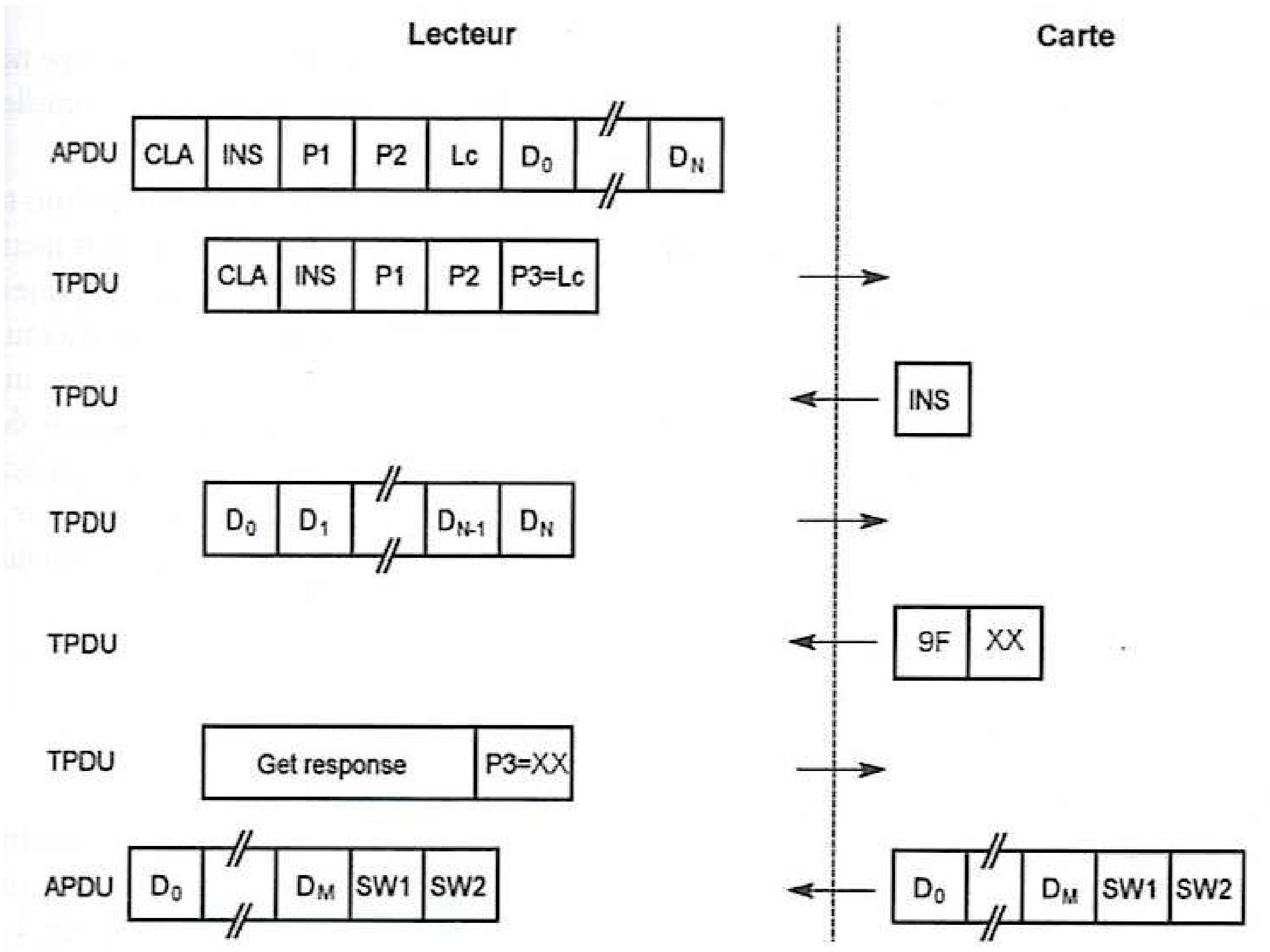
➢*Lc*: contains the length of the data sent by the terminal



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

Command with data exchanged



samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

le cnam

References

1.Technology for smart cards: architecture and programmer's guide, Zhiqun Chen, Addison Wesley, sept. 2000

2. Les Cartes à puce: théorie et mise en œuvre, Christian Tavernier, 2ème édition, Ed. Dunod, 2007.

3. EMV standards: http://www.emvco.com

4. Lecture notes on smart cards by Samia Bouzefrane (CNAM): http://cedric.cnam.fr/~bouzefra/cours_pfsem.html

5. Magazine MISCH, Hors Série, Cartes à puce : découvrez leurs fonctionnalités et et leurs limites, Nov. 2008.

6. Magazine Linux, Hors Série, Cartes à puce, Oct. 2008.

8. Interview with Roland Moreno in July 2010.

9. Exchanged emails with Michel Ugon (oct. 2013).

samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -