Introduction à la Javacard

Pascal.Urien@telecom-paris.fr

TELECOM Paris

IP PARIS

1971,
1ier micro-processeur i4004

1973
1ier micro-ordinateur i8008
François Gernelle

1975, M6502

1977, Apple II

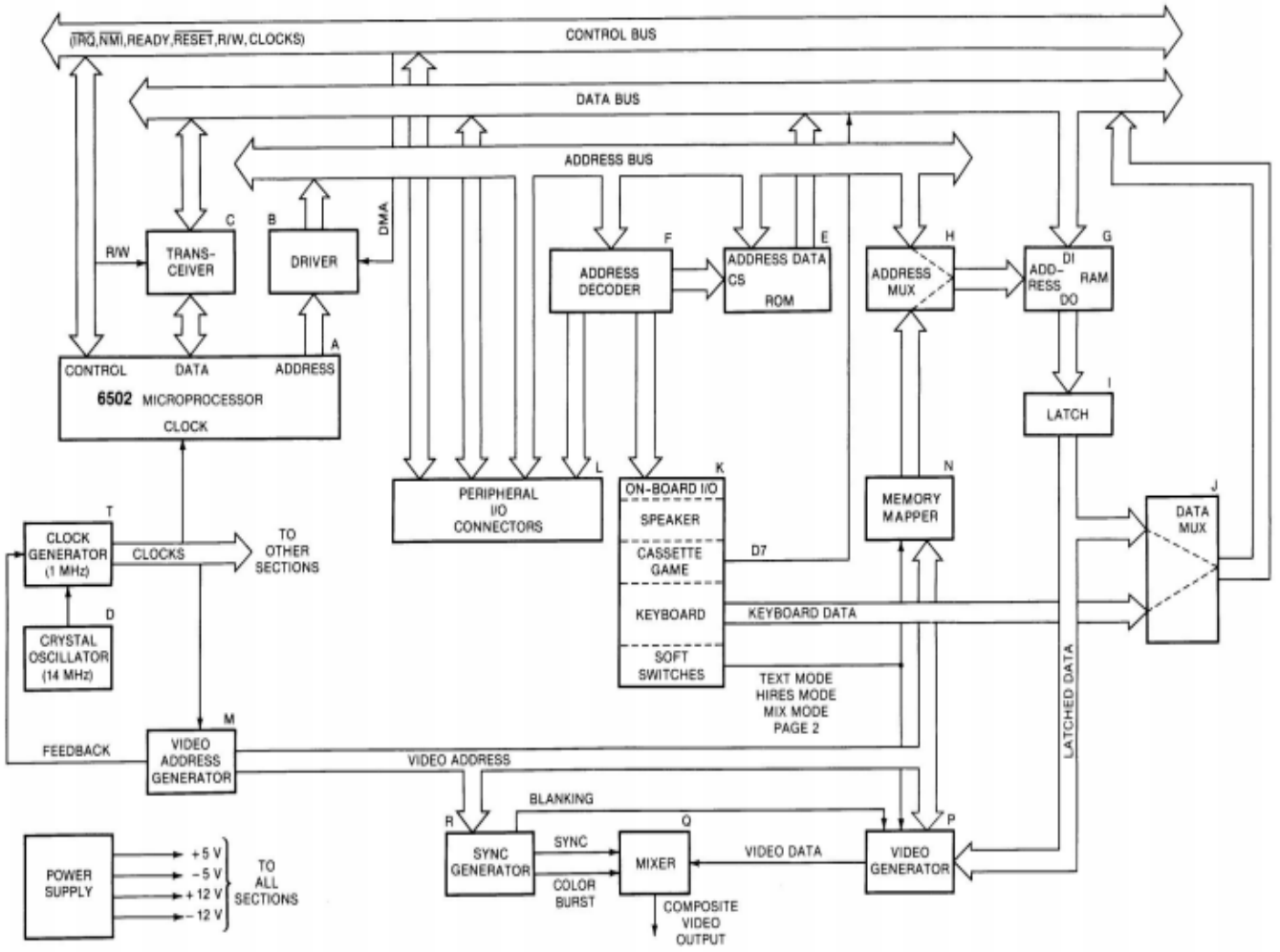


Fig. 2-1. Apple II block diagram.

Carte

Lecteur

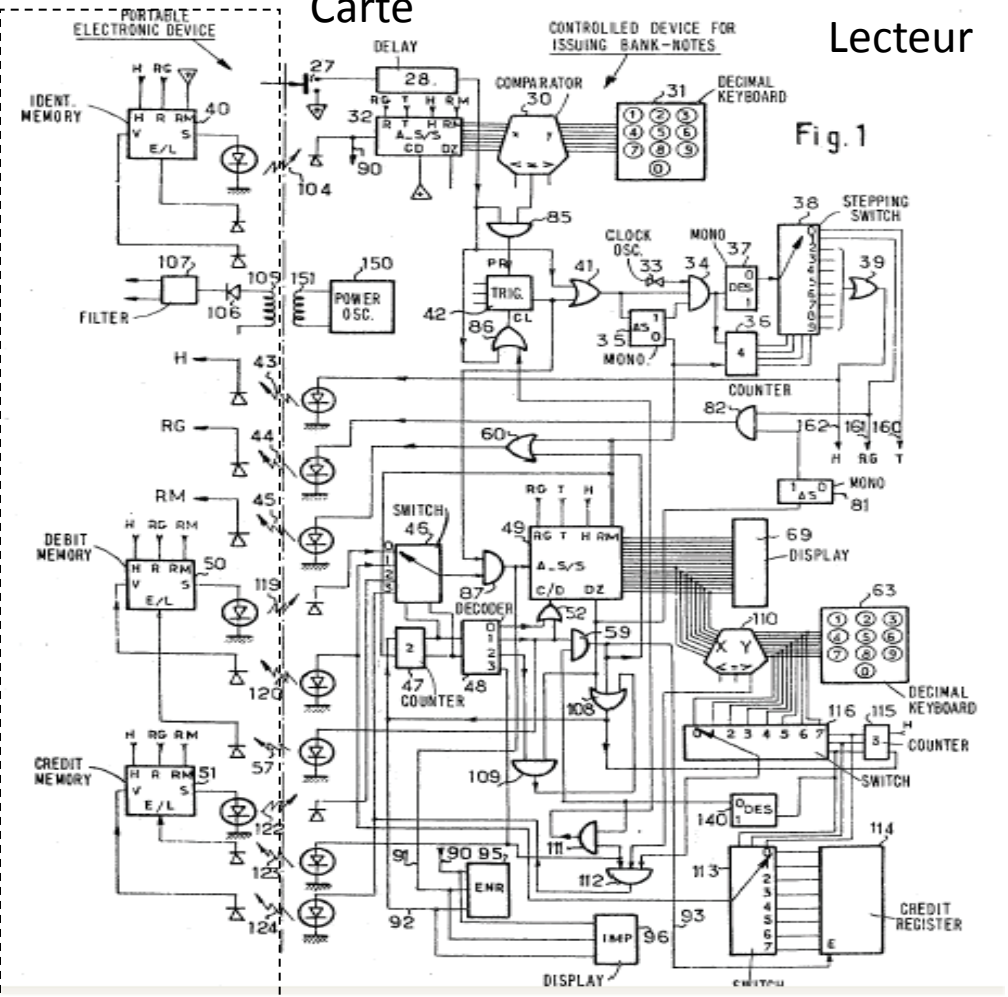
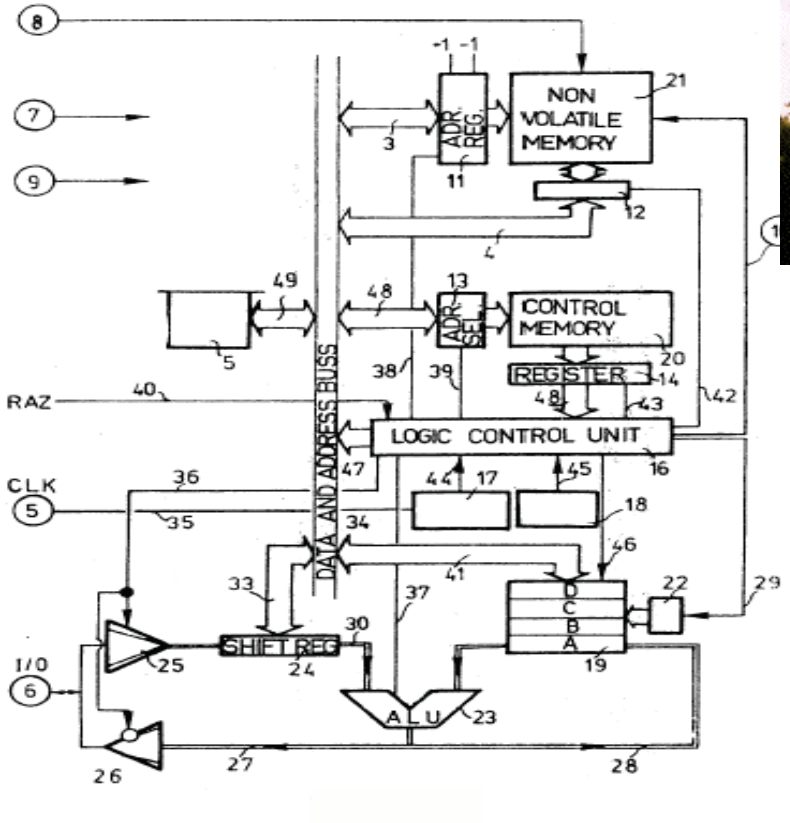


Fig. 1

Roland Moreno

- 1972, Fondateur INNOVATRON
- 25 mars 1974, Brevet 74.10191
- 21 mars 1975, US 4,007,355

1978, une télécarte 1Kbit



Michel Ugon

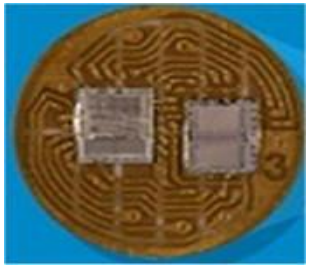
- 1976, Directeur R&D Bull CP8
- 26 août 1977, brevet 77.26107
- 25 août 1978, US 4,211,919

Marc Lassus

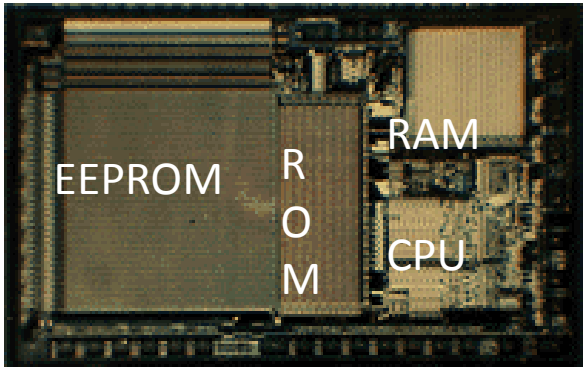
- 1979 , production (MOTOROLA) des premiers prototypes de carte à puce
- 1989 Fondateur de GEMPLUS

Le SPOM

- Mars 1979, CII-Honeywell Bull et Motorola,
  - Deux puces: une mémoire 2716 EPROM et un microprocesseur 8 bits Mostek3870.
- Octobre 1981 puce monolithique CII-Honeywell Bull et Motorola
  - SPOM, Self Programmable One chip Microcomputer



1979, carte hybride à deux puces

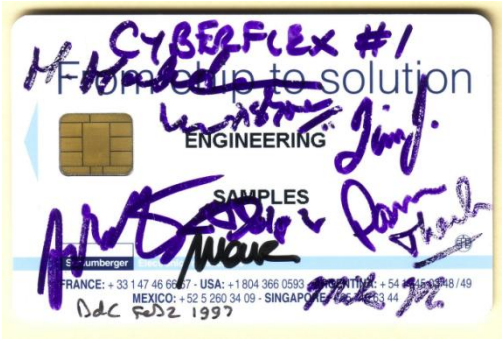


1981, chip SPOM1 en NMOS 3.5 µm (42000 transistors sur 19.5mm²).

1988, le chip 21 avec une mémoire EEPROM

La JAVACARD (1997)

- 1995, Bertrand Ducastel, R&D smart card division Schlumberger, Austin Texas
- Schlumberger Austin R&D team
  - Timothy J. Wilkinson
  - Ksheerabdhi Krishna
  - Scoot Guthery
  - Mike Montgomery
- 1997, First JavaCard
- 1997, Brevet Java Card, US 6,308,317
- 1997, création du Javacard Forum (JCF)



US 20030023954A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0023954 A1**

Wilkinson et al. (43) **Pub. Date: Jan. 30, 2003**

(54) **USING A HIGH LEVEL PROGRAMMING LANGUAGE WITH A MICROCONTROLLER**

(76) Inventors: **Timothy J. Wilkinson**, London (GB); **Scott B. Guthery**, Belmont, MA (US); **Ksheerabdhi Krishna**, Cedar Park, TX (US); **Michael A. Montgomery**, Cedar Park, TX (US)

Correspondence Address:
SCHLUMBERGER AUSTIN TECHNOLOGY CENTER
ATTN: PEHR B. JANSSON, INTELLECTUAL PROP LAW DEPT.
8311 NORTH FM 620
AUSTIN, TX 78726 (US)

(21) Appl. No.: **10/037,390**

(22) Filed: **Oct. 23, 2001**

Related U.S. Application Data

(63) Continuation of application No. 08/957,512, filed on Oct. 24, 1997, now Pat. No. 6,308,317.

(60) Provisional application No. 60/029,057, filed on Oct. 25, 1996.

Publication Classification

(51) **Int. Cl.**[7] **G06F 9/44**

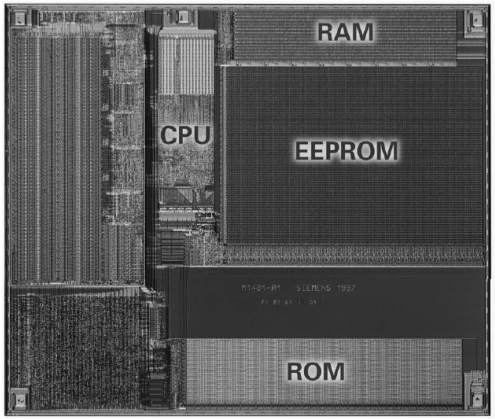
(52) **U.S. Cl.** **717/118**

(57) **ABSTRACT**

An integrated circuit card is used with a terminal. The integrated circuit card includes a memory that stores an interpreter and an application that has a high level programming language format. A processor of the card is configured to use the interpreter to interpret the application for execution and to use a communicator of the card to communicate with the terminal.

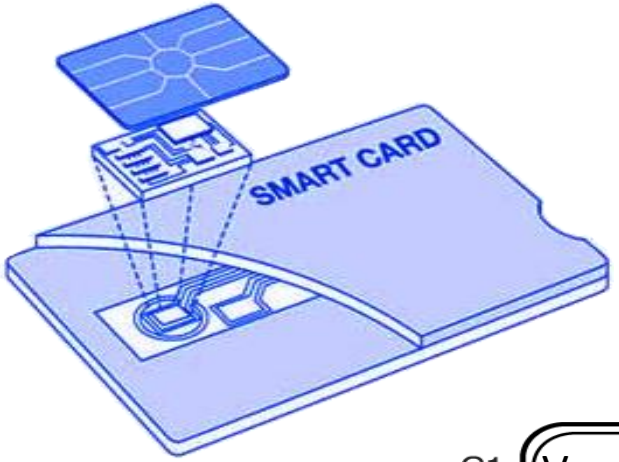
Quelques dates

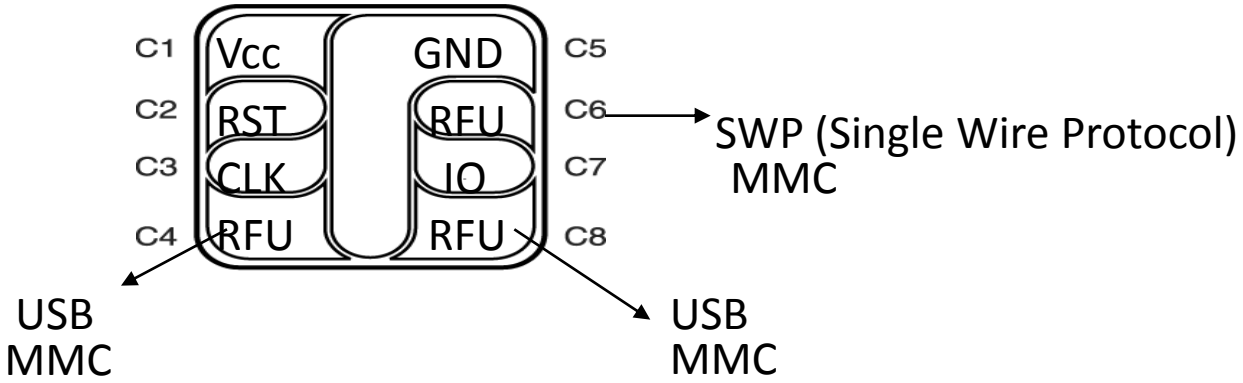
- 1974, Brevet de R.Moreno
- 1977, Brevet de M.Ugon
- 1987, Première norme ISO 7816
- 1988, Spécification de la carte SIM
- 1995, Attaque DPA Paul Kocher
- 1996, Première norme EMV
- 1997, Brevet Java Card, US 6,308,317
- 2002, Dotnet Smart Card, Hiveminded



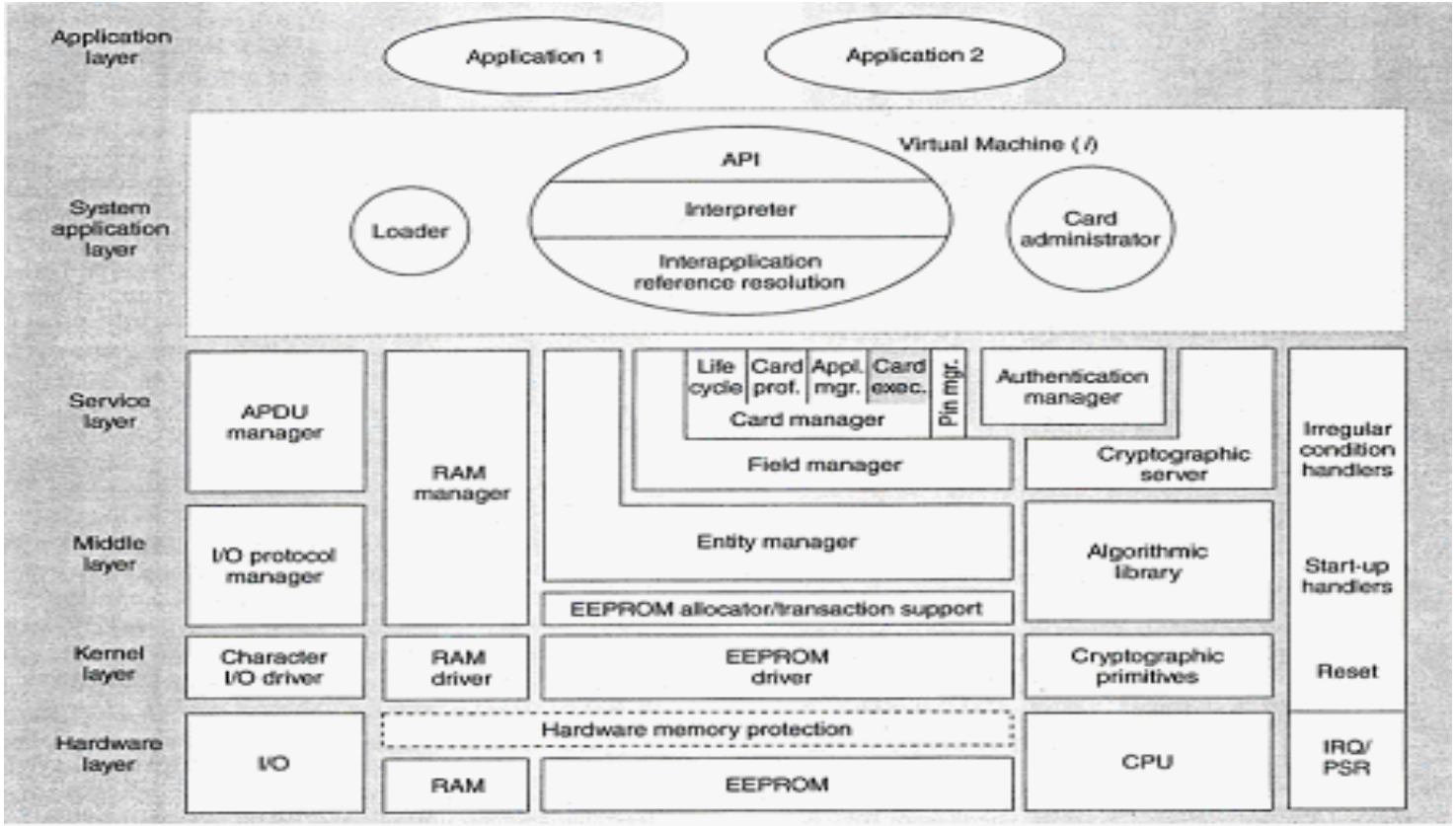
La carte à puce, aperçu de la technologie

Aperçu technologique

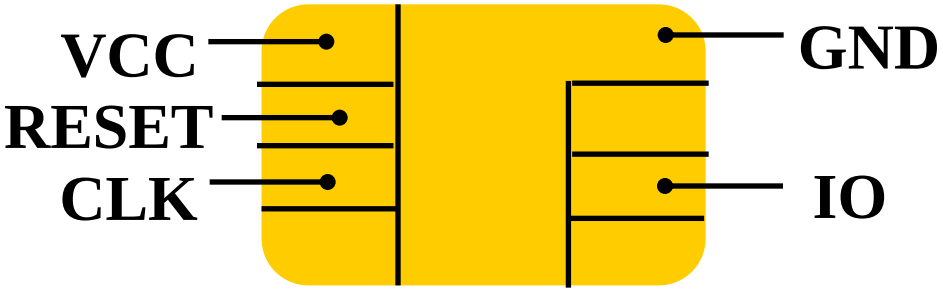


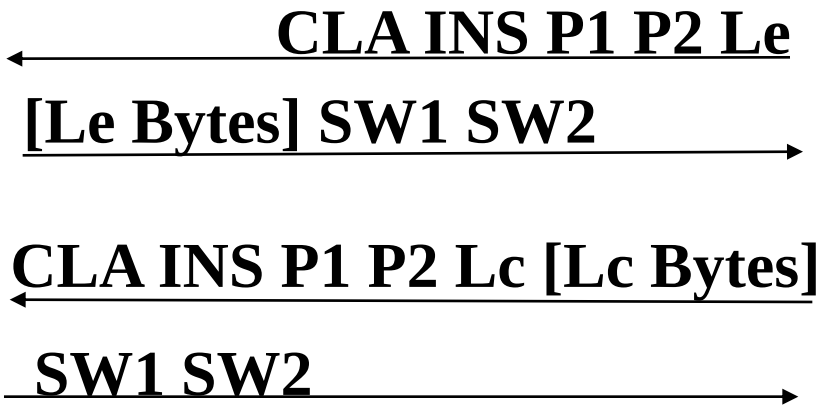


Exemple de système JavaCard



- ***Guillou,L.C, Ugon, M, Quisquater,J.J "Smartcard: a Standardized Security Device Dedicated to Public Cryptology", 1992.***
  - *"*What a smartcard does*. The five operations of a smartcard are 1-input data, 2- output data, 3- read data from non volatile memory (NVM), 4- write or erase data in NVM, 5- compute a cryptographic function."*





APDU ISO7816-4

APDU: CLA INS P1 P2 Lc [Lc Bytes] Le [Expected bytes]

APDU

```
Cas1: CLA INS P1 P2
Cas2: CLA INS P1 P2 Le
Cas3: CLA INS P1 P2 Lc Data
Cas4: CLA INS P1 P2 Lc Data Le
```

TPDU Mapping T=0

```
1: CLA INS P1 P2 P3=00
2: CLA INS P1 P2 P3=Le
3: CLA INS P1 P2 P3=Lc Data
4: CLA INS P1 P2 P3=Lc
   CLA C0 00 00 P3=Le
```

Commandes T=0, ISO7816-4

Y=F(x)

Lecture Le bytes

CLA INS P1 P2 Le

[Le Bytes] SW1 SW2

1- Ecriture xx bytes

CLA INS P1 P2 xx [xx Bytes]

SW1=61 SW2=yy

Ecriture Lc bytes

CLA INS P1 P2 Lc [Lc Bytes]

SW1 SW2

2- Lecture yy bytes

CLA INS=C0 P1=0 P2=0 P3=yy

[yy bytes] SW1 SW2

APDU: CLA INS P1 P2 Lc [Lc Bytes] Le [Expected bytes]