

# La Carte à Microprocesseur

## Un système embarqué en plein essor

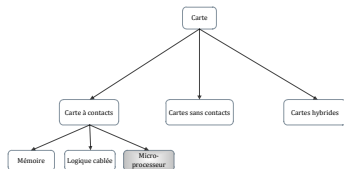
**Tegawendé F. Bissyandé**  
tegawende.bissyande@fasolabs.org

*Cours préparé pour*  
L'Institut Supérieur de Technologie (IST Burkina)

19 Fevrier 2015

# Rappel chapitres 1 & 2

## Familles de cartes à puces



### • Différents domaines d'applications

- 1 Banques, Finances
- 2 Telecommunications
- 3 Système de santé
- 4 Sécurité, Accès

### • Différents types de cartes

- 1 Avec Contact / Sans contact / Hybride (dual interface)
- 2 À mémoire, à logique câblée, à **microprocesseur**

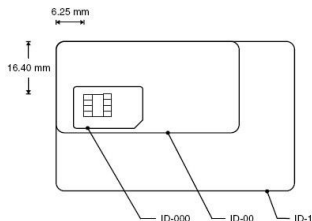


# Rappels Chapitres 1, 2 & 3: Norme 7816 (Parties 1, 2 & 3)

## ISO 7816-1 : Partie 1 de la norme ISO 7816

### Caractéristiques physiques

- Taille des cartes (format Cartes bancaires/ carte SIM)
- Contraintes de résistance physiques (torsion)
- Contraintes de résistance électrique (contacts du microconduit)

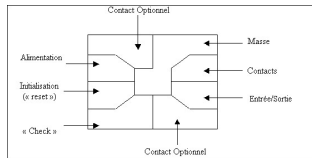


# Rappels Chapitres 1, 2 & 3: Norme 7816 (Parties 1, 2 & 3)

## ISO 7816-2 : Partie 2 de la norme ISO 7816

### La puce

- Dimension de la puce
- Position des contacts des microprocesseur

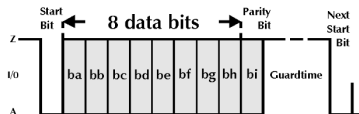


# Rappels Chapitres 1, 2 & 3: Norme 7816 (Parties 1, 2 & 3)

## ISO 7816-3 : Partie 3 de la norme ISO 7816

### Communication

- Signaux électriques et infos échangées
- Protocoles de dialogue avec le monde extérieur
- A noter :
  - 1 La carte n'a pas d'horloge
  - 2 La communication est asynchrone
  - 3 La communication est half-duplex



### Nous avons parlé aussi du système de fichier



La carte à puce ne prend jamais l'initiative...

## ...Elle ne fait que répondre à des commandes

### Structure d'une commande

Requête : CLASSE INSTRUCTION PARAMETRE\_1 PARAMETRE\_2 LONGUEUR

*CLASS INS P1 P2 LEN*

Réponse : DONNEES MOT\_DE\_STATUT\_1 MOT\_DE\_STATUT\_2

*DATA SW1 SW2*

### En détails...

- CLASS : Le groupe d'instructions concernées
- INS : L'instruction proprement dite ou la commande
- P1 & P2 : Paramètres de la commande
- LEN : Nombre d'octets après la commande ou longueur attendue de la réponse
- DATA : Zone de données de réponse
- SW1 & SW2 : Etat du déroulement de la commande

## ...Elle ne fait que répondre à des commandes

### Structure d'une commande

Requête : CLASSE INSTRUCTION PARAMETRE\_1 PARAMETRE\_2 LONGUEUR

*CLASS INS P1 P2 LEN*

Réponse : DONNEES MOT\_DE\_STATUT\_1 MOT\_DE\_STATUT\_2

*DATA SW1 SW2*

### En détails...

- CLASS : Le groupe d'instructions concernées
- INS : L'instruction proprement dite ou la commande
- P1 & P2 : Paramètres de la commande
- LEN : Nombre d'octets après la commande ou longueur attendue de la réponse
- DATA : Zone de données de réponse
- SW1 & SW2 : Etat du déroulement de la commande

## ...Elle ne fait que répondre à des commandes

### Structure d'une commande

Requête : CLASSE INSTRUCTION PARAMETRE\_1 PARAMETRE\_2 LONGUEUR

*CLASS INS P1 P2 LEN*

Réponse : DONNEES MOT\_DE\_STATUT\_1 MOT\_DE\_STATUT\_2

*DATA SW1 SW2*

### En détails...

- CLASS : Le groupe d'instructions concernées
- INS : L'instruction proprement dite ou la commande
- P1 & P2 : Paramètres de la commande
- LEN : Nombre d'octets après la commande ou longueur attendue de la réponse
- DATA : Zone de données de réponse
- SW1 & SW2 : Etat du déroulement de la commande



## ...Elle ne fait que répondre à des commandes

### Structure d'une commande

Requête : CLASSE INSTRUCTION PARAMETRE\_1 PARAMETRE\_2 LONGUEUR

*CLASS INS P1 P2 LEN*

Réponse : DONNEES MOT\_DE\_STATUT\_1 MOT\_DE\_STATUT\_2

*DATA SW1 SW2*

### En détails...

- CLASS : Le groupe d'instructions concernées
- INS : L'instruction proprement dite ou la commande
- P1 & P2 : Paramètres de la commande
- LEN : Nombre d'octets après la commande ou longueur attendue de la réponse
- DATA : Zone de données de réponse
- SW1 & SW2 : Etat du déroulement de la commande

## ...Elle ne fait que répondre à des commandes

### Structure d'une commande

Requête : CLASSE INSTRUCTION PARAMETRE\_1 PARAMETRE\_2 LONGUEUR

*CLASS INS P1 P2 LEN*

Réponse : DONNEES MOT\_DE\_STATUT\_1 MOT\_DE\_STATUT\_2

*DATA SW1 SW2*

### En détails...

- CLASS : Le groupe d'instructions concernées
- INS : L'instruction proprement dite ou la commande
- P1 & P2 : Paramètres de la commande
- LEN : Nombre d'octets après la commande ou longueur attendue de la réponse
- DATA : Zone de données de réponse
- SW1 & SW2 : Etat du déroulement de la commande

## ...Elle ne fait que répondre à des commandes

### Structure d'une commande

Requête : CLASSE INSTRUCTION PARAMETRE\_1 PARAMETRE\_2 LONGUEUR

*CLASS INS P1 P2 LEN*

Réponse : DONNEES MOT\_DE\_STATUT\_1 MOT\_DE\_STATUT\_2

*DATA SW1 SW2*

### En détails...

- CLASS : Le groupe d'instructions concernées
- INS : L'instruction proprement dite ou la commande
- P1 & P2 : Paramètres de la commande
- LEN : Nombre d'octets après la commande ou longueur attendue de la réponse
- DATA : Zone de données de réponse
- SW1 & SW2 : Etat du déroulement de la commande

# Chapitre 4 : Norme 7816 (Partie 4)

## Objectifs

- Définir les commandes inter-industries pour les échanges internationaux
- Définir les mécanismes de sécurité pour les données inscrites dans les fichiers

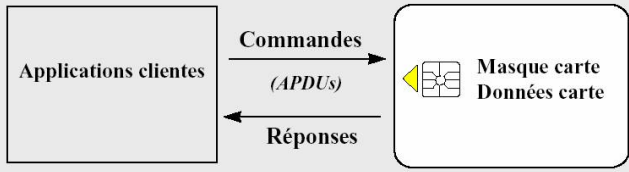
## Comment?

- Définir le format des “packets de données”
- i.e., la structure des messages

## Application Protocol Data Unit (APDU)



### Terminal



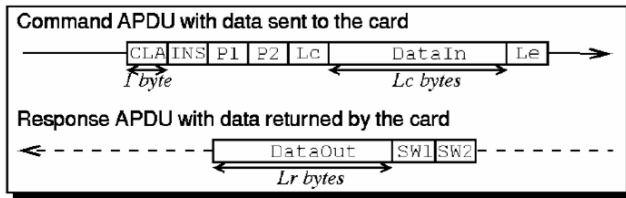
# Chapitre 4 : Norme 7816 (Partie 4)

## Details

Code	Name	Length	Description
CLA	Class	1	Class of Instruction
INS	Instruction	1	Instruction code
P1	Parameter 1	1	Instruction parameter 1
P2	Parameter 2	1	Instruction parameter 2
Lc field	Length of Command Data	variable $\leq 3$	Number of bytes present in the data field
Data field	Data	variable $= Lc$	String of data bytes sent in the command
Le field	Length of Response Data	variable $\leq 3$	Maximum number of data bytes expected in response

# Chapitre 4 : Norme 7816 (Partie 4)

## Differentes configurations Requetes/Réponses



## Differentes configurations Requetes/Réponses

CASE	COMMAND	RESPONSE
1	NO DATA	NO DATA
2	DATA	NO DATA
3	NO DATA	DATA
4	DATA	DATA

## Chapitre 4 : Norme 7816 (Partie 4)

### Instructions

INS in hex	Meaning
OE	Erase Binary
20	Verify
82	External Authentication
88	Internal Authentication
A4	Select File
B0	Read Binary
B2	Read Record
C0	Get Response
C2	Envelope
D0	Write Binary
D2	Write Record

# Chapitre 4 : Norme 7816 (Partie 4)

## Exemples

Champ de la commande APDU	Valeurs
CLA	BC = cartes de crédit françaises, cartes vitales françaises, A0 = cartes SIM (téléphonie) 00 = cartes Monéo (porte-monnaie en France), Mastercard, Visa
INS	20 = vérification du PIN, B0 = Lecture B2 = Lecture de record D0 = Écriture DC = Écriture de record A4 = Sélection du répertoire (directory) C0 = Demander une réponse (get an answer)
P1, P2	paramètres contenant des adresses à lire
LEN	longueur prévue pour la réponse ou bien longueur de l'argument de l'instruction
ARG	contient LEN octets (octets à écrire, PIN à vérifier, etc.)

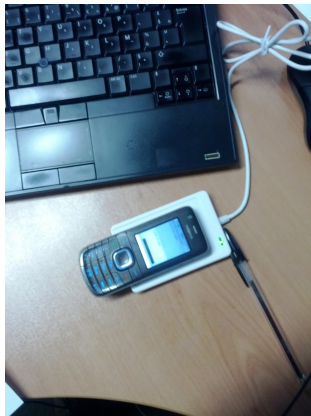


# En attendant le cours sur JavaCard... Dans mon labo(1)

## NFC (carte à puce sans contact)

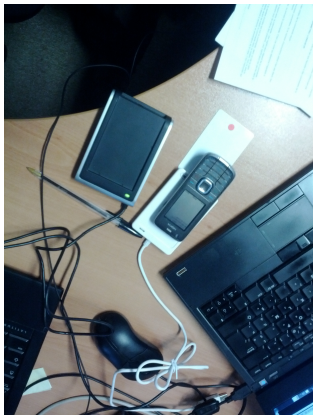


## Carte sur lecteur



# En attendant le cours sur JavaCard... Dans mon labo(2)

Lecteur de carte à contacts

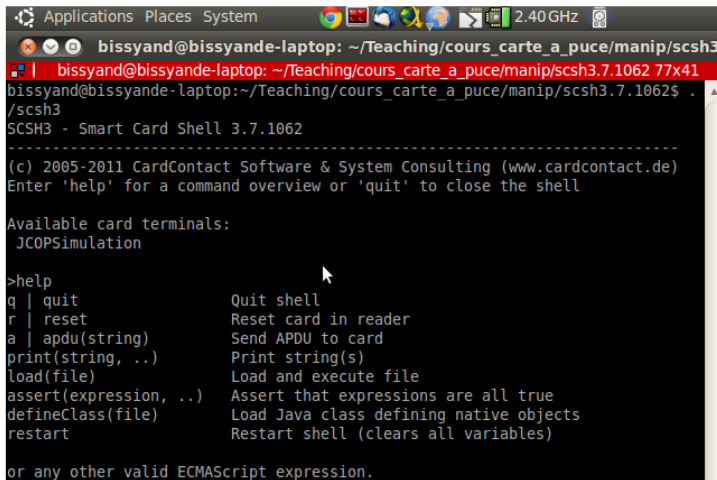


Tout mon matos...



# En attendant le cours sur JavaCard... Dans mon labo(2)

## Lecteur de carte à contacts



```
Applications Places System 2.40 GHz
bissyand@bissyande-laptop: ~/Teaching/cours_carte_a_puce/manip/scssh3
bissyand@bissyande-laptop: ~/Teaching/cours_carte_a_puce/manip/scssh3.7.1062 77x41
bissyand@bissyande-laptop:~/Teaching/cours_carte_a_puce/manip/scssh3.7.1062$ ./scssh3
SCSSH3 - Smart Card Shell 3.7.1062
-----
(c) 2005-2011 CardContact Software & System Consulting (www.cardcontact.de)
Enter 'help' for a command overview or 'quit' to close the shell

Available card terminals:
JCOPSimulation

>help
q | quit           Quit shell
r | reset          Reset card in reader
a | apdu(string)   Send APDU to card
print(string, ..)  Print string(s)
load(file)         Load and execute file
assert(expression, ..) Assert that expressions are all true
defineClass(file)  Load Java class defining native objects
restart            Restart shell (clears all variables)

or any other valid ECMAScript expression.
```