Université de Boumerdès

Faculté de Technologie

Département Ingénierie des Systèmes Électriques

Spécialité: Electronique des systèmes embarqués

Module: Cartes à puces

Chapitre 5: Protocoles de communication cartes à puce / lecteur

Mme Belkacem Samia

2021/2022

ISO 7816-3

L'ISO 7816-3

- Elle définit l'interface électrique et les protocoles de transmission :

  - ✓Les protocoles de transmission (TPDU, Transmission Protocol Data Unit)
    T=0 : protocole orienté octet, T=1 : protocole orienté paquet,
    T=14 : réservé pour les protocoles propriétaires,

  - ✓La sélection d'un type de protocole,

  - ✓La réponse à un reset (ATR, ou Answer To Reset) qui correspond aux données envoyées par la carte immédiatement après la mise sous tension,

  - ✓Les signaux électriques, tels que le voltage, la fréquence d'horloge et la vitesse de communication.

ISO 7816-3

- Caractéristiques électriques :

  Fréquence d'horloge 1 - 5 Mhz

  Vitesse des communications < 115200 bauds

- Protocole de transmission :

  TPDU (Transmission Protocol Data Unit)

  T=0 Protocole orienté octet

  T=1 Protocole orienté paquet

- Sélection du type de protocole :

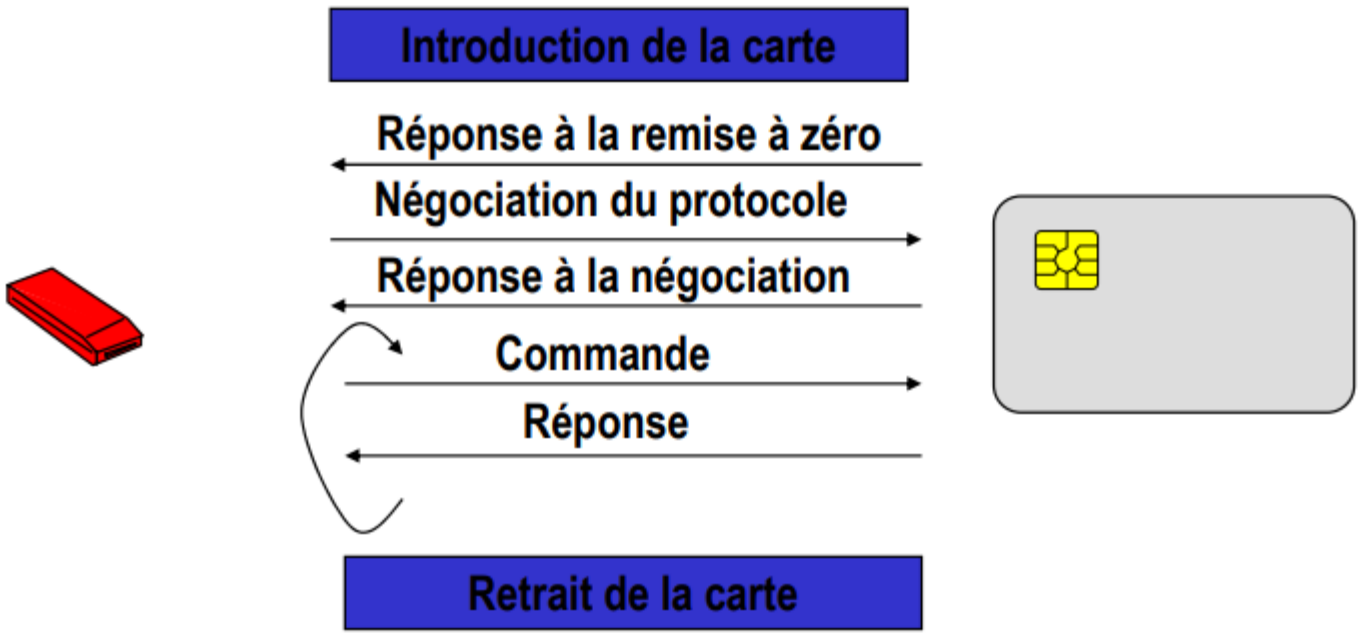
  PTS (Protocol Type Selection)

- Réponse au reset :

  ATR (Answer To Reset)

Communication Carte / Lecteur

La carte n’est jamais l’initiateur de la communication



Communication Carte / Lecteur

ISO 7816-4

APDU (Application Programming Data Units)

Command APDU						
Mandatory Header				Conditional Body		
CLA	INS	P1	P2	Lc	Data Field	Le

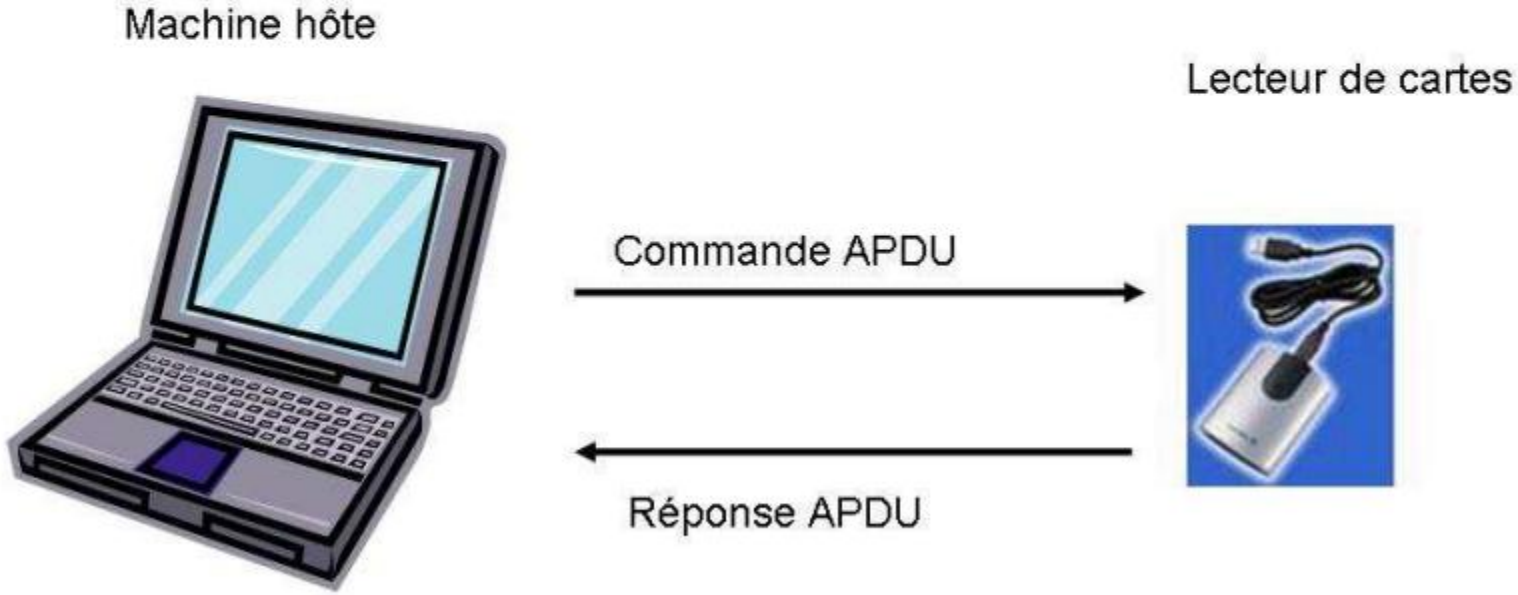
CLA : 1 octet pour identifier l'application
INS : 1 octet pour le code de l'instruction
P1 - P2 : Paramètres de l'instruction
Lc : Longueur du champ de données
Le : Longueur maxi du champ de données de la réponse

Response APDU		
Conditional Body	Mandatory Trailer	
Data Field	SW1	SW2

SW1 - SW2 : Code d'exécution
90 00 → OK

Communication Carte / Lecteur

L'ISO 7816-4 : Le protocole APDU



Communication Carte / Lecteur

Format des commandes APDU

Commande APDU						
Entête obligatoire				Corps optionnel		
CLA	INS	P1	P2	Lc	Data field	Le

- CLA (1 octet): Classe d'instructions --- indique la structure et le format pour une catégorie de commandes et de réponses APDU
- INS (1 octet): code d'instruction: spécifie l'instruction de la commande
- P1 (1 octet) et P2 (1 octet): paramètres de l'instruction
- Lc (1 octet): nombre d'octets présents dans le champ données de la commande
- Avec Le=0, - Si cde d'écriture => pas de données utiles
  - Si cde de lecture => la cde doit retourner 256 octets de données utiles
- Data field (octets dont le nombre est égal à la valeur de Lc): une séquence d'octets dans le champ données de la commande

Format des réponse APDU

Réponse APDU		
Corps optionnel	**Partie obligatoire**	
Data field	**SW1**	**SW2**
•Data field (longueur variable): une séquence d'octets reçus dans le champ données de la réponse •SW1 (1 octet) et SW2 (1 octet): Status words (Mots d'état)—état de traitement par la carte		

SW1 SW2 =	0x90 0x00	Succès
	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

Utilisation de la carte

La procédure d'utilisation de la carte est :

1) Connexion et activation des contacts par le lecteur

2) Reset de la carte

3)La carte envoie son ATR (Answer To Reset)

4) Échanges entre le lecteur et la carte, à l'initiative du premier

5) Désactivation des connecteurs par le lecteur

Activation des contacts

L'activation des contacts doit suivre la procédure suivante, pour éviter d'endommager la carte

1) RST est positionné à l'état bas
2) Vcc est positionné à l'état haut (alimentation de la carte)
3) Le lecteur s'apprête à recevoir des informations sur la ligne I/O
4) Vpp est positionné à l'état de repos
5)CLK fournit une horloge utilisable par la carte

Reset de la carte

- La carte doit renvoyer son ATR entre 40 et 40000 cycles d'horloge. La communication d'origine a lieu à un débit de 372/fi , où fi est la fréquence d'horloge initiale (entre 1MHz et 5MHz), ou à 9600 bits/s (pour une carte disposant de sa propre horloge). Pour une horloge à 3,5712MHz, cela correspond à 9600 bits/s.

Format de l'ATR

TS	T0	TA1	TB1	TC1	TD1	TA2	TB2	TC2	TD2	...	T1	...	TK	TCK

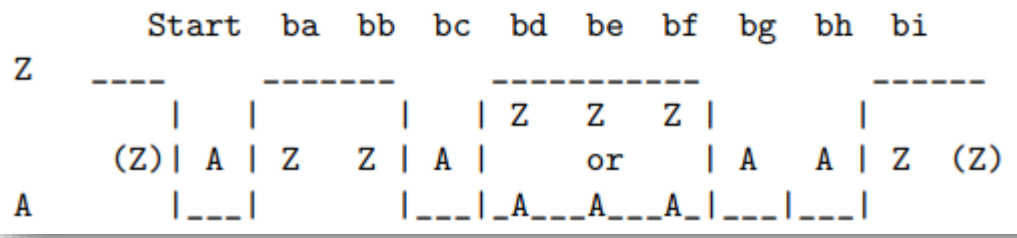
Octet TS

TS permet de déterminer :

- une mesure précise de la vitesse de transmission
- la valeur (Vcc ou GND) correspond à un 0 ou à un 1
- l'ordre des bits (plus significatif ou moins significatif d'abord)

Il existe deux conventions :

- inverse : le 1 est au niveau bas (A), le bit le plus significatif est transmis en premier (Z)ZZAAAAAAZ, transmission de 3F
- directe : le 0 est au niveau haut (Z), le bit le plus significatif est transmis en dernier(Z)ZZAZZZAAZ, transmission de 3B



Format de l'ATR (Answer to Response)

Reste de l'ATR

Les autres caractères de l'ATR sont :

T0	présence ou non des caractères TA1, TB1, TC1 et TD1, et nombre des caractères historiques
TA1, TB1, TC1, TD1	protocole à utiliser et paramètres du protocole (vitesse, temps d'attente entre les octets, etc.) ; si TD1 est présent, TA2, TB2, TC2 et TD2 peuvent être présents, etc.
T1, T2, ...	caractères historiques
TCK	checksum tel que le *xor* de tous les caractères (y compris TCK) soit zéro

Protocoles existants :

T=0	protocole de transmission par caractère half-duplex
T=1	protocole de transmission par bloc half-duplex

Format des commandes APDU

Commande APDU						
Entête obligatoire				Corps optionnel		
CLA	INS	P1	P2	Lc	Data field	Le

- Les commandes sont transmises en commençant par 5 octets :
  - CLA classe de l'instruction
  - INS instruction
  - P1 paramètre complémentaire
  - P2 paramètre complémentaire
  - Le longueur des paramètres (l'instruction détermine le sens, incoming si des données sont envoyées à la carte, entre 0 et 255, outgoing si des données viennent de la carte, entre 1 et 256)

Réponses APDU

Réponse APDU		
Corps optionnel	Partie obligatoire	
Data field	SW1	SW2

La carte peut répondre de différentes manières :

ACK	quatre valeurs possibles (INS, INS+1, $\bar{\text{INS}}$ ou $\bar{\text{INS}}$+1) et déterminent si les octets suivants doivent être envoyés d'un coup à un par un, et demande éventuellement si Vpp doit passer à l'état actif
NULL (60)	la carte demande un délai de réflexion
SW1 (6x ou 9x, sauf 60)	la carte envoie ensuite SW2

Valeurs de SW1 SW2 :

90 00	fin normale
6E xx	classe non supportée
6D xx	instruction non supportée
6B xx	référence incorrecte
67 xx	longueur incorrecte
6F 00	pas de diagnostic précis de l'erreur