

Les cartes à puce

Brique ROSE

Samuel Tardieu
sam@rfc1149.net

École Nationale Supérieure des Télécommunications

Les cartes à puce sont de plus en plus répandues :

- cartes bancaires ;
- cartes SIM pour téléphones mobiles ;
- cartes pour les décodeurs satellite et câble ;
- cartes de santé ;
- cartes d'identité et informations biométriques ;
- cartes d'identification (signature et déchiffrement) électronique ;
- cartes d'accès (avec ou sans contact).

Les différentes cartes

bande magnétique permet de stocker 80 octets de données

carte mémoire permet de stocker 2 ko de données

carte à puce système embarqué complet, aucune limitation sur la taille de données et la puissance embarquée

Plusieurs normes ISO régissent les cartes à puce avec contact :

7816-1 caractéristiques mécaniques des cartes

7816-2 emplacement et dimensions des connecteurs électriques

7816-3 description du protocole de communication entre une carte et le lecteur

7816-4 commandes portables d'une carte à l'autre (système de fichiers par exemple)

7816-5 procédure d'enregistrement d'identifiants uniques pour les applications

7816-6 éléments portables d'une carte à l'autre

7816-7 commandes d'interrogation SCQL (*Structured Card Query Language*)

7816-8 commandes portables de sécurité

Caractéristiques électriques

Une carte à puce dispose de 8 connecteurs : (ISO7816-2)

C1 Vcc

C2 RST

C3 CLK

C4 RFU (*Reserved for future use*)

C5 GND

C6 Vpp (anciennes générations d'EEPROM)

C7 I/O (bi-directionnel, en mode *half-duplex*)

C8 RFU (*Reserved for future use*)

Symbole	Minimum	Maximum	Unité
Vcc	4,75	5,25	V
Icc		200	mA

La procédure d'utilisation de la carte est :

- ➊ Connection et activation des contacts par le lecteur
- ➋ Reset de la carte
- ➌ La carte envoie son ATR (*Answer To Reset*)
- ➍ Échanges entre le lecteur et la carte, à l'initiative du premier
- ➎ Désactivation des connecteurs par le lecteur

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

Answer To Reset

La carte doit renvoyer son ATR entre 40 et 40000 cycles d'horloge. La communication d'origine a lieu à un débit de $372/f_i$, où f_i 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

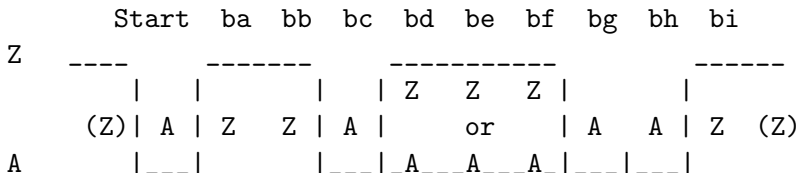
Octet TS

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)ZZAAAAAZ, 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



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

Les commandes sont transmises en commençant par 5 octets :

CLA classe de l'instruction

INS instruction

P1 paramètre complémentaire

P2 paramètre complémentaire

L 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 de la carte

La carte peut répondre de différentes manières :

ACK quatre valeurs possibles (INS , $INS+1$, \overline{INS} ou $\overline{INS}+1$) et déterminent si les octets suivants doivent être envoyés d'un coup à un par un, et demande éventuellement si V_{pp} 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

ISO7816-4 définit des commandes pour accéder à des fichiers :

- les fichiers peuvent être plats, par enregistrements ou cycliques ;
- la carte supporte la notion de répertoire courant et de fichier courant ;
- certaines opérations nécessitent une identification par PIN ou par la preuve de possession d'une clé (réponse à un challenge)