La carte à puce

Samia Bouzefrane

Maître de Conférences

CEDRIC –CNAM

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

A la mémoire de Roland Moreno qui a été sensible à mes activités pédagogiques sur la carte à puce
Un vif remerciement à Michel Ugon qui a relu et corrigé les informations contenues dans ce support. Merci aussi pour tous les documents utiles qu'il m'a fournis

La carte à puce aujourd'hui

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

La carte à puce aujourd'hui

- Aujourd'hui : plus de 5 milliards de cartes
- **Monétique** :
  - Carte bancaire : Groupement Cartes Bancaires, nouvelles cartes EMV, etc.
  - Porte-monnaie : **Octopus**, **Moneo** en France, **Proton** en Belgique, **Geldkarte** en Allemagne
- **Identification** :

Cartes d'identité nationales (**eID** en Belgique), **E-passeports** (août 2006 en France), Passeport biométrique (depuis la fin Juin 2009)

- **Enseignement** (carte d'étudiant et/ou de restauration)
- **Téléphonie mobile** (carte **SIM**)
- **Secteur médical** (carte **Vitale** en France, carte **SIS** en Belgique).
- **Titre de transport** (**Passe Navigo** à Paris, **Oyster** à Londres
- **Sécurité informatique** (authentification forte et signature électronique): carte doté d'un cryptoprocesseur pour la génération des clés et le stockage de la clé privée).

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

Exemples des Passeports

Depuis 2006 en France :
Passeport électronique comporte une puce électronique qui stocke les données personnelles du détenteur : (son nom, sa date de naissance, sa nationalité, son numéro de passeport et la photo numérisée du titulaire).

Depuis le 15 Juin 2009 :
Passeport biométrique : sur une puce RFID, qui permet de lire les informations à courte distance, sont enregistrés - outre les informations personnelles classiques et la photo numérisée - deux empreintes digitalisées des doigts du détenteur (à partir de l'âge de 6 ans).

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

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

EUROSMART

- Association fondée en 1994 pour promouvoir la carte à puce
- Membres fondateurs :

  Bull CP8, Dassault AT, FNMT, Gemplus, Giesecke & Devrient, Oberthur Smart Cards, ODS Oldenburg Datensysteme, Orga, Delarue Cartes & Systèmes, Schlumberger.

- En 2013, Executive members : EM MicroElectronic, Infineon, Obethur Technologies, Gemalto, NXP, G&D, LFoundry; Safran Morpho, Samsung, Life.augmented

- Active members, Associated Members, Partners

(voir http://www.eurosmart.com/about/members.html)

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

Marché des cartes à puce à contact

Smart Secure Device (Mu)

WW shipments forecast	2014	2015f	2016f	2015f vs 2014 % growth	2016f vs 2015f % growth
Telecom	5,200*	5.450	5.600	4,8%	2,8%
Financial services	2050	2.600	2.900	26,8%	11,5%
Government – Healthcare	380	410	455	7,9%	11,0%
Device Manufacturers	190	310	390	63,2%	25,8%
Others**	400	430	460	7,5%	6,9%
Total	8,220	9.200	9.805	11,9%	6,6%

* Source SIMAlliance

**Others include Transport, PayTV and physical and logical access cards.

Smart Secure Contactless (Mu)

Of which contactless	2014	2015f	2016f	2015f vs 2014 % growth	2016f vs 2015f % growth
Financial services	880	1.115	1.270	26,7%	13,9%
Government – Healthcare	230	250	270	8,9%	8,0%
Transport	180	210	240	16,7%	14,2%
Others***	70	70	70	0,0%	0,0%
Total	1,360	1.645	1.850	21,0%	12,4%

***Others include Transport, PayTV and physical and logical access cards.

NFC Secure Elements **(Mu)**

WW shipment forecast	2014	2015f	2016f	2015f vs 2014 % growth	2016f vs 2015f % growth
NFC Secure Elements****	350	490	590	40%	20%

**** NFC secure elements include NFC enabled UICCs and embedded secure elements and other form factors of NFC-enabled secure elements

Source Eurosmart, Novembre 2015: http://www.eurosmart.com/facts-figures.html

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

Smart Insights Weekly 2013
#13-19, #13-32, #13-41 and #13-42

Selon le rapport de ABI Research "Smart Cards in Latin America", la commercialisation des cartes à puce en Amérique latine passera de 752 millions en 2013 à 1.15 milliards en 2018, en particulier dans les cartes ID et de paiement.

Ingenico supporte la migration US EMV. Ingenico a déjà contribué à la migration EMV au Canada.

Selon IDC, la Chine doit atteindre 450 millions de Smartphones en 2014 contre 360 millions en 2013, avec Android étant l'OS le plus utilisé.

400,000 ePassports chaque année durant 5 ans en Belgique (Gemalto et Zetes)

Santander UK a lancé une nouvelle carte Etudiant qui combine carte d'accès avec une fonctionnalité de débit Visa.

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

Smart Insights Weekly 2013
#13-19, #13-32, #13-41 and #13-42

Oberthur Technologies a reconduit son partenariat avec STM (La Société de Transport de Montréal), pour 4 ans pour fournir la carte CityGo.

TCRM (Transports en Commun de la Région Messine), transport local de Metz en France, a inauguré le système sans contact 100% ticketing.

Opal smart card est maintenant disponible dans les transports ferroviaires de Sydney avec 669 terminaux.

Le sénat brésilien a approuvé la régulation des paiements mobiles, en accordant à la banque centrale du Brésil le pouvoir de réguler les transactions financières issues des téléphones mobiles.

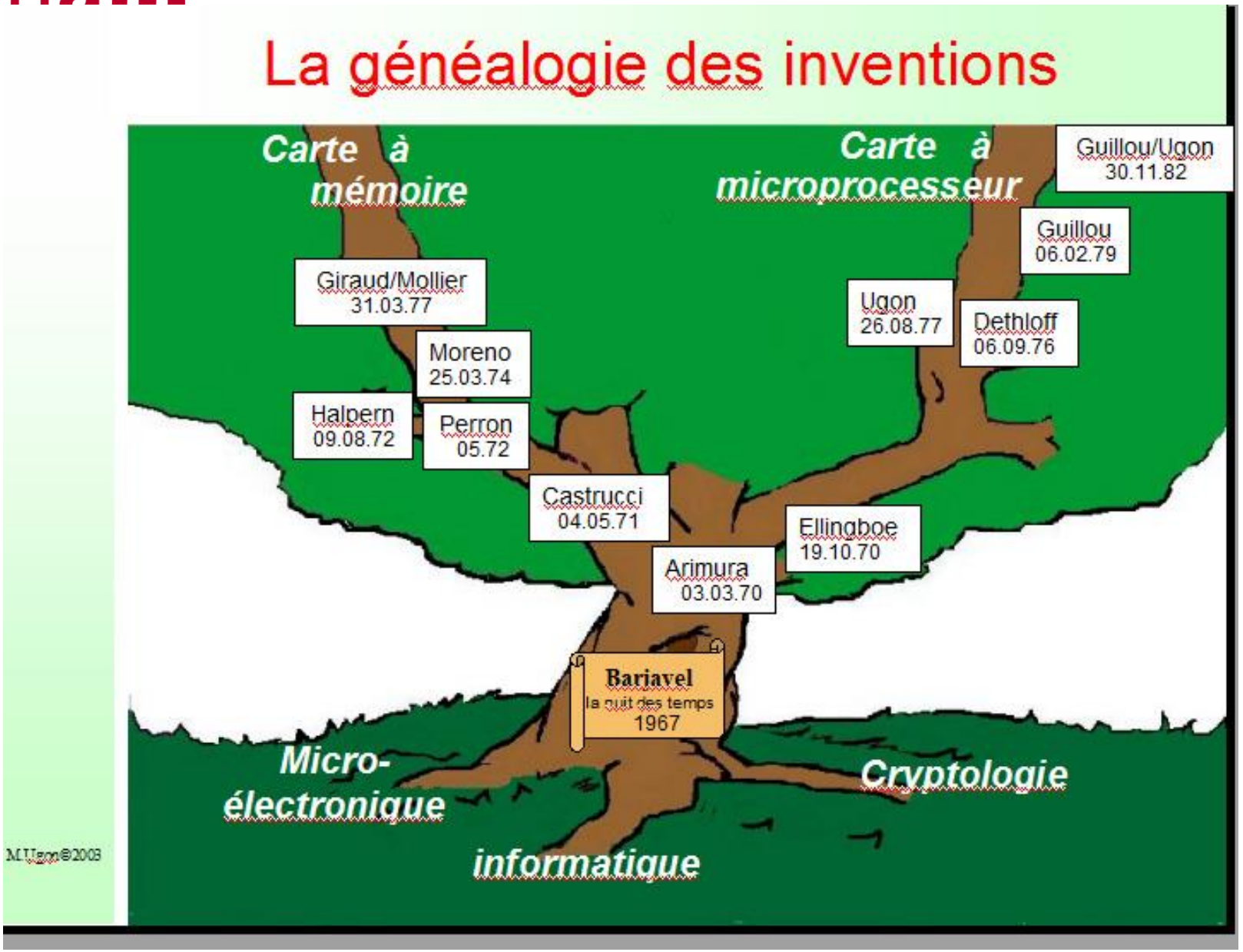
Le nombre de clients abonnés au système de paiement mobile en Bangladesh est passé à 6 millions en Août avec des transactions atteignant presque 15 millions d'euros par jour.

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

La carte à puce : Histoire

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

La généalogie des inventions



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

Les premiers inventeurs

- États-unis :
  - Pomeroy en 1967
  - Ellingboe (1970) décrit un moyen de paiement électronique sur une carte de crédit à contacts
  - Halpern (1972) avec son stylo électronique sécurisé de paiement

- Japon
  - Arimura (1970) propose une méthode d'authentification dynamique utilisée lors d'une procédure d'identification

- Allemagne : Dethloff (1977)

- France : Moreno (1974), Ugon (1977) et Guillou (1979).

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

Toute première idée de la carte à puce

Romancier Français René Barjavel dans son ouvrage « la nuit des temps », 1967.

« Chaque fois qu'un Gonda désirait quelque chose de nouveau, des vêtements, un voyage, des objets, il payait avec sa clé. Il pliait le majeur, enfonçait sa clé dans un emplacement prévu à cet effet et son compte, à l'ordinateur central, était aussitôt diminué de la valeur de la marchandise ou du service demandés. »

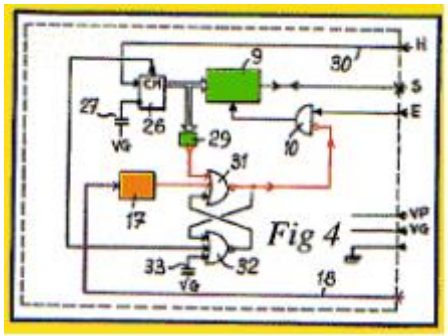
Gonda : peuple mythique
Clé : anneau magique ayant la force de mémorisation et de communication

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

Les moyens inhibiteurs par Roland Moreno

- **Moyens proposés en 1974 mais n'ont été déployés qu'en 1983**
  - **comparaison interne du code confidentiel ;**
  - **-compteur d'erreurs, qui provoque l'auto-destruction de la puce en cas de soumission répétée d'un code faux : un code inexact provoque la destruction d'un fusible en mémoire, d'où une surconsommation électrique importante.**
  - **moyens de traitement ;**
  - **-lecture irréversiblement impossible de zones prédéterminées, notamment code confidentiel, clés, etc. ;**

    écriture, modification, effacement irréversiblement impossibles de zones prédéterminées de la mémoire.



Prototype de puce portable imaginé par R. Moreno

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

Inventeurs de la carte à micro-processeur

- En 1977, l'Allemand Dethloff dépose un brevet pour une carte à mémoire avec des moyens inhibiteurs intégrés dans un micro-processeur (dont les caractéristiques n'étaient pas décrites).

- En Août 1977, le Français Michel Ugon travaillant chez Bull dépose un brevet pour une carte à micro-processeur appelée CP8, pour « Circuit Portatif des années 80 », qui a été déployée à partir de 1990, un autre brevet sur l'architecture SPOM (Self Programmable One chip Microprocessor) a été déposé en avril 1978.

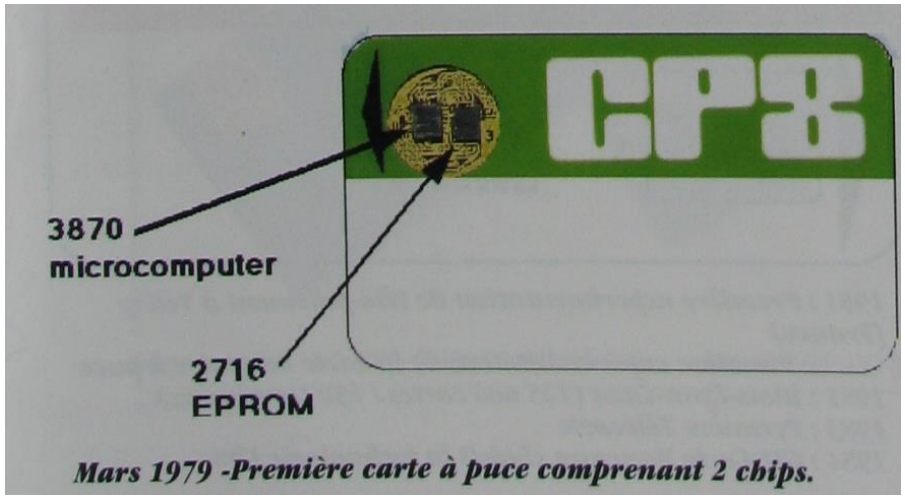
SPOM encore utilisé, permet au micro-contrôleur de modifier lui-même son programme contenu dans sa NVM (Mémoire Non Volatile) sans intervention du monde extérieur.
Ce mécanisme empêche les intrusions.

Fourni par Michel Ugon

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

Première carte à puce

- **21 Mars 1979 (Bull CP8), 1ére carte à microprocesseur** (comprenant deux puces)
  - ✓ Fabriquée par Motorola pour CII Honeywell Bull
  - ✓Possède un microprocesseur 8 bits 3870
  - ✓Avec une EPROM 2716



Mars 1979 -Première carte à puce comprenant 2 chips.

Source: *L'odyssée de la carte à puce, par Michel Ugon, Le Guide de la carte, 1994.*

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

Commentaire par Michel Ugon

- **Concernant la carte à deux puces**

**La carte 2 chips opérationnelle est vraiment la première carte à puces.
Elle a été réalisée (encartage) par Bull à l'aide de circuits imprimés circulaires de très faible épaisseur (0,5 mm) incorporant les deux puces et leurs inter-connexions, modules réalisés par Motorola à Toulouse à l'aide de composants sous licence (micro 3870 + EPROM 2716). Bull réalisa aussi le logiciel masqué dans la ROM du 3870.**

Personne ne comprit très bien ce mode de réalisation qui fut pour nous dès le départ un passage provisoire obligé pour prouver la faisabilité de la carte à microprocesseur monochip, seule capable de résister aux investigations malveillantes. La bonne preuve que nous savions de cette solution provisoire est que dans cette solution nous n'utilisions que la moitié de la mémoire EPROM de 16K car le monochip SPOM ne pouvait en supporter que 8K.

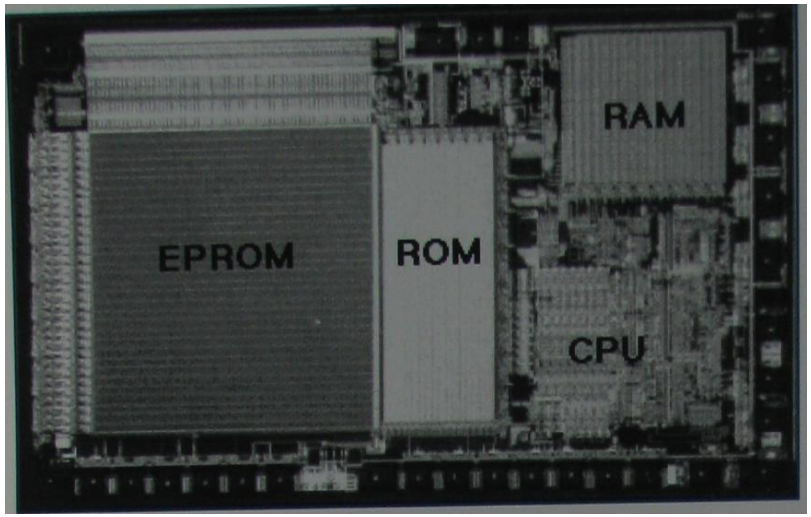
samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Carte à puce monolithique MAM

- **21 octobre 1981: Premier SPOM en service**
  - **par l'équipe de Bull dirigée par M. Ugon**
  - **Carte MAM (Microprocesseur Autoprogrammable Monolithique)**
  - **Micro-processeur 8 bits**
  - **Technologie 3,5µ de MOS**
  - **RAM : 36 bits, ROM : 1,6Kbit, EPROM : 1 Kbit,**
  - **Taille de la puce: 19,5mm2,**
  - **Nombre de transistors : 42 000 en oct. 1981.**

SPOM: Single Chip Microprocessor with On-Chip Modifiable Memory

Puce auto-programmable: capacité de programmer sa EPROM tout en exécutant un programme



Source: *L'odyssée de la carte à puce, par Michel Ugon, Le Guide de la carte, 1994.*

Premiers déploiements/1

- 1982 (Schlumberger), carte à logique câblée

- Téléphonie
  - 1983 : Sous l'impulsion de la DGT, apparition des télécartes à base de carte logique câblée, mises au point par Schlumberger et Thomson.
  - La DGT commande 20 000 publiphones à partir de 1986.
  - En 1992, il y avait 200 millions de télécartes en circulation.

- En terme de sécurité
  - Facile à frauder contrairement à la carte à micro-processeur dans laquelle un certain nombre de vulnérabilités sécuritaires des semi-conducteurs et certaines contre-mesures étaient déjà connues et même brevetées.

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

Premiers déploiements/2

- Carte à microprocesseur
- Paiement

-1981 : Carte CP8 bi-puce utilisée pour expérimenter avec la poste le télépaiement à domicile, à Vélizy.

-1982-1984 : les banques françaises conduisent trois expérimentations à Blois, Lyon et Caen en vue de tester trois techniques conçues par Philips, Schlumberger et Bull CP8 avec 125 000 cartes / 650 terminaux:

- Carte Bull CP8 mono-chip pour l'expérience de Blois
- Carte Flonic-Schlumberger à logique câblée pour l'expérience de Lyon
- Cartes Philips à 2 chips pour l'expérience de Caen

-1985 : l'expérience à Blois fût convaincante, d'où : le GIE CB commande 16 millions de cartes CP8, généralisation de la carte à puce bancaire en 1992.

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

Les entreprises de la carte à puce

La société Innovatron est créée par R. Moreno pour exploiter ses brevets.

En 1978, DGT qui deviendra France Telecom réalise des prototypes, terminaux et des cartes favorisant la création du Groupement d'Intérêt Economique (GIE) appelé *Carte à Mémoire* et regroupant 10 banques françaises.

En 1979, le géant des services pétroliers Schlumberger entre au capital d'Innovatron pour 23 %, ensuite pour 34 %.

En 1997, Schlumberger acquiert le concurrent français : SOLAIC, ensuite Bull CP8 en 2001.
En 2001, Schlumberger externalise l'activité « Cartes à puce » => Axalto

En 1988, Marc Lassus crée Gemplus en France. Gemplus était numéro 1 mondial jusqu'à sa fusion avec Axalto en 2006.

Gemalto est aujourd'hui le leader mondial, suivi par Oberthur Technologies et Giesecke & Devrient.

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

Quelques dates/1

Année	Événement
1979	Première carte fabriquée par Motorola pour Bull CP8 (à deux puces)
1981	Sortie de la première carte monolithique à micro-circuit
1983	Premières télécartes françaises
1983	Le CNET spécifie la première carte bancaire à puce
1984	Naissance du GIE « Cartes Bancaires » successeur du GIE Carte à mémoire
1985	Le GIE CB commande 16 millions de cartes à puce
1987	Premières normes ISO
1989	Premières cartes GSM pour téléphones mobiles
1992	Le GSM devient un produit commercial

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

Quelques dates/2

Année	Événement
1992	Toutes les cartes CB sont dotées d'un micro-circuit
1994	Développement de la carte de Sécurité Sociale en Allemagne (près de 70 millions en 1997)
1995	Début du projet « SESAM Vitale »
1996	Développement important du porte-monnaie électronique
1999	Généralisation de la carte vitale (près de 40 millions)
1996	Premières normes EMV
2004	Le système CB passe au standard international EMV
2004	Premières CB sans contact

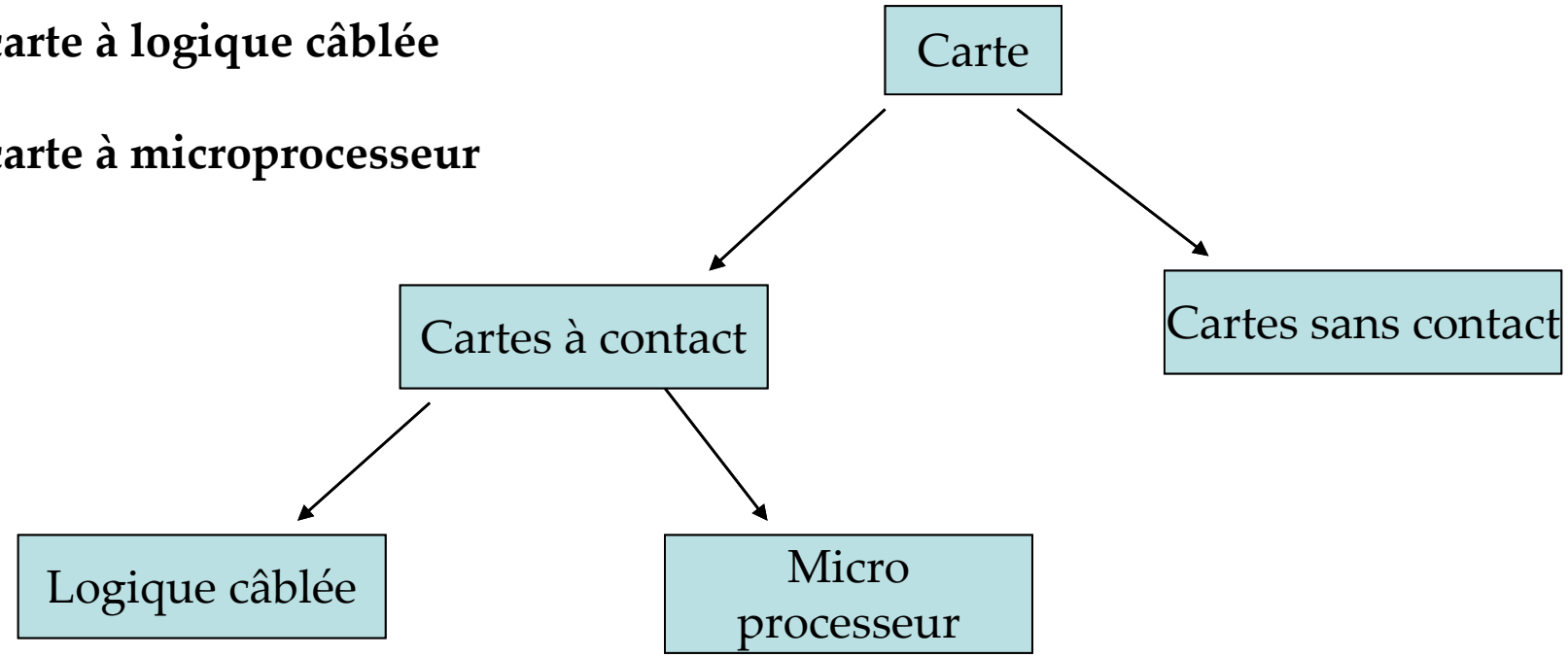
samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

La carte à puce : architecture

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

Famille de produits/1

- **carte à logique câblée**
- **carte à microprocesseur**



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

Famille de produits/2

- **Carte à logique câblée : fonctions simples fixées par les circuits électroniques entre la mémoire NVM (non volatile) et l'interface extérieure.**
  Exemples : carte de parking, de cinéma, de lavage de voiture, etc.

- **Carte à microprocesseur : stocke des données et les traite de manière sécuritaire.**

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

Cartes à microcontrôleur

- Cartes à puce intelligentes
- Comportent un microcontrôleur :

  - UC
  - PROM
  - RAM
  - EEPROM
  - interface d'E/S
  - crypto processeur

  } dans le même circuit

- Processeur : 16 ou 32 bits
- EEPROM : de 1Ko à 128 Ko (256 Ko pour une Java Card ou une Basic Card)
- Interface série: UART simplifié

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

Types de mémoires/1

- technologie CMOS (Complementary Metal Oxide Semiconductor)
  très faible consommation

- Mémoire à accès aléatoire (RAM : Random Access Memory) utilisée comme registres de travail et perdent leurs informations dès la coupure de courant.

Une RAM statique (SRAM) occupe 20 fois plus de place que la ROM, c'est ce qui explique la faible taille de la RAM.

Remq. Dans une mémoire statique, pas de rafraîchissement périodique de son contenu contrairement à la mémoire dynamique.

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

Types de mémoires/2

➢ **Les mémoires non volatiles (NVM) : gardent les informations en l'absence d'alimentation.**

Les mémoires mortes (ROM) : accessibles uniquement en lecture. L'inscription de la ROM est réalisée par masquage pendant la fabrication du circuit intégré.

Les mémoires mortes programmables (PROM) : peuvent être programmées (écrites) par l'utilisateur.

EPROM (Erasable PROM) : effacement par rayonnement ionisant, Inc. Le nombre de reprogrammation des cellules mémoire est limité.

EEPROM (Electrically Erasable PROM) : utilisée aujourd'hui, l'effacement et la reprogrammation par application d'une tension électrique.

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

Types de mémoires/3

➢ 1 cycle d'écriture dans une EEPROM est 1000 fois plus lent que celui d'une RAM. Une EEPROM est 3 fois plus encombrante qu'une SRAM. Une EEPROM peut aller jusqu'à 512Ko.

➢ **Mémoire Flash :**

- Écriture en deux phases : enlever les charges d'un bloc de cellules mémoires puis la cellule est programmée par injection d'électrons. Faible encombrement (équivalent à la ROM).

- Meilleure performance que les mémoires EEPROM.

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

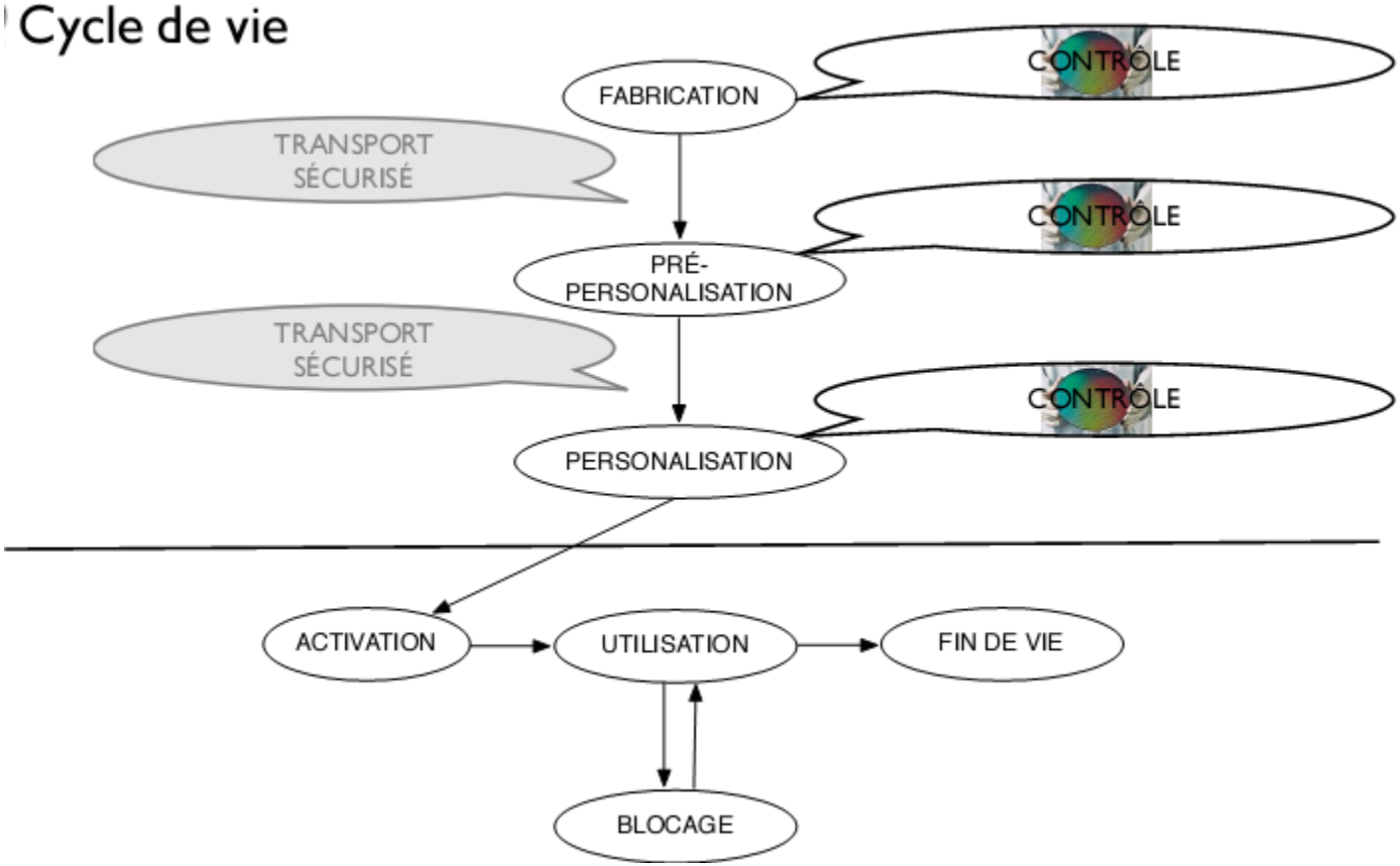
Comparaison entre les types de mémoires

	EEPROM	**Flash**	**MRAM**
Granularité	octet/mot	bloc/secteur	bit
Endurance (en cycles)	10^6	10^5	$>10^{14}$
Temps d'écriture (programmation/effacement)	ms/ms	µs/ms	<100ns
Puissance en écriture	10V × 100µA	5V × 1mA	1,8V ×10mA

MRAM: *Magnetic Random Access Memory* (Les données, contrairement aux données des autres RAM, ne sont pas stockées sous forme d'une charge électrique mais suivant une orientation magnétique)
http://fr.wikipedia.org/wiki/Magnetic_Random_Access_Memory

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

Cycle de vie d'une carte



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

Éléments composant la carte

- Une carte à puce est constituée de 3 éléments :

  - une carte en matière plastique avec ou non une piste magnétique

  - un module électronique supportant les contacts électroniques

  - un circuit intégré en silicium.

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

Étapes de fabrication

-Fabrication de puces rectangulaires à partir de tranches circulaires de silicium (wafer).

-Test des puces directement sur le wafer

-Découpage des puces

-Interconnexion des plots de la puce aux contacts du module

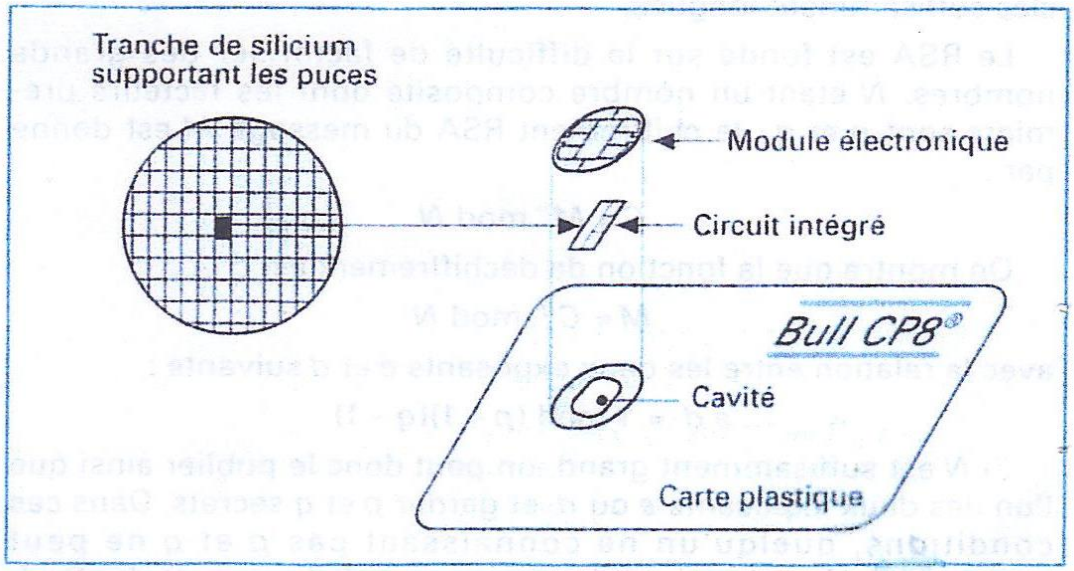
-Encartage : collage du module électronique dans la carte, qui doit tenir sur une épaisseur inférieure à 0,6mm (épaisseur normalisée : 0,76mm).

- Test automatique du composant

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

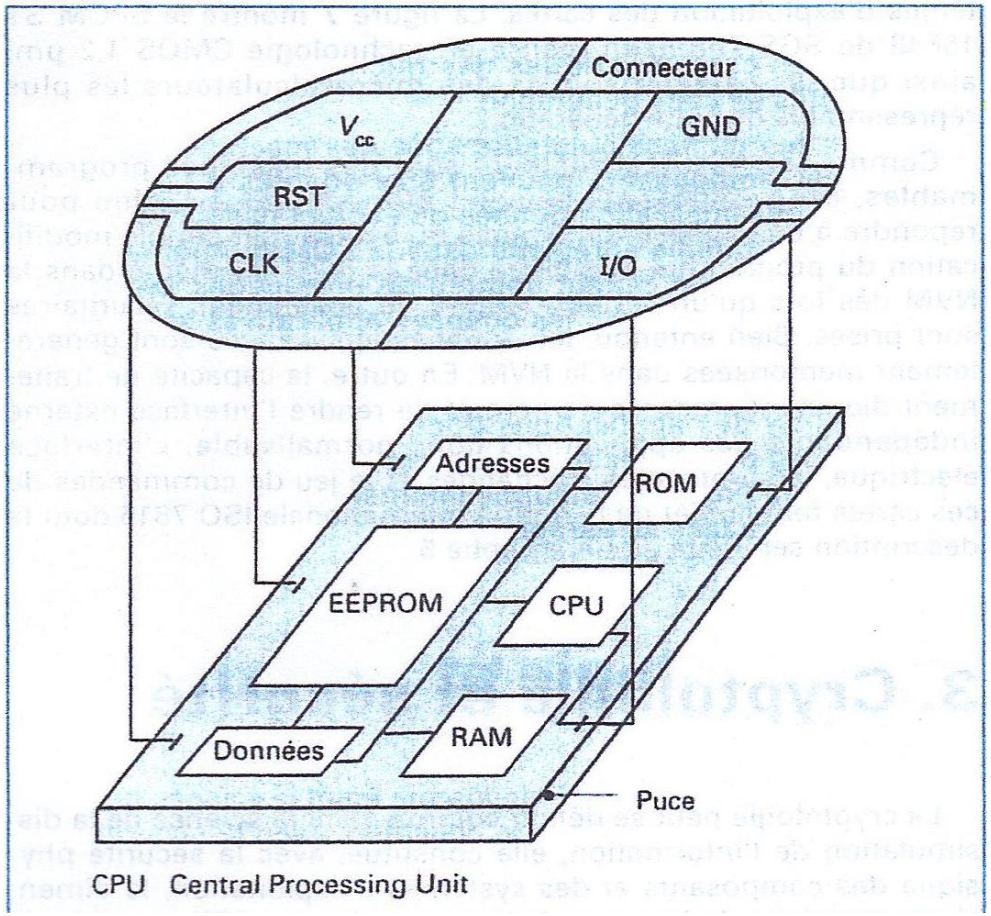
Découpage des puces

wafer (source : wikipédia)



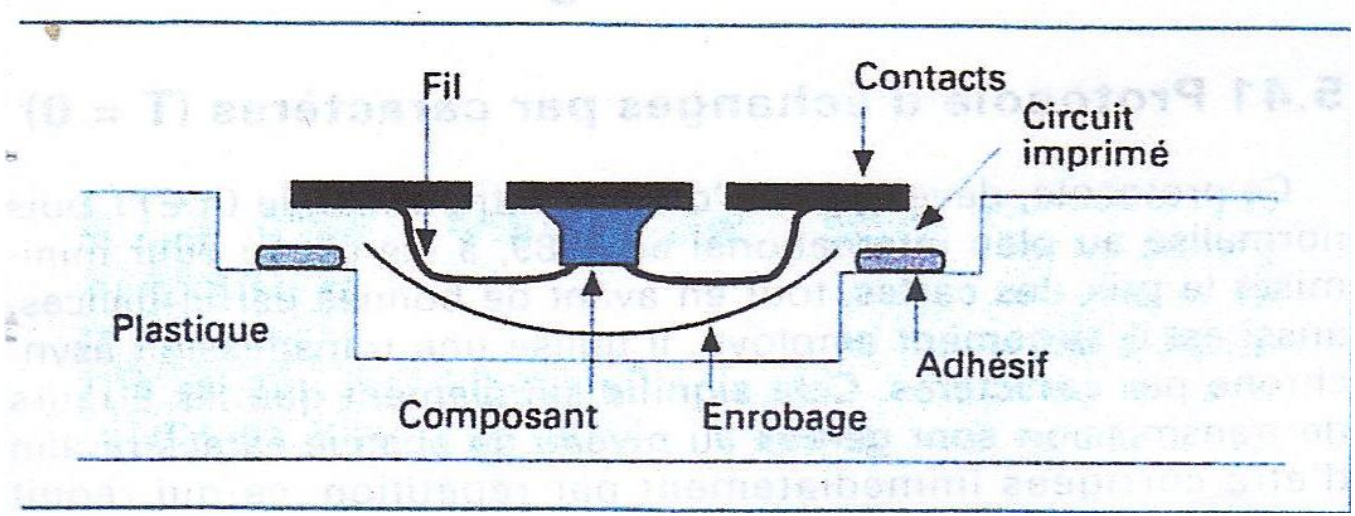
samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Interconnexion de la puce avec le module des contacts



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

Coupe transversale d'une carte à puce



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

Le système d'exploitation (OS)

- Gestion des échanges entre la carte et le monde extérieur via un protocole d'échange
- Gestion des accès aux informations et aux fonctions (sélection de fichier, lecture, écriture, etc.)
- Gestion des fichiers et des données à l'intérieur de la mémoire
- Gestion de la sécurité (authentification, signature, confidentialité) de la carte et de la mise en œuvre des algorithmes cryptographiques.
- Gestion des erreurs
- Gestion du cycle de vie de la carte (fabrication, personnalisation, utilisation, fin de vie).

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

Types de système d'exploitation

- **OS mono-application** (exemple de la carte bancaire B0) : se base sur un fichier maître contenant un certain nombre de fichiers élémentaires. Ces fichiers possèdent des droits d'accès pour la lecture, l'écriture et l'effacement. L'application est associée au système de fichiers.

- **OS multi-application** : présente plusieurs niveaux de répertoires et de fichiers. Chaque répertoire est associé à une application particulière.

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

Les grandes familles de SE

- Les prémisses (avant 1990):
  - M4, BO, B1, PC1, PC2, COS, etc.
    - Mono-application
    - Plus ou moins figé dans les fonctions et structures
    - COS : possibilité d'ajouter des fonctions

- Les évolutions (1990-1995) :
  - MP, MP100, MCOS
  - Multi-application
  - CQL (1993), Basic Card, etc.

- En avant vers l'ouverture
  - Java Card (depuis 1996)
  - .Net

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

Architecture matérielle aujourd'hui

- CPU : 8, 16 & 32 bits,
  - Coeur 8051, AVR, ARM, MIPS, propriétaire

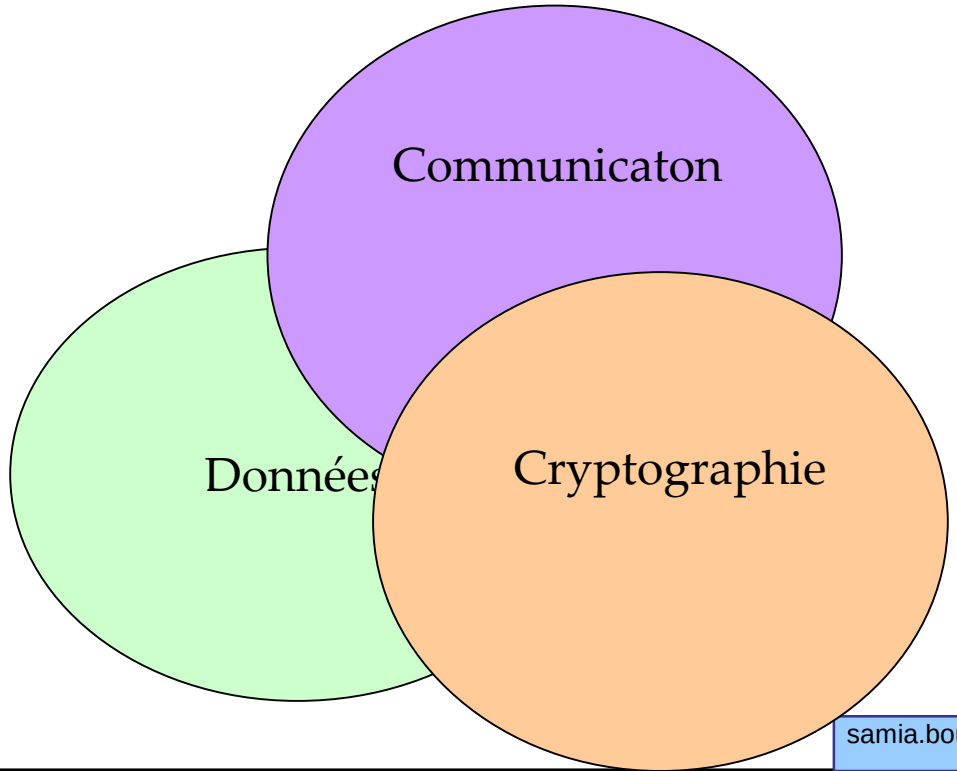
- Mémoires :
  - RAM : 1 à 4 Ko
  - NVM (EEPROM/Flash) : 16 à 32 Ko
  - ROM : 32 à 64Ko

- Co-processeur
  - Java Card : exécution directe du Byte Code Java Card

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

Architecture logicielle

- Gestion protocole d'E/S
- Gestion de la mémoire/des données (traitée dans les cartes SIM et EMV)
- Fonctions cryptographiques (voir cours de Sécurité)



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

La normalisation

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

Les standards

Les normes liées à la carte :

- **ISO,**
- **ETSI, (télécommunications, GSM)**
- **EMV, (cartes de paiement)**
- **ICAO (*International Civil Aviation Organization*, agence de l'ONU, biométrie, passeport)**
- **Santé,**

...

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

Normalisation AFNOR / ISO

- La position des contacts : position AFNOR et position ISO

Carte ISO

Carte AFNOR

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

Normes principales des cartes à contact : l'ISO 7816

- **L'ISO 7816 « Idenfication cards – Integrated circuit cards with contacts »**
  - ✓publié par l'ISO (International Organisation for Standardisation)
  - ✓le plus important standard définissant les caractéristiques des cartes à puce qui fonctionnent avec un contact électrique
  - ✓15 normes sont proposées pour les cartes à contact.

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

Normes principales des cartes à contact

- La norme ISO 7816-1 précise les caractéristiques physiques de la carte
- La norme ISO 7816-2 définit la position et le brochage des contacts de la carte
- La norme ISO 7816-3 définit les niveaux électriques utilisés pour le dialogue avec la carte
- La norme ISO 7816-4 définit les commandes de base des cartes à puce

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

La norme ISO 7816-1

➢**ISO 7816-1 : révisé en mars 1998**
définit les caractéristiques physiques des cartes à puce à contact, ex : la géométrie, la résistance, les contacts, etc.

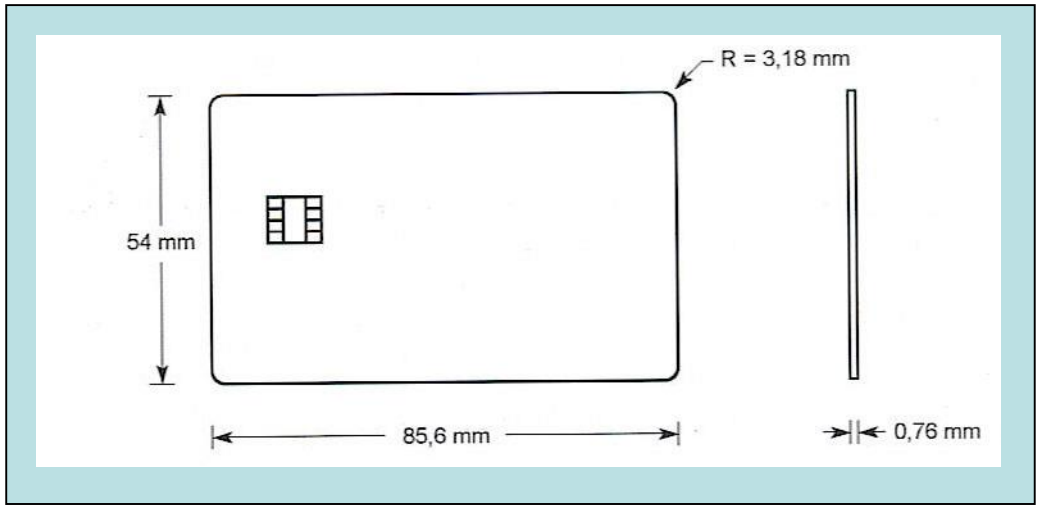
samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Caractéristiques mécaniques des cartes à puce

- Même si on connaît en général deux formats de la carte à puce
  - ✓Celui de la carte bancaire
  - ✓Celui de la carte SIM
- 3 formats normalisés : ID1, ID00 et ID000

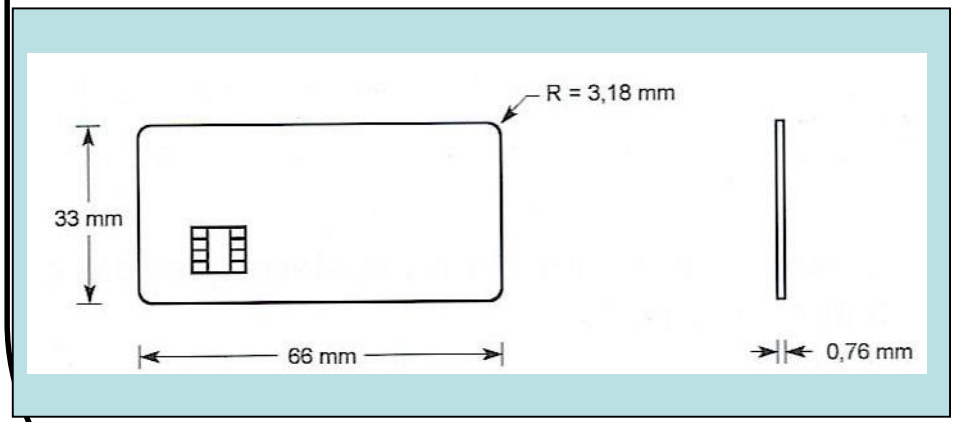
samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Les 3 formats

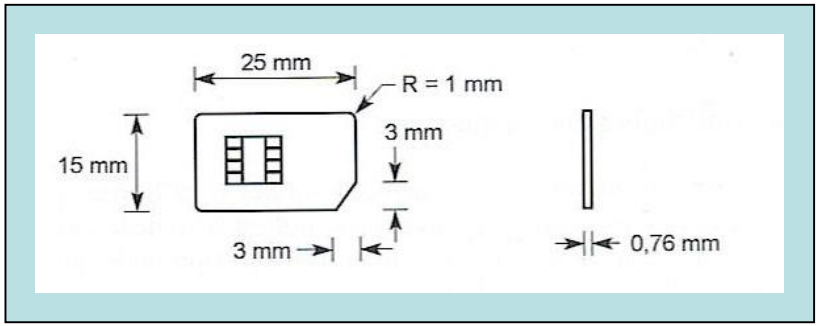


ID 01

ID 00



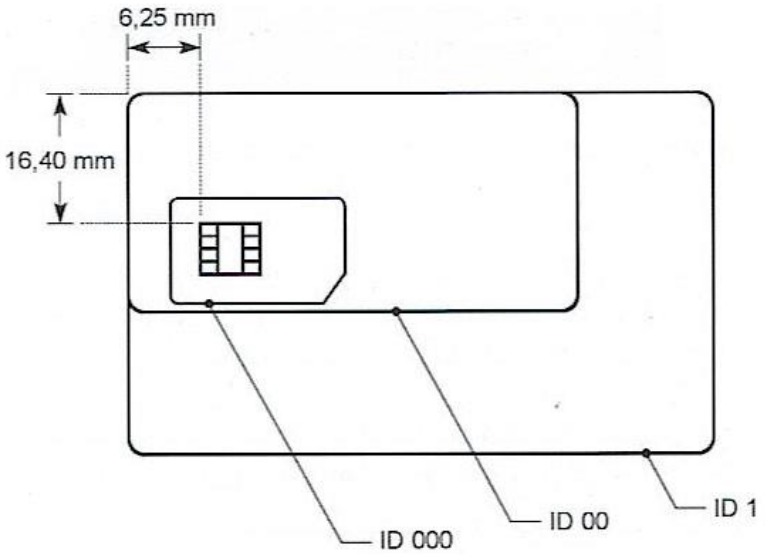
ID 000



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

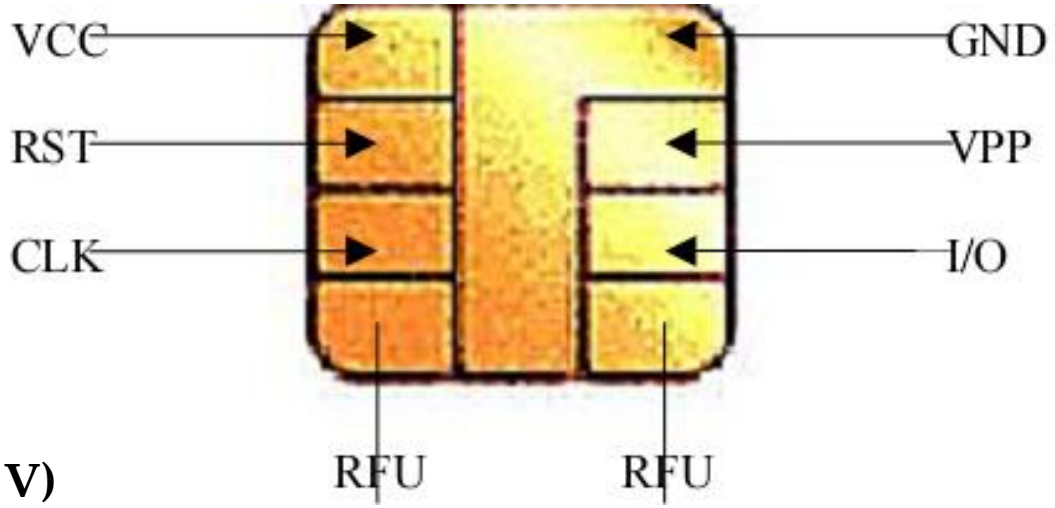
Les 3 formats

➢**Le fabricant produit une seule taille (ID1), le client final pourra réduire ses dimensions au format ID00 ou ID000 (ex. carte SIM)**



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

L'ISO 7816-2



Vcc: tension électrique (3 à 5 V)
RST: c'est le « reset », initialise le microprocesseur (warm reset)
cold reset = coupure et rétablissement de l'alimentation
CLK: signal d'horloge car pas d'horloge sur la carte
GND: masse
I/O: utilisé pour le transfert des données et des commandes entre la carte et le lecteur. La communication half-duplex.
Vpp: destiné à l'origine à recevoir la tension de programmation des mémoires non-volatiles EPROM. Cette tension était de 25 Volts à l'origine, puis 21 Volts, puis devenue inutile avec l'utilisation d' EEPROM qui possèdent leur propre générateur de tension de programmation sur la puce à partir du 5 Volts (Vcc).

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

Signification des contacts

- **Vcc : tension d'alimentation positive de la carte fournie par le lecteur**
  (4.75V ≤ Vcc ≤5.25V) Vcc=3.3V pour une carte SIM
- **RST: commande de reset de la carte, fournie par le lecteur**

- **CLK: Clock, horloge fournie à la carte par le lecteur**
  - rythme les échanges de données entre la carte et le lecteur

- **RFU (Reserved for Future Use) non utilisés**

- **GND masse électrique de la carte**

- **Vpp: tension de programmation de la carte fournie par le lecteur**
  -inutilisé aujourd'hui
  -21V nécessaire dans les premières cartes pour écrire dans des EPROM

- **I/O entrées/sorties des données**
  - ligne bidirectionnelle (carte => lecteur et lecteur => carte)

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

Caractéristiques électriques

- **Vcc : (4.75V ≤ Vcc ≤ 5.25V) Vcc=3.3V pour une carte SIM**
- **RST: valeur min = 4V ou Vcc-0.7V**
- **CLK: Min = 2.4V ou 0.7Vcc ou encore Vcc-0.7V**
  Max=Vcc
- **I/O : état haut (Z) : en mode réception de la carte**
  : état bas (A) : imposé par le lecteur
  - en fonctionnement normal, les 2 extrémités de la liaison ne doivent jamais être en mode émission simultanément

I: Min= 2V ou 0.7Vcc
Max=Vcc
O: Min=2.4V ou 3.8V
Max=Vcc

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

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.

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

Insertion de la carte dans un lecteur

- **La norme ISO 7816-3 précise la mise sous tension de la carte et son arrêt**
- **Dans le lecteur, il y a un circuit d'interface :**
  - ✓ Connexion de la carte et activation de ses contacts par le circuit d'interface
  - ✓ Reset de la carte
  - ✓ Réponse au reset ou ATR émanant de la carte
  - ✓ Dialogue entre la carte et l'application via le circuit d'interface
  - ✓ désactivation des contacts par le circuit d'interface
  - ✓ Retrait de la carte

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

ATR défini dans l'ISO 7816-3

- **ATR (Answer To Reset):**
  - ✓**Dès que la carte est mise sous tension, elle envoie un message de réponse d'initialisation appelé ATR, il peut atteindre une taille maximale de 33 octets. Il indique à l'application cliente les paramètres nécessaires pour établir une communication avec elle.**

  - ✓**Paramètres envoyés par la carte :**

    - Le protocole de transport ;
    - Taux de transmission des données ;
    - Numéro de série de la puce …

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

Comportements de la carte et du lecteur lors d'un Res

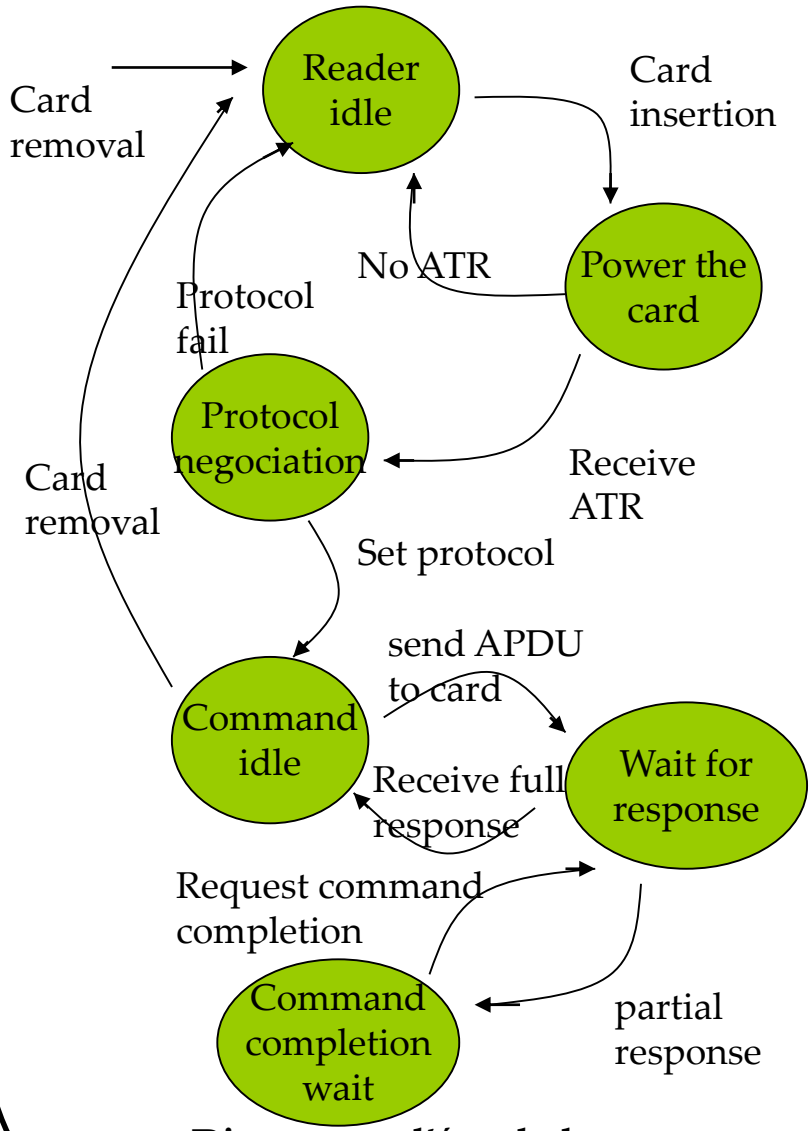


Diagramme d'état du lecteur

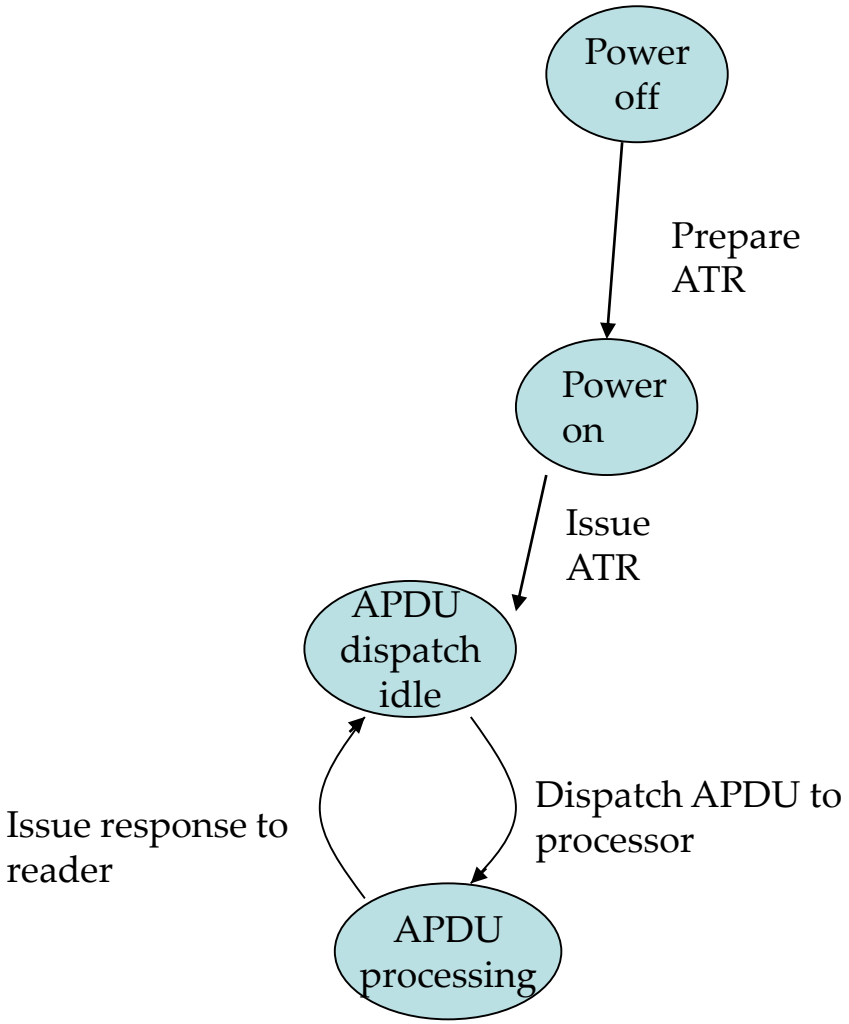


Diagramme d'état de la carte

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

L'ATR dans les vraies cartes à puce

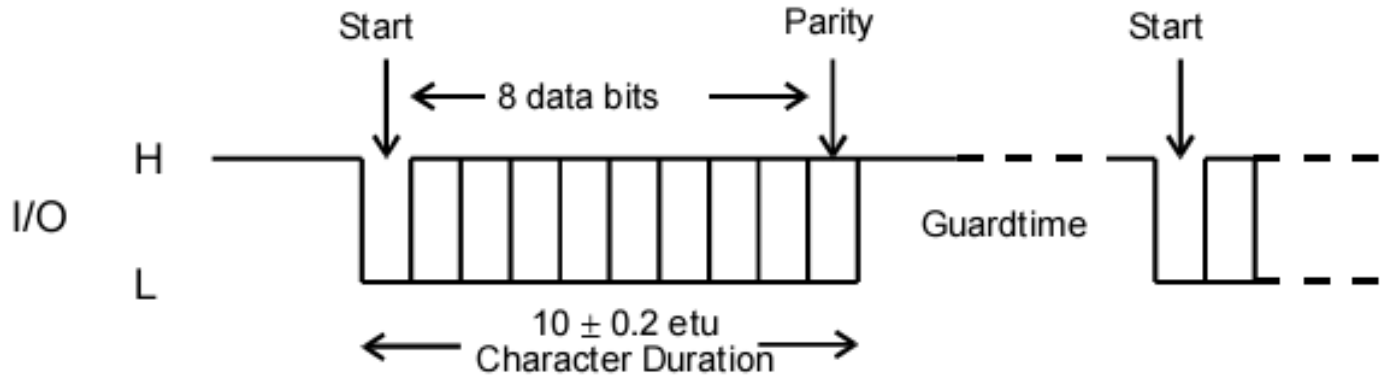
- L'ATR est la réponse de la carte au reset du lecteur
- l'ATR au minimum = 2 octets, au maximum = 33 octets
- Transmission en mode asynchrone semi-duplex
- La fréquence d'horloge comprise ente 1 et 5 MHz pour permettre à n'importe quel lecteur de lire le 1er caractère
- Communication entre le lecteur et la carte via la ligne I/O

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

Chronogramme de la réponse reset

- Comm. Asynchrone : bit start + 8 bits de données (ba à bh) + bit de parité paire + TG (Temps de Garde = un ou plus bits Stop)

- A :niveau bas et Z niveau haut
- le délai entre 2 caractères est au moins de 12 etu et TG = 2 etu



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

Caractère initial de l'ATR

- Premier caractère de l'ATR = TS (caractère initial)

- TS peut prendre 2 valeurs : (ZZAAAAAA)[1] ou (ZZAZZZAA)[2]

- 1: convention inverse :
  - niveau bas A = « un » logique
  - niveau haut Z = « zéro » logique
  - ba (bit transmis en premier) = bit 7 de poids fort
  - bh (bit transmis en dernier)=bit 0 de poids faible

  TS = 0011 1111 (3F, en héxa)

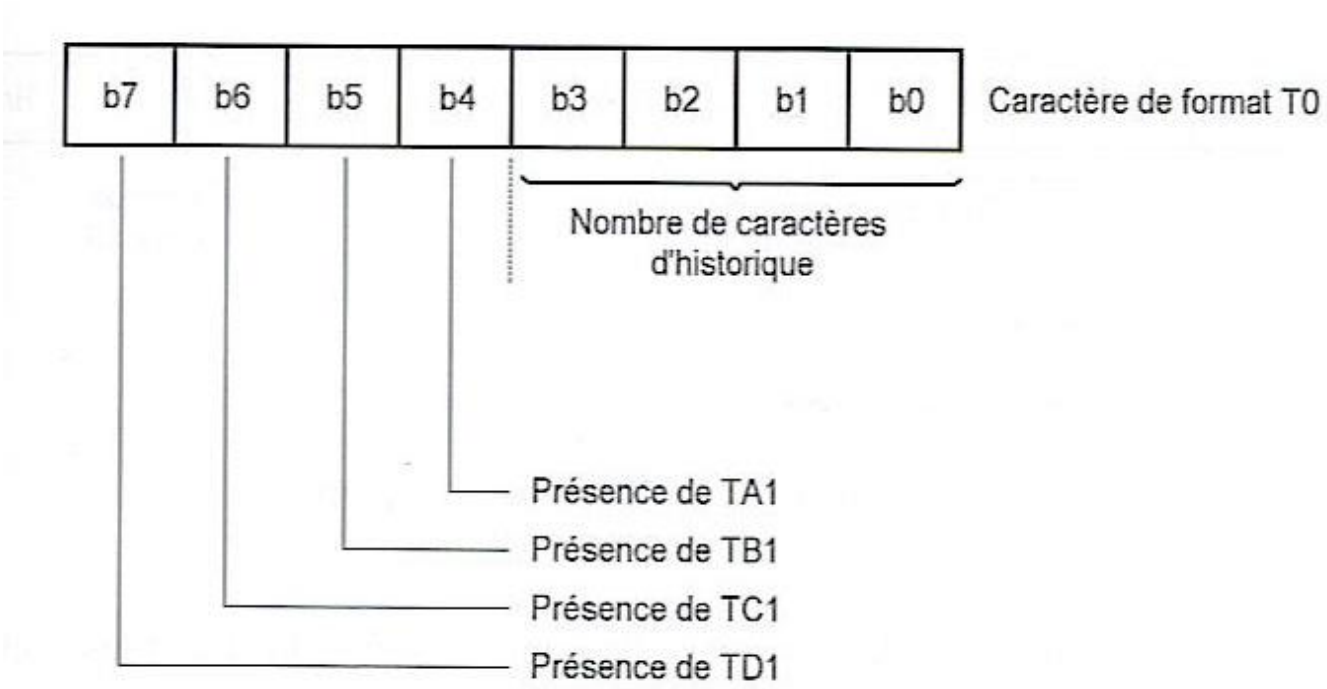
- 2: convention directe :
  - niveau bas A = « 0 » logique
  - niveau haut Z = « 1 » logique
  - ba (bit transmis en premier) = bit 0 de poids faible
  - bh (bit transmis en dernier)=bit 7 de poids fort

  TS = 0011 1011 (3B, en héxa)

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

Caractère de format

- appelé aussi caractère T0
- 2ème caractère de l'ATR
- composé de :
  - -Partie Y1 (b_7 à b_4)
  - -Partie K (b_0 à b_3) facultative (n'est pas normalisée)



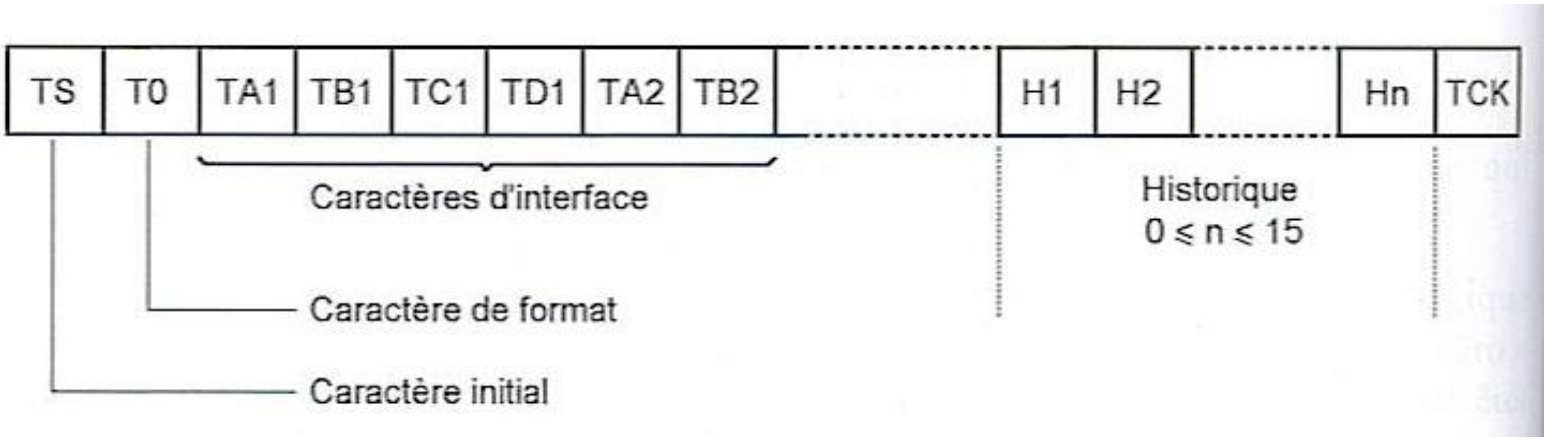
samia.bouzefrane@cnam.fr - CEDRIC (CNAM) -

Caractère de format (suite)

- b_4=1 si le car TA_1 est transmis dans l'ATR
- b_5=1 si le car TB_1 est transmis dans l'ATR
- b_6=1 si le car TC_1 est transmis dans l'ATR
- b_7=1 si le car TD_1 est transmis dans l'ATR

- Les poids forts de TD_1 indique si les caractères supérieurs sont transmis dans l'ATR, par ex. :

  -Si TD_1 contient 1010 => TD_2 et TB_2 sont transmis



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

Caractère TA1

TA1

b7	b6	b5	b4	b3	b2	b1	b0

F D

b7	b6	b5	b4	F	fs max (MHz)
0	0	0	0	Interne	-
0	0	0	1	371	5
0	0	1	0	558	6
0	0	1	1	744	8
0	1	0	0	1116	12
0	1	0	1	1488	16
0	1	1	0	1860	20
0	1	1	1	RFU	-
1	0	0	0	RFU	-
1	0	0	1	512	5
1	0	1	0	768	7,5
1	0	1	1	1024	10
1	1	0	0	1536	15
1	1	0	1	2048	20
1	1	1	0	RFU	-
1	1	1	1	RFU	-

RFU : Réservé pour un usage futur

b3	b2	b1	b0	D
0	0	0	0	RFU
0	0	0	1	1
0	0	1	0	2
0	0	1	1	4
0	1	0	0	8
0	1	0	1	16
0	1	1	0	RFU
0	1	1	1	RFU
1	0	0	0	RFU
1	0	0	1	RFU
1	0	1	0	1/2
1	0	1	1	1/4
1	1	0	0	1/8
1	1	0	1	1/16
1	1	1	0	1/32
1	1	1	1	1/64

RFU : Réservé pour un usage futur

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

Caractère TA1 (suite)

- F et D définissent la vitesse de transmission utilisée après l'ATR
- Vitesse de transmission= $D*f_s/F$ bits/s avec f_s fréquence d'horloge en Hz
- Durée d'un bit (etu)= $F/(D*f_s)$ secondes
- Valeur min de f_s = 1 MHz (selon la norme)
- Valeur max de f_s : dictée par TA_1

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

Caractère TB1 / TC1

- **TB1 : n'est plus utilisé**

- **est censé contenir la valeur de la haute tension de programmation (tension à appliquer sur Vpp pour écrire sur la carte)**

- **TC1 code un paramètre N= temps de garde supplémentaire**

Si 0 ≤ N ≤ 254 (FE en Hexa), TG=N*etu
Si N=255 (FF en Hexa), TG = 11*etu

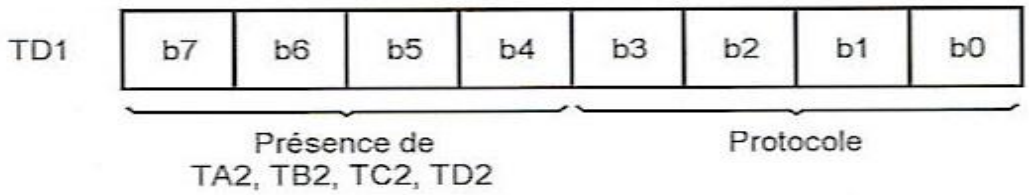
- **Pour les caractères envoyés par la carte TG=2*etu.**

TC1 demandé par la carte permet un TG supplémentaire uniquement dans le sens Lecteur -> Carte

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

Caractère TD1

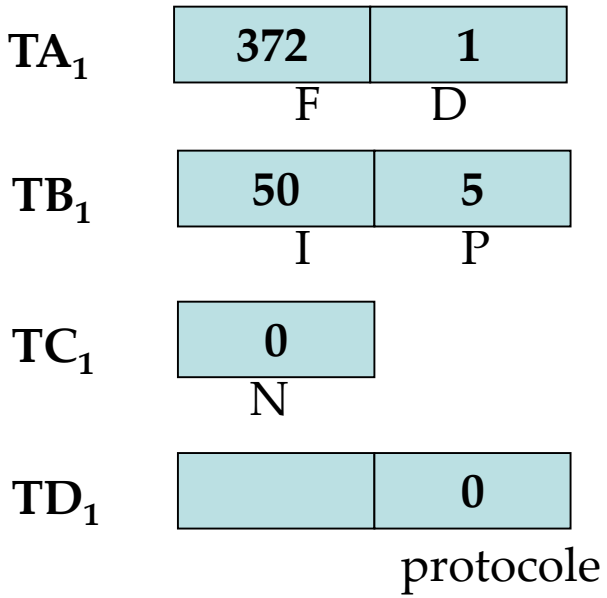
- Code le caractère TA_2, TB_2, TC_2 et TD_2 (bits poids forts)
- bits de poids faible (numéro du protocole utilisé, T=0 et T=1)



b3	b2	b1	b0	Protocole T =
0	0	0	0	0
0	0	0	1	1
0	0	1	0	2
0	0	1	1	3
0	1	0	0	4
0	1	0	1	5
0	1	1	0	6
0	1	1	1	7
1	0	0	0	8
1	0	0	1	9
1	0	1	0	10
1	0	1	1	11
1	1	0	0	12
1	1	0	1	13
1	1	1	0	14
1	1	1	1	15

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

ATR par défaut



- **TCK présent si protocole ≠ 0 dans TD1**
- **TCK = valeur de sorte qu'un Ou exclusif entre les octets de T0 (inclus) et TCK (inclus) soit nul**

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

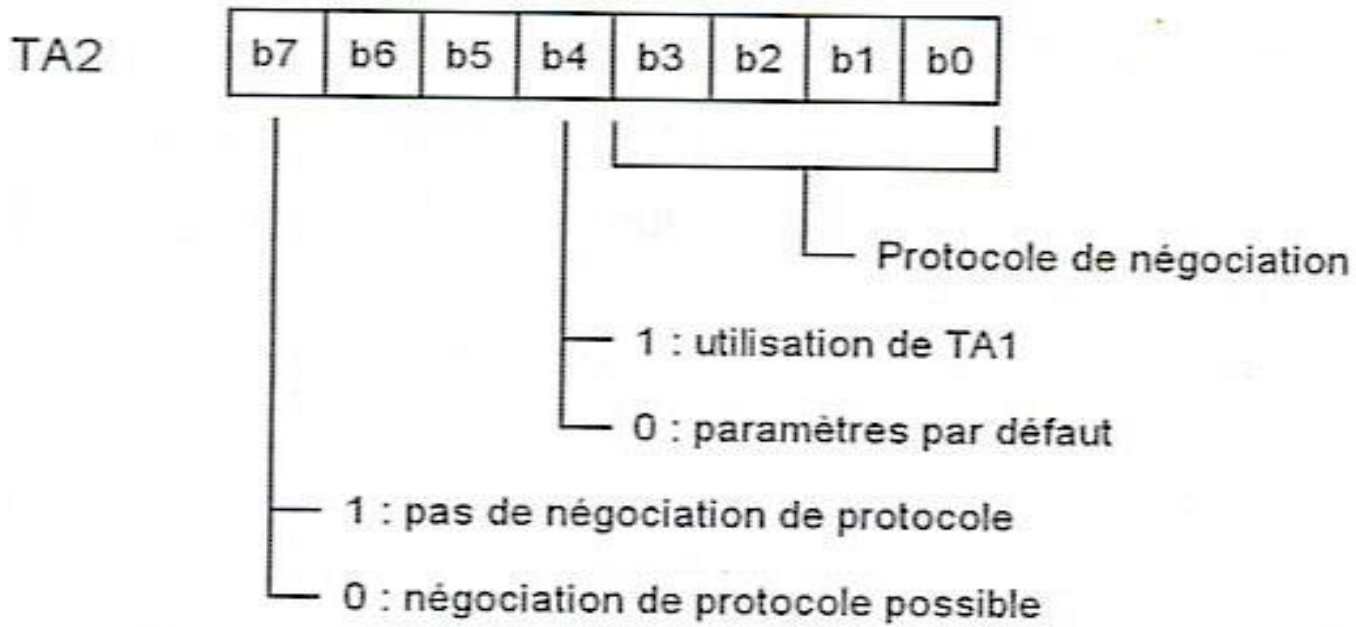
Négociation de vitesse de dialogue

- Mécanisme proposé depuis l'existence de la norme ISO 7816-3 en 1999
- Implanté plus récemment dans les cartes
- Idée : changer de vitesse au cours des échanges pour augmenter la sécurité en brouillant les simples amateurs de piratage
- Les cartes dialoguent à 9600 bits/s pendant l'ATR (vitesse connue de tout port série RS232 facilite la réalisation d'espions)

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

Caractère TA2

- **Si caractère TA2 existe => il indique les conditions de négociation**



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

Les protocoles TPDU/APDU

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

L'ISO 7816-4

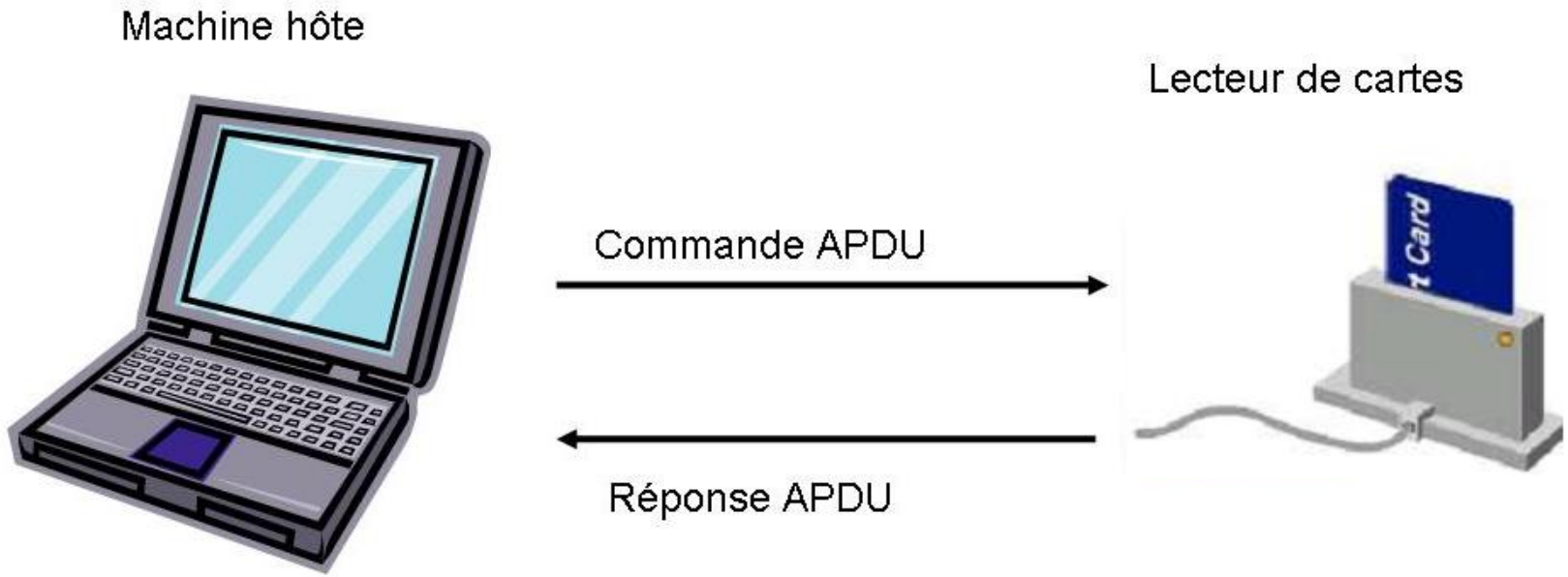
- Elle définit les messages APDU (Application Protocol Data Units) utilisés par les cartes à puce pour communiquer avec le lecteur.

- Les échanges s'effectuent en mode client-serveur,

- Le terminal est toujours l'initiateur de la communication.

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

L'ISO 7816-4 : Le protocole APDU



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

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

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

Format des réponses 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

Exemples de cartes

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 anwer)
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.)

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

Protocole APDU (ISO 7816-4)

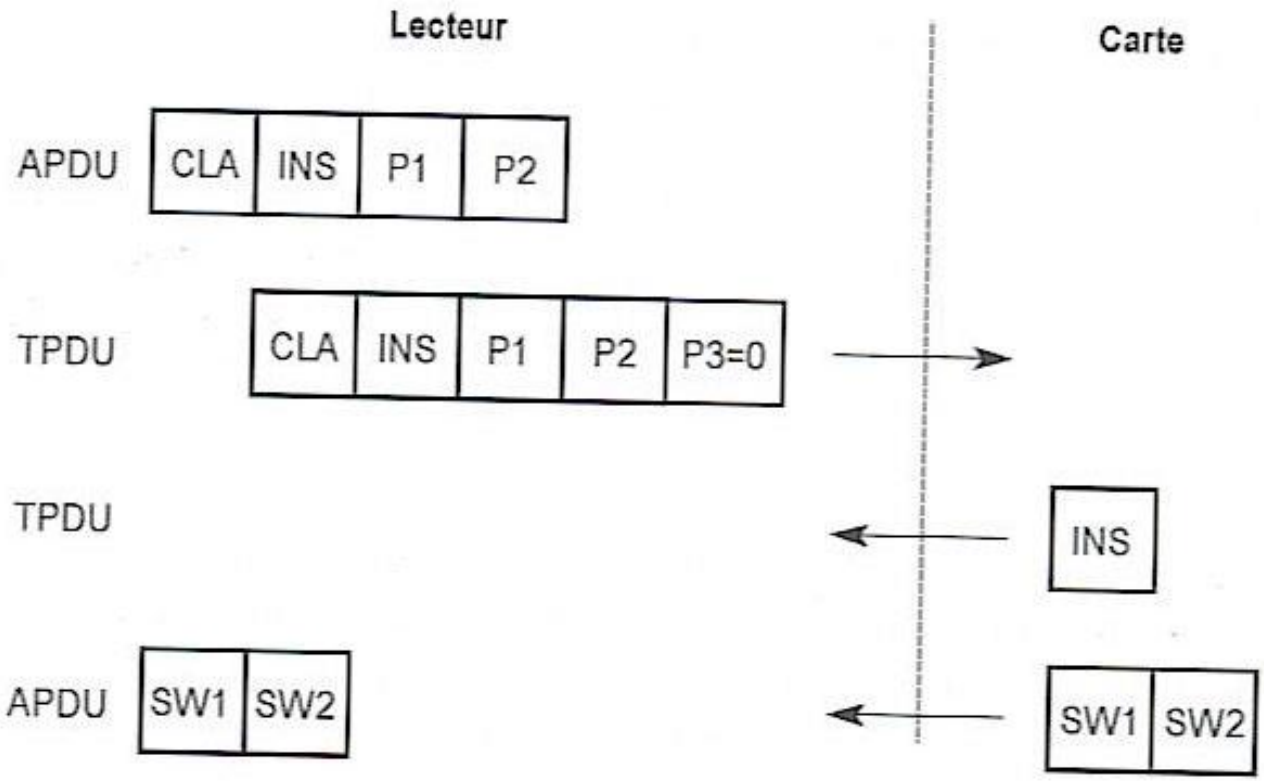
- La norme relative aux cartes à puce a essayé de se conformer au modèle OSI

- Couche application (APDU) n'est pas vraiment séparée de la couche transport (TPDU)

- Il existe 5 types de commandes APDU selon qu'il y a ou non échange de données utiles

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

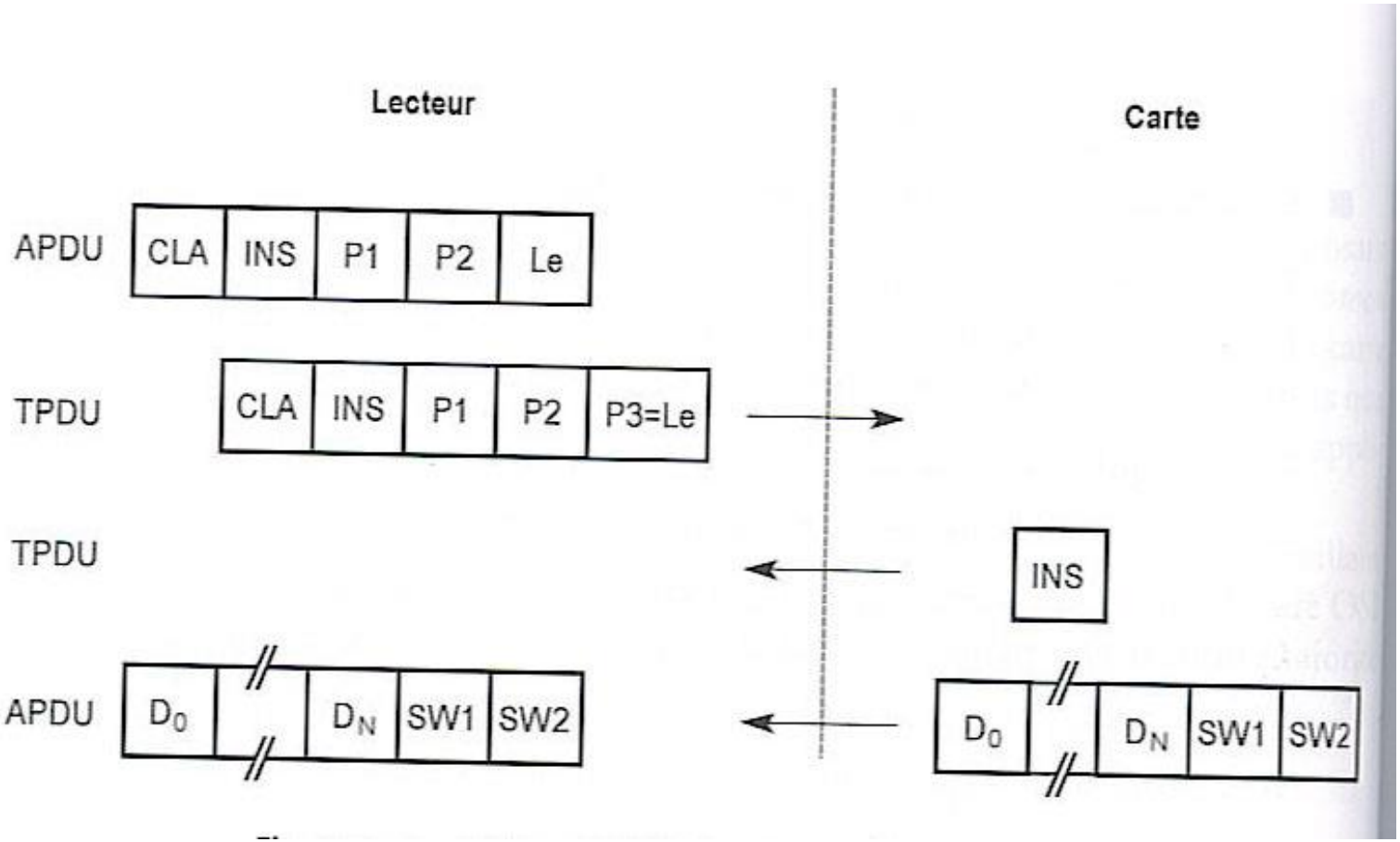
Envoi d'une commande sans données utiles



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

Commande avec réception de données utiles depuis la carte

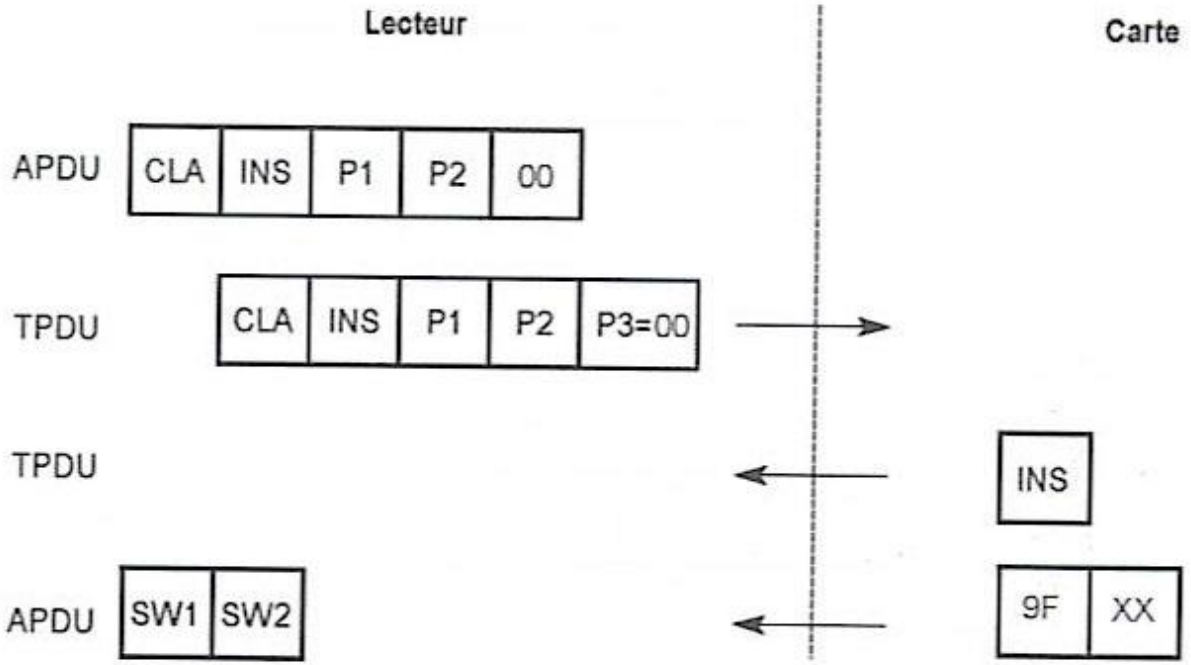
- Le nb d'octets retournés peut être différent de *Le*



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

Commande avec invitation à lire des données depuis la carte

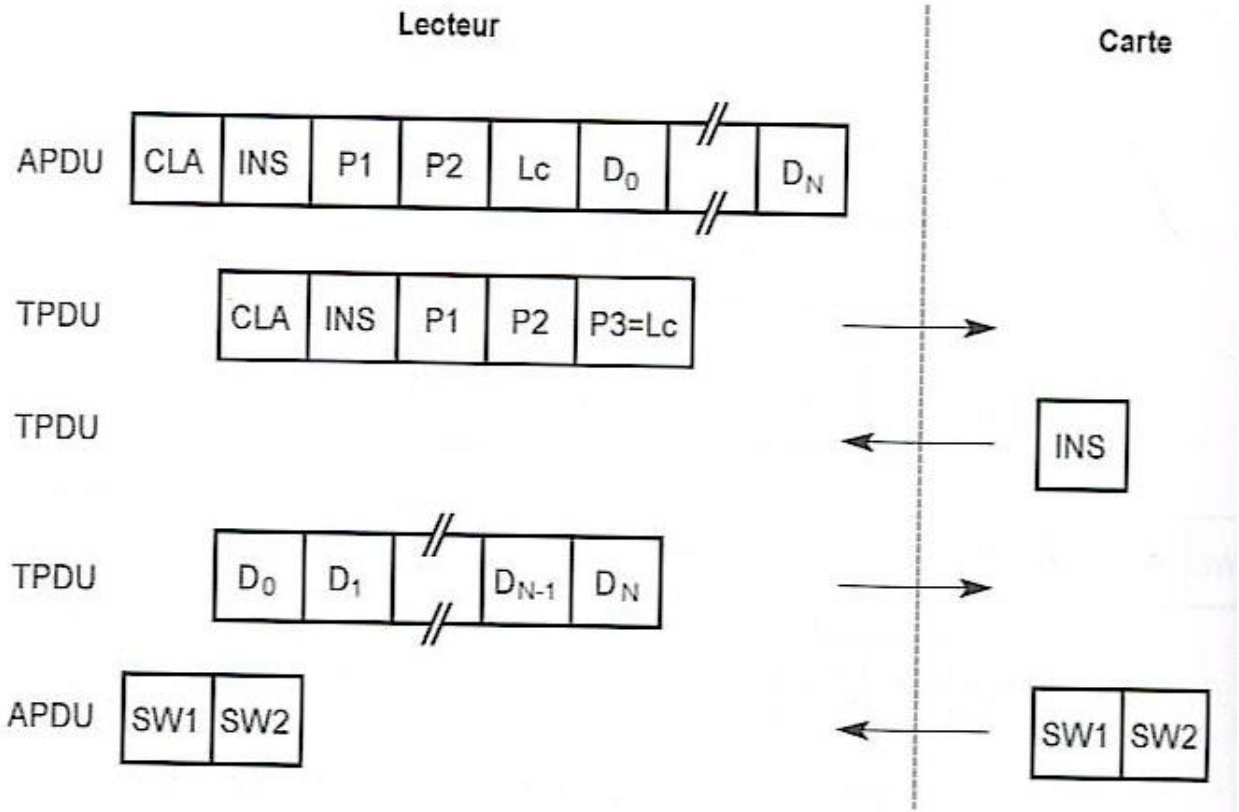
- *Le=0* car le nb d'octets attendus est inconnu
- SW1 SW2 = 9F XX (avec XX le nb d'octets disponibles pour cette cde
- Le lecteur doit refaire sa commande avec ce nb d'octets



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

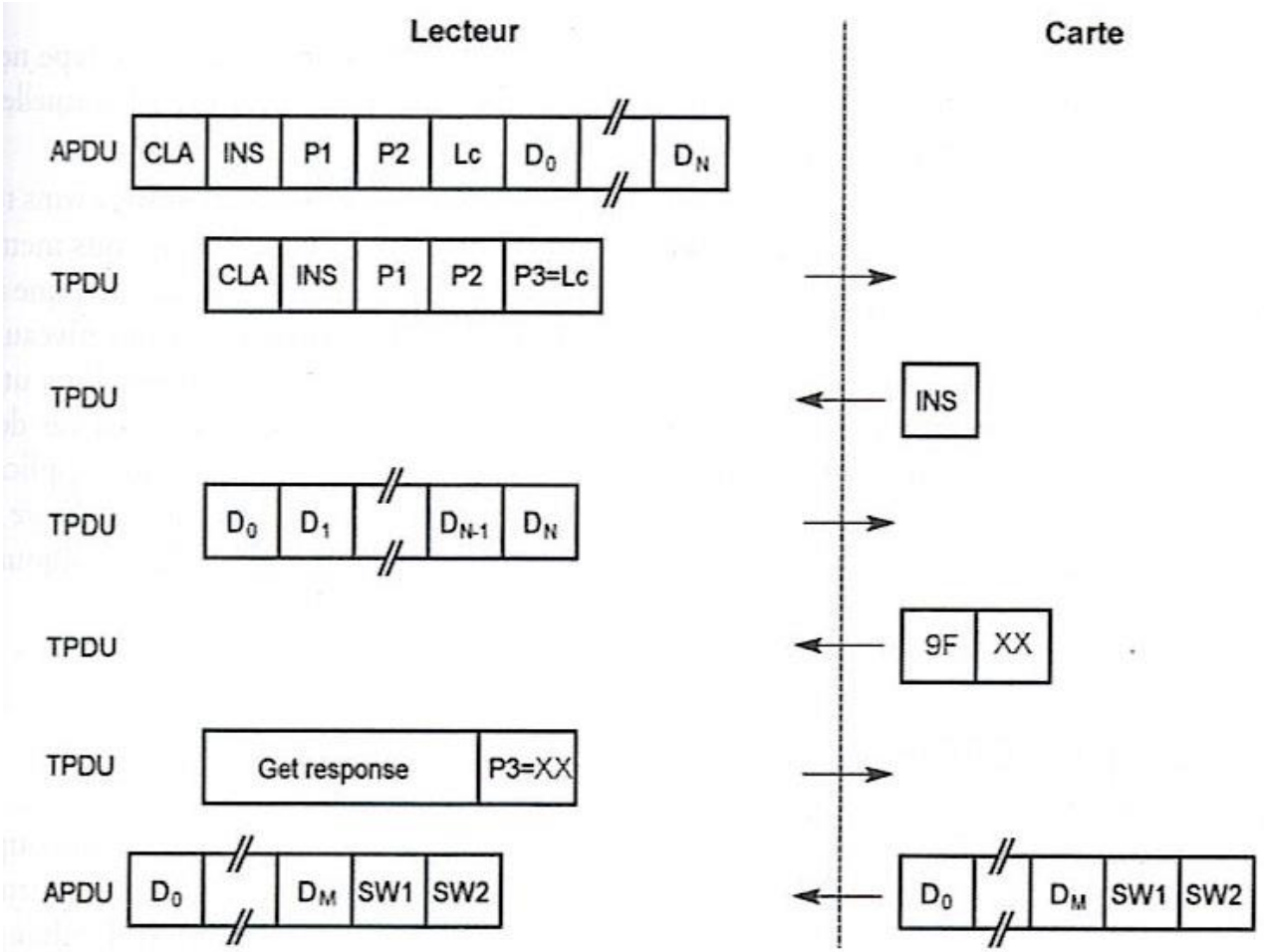
Commande avec envoi de données utiles vers la carte

- *Lc*: est le nb d'octets envoyés



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

Commande avec envoi et réception de données utiles



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

L'ISO 7816-5

- Elle définit la procédure d'enregistrement et d'attribution des identifiants des applications (AID, ou *Application IDentifier*).

- Un unique AID est associé à chaque application = {RID, PIX}

- RID : le numéro d'enregistrement du fournisseur d'application attribué par l'ISO.
  Le RID doit être le même pour le paquetage et l'applet.

Application identifier (AID)	
National registered application provider (RID)	Proprietary application identifier extension (PIX)
5 octets	0 to 11 octets

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

Bibliographie

1. Zhiqun Chen , « Technology for smart cards: architecture and programmer's guide », Addison Wesley, sept. 2000
2. Christian Tavernier, « *Les Cartes à puce: théorie et mise en œuvre* », 2ème édition, Ed. Dunod, 2007.
3. Normes EMV : http://www.emvco.com
4. S. Bouzefrane, P. Paradinas - *Les Cartes à puce*, Sept. 2013, Hermès, pp. 350, (isbn: 9782746239135).
5. Magazine MISCH, Hors Série, Cartes à puce : découvrez leurs fonctionnalités et leurs limites, novembre 2008.
6. Magazine Linux, Hors Série, Cartes à puce, octobre 2008.
7. Entretien avec Roland Moreno en Juillet 2010.
8. Échange de mails et de documents avec Michel Ugon que je remercie, octobre 2013.
9. Michel Ugon, « *1981 Naissance du microprocesseur auto-programmable monolithique, le plus petit micro-ordinateur au monde* », dans Applications, Cartes & Systèmes, n°14, oct. 1994.
10. Michel Ugon, « *Cartes à puces* » (directeur général adjoint de Bull CP8, R&D), Collection Techniques de l'Ingénieur E3 520, traité Électronique, 1994.
11. Jean-Pierre Tual, « *Cartes à puce* », Techniques de l'ingénieur, traité Électronique, E3 440 (actualise le E3 520 rédigé par M. Ugon), 2005.

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

Cartes à puces

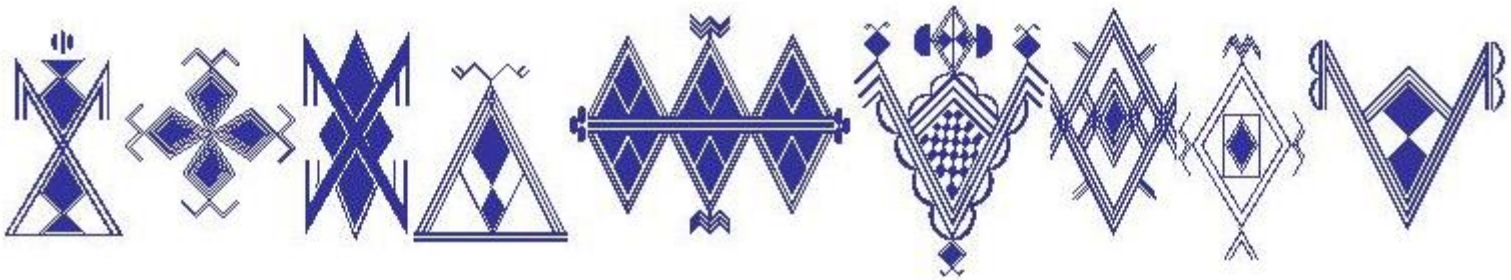
A Samia Bouzefrane
Par souci de la vérité, et
pour la postérité
Cordialement

par **Michel UGON**
Directeur Général Adjoint de Bull CP8
Recherche et Développement

Octobre 2013

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

Fin



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