# La norme EMV

*Samia Bouzefrane*

Maître de Conférences

CEDRIC –CNAM

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

# La norme EMV : introduction



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

# Contexte de la norme

➢EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card **Specifications** for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers **testing** and approval processes to evaluate **compliance** with the EMV Specifications. EMVCo is currently owned by **American Express, JCB, MasterCard and Visa**.

➢A primary goal of EMVCo and the EMV Specifications is to help facilitate global **interoperability** and **compatibility** of chip-based payment cards and acceptance devices. This objective extends to new types of payment devices as well, including **contactless** payment and **mobile** payment.

**Source : http://www.emvco.com (2009)**



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

# EMV

➢ **Standard des cartes de paiement depuis 1995**

➢ **Organismes fondateurs (déc. 1993):**
- **Europay** International (racheté par Mastercard en 2002) ;
- **MasterCard** International ;
- **Visa** International ;

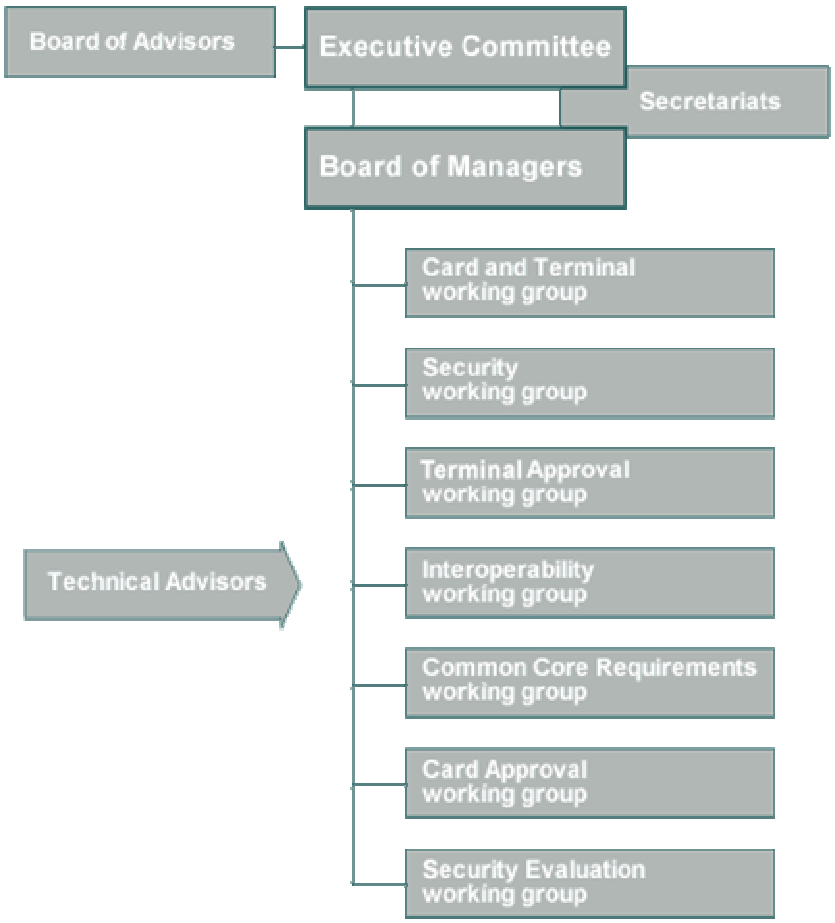
Rejoint par :
-le japonais **JCB International** (depuis Déc. 2004)
-l'américain **American Express** (depuis Fév. 2009)

➢ **Première version des spécifications en 1996.**

➢ En France, depuis fin 2006 les cartes bancaires et les terminaux de paiement électroniques (TPE) respectent le standard EMV.


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

# Structure de l'organisation






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

# Spécifications EMV

- **Spécifications disponibles sur http://www.emvco.com**
- **Longue spécification**
  - ✓ de l'ordre de 867 pages



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

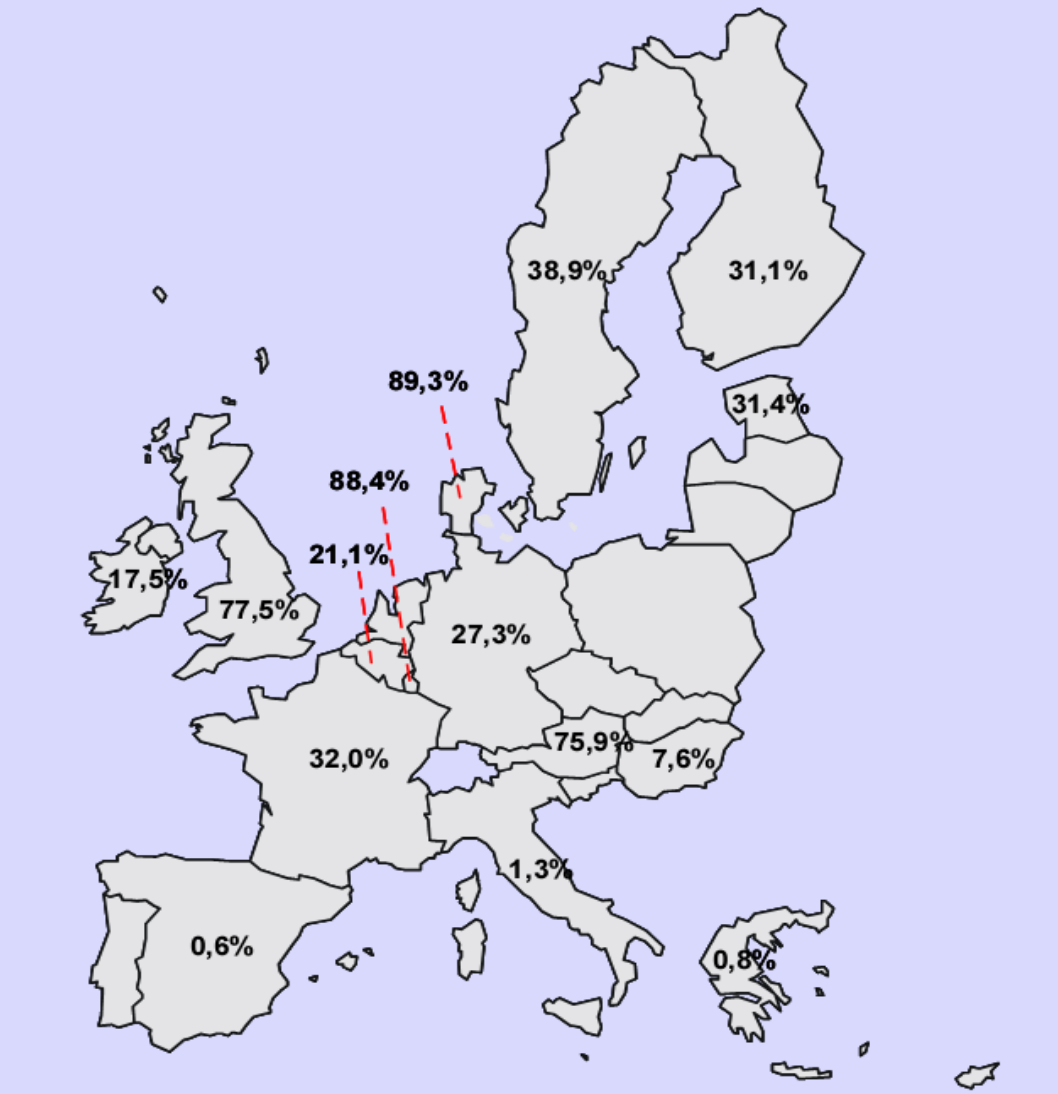
# Plusieurs parties

- **Integrated Circuit Card (ICC) Specifications for Payment Systems**
- **Version 4.1, mai 2004**
- **Book 1**
  - ✓ Application Independent ICC to terminal
- **Book 2**
  - ✓ Security and Key Management
- **Book 3**
  - ✓ Application Specification
- **Book 4**
  - ✓ Cardholder, Attendant, and Acquirer


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

# Déploiement EMV

En 2005, il y avait :
176 millions cartes EMV
sur 550 millions de cartes
circulant en Europe

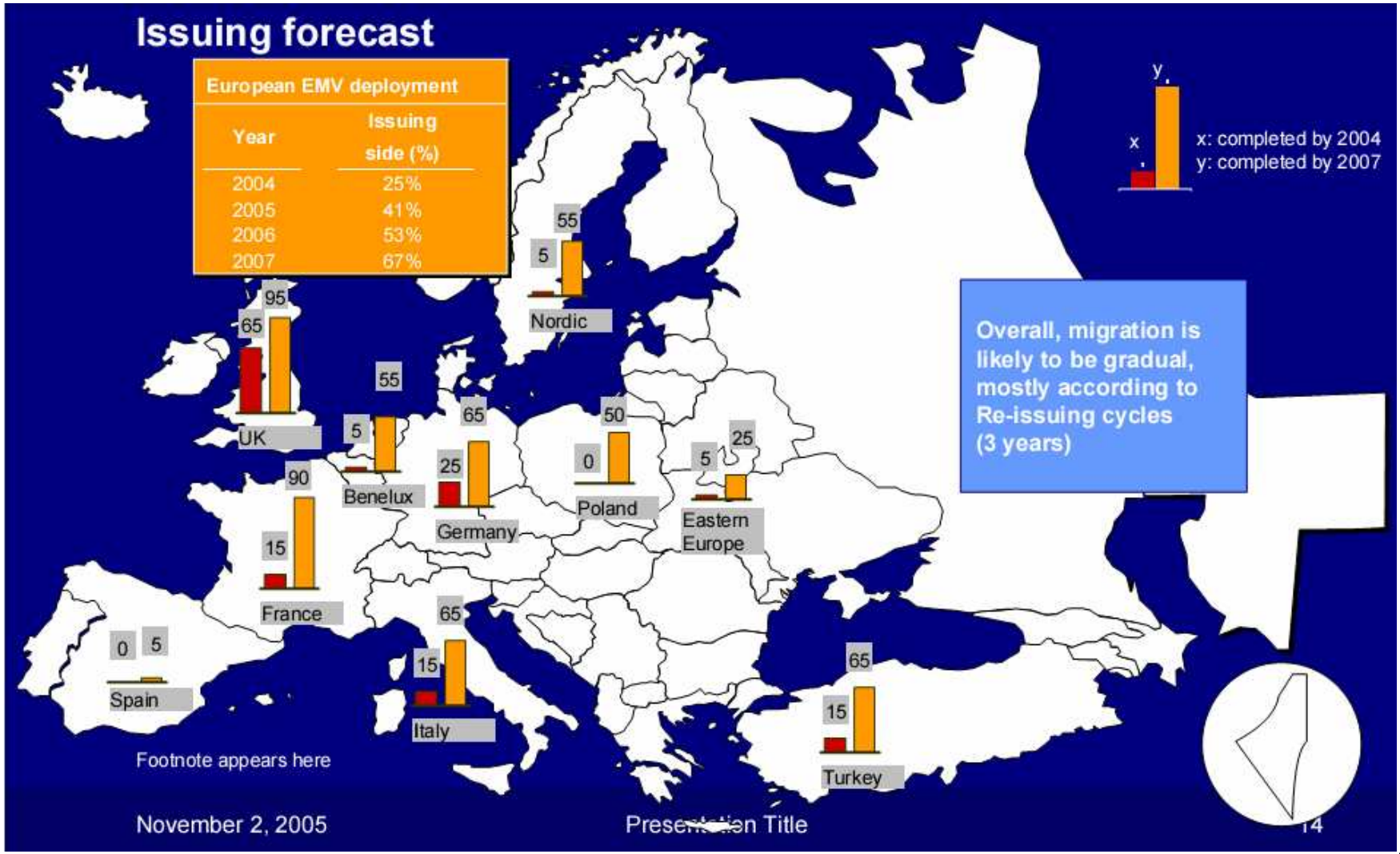



Source: European Payments Council – As of the end of the first quarter of 2005



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

# Déploiement de cartes EMV

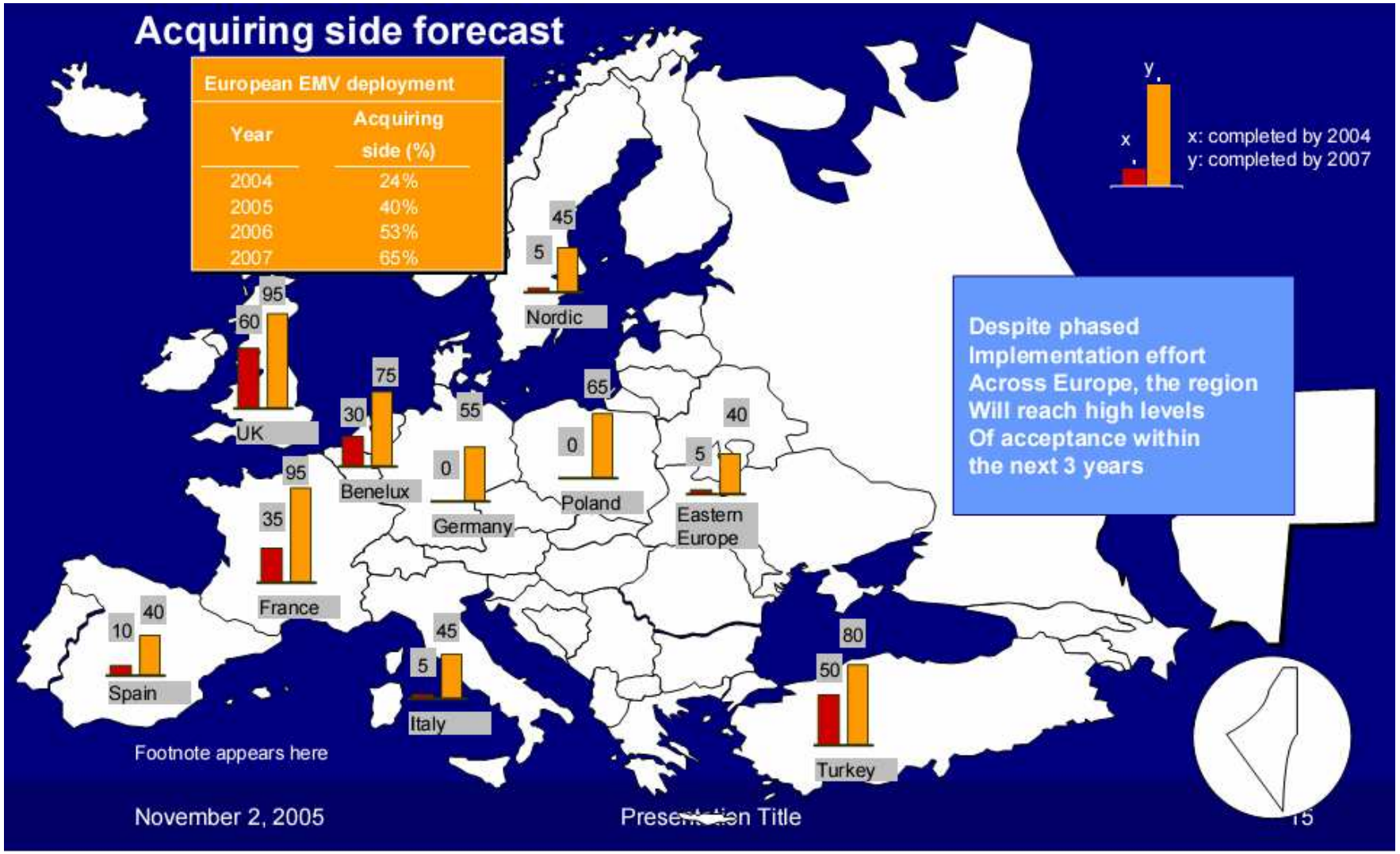



Source : International Master Card



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

# Déploiement de terminaux EMV




Source : International Master Card



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

# Déploiement de l'EMV aujourd'hui

- **Europe** :
  - Zone SEPA (Single Euro Payment Area)
  - Migration vers l'EMV de Janvier 2008 au 31 Décembre 2010.
  - En 2010: 100% des cartes doivent être conformes à l'EMV
  - En 2010, 590 millions de cartes bancaires EMV seront en circulation

- **Dans le monde** (Europe, Asie et Amérique Latine)
  - En 2010, 830 millions de cartes EMV en circulation.

- **USA** : pas de cartes conformes à l'EMV, idem pour les cartes e-ID.


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

# Raisons de la migration

- **Liability shift**

  **les coûts induits par une fraude lecteur ou terminal seront pris en charge par les banques (émetteurs de la carte) ou les commerçants dont les matériels ne seraient pas conformes à EMV**

- **Fraude**

  **différente selon les pays et les systèmes de paiement**



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

# Spécifications EMV

➢**Spécifications EMV:**
-basées sur la norme ISO/IEC 7816
-doivent être lues conjointement avec la norme ISO

➢ Si des définitions fournies dans EMV sont différentes de la norme ISO alors les définitions de la norme EMV remplacent celles de l'ISO

➢ Ces spécifications doivent être utilisées par :
-Les fabricants de ICC et de terminaux
-Les concepteurs de systèmes de paiement
-Les institutions financières qui implantent des applications financières sur ICC


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

# Book 1 : Application Independent ICC to Terminal Interface Requirements



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

# Book1 : la carte

- **Décrit**

  - **les caractéristiques mécaniques : contact, dimension, etc.**
  - **les caractéristiques électriques : voltage, impédance**
  - **Answer to Reset**
  - **Description du protocole de transaction**
  - **Sélection d'application**

- **Conforme aux spécifications de l'ISO 7816**



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

# Normalisation parfaite

- **Quel que soit le fabricant de la carte à puce, celle-ci doit être lue par n'importe quel distributeur dans le monde**

- **Pour garantir cette interopérabilité, la normalisation concerne au moins 3 points:**

**-Des paramètres physiques : taille de la carte, position de la puce et ses contacts**

**-Des paramètres électriques : tension d'alimentation, niveaux électriques utilisés**

**-Des paramètres logiciels qui définissent le mode de dialogue avec la carte (commandes)**



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

# Caractéristiques mécaniques

- La carte doit être opaque aux rayons UV (la puce insensible aux rayons UV)
- La carte doit résister aux détériorations de sa surface
- la carte doit protéger la puce lors de manipulation de stockage lors d'une utilisation normale
- La zone des contacts doit résister à la pression causée par une bille d'acier de 1,55 mm de diamètre appliquée avec une force intérieure ≤ 1,5 N.
- La puce doit résister aux rayons X
- La carte ne doit pas être endommagée par un champ magnétique statique de 79 500 A/tr.m.

etc.



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

# Comme dans la norme ISO 7816-1

- **définit les caractéristiques physiques des cartes à puce à contact, ex : la géométrie, la résistance, les contacts, etc.**



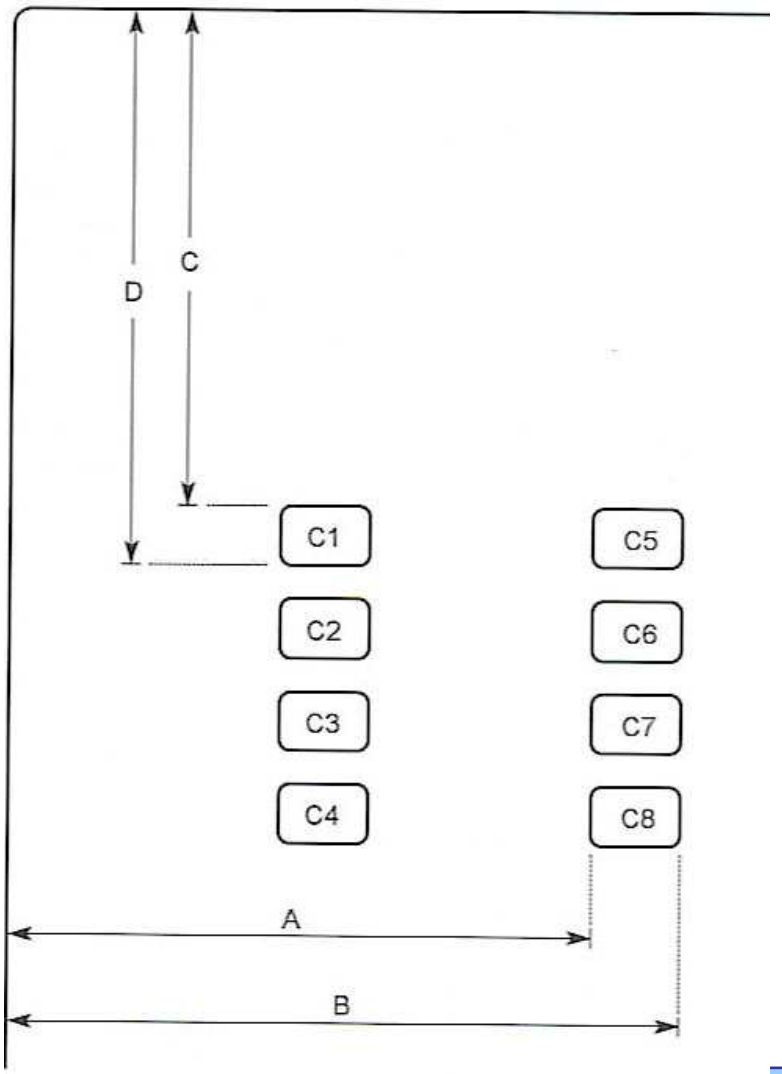

samia.bouzefrane@cnam.fr - CEDRIC ( CNAM) -

# Comme dans l'ISO 7816-2

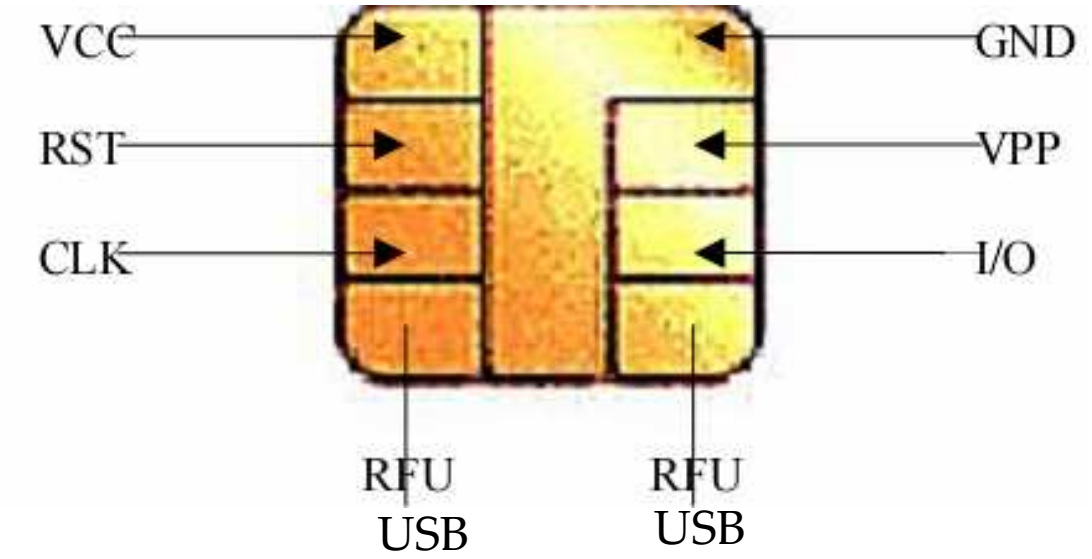
| | A | B | C | D |
|---|---|---|---|---|
| C1 | 10,25 | 12,25 | 19,23 | 20,93 |
| C2 | 10,25 | 12,25 | 21,77 | 23,47 |
| C3 | 10,25 | 12,25 | 24,31 | 26,01 |
| C4 | 10,25 | 12,25 | 26,85 | 28,55 |
| C5 | 17,87 | 19,87 | 19,23 | 20,93 |
| C6 | 17,87 | 19,87 | 21,77 | 23,47 |
| C7 | 17,87 | 19,87 | 24,31 | 26,01 |
| C8 | 17,87 | 19,87 | 28,85 | 28,55 |

Position ISO 7816

Valeurs en mm



# Les différents contacts




SWP (Single Wire Protocol)

**Vcc: tension électrique (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**
**Vpp: utilisé dans les anciens modèles pour avoir une autre source d'alimentation**
**I/O: utilisé pour le transfert des données et des commandes entre la carte et le terminal. La communication est half-duplex.**


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

# Signification des contacts

- **Vcc : tension d'alimentation positive de la carte fournie par le terminal**
  **`Vcc=5V +- 0.5V`**
- **RST: commande de reset de la carte, fournie par le terminal**
  (tension électrique maximale = Vcc)

- **CLK: Clock, horloge fournie à la carte par le terminal**
  -rythme les échanges de données entre la carte et le terminal
  -Fréquence entre 1 MHz et 5 MHz

- **RFU n'ont pas besoin d'être présents physiquement (utilisés pour l'USB)**

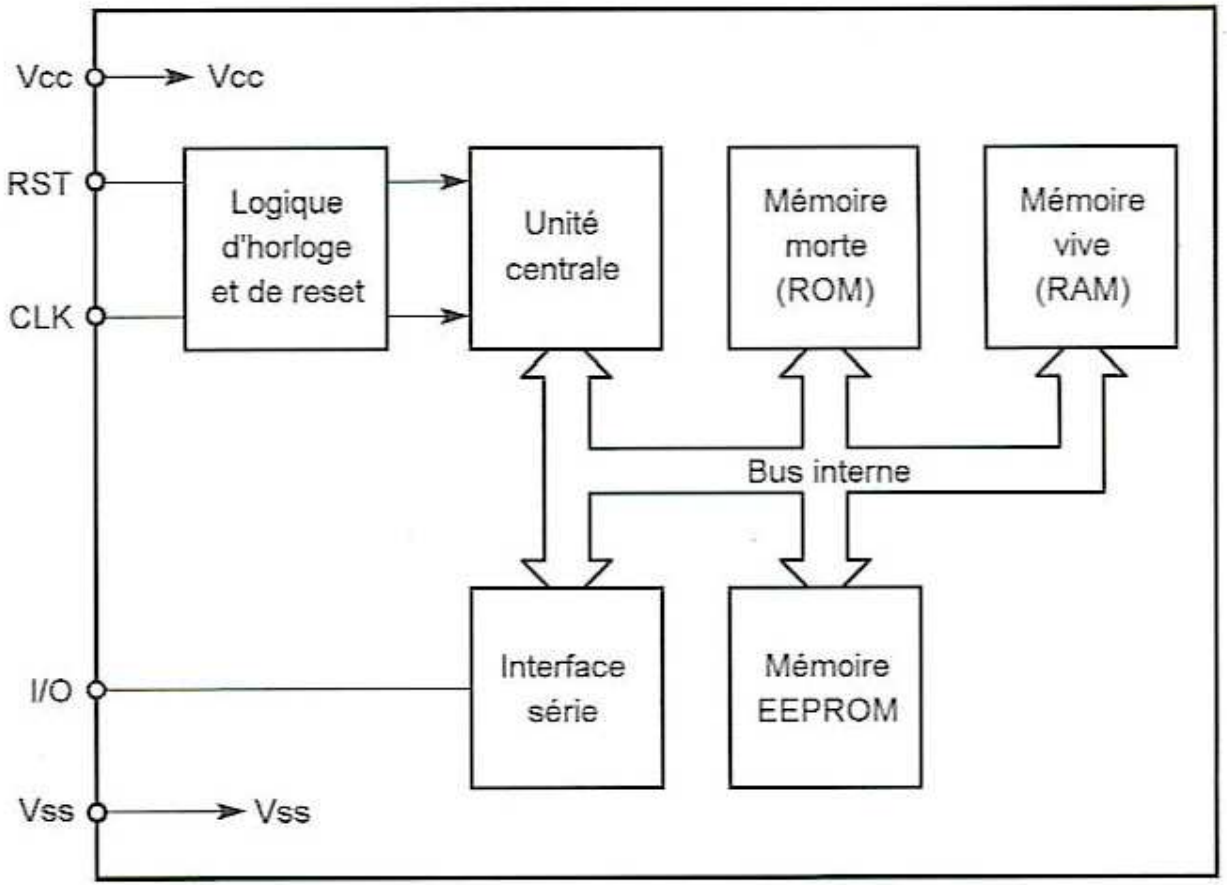
- **GND masse électrique de la carte**

**Vpp: utilisé aujourd'huipar SWP (Single Wire Protocol)**

- **I/O entrées/sorties des données (tension max = Vcc)**
  - ligne bidirectionnelle (carte ⇔ terminal)


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

# Synoptique interne d'une carte à circuit intégré






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

# Insertion de la carte dans un terminal

➢**Dans le terminal, il y a un circuit d'interface (IFD: InterFace Device):**

✓ Connexion de la carte (ICC) et activation de ses contacts par le circuit d'interface

✓ Reset de la carte

✓ Réponse au reset ou ATR (Answer to Reset) 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 (Answer to Reset)

➢**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.**

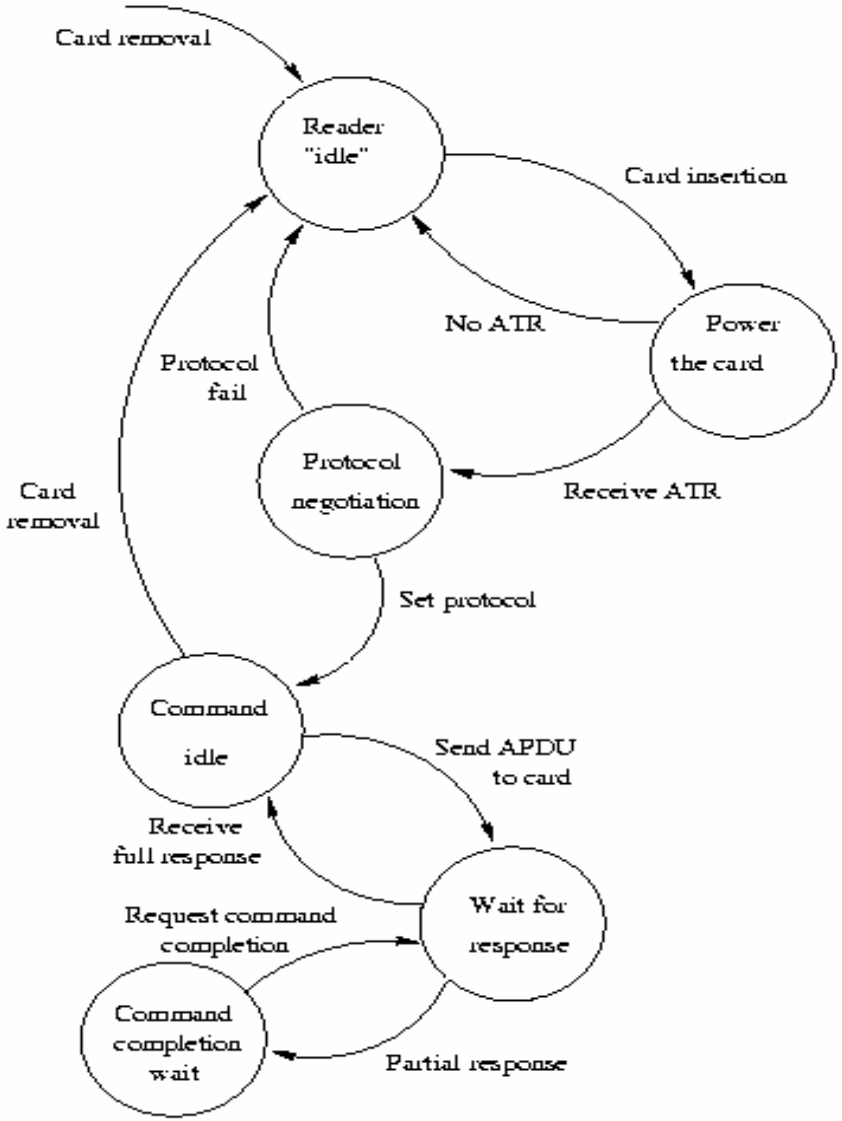
✓**Paramètres envoyés par la carte :**

- Le protocole de transport ;
- La vitesse de transmission des données ;
- etc.

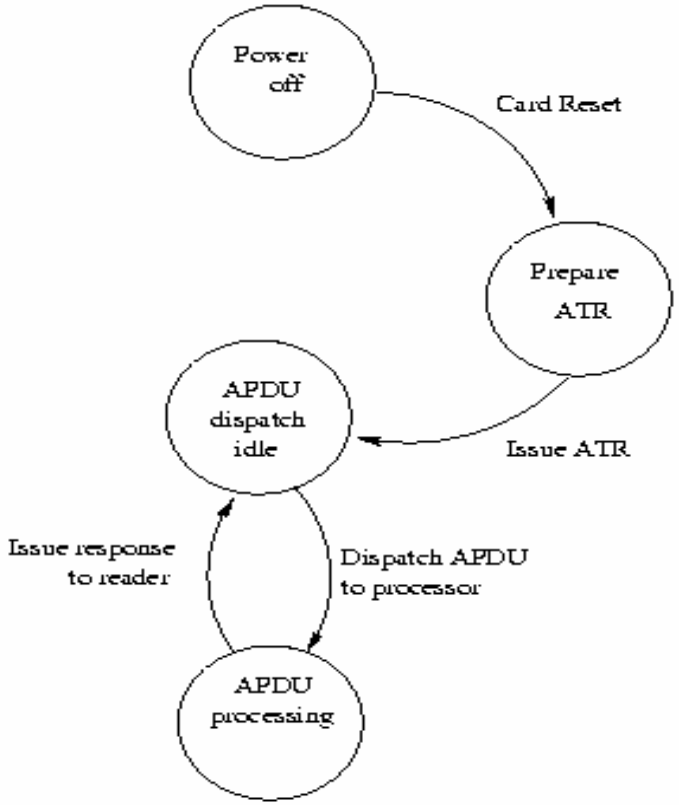


samia.bouzefrane@cnam.fr - CEDRIC ( CNAM) -

# Comportements de la carte et du terminal lors d'un Reset




**Reader State Diagram**




**Card State Diagram**

# Caractéristiques de l'ATR

- L'ATR est la réponse de la carte au reset du terminal
- 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 1$^{er}$ caractère
- Communication entre le lecteur et la carte via la ligne bidirectionnelle I/O

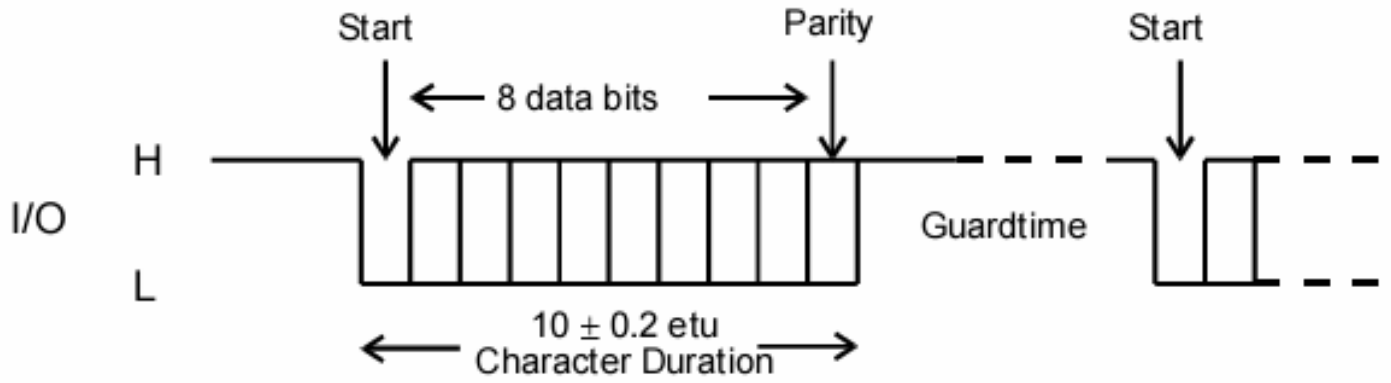

samia.bouzefrane@cnam.fr - CEDRIC ( CNAM) -

# Chronogramme de la réponse reset

- **Comm. Asynchrone : bit start + 8 bits de données + bit de parité paire + Temps de Garde (un ou plus bits Stop)**

- **L :niveau bas et H: niveau haut**

- **le délai entre 2 caractères est au moins de 12 etu et TG = 2 etu**

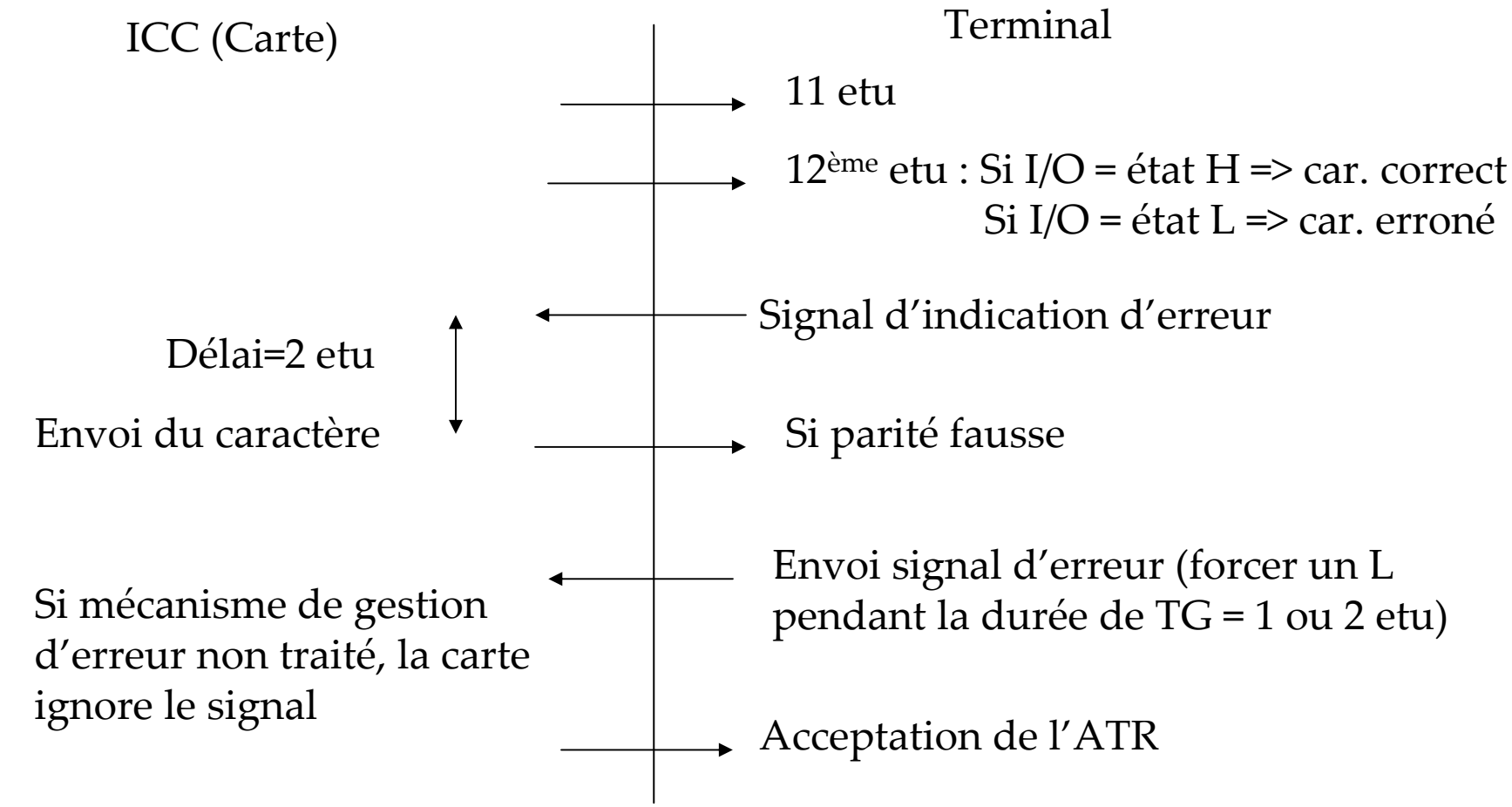





samia.bouzefrane@cnam.fr - CEDRIC ( CNAM) -

# Procédure de détection d'erreurs

- **Si protocole T=0 est utilisé :**






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

# Caractère initial de l'ATR

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

- TS peut prendre 2 valeurs : (HHLLLLLL)[1] ou (HHLHHHLL)[2]

- 1: convention inverse :
  - niveau bas L = « un » logique
  - niveau haut H = « zéro » logique
  - bit transmis en premier = bit 7 de poids fort
  - bit transmis en dernier=bit 0 de poids faible

  TS = 3F (en héxa)

- 2: convention directe :
  - niveau bas L = « 0 » logique
  - niveau haut H = « 1 » logique
  - bit transmis en premier = bit 0 de poids faible
  - bit transmis en dernier =bit 7 de poids fort

  TS = 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 ($b_8$ à $b_5$)**
  - **-Partie K ($b_1$ à $b_4$) facultative (n'est pas normalisée, caractères d'historique)**

Y1 K

| | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | |
|---|---|---|---|---|---|---|---|---|---|
| T=0 only | 0 | 1 | 1 | 0 | x | x | x | x | (=6x) |
| T=1 only | 1 | 1 | 1 | 0 | x | x | x | x | (=Ex) |

Présence ou non de $TA_1$

Présence ou non de $TB_1$

Présence ou non de $TC_1$

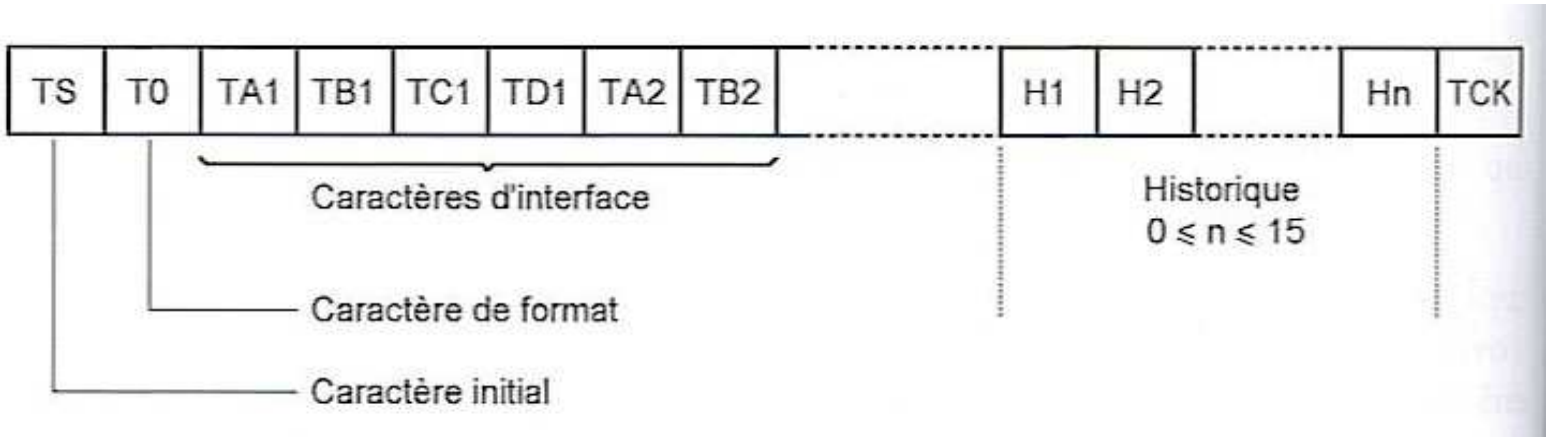
Présence ou non de $TD_1$



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

# Caractère de format (suite)

- **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 $TA_1$

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 $TA_1$ (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 $TA_1$
- Si $TA_1$ absent alors valeurs par défaut utilisées ( *D=1 et F=372*)



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

# Caractère $TB_1$ / $TC_1$

- **TB1 : non utilisé (valeur = 0)**

- **contient la valeur de la haute tension de programmation (Vpp) dans les anciennes cartes**

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

**Si $0 \leq N \leq 254$ (FE en Hexa), TG=N*etu**
**Si N=255 (FF en Hexa), TG = 11 etu si protocole T=1 et = 12 etu si protocole T=0**

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

**$TC_1$ demandé par la carte permet un TG supplémentaire uniquement dans le sens Lecteur -> Carte**


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

# Caractère $TD_1$

- Code le caractère $TA_2$, $TB_2$, $TC_2$ et $TD_2$ (bits poids forts)
- bits de poids faible (numéro du protocole utilisé T=1)
- TD1 est absent si protocole utilisé est T=0

Présence de
$TA_2$, $TB_2$, $TC_2$, $TD_2$ protocole

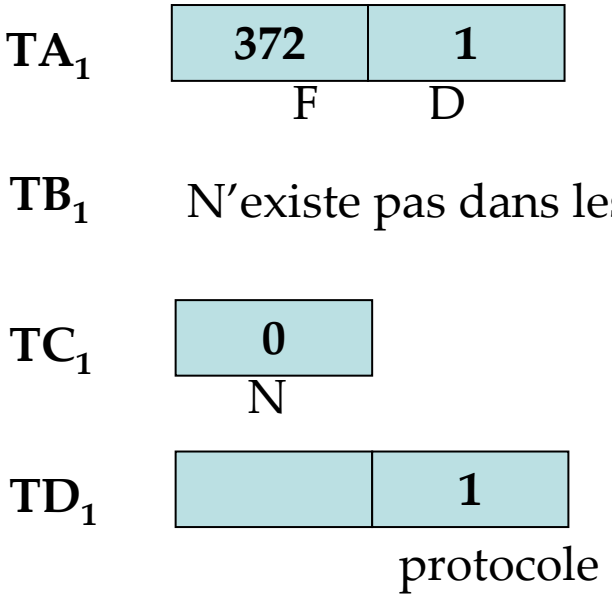
| | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|---|---|---|---|---|---|---|---|---|
| T=1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

=(81)



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) -

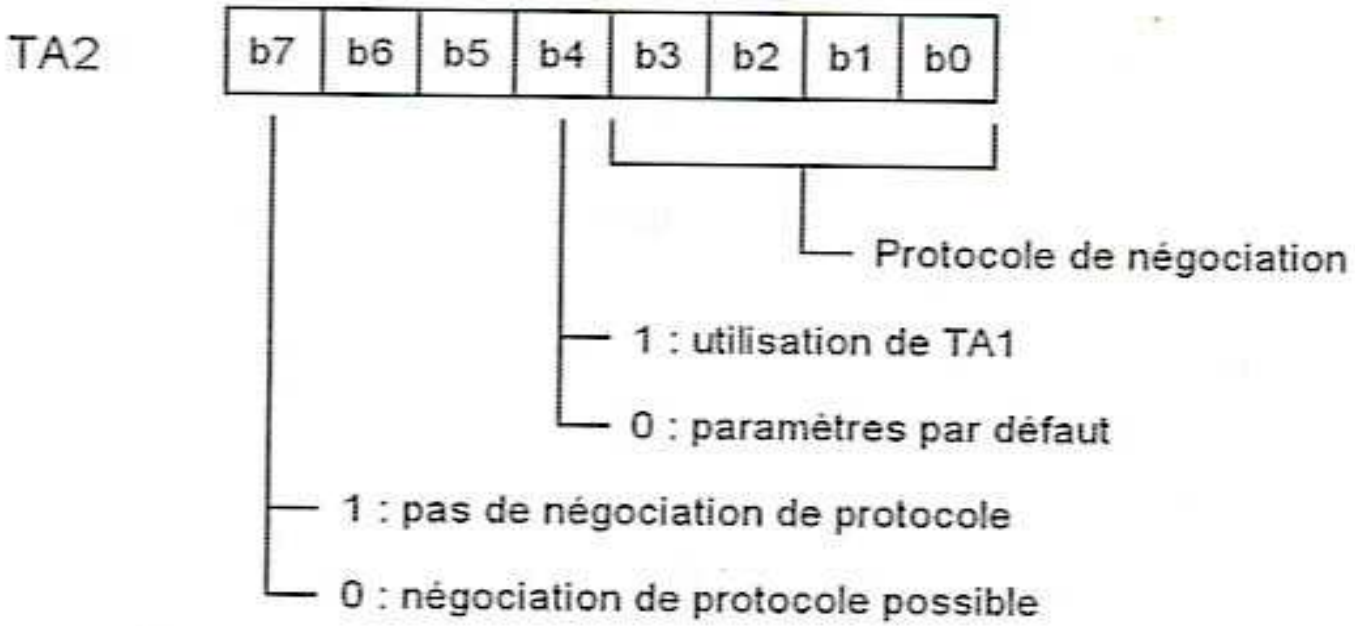
# Négociation de vitesse de dialogue

- 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 $TA_2$

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






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

# Caractères $TB_2$ et $TC_2$

- Le terminal rejette une ATR qui contient $TB_2$ (censée contenir Vpp)
- $TC_2$ est défini pour le protocole T=0
- $TC_2$ définit le temps qui sépare le bit start de deux caractères successifs émanant de l'ICC ou bien de l'ICC et du terminal (work waiting time)
- Le terminal rejette une ATR qui contient $TC_2$='00'
- Le terminal accepte une ATR qui contient $TC_2$='0A'
- Le terminal rejette une ATR qui contient toute autre valeur pour $TC_2$


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

# Caractères $TD_2$

- L'ATR ne doit pas contenir $TD_2$ si T=0 est utilisé
- L'ATR doit contenir $TD_2$ = '31' si T=1 est utilisé, indiquant que $TA_3$ et $TB_3$ sont présents et que le protocole T=1 doit être utilisé.

| | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|---|---|---|---|---|---|---|---|---|
| T=1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |


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

# Les protocoles de transmissionTPDU/APDU



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

# Protocoles de transport

- Basés sur les protocoles T=0 ou T=1 définis dans l'ISO 7816-3 et 4
- Différents niveaux :
  - ✓Couche physique (même couche pour les deux protocoles)
  - ✓Couche liaison de données (gestion d'erreurs, options spécifiques pour les deux protocoles)
  - ✓Couche de transport (terminal transport layer)
  - ✓Couche application


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

# Protocoles TPDU

- Il existe deux protocoles T=0 et T=1 (T=0 le plus utilisé)

- Protocole T=0 (TPDU : Transmission Protocol Data Unit)
  - est de type caractère
  -mode de fonctionnement de type commande/réponse
  -Le terminal est l'initiateur des échanges



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

# Les échanges

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

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

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



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) -

# C-APDU

| Case | Structure |
|---|---|
| 1 | CLA INS P1 P2 |
| 2 | CLA INS P1 P2 Le |
| 3 | CLA INS P1 P2 Lc Data |
| 4 | CLA INS P1 P2 Lc Data Le |



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<br>•SW1 (1 octet) et SW2 (1 octet): Status words (Mots d'état)—état de traitement par la carte | | |

| SW1 | SW2 | Meaning |
|---|---|---|
| '62' | '81' | Part of returned data may be corrupted |
| '67' | '00' | Length field incorrect |
| '6A' | '86' | P1 P2 ≠ '00' |
| '6F' | '00' | No precise diagnosis |



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

# Exemples de cartes

| Champ de la commande APDU | Valeurs |
|---|---|
| CLA | 00 = cartes Monéo (porte-monnaie en France), Mastercard, Visa |
| INS | 20 = présentation du code PIN,<br>40 = validation (ratification du code PIN)<br>B0 = Lecture<br>B2 = Lecture de record<br>D0 = Écriture<br>DC = Écriture de record<br>A4 = Sélection du répertoire (directory)<br>C0 = Demander une réponse (get an answer) |
| P1, P2 | paramètres contenant des adresses à lire |
| Lc | longueur prévue pour la réponse ou bien longueur de l'argument de l'instruction |
| Data | contient Lc octets (octets à écrire, PIN à vérifier, etc.) |


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

# Couche Application

| Case | Command Data | Response Data |
|---|---|---|
| 1 | Absent | Absent |
| 2 | Absent | Present |
| 3 | Present | Absent |
| 4 | Present | Present |



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

# Le protocole T=1 (ISO7816-3)



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

# Protocole T=1

- Protocole ambitieux
- Protocole peu utilisé
- Protocole plus proche du modèle OSI
- Échange de blocs structurés



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

# Structure d'un bloc

- Chaque bloc commence par un champ obligatoire
  - prologue field
  - données
  - champ de contrôle

-NAD = (adr du destinataire, adr émetteur)

-LEN: nb d'octets de données (tte la cde APDU)

-PCB: octet de contrôle ($b_7b_6$=11 si bloc supérieur, =00 si bloc d'infos, =10 si réception prête)

-LRC: résultat du OuX de tous les octets le précédant

| Prologue | | | Information | Épilogue |
|---|---|---|---|---|
| NAD | PCB | LEN | « Données » (APDU) | LRC |
| 1 octet | 1 octet | 1 octet | 0 à 254 octets | 1 octet |



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

# Book 2 : Security and Key Management



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

# Book 2

- Static Data Authentication
- Dynamic Data Authentication
- Cryptage du code PIN hors ligne
- Intégrité et confidentialité
- Mécanismes de sécurité : cryptage symétrique, asymétrique, signature numérique.
- Algorithmes cryptographiques : RSA, DES, SHA-1


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

# Acteurs du protocole EMV

- La banque du client : émetteur de la carte
- Le client : Carte bancaire
- Le TPE (Terminal de Paiement Electronique ou le DAB (Distributeur Automatique de Billets): marchand
- Une autorité de certification : CA



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

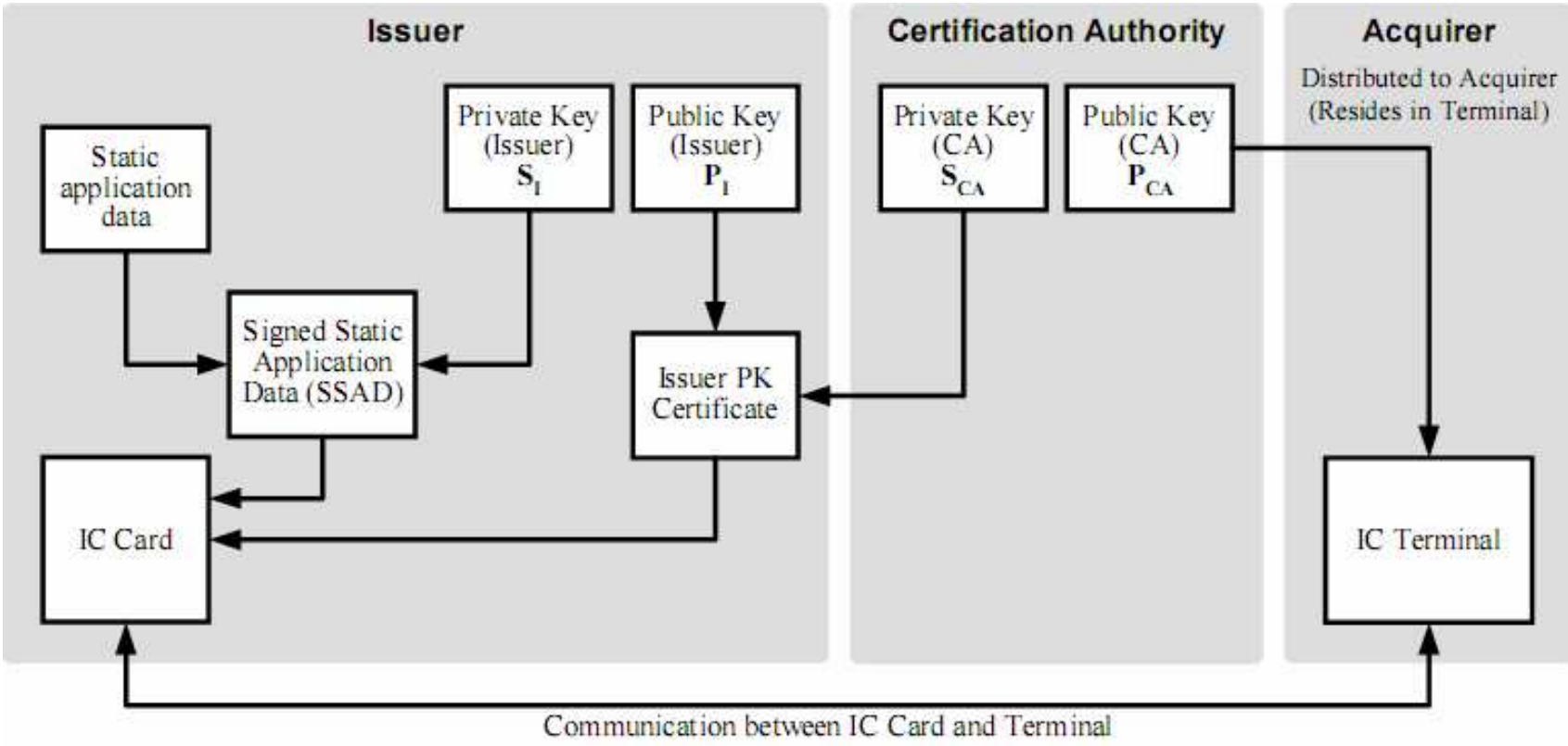
# Mécanismes d'authentification

- **Processus SDA : Static Data Authentication**
  **consiste pour le terminal à vérifier une donnée signée mise dans la carte durant sa personnalisation**

- **Processus DDA : Dynamic Data Authentication**
  **en plus d'un authentification statique, vérifie si la carte possède un secret délivré par l'émetteur de la carte**


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

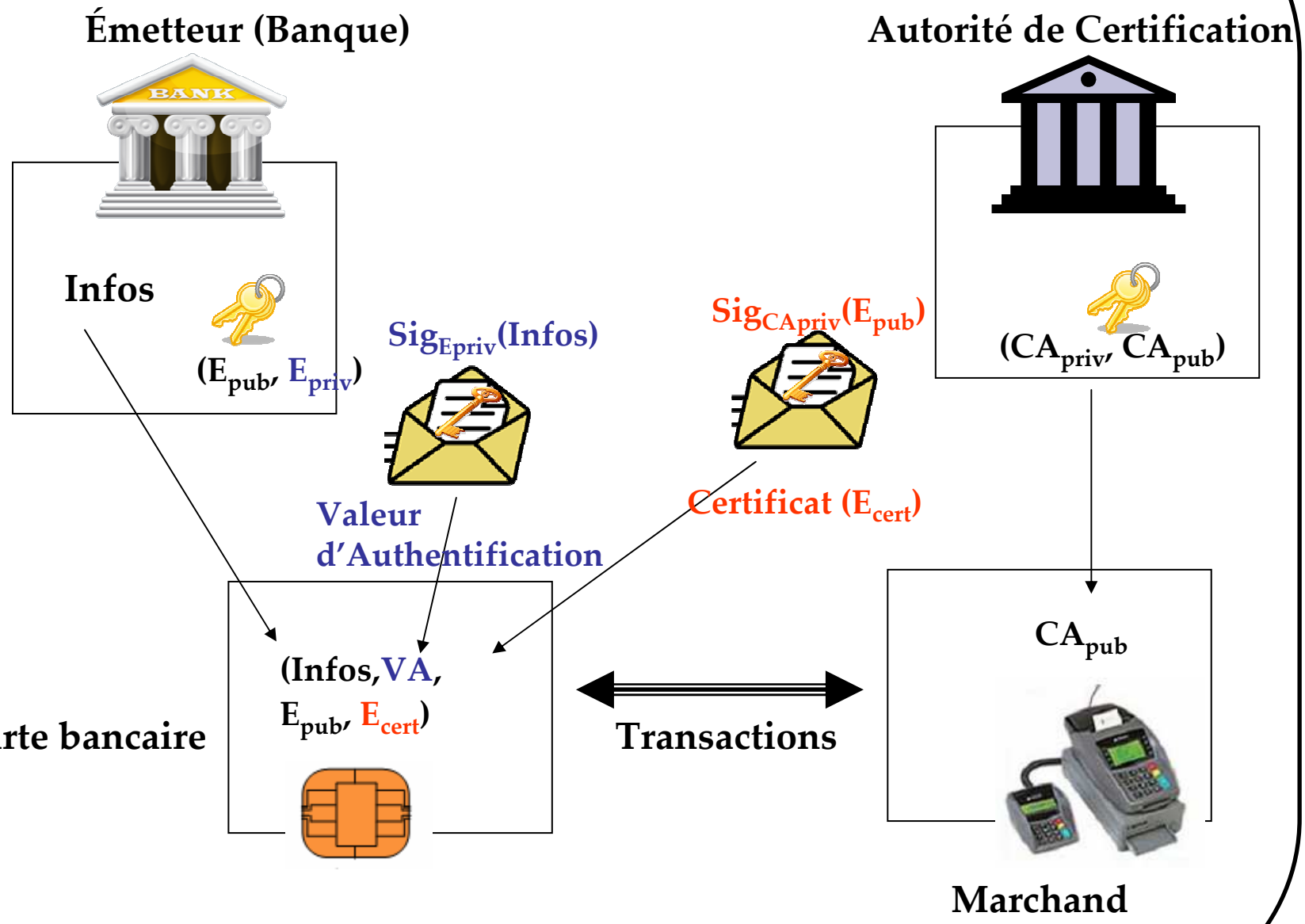
# SDA : Static Data Authentication






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

# Organisation des acteurs dans SDA






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

# SDA : à la personnalisation

➢ **Pendant la phase de personnalisation, la carte reçoit les informations suivantes:**

- **Le nom du porteur, le numéro de la carte ou encore la date limite de validité de celle-ci (notés `Information`).**
- **une valeur d'authentification (noté VA), signature RSA d'*`Informations`* générée avec la partie privée de la clé de l'émetteur (`VA=Sig`$_{\texttt{Epriv}}$`(Information)`)**
- **le certificat de l'émetteur ($E_{cert}$) contenant sa clé publique signée par une autorité de certification**
- **le code PIN transmis au porteur de cette carte.**



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

# Lors de l'utilisation

$VA = Sig_{Epriv}(Infos)$

$E_{cert} = Sig_{CApriv}(E_{pub})$

(Infos, VA, $E_{cert}$)

(Infos, VA, $E_{cert}$)

(Infos, VA, $E_{pub}$, $E_{cert}$)
Code PIN

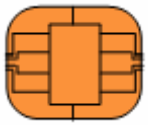
$RSA(E_{cert}, CA_{pub})=E_{pub}$

$CA_{pub}$

$RSA(VA, E_{pub})=Infos'$ ?= Infos

Demande du code PIN

Code PIN en clair



Carte bancaire

Marchand



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

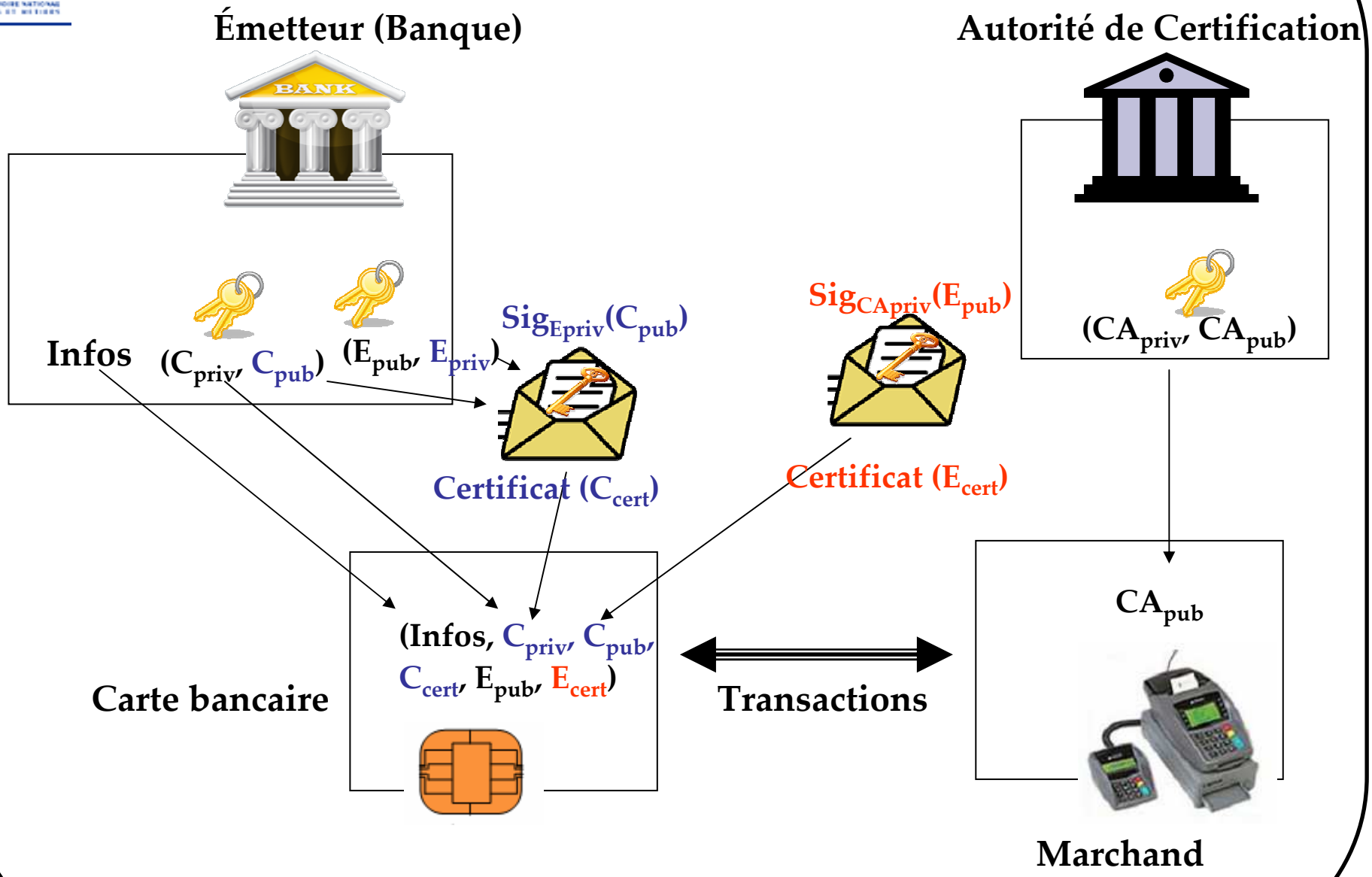
# SDA : à la l'utilisation

- Avant toute transaction :
  - la carte fournit au terminal `Informations`, le certificat $E_{cert}$ de la banque émettrice, ainsi que la valeur d'authentification `VA`
  - le terminal vérifie $E_{cert}$ avec la clé publique de l'autorité de certification ($CA_{pub}$) et vérifie `VA` avec la clé publique de la banque émettrice
  - le terminal demande à l'utilisateur le code PIN et le transmet (en clair) à la carte pour qu'elle le vérifie.



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

# Dynamic Data Authentication : DDA






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

# DDA : à la personnalisation

➢ **Pendant la phase de personnalisation, la carte reçoit les informations suivantes:**

- **Le nom du porteur, le numéro de la carte ou encore la date limite de validité de celle-ci (notés `Information`).**
- **une paire de clés RSA ($C_{pub}$, $C_{priv}$)**
- **un certificat ($C_{cert}$) contenant $C_{pub}$ signée par l'émetteur**
- **le certificat de l'émetteur ($E_{cert}$) contenant sa clé publique $E_{pub}$ signée par une autorité de certification**
- **le code PIN transmis au porteur de cette carte.**



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

# Lors de l'utilisation

$C_{cert} = Sig_{Epriv}(C_{pub})$

$E_{cert} = Sig_{CApriv}(E_{pub})$

(Infos, $C_{cert}$, $E_{cert}$)

$T_{alea}$

(Infos, $C_{pub}$, $C_{priv}$, $C_{cert}$, $E_{pub}$, $E_{cert}$)
Code PIN

$Res=Sig_{Cpriv}(C_{alea}, T_{alea}), C_{alea}$

(Infos, $C_{cert}$, $E_{cert}$)

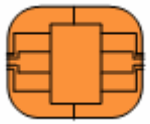
$CA_{pub}$

$RSA(E_{cert}, CA_{pub})=E_{pub}$

$RSA(C_{cert}, E_{pub})=C_{pub}$

$Décrypt(Res, C_{pub}) ?= C_{alea}, T_{alea}$

Demande du code PIN



Carte bancaire

$Crypt_{Cpub}$(Code PIN, alea1, alea2)

Marchand



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

# DDA : à la l'utilisation

➢ **Avant toute transaction :**

- la carte fournit au terminal `Informations`, le certificat $E_{cert}$ de la banque émettrice, et son certificat $C_{cert}$
- le terminal génère une valeur aléatoire $T_{alea}$ et l'envoie à la carte
- la carte génère une valeur aléatoire $C_{alea}$. Puis, elle signe $T_{alea}$ et $C_{alea}$ avec sa clé privée $C_{priv}$. Elle envoie le résultat de la signature et $C_{alea}$ au terminal.
- le terminal vérifie $E_{cert}$ avec $CA_{pub}$ et vérifie $C_{cert}$ avec $E_{pub}$. Puis, il vérifie la signature des aléas avec $C_{pub}$.
- le terminal demande à l'utilisateur le code PIN et le transmet (chiffré par $C_{pub}$) à la carte pour qu'elle le vérifie. Le code PIN est d'abord concaténé avec deux nouvelles valeurs aléatoires fournies par la carte et le terminal, afin d'éviter les attaques par rejeu.


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

# Mode de gestion des transactions

- La transaction est finalisée en ligne ou hors ligne, choix fait par la carte ou le terminal selon une politique de gestion de risques :
  - sélection aléatoire
  - validation en ligne pour *n* validations hors ligne
  - en fonction du montant de la transaction
  - en fonction du montant cumulé des transactions déjà effectuées hors ligne ou d'un plancher fixé par le marchand.


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

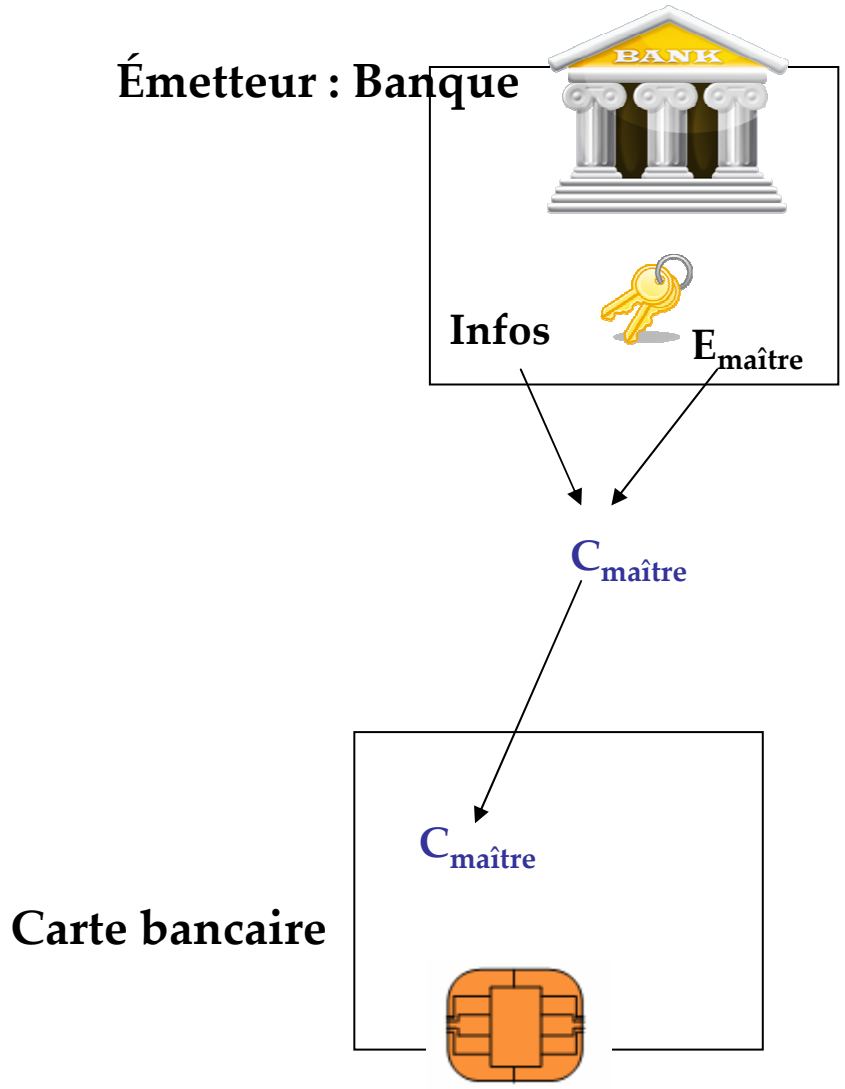
# Fonctionnement en ligne et hors ligne

- **Une clé secrète (clé 3DES de 112bits) est utilisée :**
  - **unique par transaction**
  - **notée $C_{trans}$ calculée à partir de $C_{maitre}$ et d'un compteur de transactions (*ATC*: Application Transaction Counter)**
  - **$C_{maitre}$ est une clé de la carte générée par la banque émettrice à partir d'une clé maître de la banque $E_{maitre}$ et des informations bancaires**
  - **$C_{maitre}$ est mise dans la carte lors de la personnalisation**
  - ***ATC* est un compteur sur deux octets géré par la carte et incrémenté à chaque transaction.**



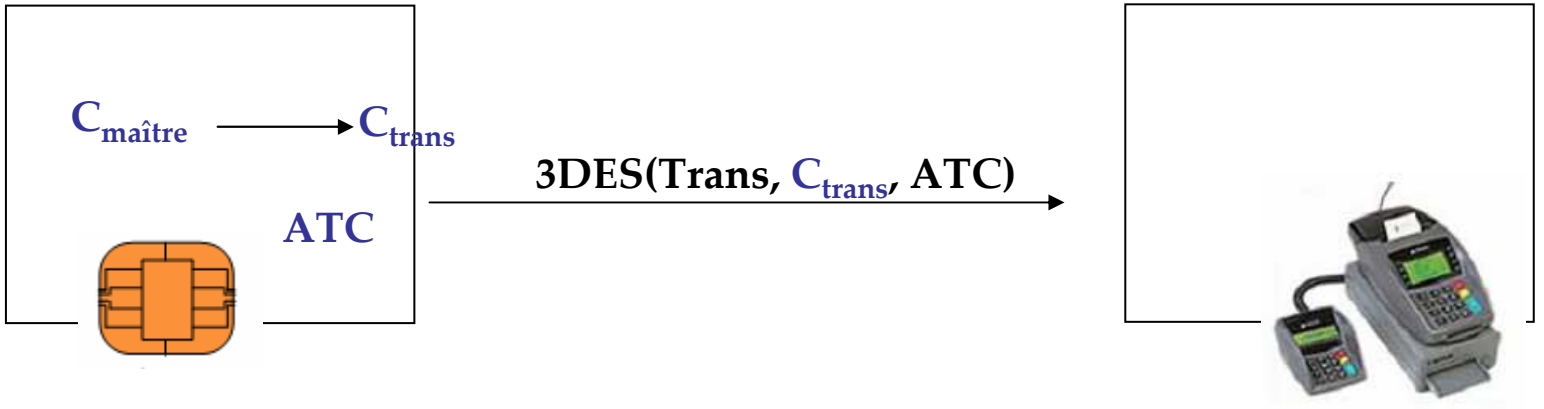
samia.bouzefrane@cnam.fr - CEDRIC ( CNAM) -

# Transaction: personnalisation



# Transaction: utilisation

**Dérivation d'une clé unique par transaction:**




**Carte bancaire**

**Marchand**



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

# Fonctionnement hors ligne

- Le terminal envoie à la carte les détails de la transaction

- La carte produit alors un certificat de transaction **TC** en signant ses données (algorithme DES CBC-MAC) à l'aide de $C_{trans}$.

- Le terminal ne peut pas vérifier **TC** mais le garde pour validation ultérieure auprès de sa banque.



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

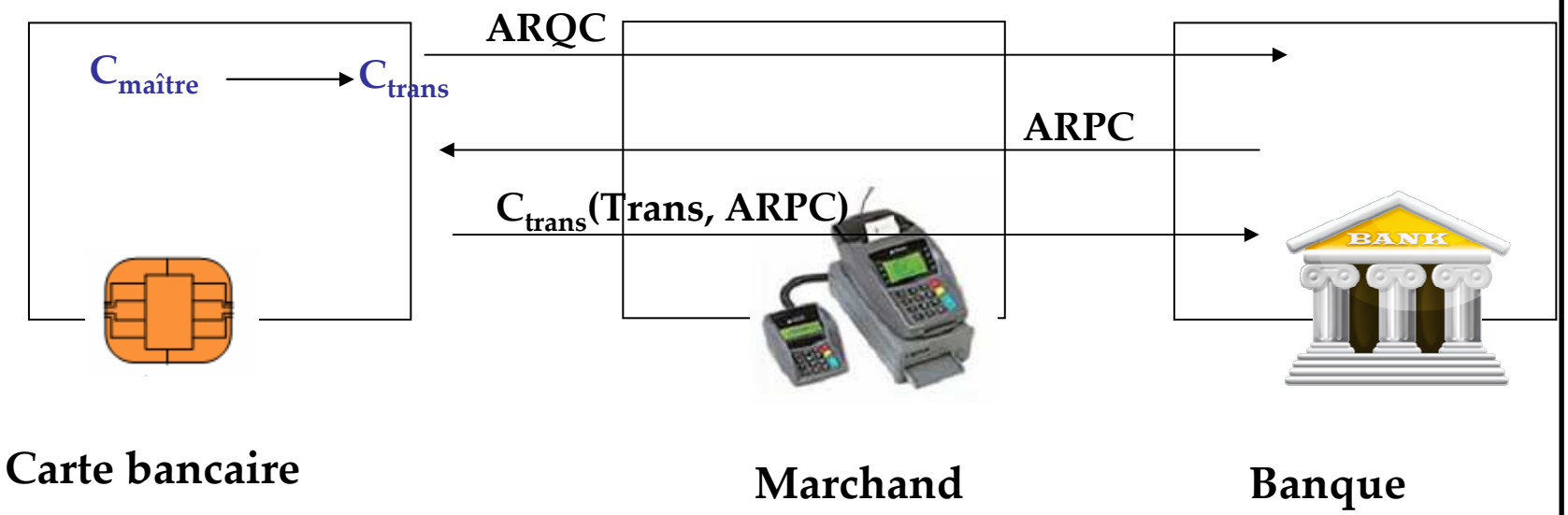
# Authentification CDA

- CDA : Combined Data Authentication, variante de DDA
- utilise **TC**
- inclut **TC** dans le bloc de données signé par la carte
- Si la transaction doit être approuvée en ligne, le terminal envoie à la banque émettrice le cryptogramme généré par la carte (**ARQC** Authorization ReQuest Cryptogram).
- La banque le vérifie et génère un cryptogramme réponse (**ARPC** Authorization ResPonse Cryptogramm) envoyé à la carte via le terminal
- Le terminal redemande alors à la carte de lui générer un certifcat de transaction qui inclut l'autorisation de la banque.


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

# Transaction en ligne

**Dérivation d'une clé unique par transaction:**



# Book 3 : Application specifications



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

# Book III : Spécification de l'application

## Partie 1: Les données et les commandes

## Partie 2: Flux transactionnel



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

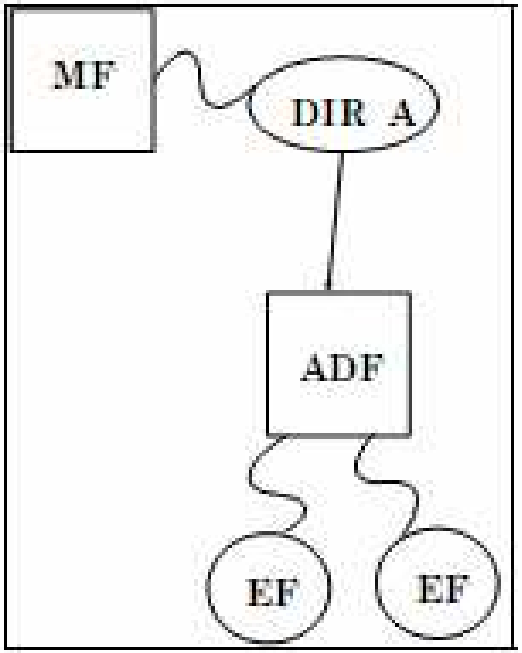
# Structure des fichiers

- Les fichiers d'un ICC sont vus du terminal comme une structure arborescente. Chaque branche de l'arbre est :
  - ✓ Un ADF (Application Definition File)
    - ✓Un ADF est un point d'entrée pour un ou plusieurs AEF
    - ✓AEF (Application Elementary Files) : fichiers élémentaires
  - ✓ ou un DDF (Directory Definition File)
    - ✓Un DDF est un point d'entrée à d'autres ADF ou DDF
- Un ADF est associé à chaque application


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

# Exemple simple d'arborescence

- **MF (Master File): fichier maître, c'est le répertoire racine identifié par '3F 00'**



# Identification et nommage des fichiers

- **Identification par nom**
  - **un DDF ou un ADF peut être référencé à l'aide d'un nom.**
  - **Le nom d'un ADF correspond à l'AID ou bien contient l'AID comme début du nom**
  - **Chaque nom doit être unique au sein d'une carte**

- **Identification par SFI ( Short File Identifier)**
  - **Les SFI sont utilisés pour sélectionner des AEF.**
  - **Chaque AEF d'une application est identifié par un SFI à 5 bits ayant des valeurs entre 1 et 30.**
  - **Un SFI doit être unique dans une application**


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

# READ RECORD

- Lit les enregistrements d'un fichier à structure linéaire (basé sur les enregistrements)
- L'ICC retourne l'enregistrement

| Code | Value |
|---|---|
| CLA | '00' |
| INS | 'B2' |
| P1 | Record number |
| P2 | Reference control parameter (see Table 39) |
| Lc | Not present |
| Data | Not present |
| Le | '00' |

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| x | x | x | x | x | | | | SFI |
| | | | | | 1 | 0 | 0 | P1 is a record number |

Table 39: READ RECORD Command Reference Control Parameter



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

# PSE (Payment System Environment)

- **Un système de paiement comprend :**

  **-Un ensemble de fichiers dans l'ICC**

  **-Des données au niveau du terminal fournies par le marchand**

  **- Un protocole d'application compris par l'ICC et le terminal**

  **- Les applications sont identifiées par AIDs de manière unique conformément à l'ISO7816-5**



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

# Identification d'applications de paiement

- **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 : numéro unique par fournisseur d'application**

| 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) -

# Interopérabilité

- **Le terminal doit être capable de travailler avec tous les ICC supportant des PSE**
- **Conformité avec la norme ISO**
- **Les ICCs doivent être capables de supporter des applications multiples, pas uniquement des applications de paiement**


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

# Commandes conformes à l'ISO 7816

- SELECT : sélection de l'application (spécifié dans Book 1)
- READ RECORD
- VERIFY : vérification hors ligne du code PIN (crypté ou en clair)
- INTERNAL AUTHENTICATE
- EXTERNAL AUTHENTICATE
-GET CHALLENGE
…

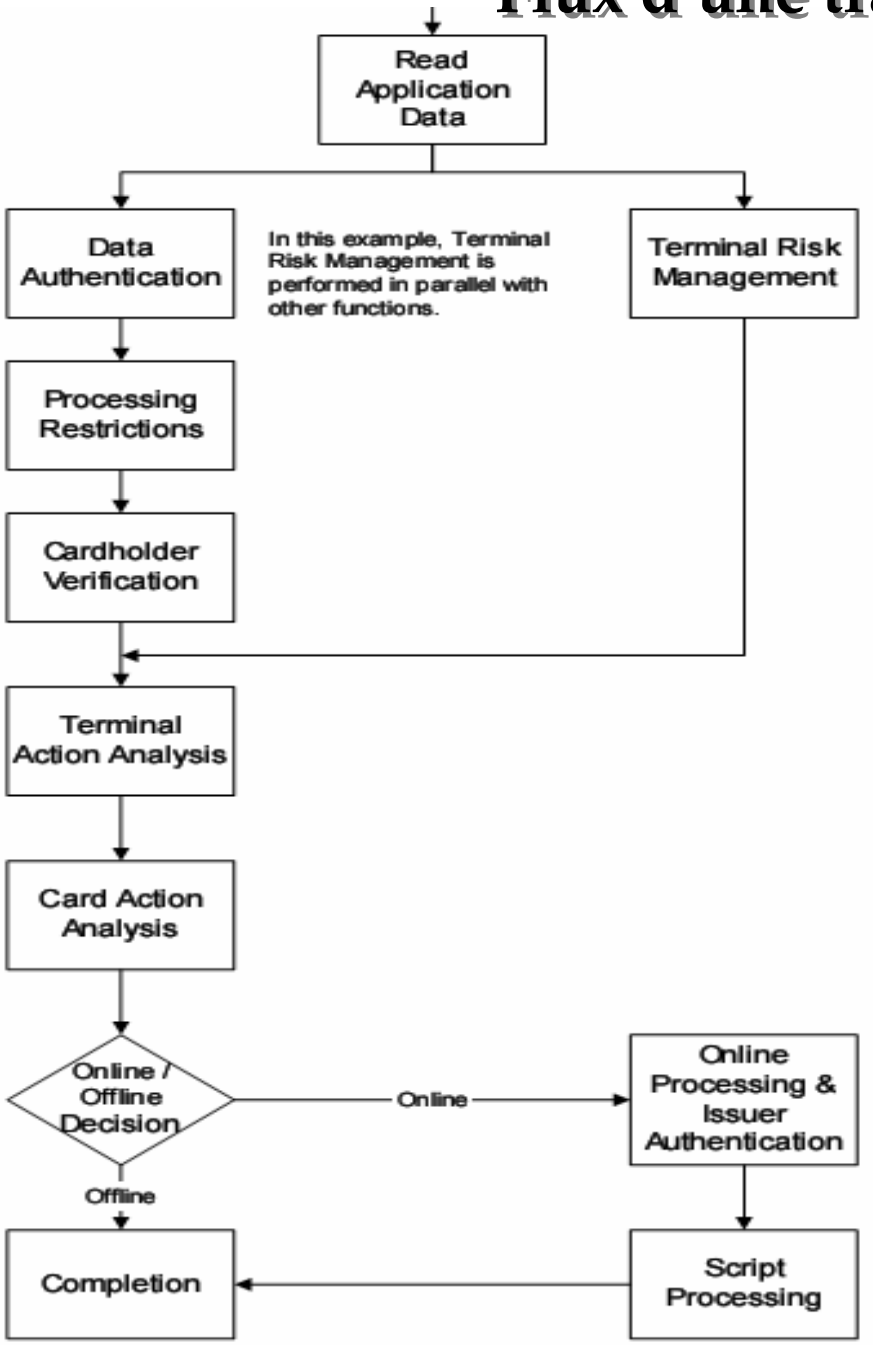

samia.bouzefrane@cnam.fr - CEDRIC ( CNAM) -

# Commandes spécifiques à l'EMV

- GET PROCESSING OPTION :
- GENERATE AC : produit un cryptogramme
- APPLICATION BLOCK : bloque l'application courante
- APPLICATION UNBLOCK : débloque une application bloquée
- CARD BLOCK : bloque la carte
- PIN CHANGE/UNBLOCK: change ou débloque le code PIN


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

# Flux d'une transaction






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

# Application Selection

- Le terminal choisit l'application en sélectionnant l'AID de l'appli (MasterCard, Visa, etc.)
- L'ADF est sélectionné
- La carte retourne le FCI (File Control Information) de l'ADF


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

# Initiate Application Processing

- Informe l'ICC que le traitement d'une nouvelle transaction va commencer
- Opération effectuée après la sélection de l'application
- Obtient de la carte le profile d'échange(AIP: Application Interchange Profile) et la liste des fichiers à utiliser durant la transaction : SDA ou DDA supporté, vérification du détenteur de la carte, authentification de l'émetteur, etc.


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

# Read Application Data

- Le terminal lit les données contenues dans les fichiers de la carte et utilise les données de la carte pour vérifier l'authentification SDA ou DDA

- Le terminal utilise Read Record

- Opération effectuée après l'opération Initiate Application Processing



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

# Processing restrictions

- **Vérification :**

  **- du numéro de version de l'application**

  **- de l'Application Usage Control**

  **- des dates d'expiration de l'application**



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

# Application Usage Control

| If: | and if Issuer Country Code: | then the following bit must be set to 1 in Application Usage Control: |
|---|---|---|
| Transaction Type indicates cash transaction | matches Terminal Country Code | 'Valid for domestic cash transactions' |
| | does not match Terminal Country Code | 'Valid for international cash transactions' |
| Transaction Type indicates purchase of goods | matches Terminal Country Code | 'Valid for domestic goods' |
| | does not match Terminal Country Code | 'Valid for international goods' |
| Transaction Type indicates purchase of services | matches Terminal Country Code | 'Valid for domestic services' |
| | does not match Terminal Country Code | 'Valid for international services' |
| transaction has a cashback amount | matches Terminal Country Code | 'Domestic cashback allowed' |
| | does not match Terminal Country Code | 'International cashback allowed' |



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

# Cardholder Verification

- **Vérification du détenteur de la carte**

- **La carte doit être capable de supporter au moins une méthode de vérification de détenteur de carte (CVM: Cardholder Verification Method). Ceci doit être spécifié dans le profile d'échange envoyé par la carte. Le terminal doit utiliser cette méthode.**


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

# Codes CVM

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | | | | | | | | RFU |
| | 0 | | | | | | | Fail cardholder verification if this CVM is unsuccessful |
| | 1 | | | | | | | Apply succeeding CV Rule if this CVM is unsuccessful |
| | | 0 | 0 | 0 | 0 | 0 | 0 | Fail CVM processing |
| | | 0 | 0 | 0 | 0 | 0 | 1 | Plaintext PIN verification performed by ICC |
| | | 0 | 0 | 0 | 0 | 1 | 0 | Enciphered PIN verified online |
| | | 0 | 0 | 0 | 0 | 1 | 1 | Plaintext PIN verification performed by ICC and signature (paper) |
| | | 0 | 0 | 0 | 1 | 0 | 0 | Enciphered PIN verification performed by ICC |
| | | 0 | 0 | 0 | 1 | 0 | 1 | Enciphered PIN verification performed by ICC and signature (paper) |
| | | 0 | x | x | x | x | x | Values in the range 000110-011101 reserved for future use by this specification |
| | | 0 | 1 | 1 | 1 | 1 | 0 | Signature (paper) |
| | | 0 | 1 | 1 | 1 | 1 | 1 | No CVM required |
| | | 1 | 0 | x | x | x | x | Values in the range 100000-101111 reserved for use by the individual payment systems |
| | | 1 | 1 | x | x | x | x | Values in the range 110000-111110 reserved for use by the issuer |
| | | 1 | 1 | 1 | 1 | 1 | 1 | This value is not available for use |



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

# PIN Verification

- La vérification du PIN

  - peut se faire en ligne ou hors ligne selon les valeurs de CVM
  - peut nécessiter le chiffrement du PIN
  - peut être complétée par une signature manuelle

- VERIFY PIN : vérification du code PIN (crypté ou non) hors ligne

- GET CHALLENGE: le terminal demande un nombre aléatoire (nb) à la carte



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

# Terminal Risk Management

- **Mécanismes utilisées pour éviter la fraude :**

  **- floor limit checking :vérification d'informations relatives à la transaction sur le terminal (numéro de compte, montant de la transaction, date de la transaction, etc.)**
  **- velocity checking : vérifier que les transactions effectuées hors ligne seront complétées en ligne.**
  **- algorithmes de gestion des risques propres à l'émetteur de la carte**


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

# Card Action Analysis

➢**Comme conséquence à la gestion des risques :**

**- la carte peut accepter une transaction hors ligne en générant un certificat de transaction TC.**

**- la carte peut demander une autorisation en ligne en générant ARQC.**

**- la carte peut décider de rejeter la transaction.**



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

# Online Processing

- **Online Processing : sert à s'assurer que l'émetteur de la carte peut réviser, autoriser ou rejeter les transactions.**

- **EXTERNAL AUTHENTICATE : le terminal envoie les données d'authentification de la banque**

- **La carte vérifie les données d'authentification et génère un cryptogramme.**



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

# Script Processing

- **Script Processing : ne fait pas partie de l'application**
- **Ensemble de commandes adressées à la carte en mode administrateur :**

  **- PIN CHANGE/ UNBLOCK**
  **- APPLICATION BLOCK/UNBLOCK**
  **- CARD BLOCK.**


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

# Book 4

- Besoins fonctionnels et caractéristiques physiques
- Gestion des données et du logiciel
- Interfaces utilisées



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

# Sur Internet

- L'utilisation des 16 chiffres visibles de la carte n'est pas un protocole de paiement sûr.
- Ce numéro à 16 chiffres n'est plus imprimé sur les facturettes
- 9 chiffres sont encore inscrits sur les facturettes et correspondent à peu près à l'aléa choisi par la banque. => possibilité de reconstituer le numéro entier
- En 2001, un cryptogramme a été rajouté et imprimé uniquement sur la carte, appelé CVV (Card Verification Value) chez Visa et CVC (Card Validation Code) chez MasterCard
- Ce code est généré par la banque à partir des informations bancaires du client et de données secrètes de la banque
- Ce code ne peut être reconstruit car l'algorithme est secret
- Depuis 2004, le cryptogramme doit être demandé par tout site marchand en plus du numéro de la carte afin de valider toute transaction à distance auprès de la banque émettrice.
- Ce numéro n'est écrit nulle part sauf sur la carte.


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

# Conclusion

- L'authentification DDA n'est pas obligatoire et
- DDA est plus robuste mais plus chère
- En France, la majorité des cartes aujourd'hui supportent DDA

- L'authentification SDA :
  - Code PIN envoyé en clair
  - Clé RSA de 1984 bits mais la donnée d'authentification peut être lue sans présentation de code

- Aujourd'hui, il manque des liens entre l'authentification, la vérification du code PIN et la génération de TC : les requêtes envoyées par le terminal peuvent être interceptées en forgeant des réponses à envoyer

- Nouvelle tendance de paiement : paiement sans contact (ISO 14443) => nouveaux systèmes, nouveaux protocoles et nouvelles failles …


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

# Bibliographie


1. Technology for smart cards: architecture and programmer's guide, Zhiqun Chen, Addison Wesley, sept. 2000

2. Les Cartes à puce: théorie et mise en œuvre, Christian Tavernier, 2ème édition, Ed. Dunod, 2007.

3. Normes EMV : http://www.emvco.com

4. Cours sur la carte à puce et la norme EMV par Pierre Paradinas (CNAM)

5. Magazine MISCH, Hors Série, Cartes à puce : découvrez leurs fonctionnalités et et leurs limites, paru en novembre 2008.

6. Magazine Linux, Hors Série, Cartes à puce, paru en octobre 2008.




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