Cartes à Puce (smart cards / IC Cards) et identifiants radiofréquences (RFID tags)

Yves ROUDIER

Historique

- 1974 : Dépots de brevets par Roland Moreno sur un objet portable à mémoire – fonde Innovatron – mis en contact avec Bull – Jürgen Dethloff dépose quasi simultanément des brevets sur les carte IC sur lesquels il travaille depuis quelques années.
- 1978 : M. Ugon (Bull CP8) invente la carte à microprocesseur, le Microprocesseur Auto-programmable Monolithique (M.A.M / SPOM en anglais)
- 1981 : Début de la normalisation AFNOR
- 1982 : Prototypes de publiphones à carte
- 1983 : Lancement de la «télécarte» par la D.G.T.

  Début de la normalisation ISO

  Décodeur Canal+ avec une carte mémoire

Historique

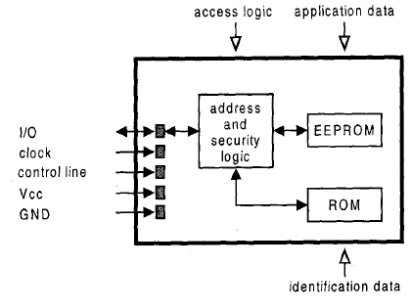
- 1984 : Adoption de la Carte Bleue (technologie Bull CP8)
  Création du groupement des cartes bancaires
- 1984 : Système d'exploitation B0 (cartes françaises)
- 1987 : Téléphonie mobile (GSM) avec carte SIM
- 1988 : introduction des standards ISO 7816
- Depuis 1992 : Essor des applications
  - Toutes les CB en France ont une puce
  - Cartes santé (Sesame Vitale)
  - Porte-monnaies électroniques (Proton)
  - Premières Javacard (1996)
  - Cartes .Net (2005)
- 1997 : EMV, standard financier international (Eurocard, MasterCard, Visa)
- 1999 : Lancement de Moneo
- 2002 : 400 Millions de cartes bancaires
  Carte à puce sonore

La carte et ses caractéristiques techniques

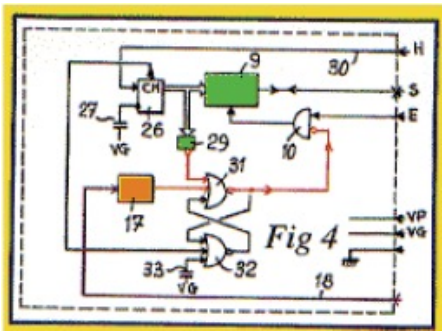
- carte à puce, carte à circuit intégré, IC card, smart card
- Principales caractéristiques:
  - objet portable, qui loge des données et/ou des procédures.
  - objet sécurisé
  - difficile de lire les données stockées dans les mémoires de la puce, clés protégées
  - Code exécuté dans un espace de confiance
  - objet de faible prix mais personnalisable pour des centaines de millions d'exemplaires.
    - 1-5$ pour les SPOM
    - 0,1-0,5$ pour les cartes magnétiques
  - ne peut fonctionner seule, nécessite
    - un CAD (*Card Acceptance Device) qui lui délivre de l'énergie* (en général un lecteur de cartes)
    - *une horloge (base de temps)*
    - *un lien de communication*

La carte et ses caractéristiques techniques

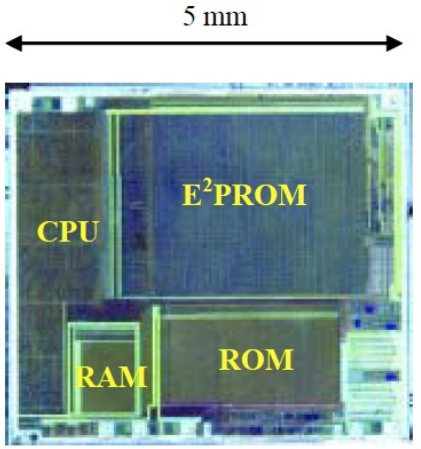
- Carte à mémoire :
  - Simple mémoire (lecture / écriture) (EPROM / EEPROM)
  - Non standardisé



- Carte à logique cablée :
  - La carte comporte un dispositif « câblé » de protection des données procurant un certain niveau de sécurité
  - Electronique dédiée reliant pins d'entrée et sortie
  - Non standardisé

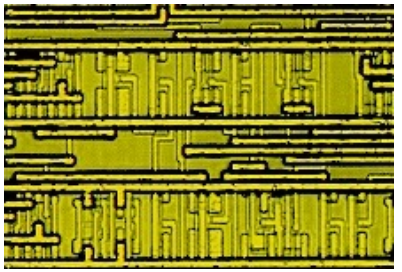


- Carte à microprocesseur (SPOM/MAM) :
  - Mémoire + processeur → programmable
  - Algorithmes de sécurité (ex: DES, RSA)
  - Normes ISO 7816
  - Carte à contacts et sans contacts
  - 1ère implémentation Bull CP8: 36o de RAM, 1 Ko EPROM, 1,6 Ko ROM

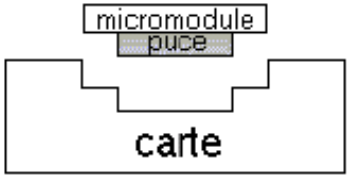


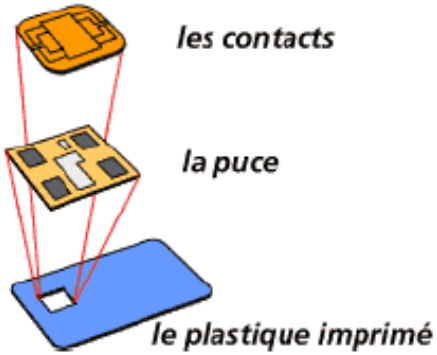
Composition de la carte à puce

- La puce électronique
  - Un micro-circuit (circuit intégré) construit à partir d'une galette de silicium
- Le micromodule
  - Très mince circuit imprimé logé dans l'épaisseur de la carte qui accueille les contacts(visibles) du connecteur sur une face et la puce (cachée sous les contacts du micromodule) sur l'autre
- La carte plastique
  - Deux principaux types de plastique sont utilisés
    - Le PVC non recyclable mais embossable
    - L'ABS non embossable mais recyclable



Détail d'un circuit intégré





Architectures matérielles

- CPU : 8, 16 & 32 bits,
  - Coeur 8051, AVR, ARM, MIPS, propriétaire
- Mémoires :
  - RAM : 128o à 8/(**16+16)ko**
  - NVM (EEPROM/Flash) : **768 ko + user page 256 ko**
  - ROM : 256/512 ko
- Co-processor
- Java Card : exécution directe de Byte Code Java Card Technology 2.2

Mémoires

- MMU :
  - User Flash 768ko + 256 ko User Page Flash,
  - Organisée en secteur
  - User Flash : 12*64 ko (sous secteur de 8 ko)
    - Effacement 1.5 s, programmation de mot de 32-bit 100 µs
  - User Page Flash : 128 * 2 ko
    - Effacement sous secteur : 50 ms, programmation de mot de 32-bit 200 µs
    - 32-bit word Erase in 2 ms typical3 V TO 5.5 V SUPPLY VOLTAGE
  - La Ram user peut servir de “page” à des secteurs de la Flash

Accès aux mémoires

- Le chargement du code peut être sécurisé
  - chargement chiffré
  - déchiffrement dans la carte
- Un MPU contrôle :
  - 1 accès code et 1 accès data par BUS séparé,
  - Pare feu entre application,
  - Accès aux périphériques (I/O, générateur de nombre aléatoire, timer,...)

Carte à puce : les intervenants

- *Fondeurs, fabricants de puces (ICs) et systèmes d'exploitation*
  - Conçoivent et fabriquent le matériel (puces de silicium)
  - Ex: STMicroélectronics, Siemens, Hitachi, Motorola, Renesas, Atmel, Philips, etc.
- *Encarteurs, fabricants de cartes*
  - fabriquent la carte proprement dite
  - intègrent la puce dans une carte plastique ou un autre facteur de forme
  - Ex: Gemalto, Oberthur, G&D
- *Fabricants de lecteurs*
  - Compléments indispensables des fabricants de cartes
  - terminaux de paiement électronique, DAB, téléphone GSM, etc
  - Ex: Ingénico, Dassault, Siemens
- *Développeurs, SSII, VARS (Value Added Resellers)*
  - Réalisent le système d'exploitation
  - Réalisent les logiciels (applets) qui s'exécutent dans la carte à puce elle même.
  - Ex: SSII : ATOS, Steria, Expérian ; VARS : Berger-Levrault, Horanet, Trusted Logic, Aspect Software
- *Émetteurs*
  - Sont responsables des fonctionnalités de la carte, des applications acceptées, etc.
  - Ex: VISA, MarsterCard, gouvernements, communes, …
- *Opérateurs*
  - Déploient la carte
  - Intègrent la carte dans leur système d'information
  - Ex: Orange, GIE Carte Bancaire …

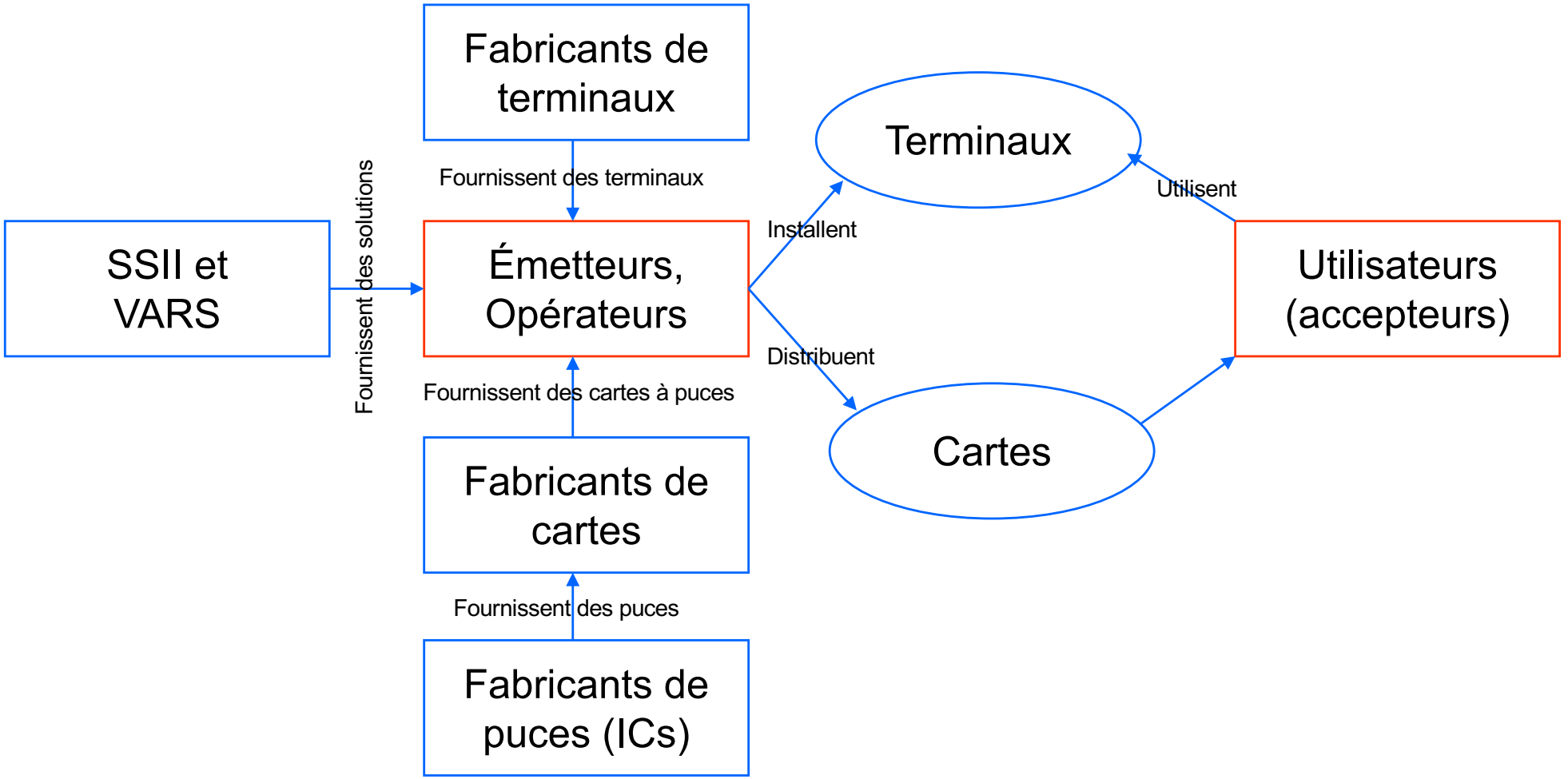
Carte à puce : les intervenants

- Quelques fondeurs:
  - Gemalto
    - fusion de Gemplus et Axalto
    - lui-même fusion de Schlumberger et Bull CP8)
    - Plus de 50% du marché
  - Oberthur
    - 20% du marché
  - Giesecke & Devrient

Origine des intervenants

- Silicium
- Impression fiduciaire (G&D)
- Société de service (Sligos racheté par Schlumberger/Axalto)
- Grand de l'informatique (Bull, Sun, Microsoft),
- Opérateur (Chine)

Organisation des acteurs



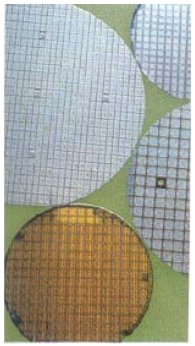
Cycle de vie d'une carte à puce

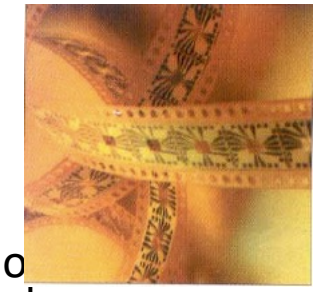
- La vie d'une carte à puce est constituée de 2 phases
  - Phase amont :
    - développement du système d'exploitation
    - conception de la puce
  - Phase de création :
    - Fabrication
    - Encartage
    - initialisation
  - Phase de circulation :
    - Personnalisation
    - Distribution
    - utilisation et gestion du parc
    - mort

Cycle de vie : phase amont

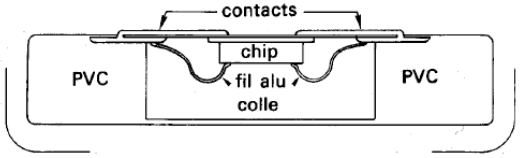
- Phase amont
  - Développement de l'applicatif
    - développement du système d’exploitation de la carte à puce
    - spécification des informations nécessaires à la pré-personnalisation
  - Conception de la puce
    - A partir du schéma de conception de la puce, des logiciels dédiés et de l'applicatif, le concepteur dessine la puce
    - il réalise la "database construction" qui va servir à la fabrication du photomasque de la puce

Cycle de vie : phase de création (1/2)



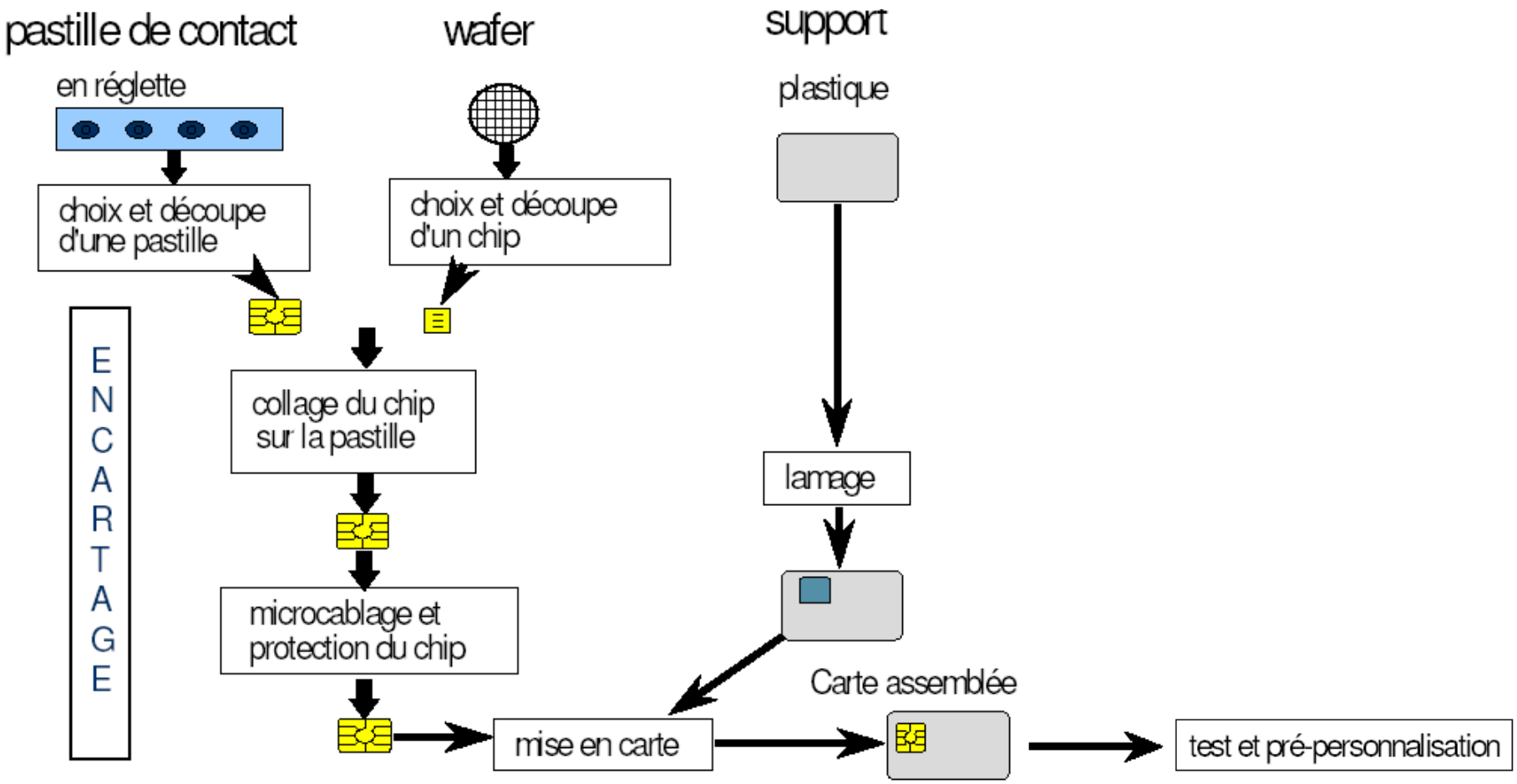


- Phase de création
  - Fabrication de la puce (fondeur)
    - Fabrication du mico-circuit à partir des galettes de silicium
    - Un programme est inscrit en mémoire ROM définissant les fonctio base de la carte : "masque" figé sachant traiter un nombre limité de commandes pré-définies (gestion des entrées sorties, réponse au reset, etc.), c'est le système d'exploitation
  - Encartage, test et pré-personnalisation (encarteur)
    - assemblage de la puce, du micromodule et du support plastique
    - Test et pré-personnalisation (inscription du numéro de série de la carte)



  - Initialisation
    - Inscription en mémoire des données spécifiques propres à l'application dans laquelle la carte va s'insérer
    - la mémoire est organisée et répartie suivant les différents besoins
    - Les zones de travail sont définies et repérées par des indicateurs représentatifs de leur mode de fonctionnement : lecture seule, lecture/écriture, etc.

Cycle de vie : phase de création (2/2)



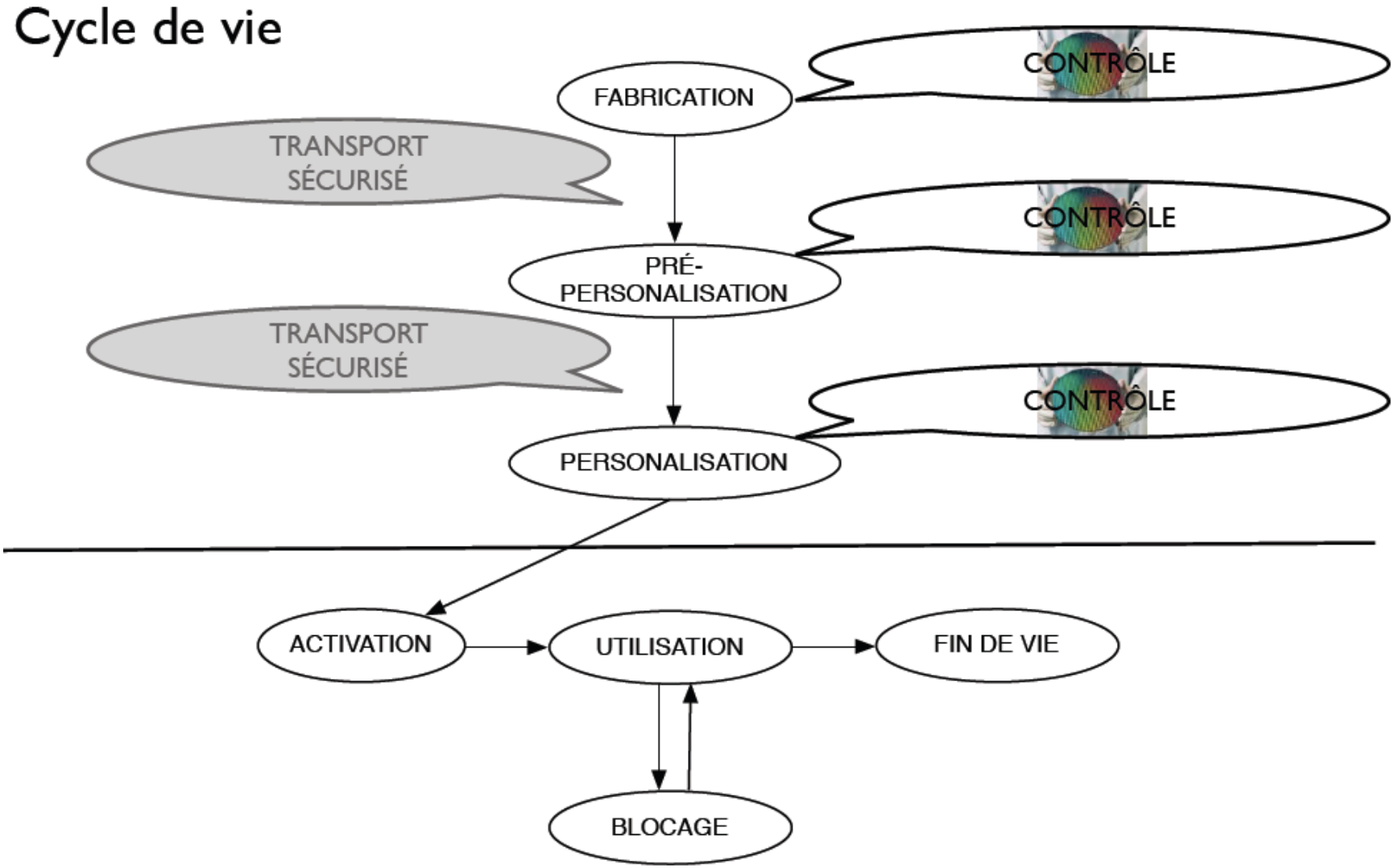
Cycle de vie : phase de circulation (1/2)

- Personnalisation (émetteur)
  - adaptation au porteur final de la carte
  - Personnalisation électrique : écriture par exemple du nom du porteur, du numéro d'abonné ou de toute autre information pertinente dans la ROM
  - Personnalisation graphique : impression et/ou embossage sur le recto et/ou le verso de tout logo, signe, photographie ou hologramme permettant une identification visuelle rapide de la carte
- Distribution (opérateur)
  - Remise de la carte (en face à face, par envoi postal, etc.)
  - Remise du code PIN
  - Communication éventuelle sur le fonctionnement
  - Toutes les étapes de la distribution doivent avoir un niveau de sécurité supérieur ou égal au niveau recherché pour l’ensemble de la vie de la carte

Cycle de vie : phase de circulation (2/2)

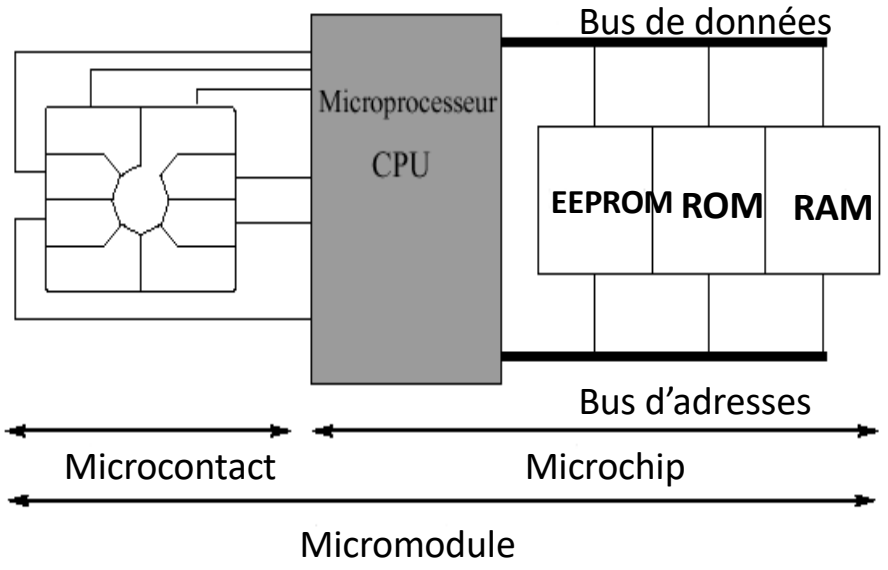
- Utilisation
  - Traitement des commandes par le masque de la carte
  - Utilisation et modifications éventuelles des données inscrites dans la carte
- Gestion du parc (opérateur)
  - Pertes
  - Remplacements
  - éventuelles oppositions
- Fin de la vie d’une carte
  - Par invalidation logique, saturation de la mémoire, bris, etc.
  - Le système d'exploitation devient non fonctionnel

Cycle de vie : en résumé



Carte à microprocesseur : fonctionnement

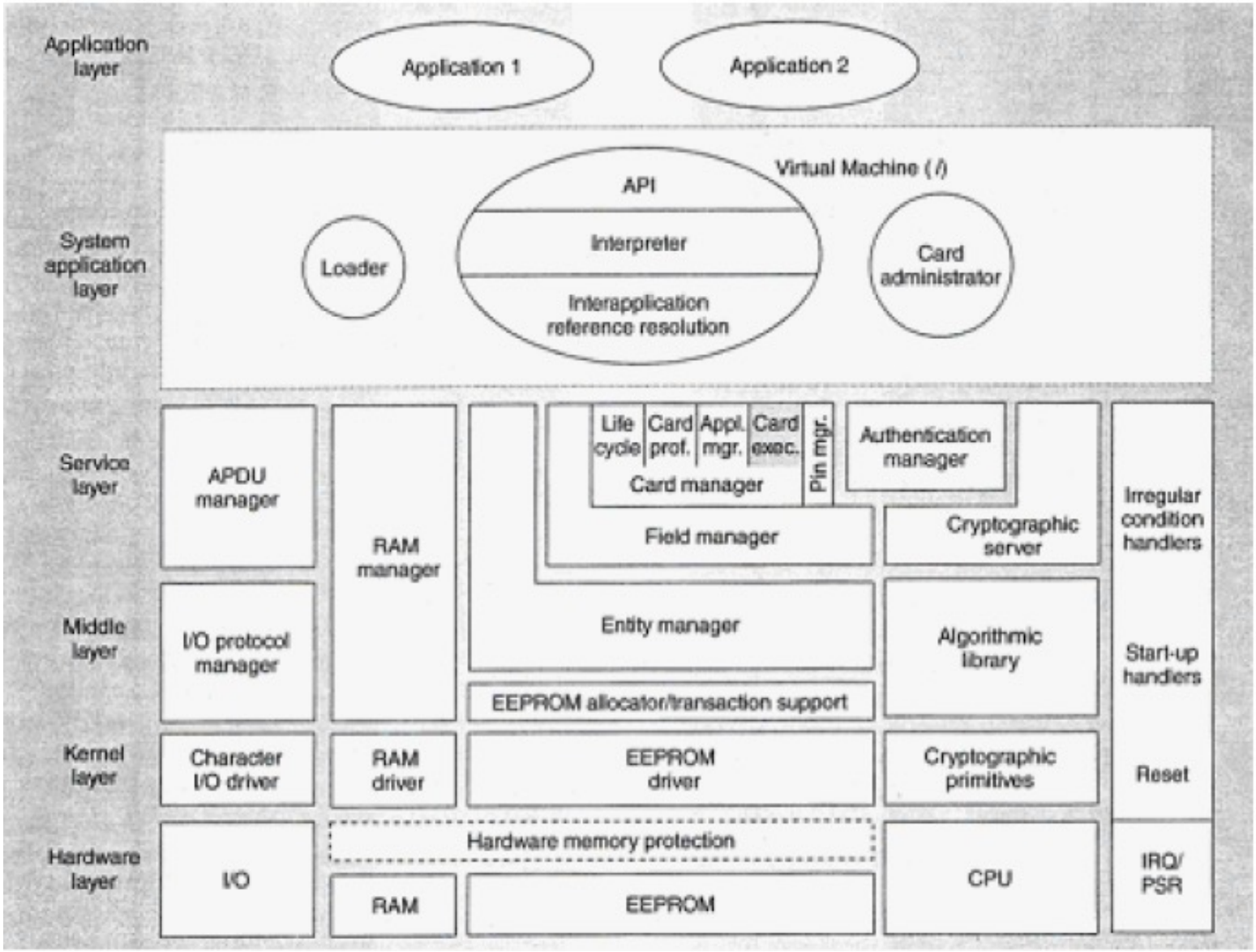
- Un microprocesseur est constitué essentiellement par :
  - Une unité de traitement (CPU)
  - Des mémoires
    - Mémoire non volatile à lecture seule, la ROM (Read Only Memory)
      - Système d'exploitation
    - Mémoire volatile à accès rapide, la RAM (Random Access Memory)
      - Sert aux calculs intermédiaires
    - Mémoire utilisateur MU, non volatile réinscriptible (EEPROM, FLASH ou FeRAM)
      - Identité, abonnements, journal des actions, etc.
  - Des dispositifs anti-intrusion
  - Une interface entrée-sortie normalisée



Le système d'exploitation

- Le système d’exploitation ou OS (Operating System)
  - ajusté pour un composant électronique particulier
  - il est aussi appelé masque
  - stocké dans la ROM du composant lors du processus de fabrication
  - Le système d'exploitation est doté des fonctionnalités qui permettent le déroulement de programmes applicatifs à travers la mise en œuvre des opérations suivantes :
    - Gestion des entrées/sorties
    - Organisation de la mémoire en zones de travail avec gestion des codes confidentiels
    - Gestion des autorisations d’accès (codes confidentiels) en lecture et en écriture au niveau de chaque zone
    - Chargements éventuels de sous-programmes spécifiques lors de la personnalisation ou pendant la durée d’utilisation de la carte

Un exemple de système d'exploitation

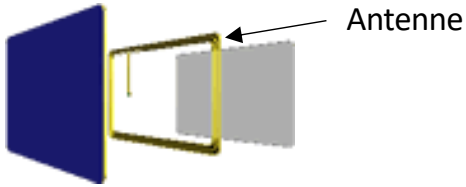


Systèmes dédiés et systèmes ouverts

- On peut distinguer deux types de systèmes d'exploitation de cartes à puces :
  - Les systèmes fermés ou dédiés
    - Généralement mono application; dédiés à un usage unique ; par exemple les cartes bancaires (B0'), les cartes santé (Vitale), les cartes pour la téléphonie mobile (SIM)
  - Les systèmes ouverts
    - Ils ne sont pas destinés à une application particulière et il est possible de "charger" des logiciels (applets) après la réalisation du masque et l'encartage ; par exemple JavaCard, ou le système d'exploitation Multos ou encore le système Windows SC

Cartes avec contact, sans contact, mixtes

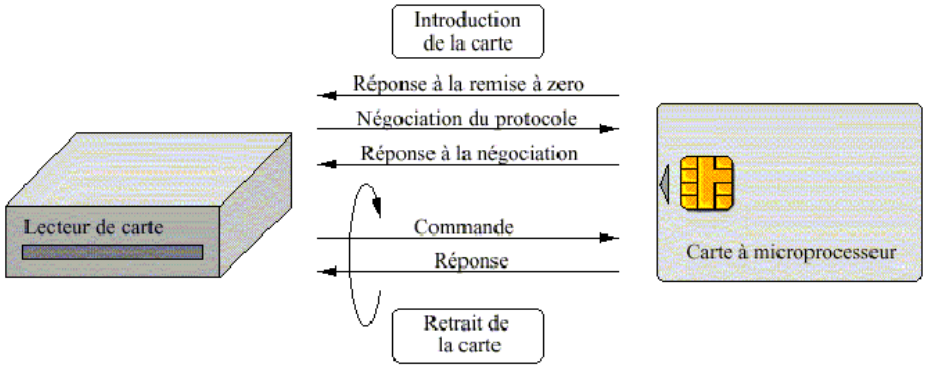
- Les cartes avec contact (carte à puce classique)
- Les cartes sans contact
  - Elle contient, en plus d'une puce classique, une interface radiofréquence permettant la récupération des données à distance
    - Distance : de 10cm à quelques mètres
  - Avantages
    - La vitesse de transfert (moins de 150 ms)
    - Economie dans la maintenance des terminaux



- Les cartes mixtes (avec et sans contact) peuvent s'organiser de deux manières différentes
  - Cartes Combi disposant d’une double interface gérée par le microprocesseur
  - Cartes Twin dont la mémoire est partagée en deux compartiments dissociés : une partie réservée aux applications à contact et l’autre aux applications sans contact

Carte/terminal : la connexion

- La connexion
  - Lors de sa phase d'utilisation, une carte à microprocesseur subit des cycles de trois étapes qui constituent une connexion :
    - L'introduction de la carte : lorsque la carte est insérée dans le lecteur (ou présentée devant), elle se trouve de nouveau alimentée en énergie et est réinitialisée
    - L'exécution de la commande : elle consiste en la réception d'une commande sur le port d'entrée / sortie et à l'exécution de celle-ci. Cette phase peut être renouvelée autant de fois que nécessaire pour la bonne fin de l'application
    - La déconnexion : elle correspond à une coupure franche de l'alimentation électrique de la carte. Elle se retrouve alors dans l'impossibilité de faire quoi que ce soit

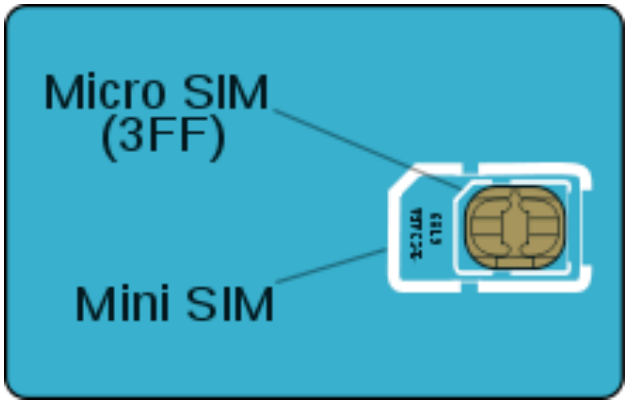


Carte/terminal : le dialogue

- Le dialogue
  - La demande provient toujours du lecteur : la carte ne peut pas émettre de requête, elle peut juste répondre à un ordre du lecteur
  - La communication entre la carte et le terminal s'effectue selon des protocoles de communication normalisés
    - Ces protocoles définissent les ordres que l'on peut envoyer à la carte (ordres entrants), ainsi que les ordres qui demandent des données de la carte (ordres sortants)
    - Toutes les communications entre la carte et le lecteur se terminent par l'envoi de deux mots d'état, soit pour signaler que l'ordre a bien été exécuté (ordre entrant), soit pour dire que toutes les données ont été transmises (ordre sortant).
    - Le format des ordres est normalisé ; les commandes sont appelées commandes APDU

Apparence (form factor)

- Cartes:
  - Cartes plastiques
    - Carte indépendante
    - Téléphones mobiles
      - Mini-SIM, Micro-SIM, Nano-SIM (G&D)



  - iButton
    - Deux contacts
    - protocole série
    - Porte-clé, bague (Java Ring)

Apparence des lecteurs

- Boitier séparé: connexion série, USB, dongle USB
- Intégré à l'ordinateur: carte PCMCIA, Expresscard

- Terminal sécurisé: marchand, client (ex: 3D-secure)

- Téléphones mobiles

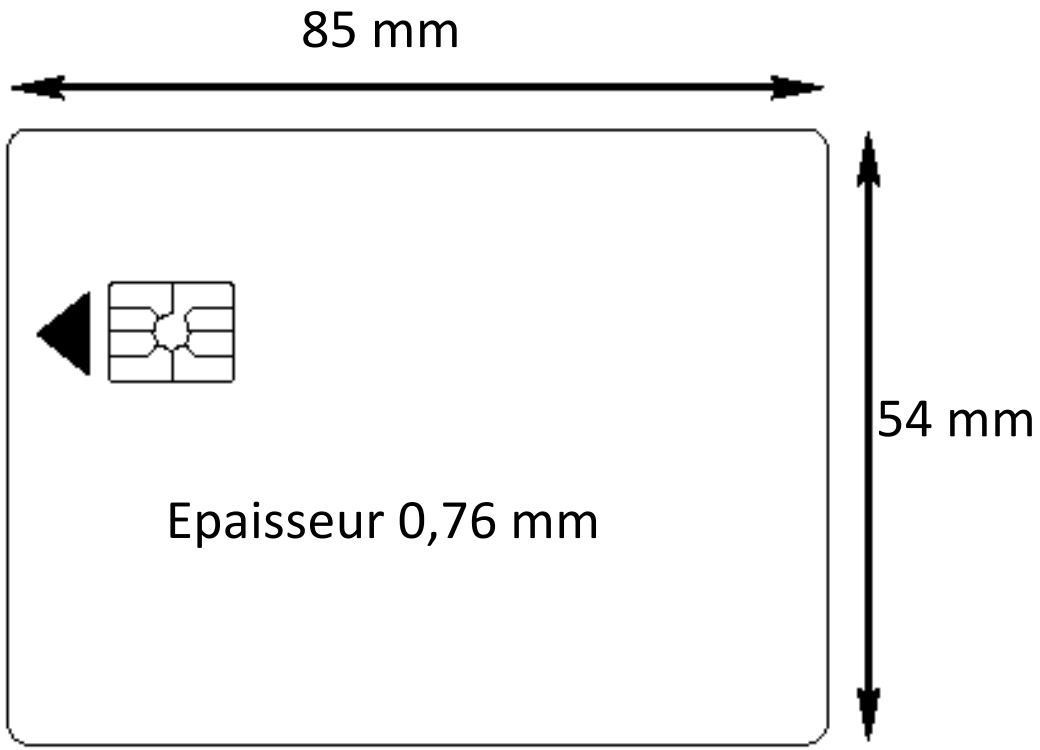
- Intégré aux objets (connexion série 1-fil iButton)

Les standards ISO 7816

- Les cartes sont très standardisées car elles doivent être utilisables avec la gamme la plus large possible de lecteurs dans le monde entier
- C'est la raison pour laquelle les caractéristiques des cartes à puce ont été fixées par des règles reconnues universellement qui appartiennent à une famille de standards et protocoles internationaux dénommés ISO 7816
  - Caractéristiques physiques
    - Dimension de la carte, des fonctions et du placement des contacts du micromodule
  - Caractéristiques électroniques
    - Signaux électroniques et protocoles de transmission utilisés dans les échanges entre la carte et le terminal
  - Parties:
    - 1 Caractéristiques physiques.
    - 2 Dimensions et positions des contacts.
    - 3 Signaux électriques et protocoles de transmission.
    - 4 Commandes intersectorielles pour les échanges.
    - 5 Système de numérotation et procédure d'enregistrement pour les identificateurs d'applications.
    - 6 Eléments de données interindustrielles.
    - 7 Commandes intersectorielles pour langage d'interrogation de carte structurée (SCQL).
    - 8 Commandes intersectorielles de sécurité
    - 9 Commandes intersectorielles additionnelles et attributs de sécurité.
    - 10 Réponse à la RAZ des cartes synchrones.
    - 11 Architecture de sécurité.

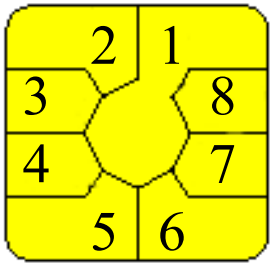
ISO 7816-1

- Caractéristiques physiques, dimensions
- Contraintes: flexion et torsion
- AMD 1 (Amendement 1) : décalage maximum des contacts de la puce par rapport à la surface 0.1 mm



ISO 7816-2

- Emplacement des contacts et aspects électriques

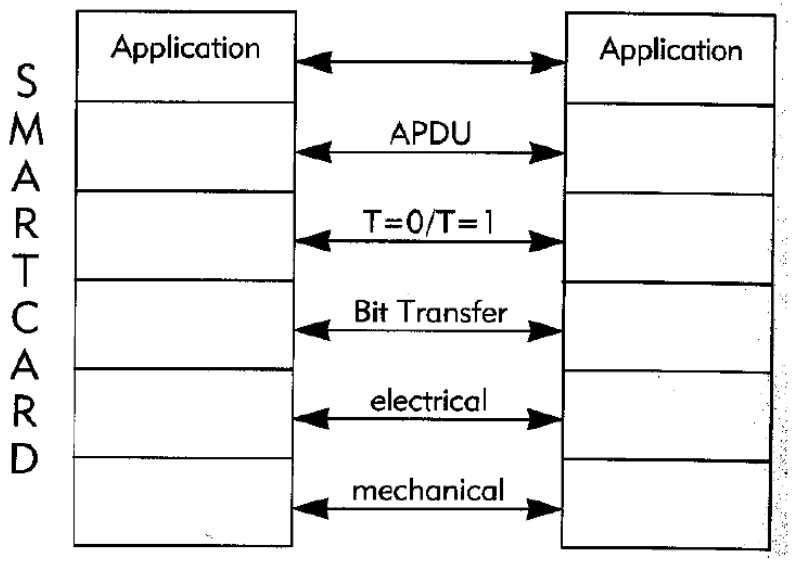


1 - 2 : Alimentation 3 à 5 V
3 : Horloge
4 : Remise à Zéro
5 : Optionnel
6 : Optionnel
7 : I/O asynchrone
8 : Ecriture EEPROM

ISO 7816-3

- Caractéristiques électriques :
  - Fréquence d'horloge 1 - 5 Mhz
  - Vitesse des communications < 115200 bauds

- Protocole de transmission :
  - TPDU (Transmission Protocol Data Unit)
  - T=0 à 15
  - T=0 Protocole orienté octet
  - T=1 Protocole orienté paquet



- Sélection du type de protocole :
  - PTS (Protocol Type Selection)

- Réponse au reset :
  - ATR (Answer To Reset)

Au démarrage :
•Le lecteur doit activer la carte mise (sous tension) et effectuer un RESET à
•froid,
•La carte et le lecteur peuvent échanger de l'information,
•La carte est désactivée électriquement

ISO 7816-4

APDU (Application Programming Data Units)

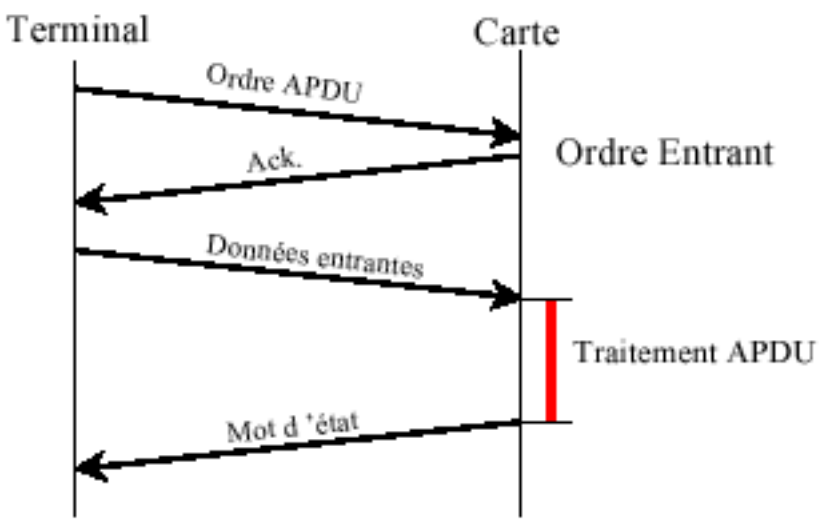
Command APDU						
Mandatory Header				Conditional Body		
CLA	INS	P1	P2	Lc	Data Field	Le

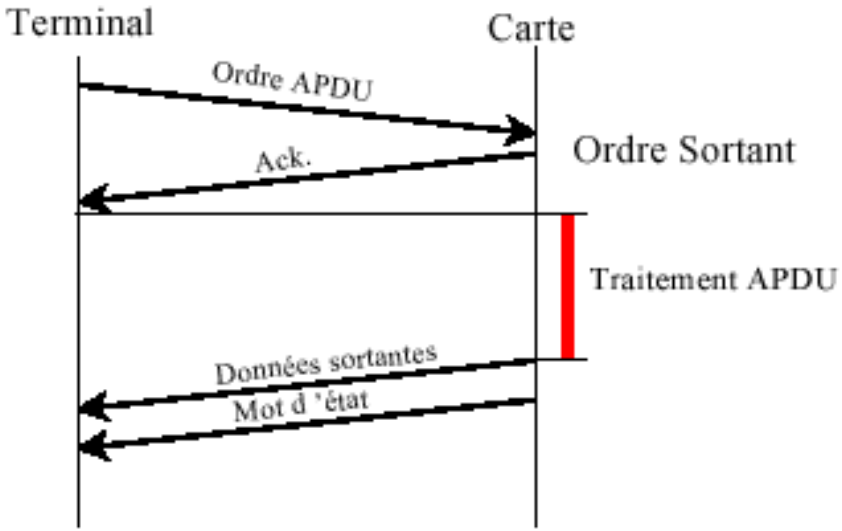
CLA : 1 octet pour identifier l'application
INS : 1 octet pour le code de l'instruction
P1 - P2 : Paramètres de l'instruction
Lc : Longueur du champ de données
Le : Longueur maxi du champ de données de la réponse

Response APDU		
Conditional Body	Mandatory Trailer	
Data Field	SW1	SW2

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

ISO 7816-4


Terminal
Carte
Ordre APDU
Ordre Entrant
Ack.
Données entrantes
Traitement APDU
Mot d 'état

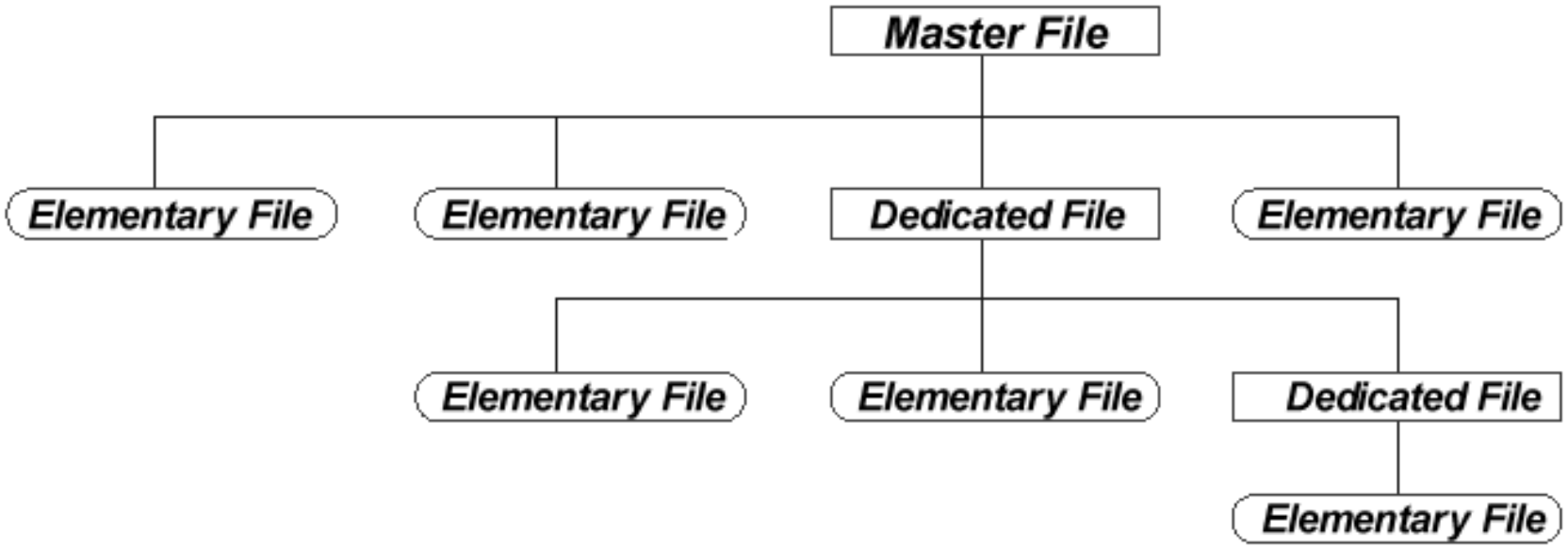

Terminal
Carte
Ordre APDU
Ordre Sortant
Ack.
Traitement APDU
Données sortantes
Mot d 'état

ISO 7816-4

- Le système de fichiers des cartes à puce.

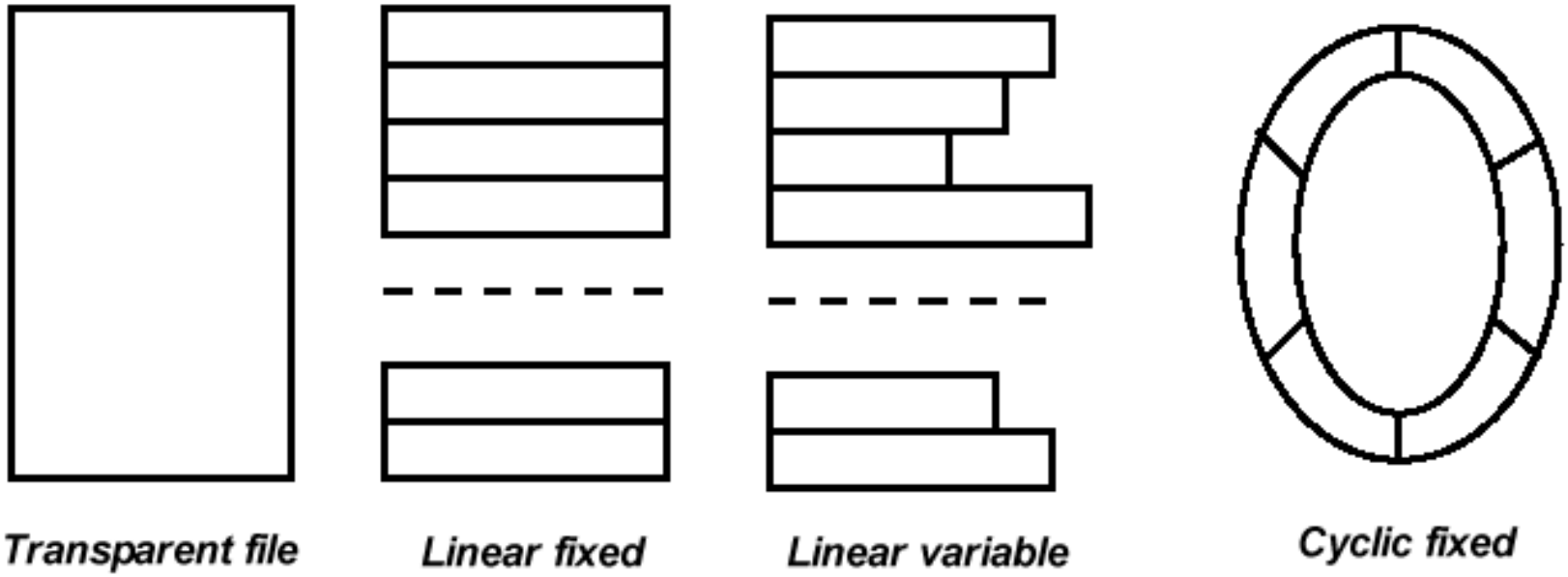
Système de fichiers hiérarchique qui peut contenir 3 types de fichiers :

"Master File" (Fichier racine)
"Dedicated File" (Répertoire + qq infos)
"Elementary File" (Fichier de données)



ISO 7816-4

- 4 structures de données :



ISO 7816-5

- Spécifie des identifiants d’applications (Application IDentifier)

Un AID = identication unique d'une application de la carte
et de certains types de fichiers.

ISO 7816-6

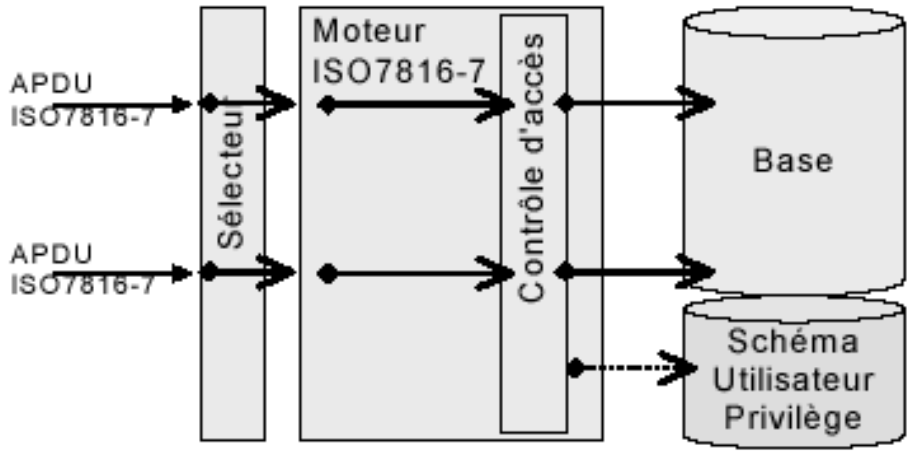
- Spécifie les éléments de données inter-industrie :
  - Nom du porteur de la carte
  - Date d'expiration
  - …

Etiquette	Longueur	valeur

ISO 7816-7

- Données organisées en tables, avec des colonnes, lignes, … (Similarité aux bases de données)

- Langage spécifique de requêtes : SCQL (Smart Card Query Language)



2000 PicoDBMS : Un SGBD sur carte à puce

ISO 7816-8 à 10

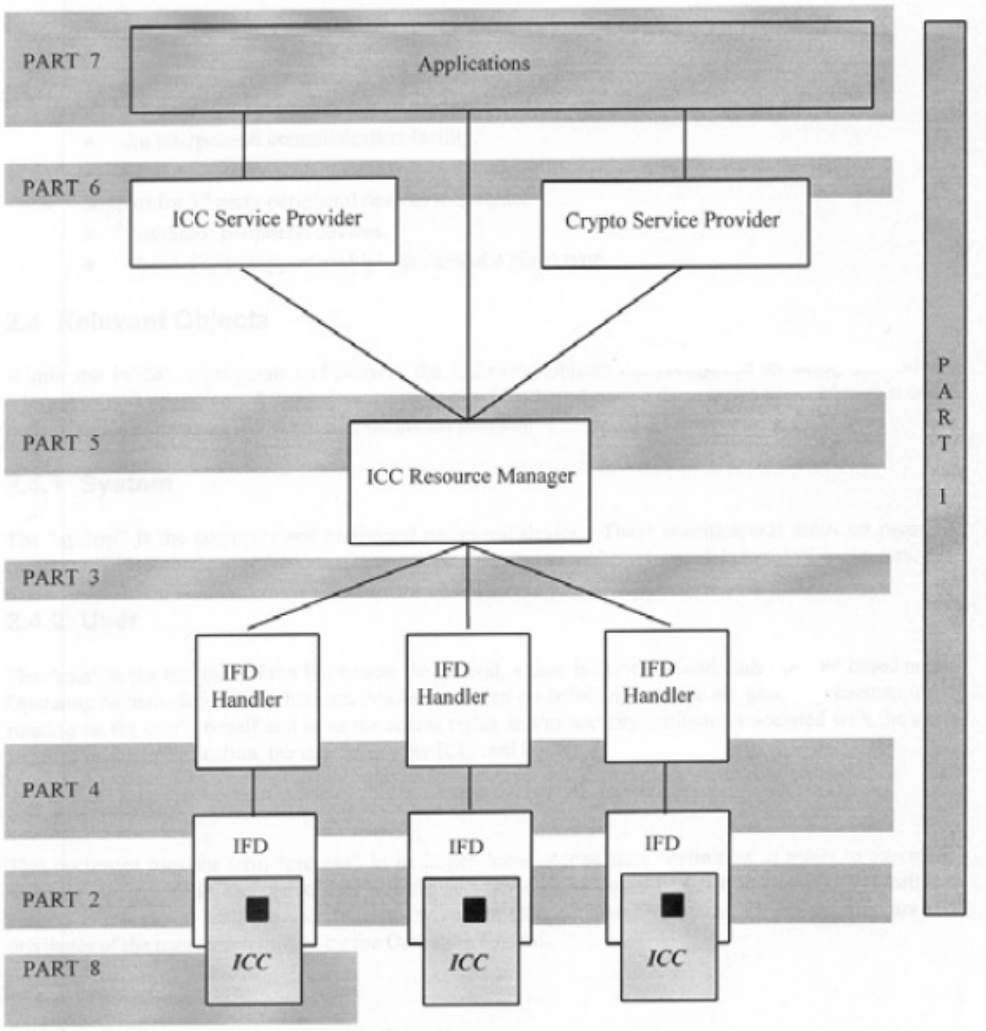
- ISO 7816-8 : Sécurité de l'architecture et des commandes inter-industrie.
- ISO 7816-9 : Commandes inter-industries améliorées
- ISO 7816-10 : Spécifiques aux cartes synchrones

Les standards indépendants du domaine

- JavaCard
  - Type de carte fonctionnant avec un système d'exploitation ouvert destiné aux cartes multiapplicatives
  - Les spécifications de la JavaCard sont la propriété de SUN et sont élaborées par le JavaCard Forum. La version actuelle est JC 2.1
- Multos
  - Système d'exploitation, défini par un consortium industriel, destiné aux cartes multiapplicatives
- Gestion des lecteurs et communication
  - PC/SC
  - SmartCard for Windows
  - OpenCard Framework (OCF)
  - JavaCard RMI
  - JPCSC
  - Smart Card I/O
- Global Platform
  - Interface entre applications et système de gestion/administration "hors-carte"
  - CardManager: composant central qui gère notamment les clés cryptographiques spécifiques à l'émetteur de la carte (Card Issuer) et aux fournisseurs d'applications (Application Provider)

Standard PC/SC

- intégration de lecteurs de carte à puces aux PCs (Interface Device – IFD).
- Concept : offrir une interface de type API (niveau 6) aux applications qui utilisent les ressources des cartes aux moyens de DLLs.
-
- 1 Introduction and Overview
- 2 Interface Requirements for compatible IC Cards and Readers.
- 3 Requirement for PC-Connected Interface Devices
- 4 IFD Design considerations and Reference Design Information
- 5 ICC Resource Manager Definition (définition des APIs carte)
- 6 ICC Service Provider Interface Definition.
- 7 Application Domain and Developer Design Considerations.
- 8 Recommendations for ICC Security and Privacy Devices



L’API OpenCard

3 raisons :

- Les terminaux des cartes, n’ont pas d’interfaces standardisées → différents protocoles

- Card Operating System divers → différentes commandes et codes de réponse

- Les émetteurs des cartes décident de l’emplacement des applications sur la carte

→ But : Rendre le développement d’applications indépendant des fabricants, technologies, …

OpenCard Framework : classes importantes

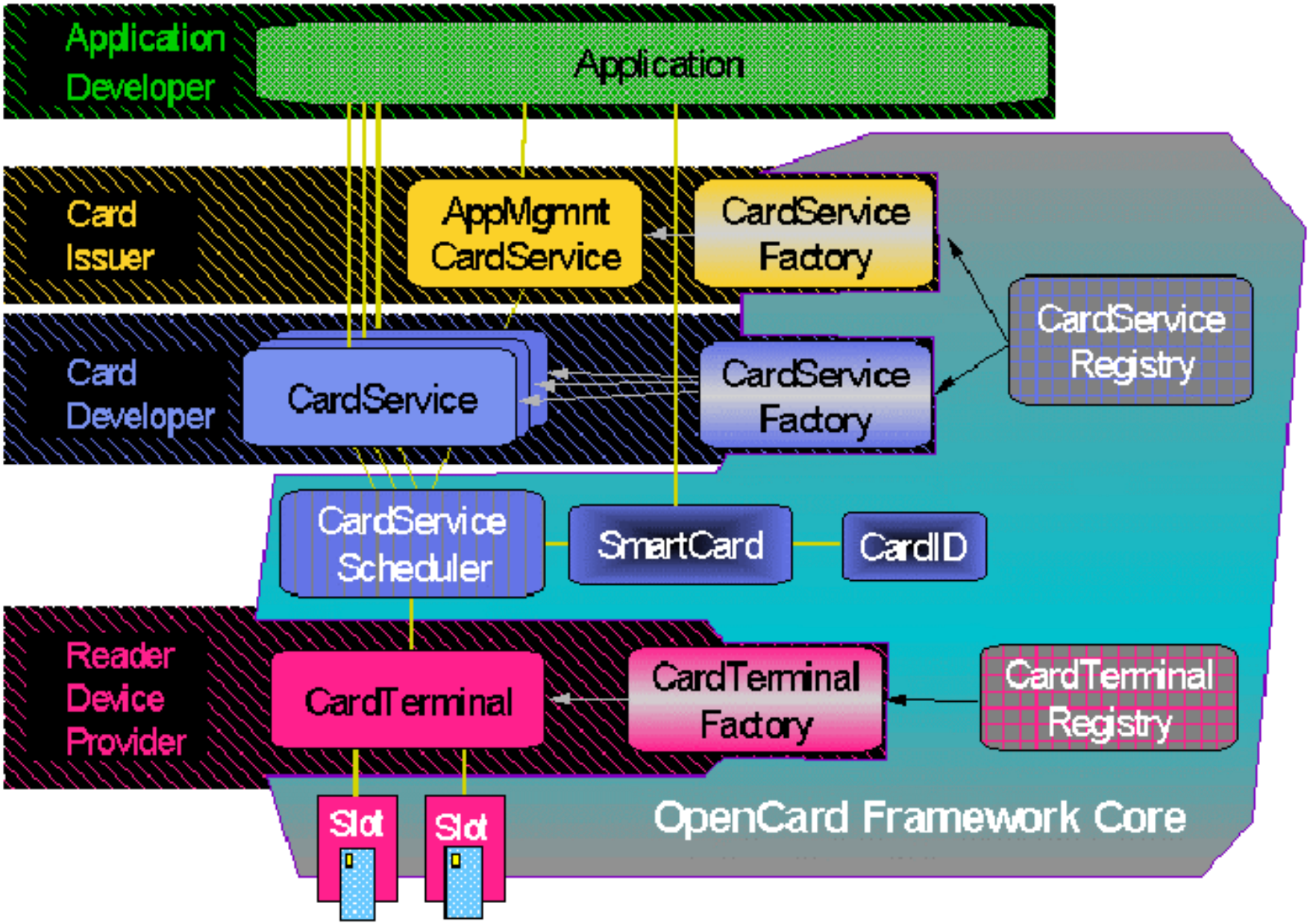
- **CardTerminal layer** permet de faire abstraction des terminaux.

Fournit des accès au lecteur et à la carte insérée.

- **CardService layer** permet de faire abstraction des Card Operating System.

Ex : FileAccessCardService, SignatureCardService, ApplicationManagementCardService, `PurseCardService`

OpenCard : Schéma des APIs



OpenCard : Exemple de programmation

Phase d'initialisation :

```
// Initialize the framework
SmartCard.start ();
// register the new SignatureCard as a Card Terminal Event Listener
CardTerminalRegistry.getRegistry().addCTListener(this);
```

Phase de récupération des paramètres :

```
public void cardInserted(CardTerminalEvent ctEvent)
try {
fileService = (FileAccessCardService)card.getCardService(FileAccessCardService.class, true);
signatureService =
        (SignatureCardService)card.getCardService(SignatureCardService.class, true);

        SBCHVDialog dialog = new SBCHVDialog();
        fileService.setCHVDialog(dialog);
        signatureService.setCHVDialog(dialog);
} catch(Exception e) {
        e.printStackTrace();
  }
}
```

OpenCard : Exemple de programmation

Phase de lecture dans le fichier :

```
...
// mount file system to get access to the root directory
CardFile root = new CardFile(fileService);
// This is the file holding card holder name and e-Mail address
CardFile file = new CardFile(root, ":C009");
// Create a CardFileInputStream for file
DataInputStream dis = new DataInputStream(new CardFileInputStream(file));
// Read in the owner's name
byte[] cardHolderData = new byte[file.getLength()];
dis.read(cardHolderData);
// Explicitly close the InputStream to yield the smart card to other applications
dis.close();
...
```

OpenCard : Exemple de programmation

Génération de la signature numérique :

```
// specify the key used for signing
PrivateKeyFile kf = new PrivateKeyFile (new CardFilePath(":C110"), keyNumber);

// Let the card generate a signature
signature = signatureService.signData(kf, JCAStandardNames.SHA1_RSA,
JCAStandardNames.ZERO_PADDING, data);
```

Terminaison :

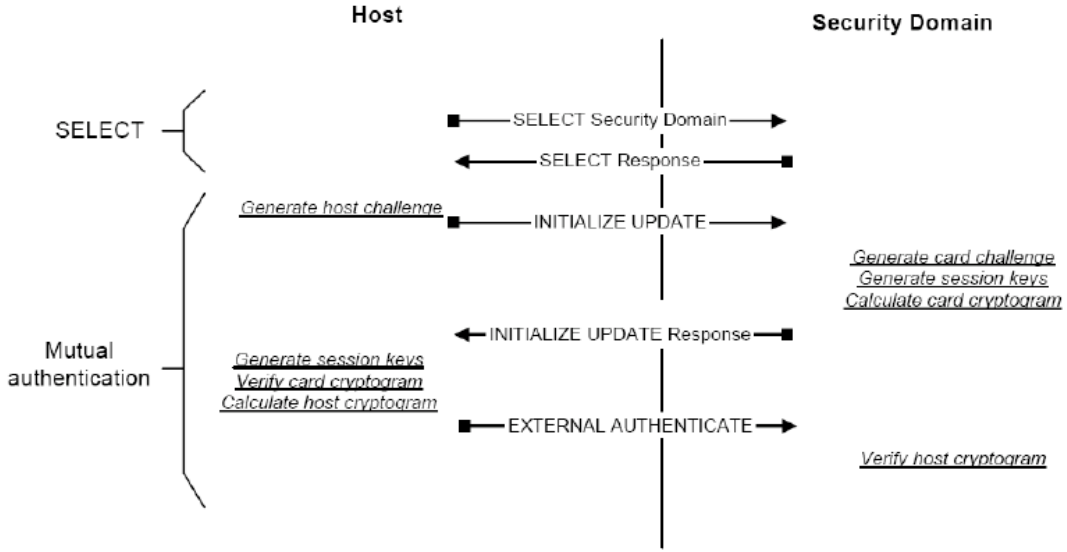
```
SmartCard.shutdown ();
```

New Terminal side libraries

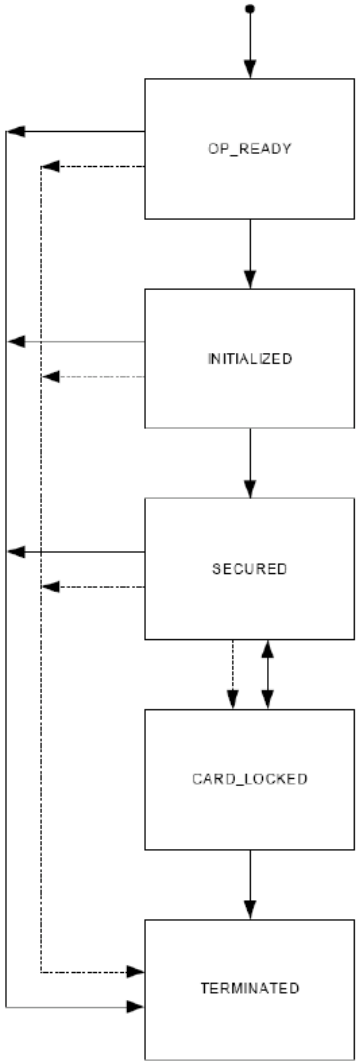
- JavaCard RMI (Remote Method Invocation): Since Javacard 2.2.1, this library provides an object-oriented communication through the automated generation of stubs and skeletons.
- JPCSC (Java PCSC wrapper): this library provides a simple APDU based interface.
- Smart Card I/O (javax.smartcardio package a.k.a JSR 268): the library offers a more recent, object-oriented support for:
  - PCSC - CardTerminal among a list of CardTerminals, TerminalFactory
  - Card management: isCardPresent(), waitForCardPresent(), connect(), disconnect()
  - APDUs: CommandAPDU and ResponseAPDU sent over a CardChannel

Global Platform (GP)

- Le Card Manager offre un certain nombre de services :
  - Gestion des APIs utilisées par les applications
  - Traitement des commandes, c'est-à-dire routage des APDUs
  - Gestion des canaux logiques, assurant la confidentialité et de l'intégrité des informations échangées.
  - Gestion du contenu de la carte
- Gestion de domaines de sécurité
  - Gère le cycle de vie d'un ensemble d'applications
  - Associé à un AID
  - Issuer Security Domain: peut installer d'autres domaines
  - Application Provider Security Domain
- Standardise la sécurité des communications vers la carte :

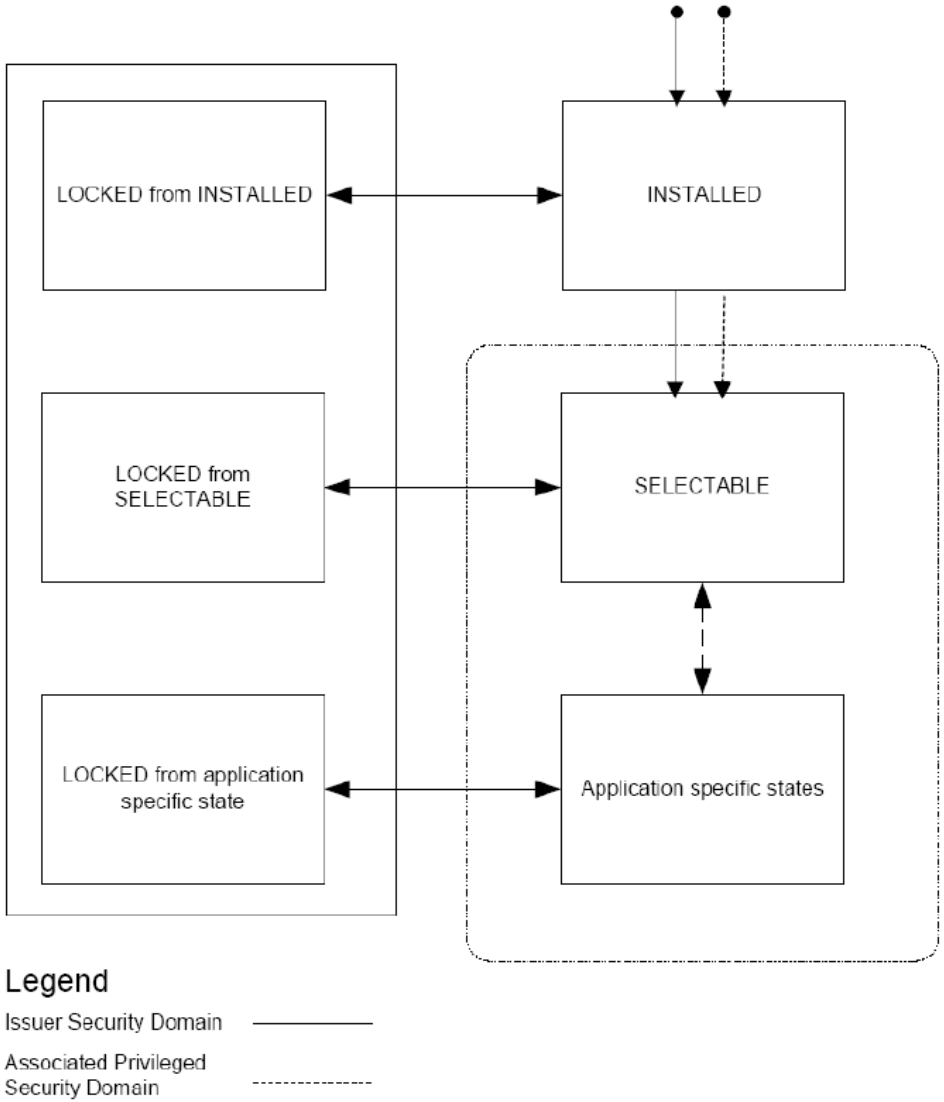


GP: Cycle de vie de la carte



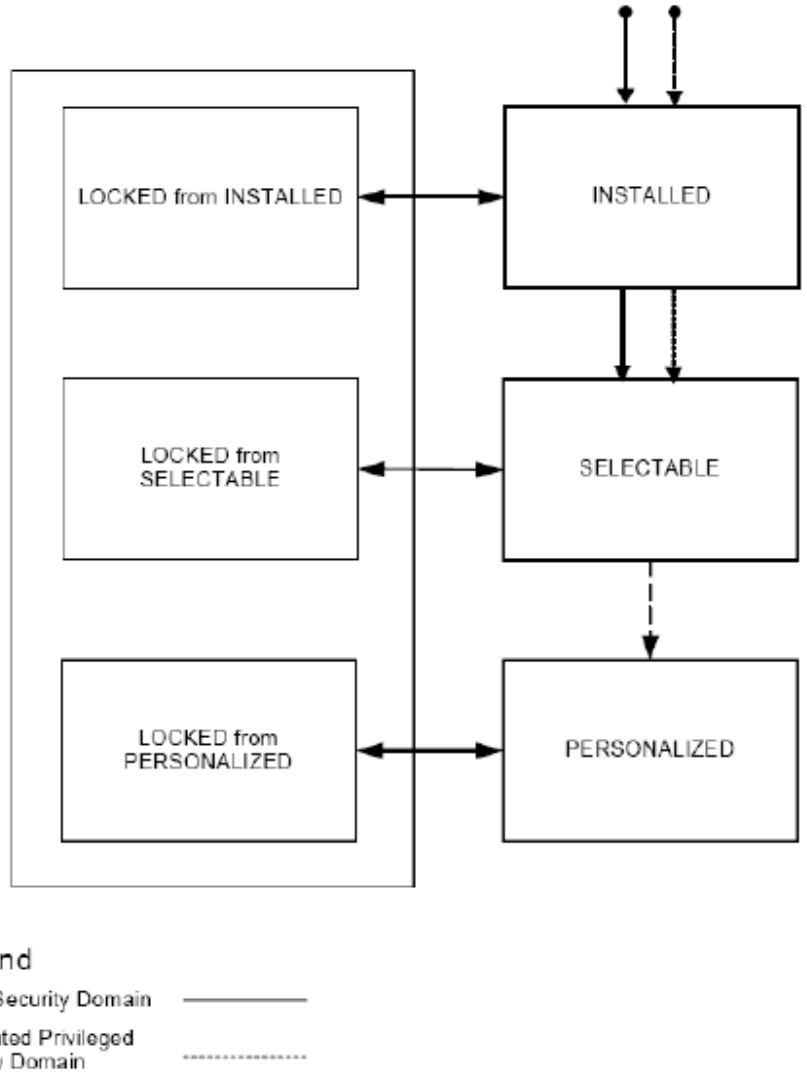
- OP_READY: environnement d'exécution et domaine de sécurité de l'émetteur disponibles
- INITIALIZED: pendant la production de la carte – transition irréversible
- SECURED: le Card Manager contrôle la politique de sécurité – transition irréversible
- CARD_LOCKED: carte contrôlée par le domaine de sécurité de l'émetteur
- TERMINATED: fin du cycle de vie – transition irréversible

GP: Cycle de vie des applications



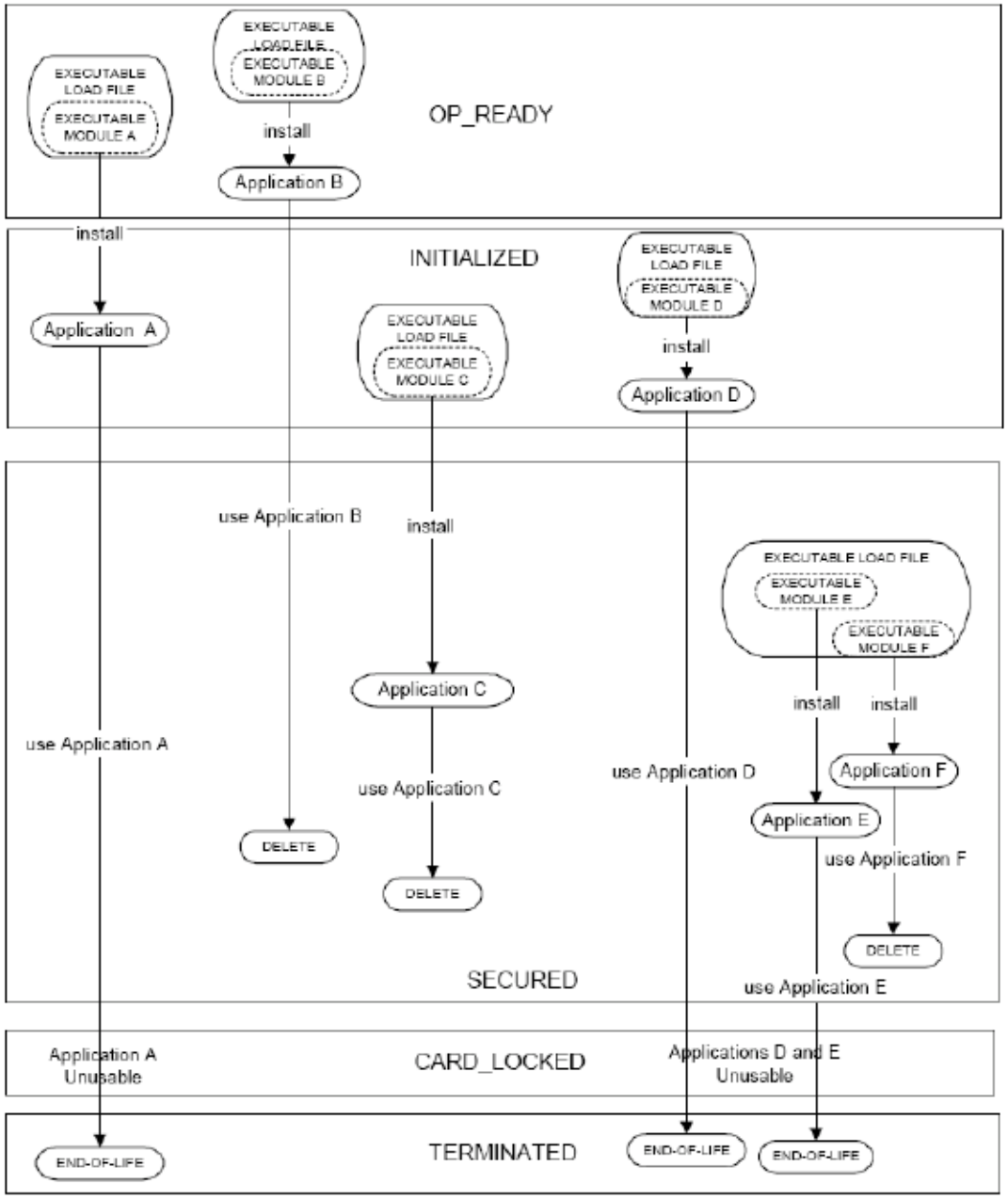
- INSTALLED: code et données de l'application sont chargés en mémoire
- SELECTABLE: l'application est prête à recevoir des commandes (APDUs) du système hôte – transition de INSTALLED à SELECTABLE irréversible
- LOCKED: interdit sélection et exécution de l'application – transition réversible et contrôlée par le domaine de sécurité de l'émetteur
- Une application peut être détruite par le système de gestion Open Platform à tout moment

GP: Cycle de vie des domaines de sécurité



- INSTALLED: le domaine de sécurité est accessible depuis une entité authentifiée
- SELECTABLE: le domaine de sécurité reçoit typiquement ses clés cryptographiques – transition irréversible
- PERSONALIZED: le domaine de sécurité possède toutes les données (clés..) nécessaires et peut gérer des applications – transition irréversible
- LOCKED: le domaine de sécurité est hors service
- Un domaine de sécurité peut toujours être détruit

GP: un exemple avec plusieurs applications

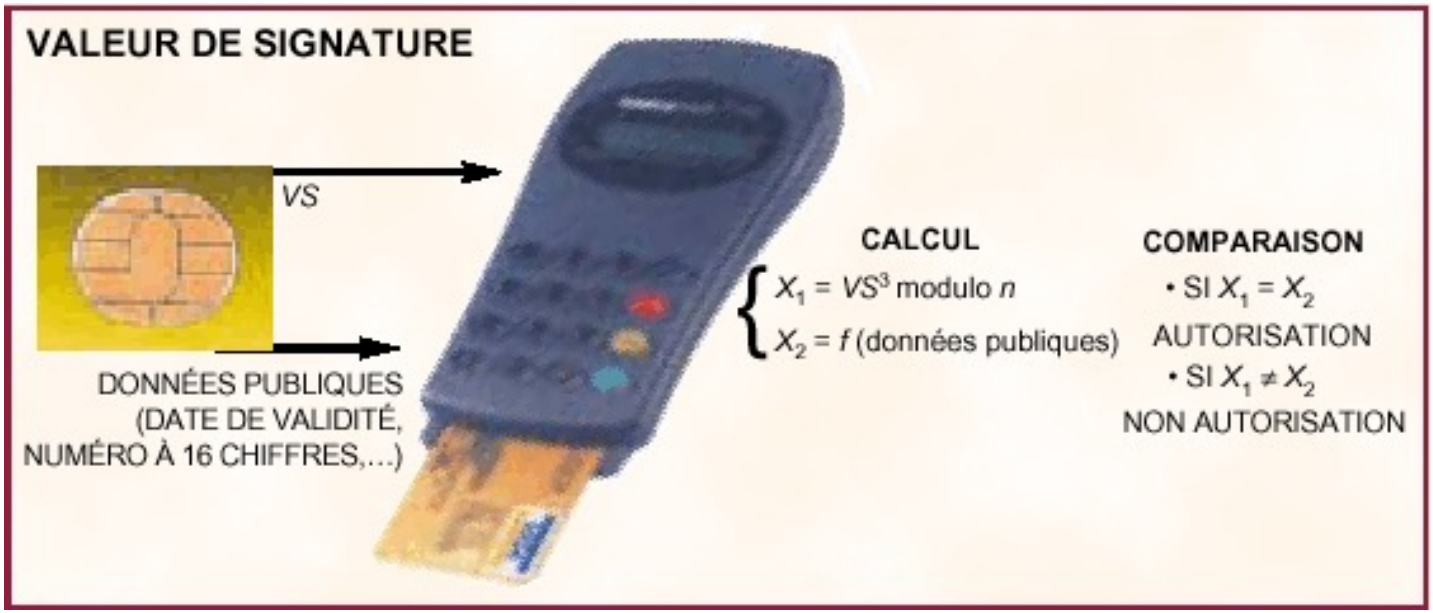


Les standards financiers

- CEN Purse EN 1546
  - Le standard CEN (TC224, WG10) intervient dans le domaine financier et plus particulièrement les applications du porte-monnaie électronique (PME) multiservices
  - Il définit les données et les instructions de la carte, ainsi que les transactions et les applications utilisant ce PME
- CEPS
  - standard ouvert dont le but est d'assurer que 90% des porte-monnaies électroniques du monde soient inter-opérables
  - CEPS est le standard *de facto* du porte-monnaie électronique
- EMV
  - Ce standard a été défini par les institutions financières internationales Europay, Mastercard et Visa en 1996, puis une autre version en 2000
  - Ce standard couvre le protocole, les données, les instructions et les transactions des cartes bancaires à puce
  - Ce standard répond à une double exigence de sécurité et d'interopérabilité
- VISA OP (Open Platform)
  - Standard pour cartes et terminaux
  - 3 types d'APIs Java
    - Card Manager. Ce module contrôle la carte et son contenu.
    - Global Platform APIs
    - Provider Security Domains. Gestion de la sécurité d'une carte multi application
- FINREAD
  - Standard de lecteur de carte pour l'e-business

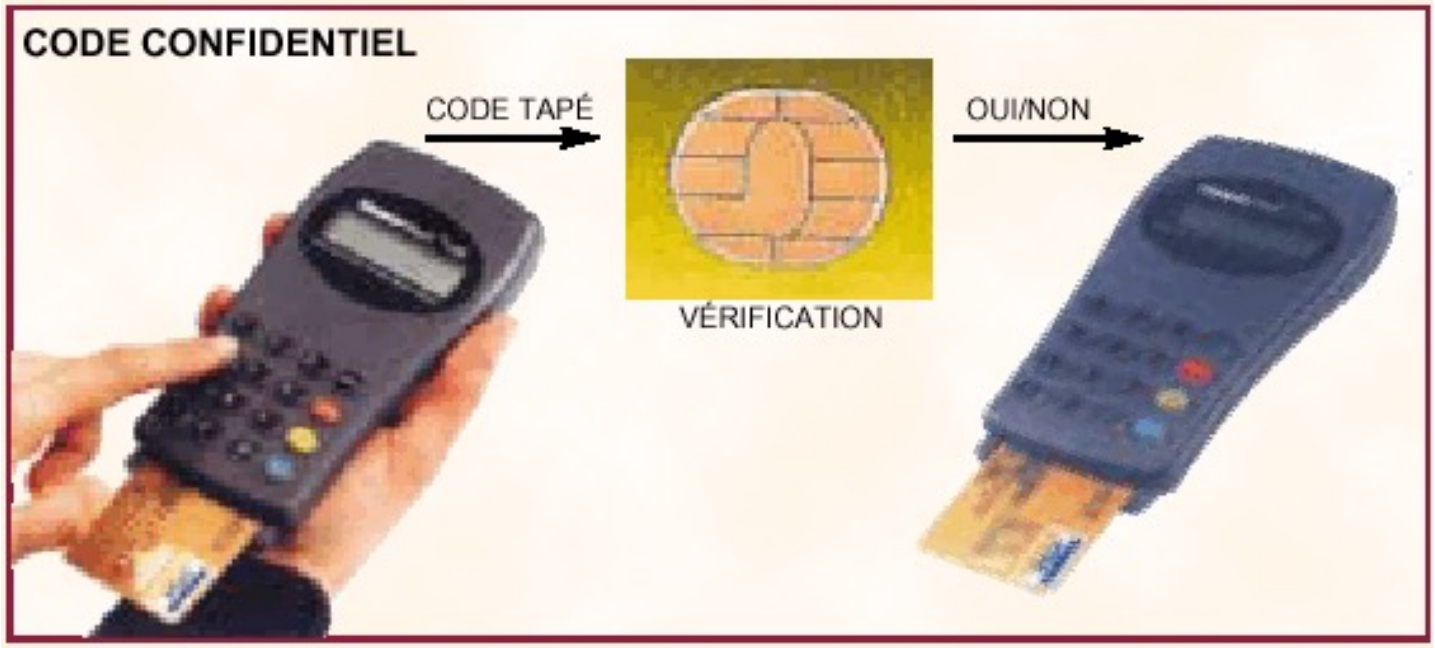
Mécanisme de paiement par carte bancaire

- Authentification de la carte : Algorithme RSA, fonctions de tests, identifie la carte de manière unique.



Mécanisme de paiement par carte bancaire

- Code confidentiel : Terminal de paiement envoie requête à la carte, carte calcule puis envoi réponse au terminal.



- Authentification de la transaction : Algorithmes DES et TDES, fonctions de tests, code les informations de la transaction.

Le standard EMV

(Europay Mastercard Visa)

Le standard décrit les terminaux, les cartes et leur interaction.
EMV'96 Specification for Payment Systems comporte:
•1 caractéristiques mécaniques, électriques, interface logique et protocoles de transport des cartes (ICC).
•2 Jeu de commandes APDUs
•3 Mécanismes de sélection des applications.
•4 Sécurité, méthodes d'authentification et de signature

- Transaction cryptée par TDES avec une clé de 90 bits
- Signature RSA doit passer à 1024 bits pour être tranquille 10 ans.
- Protocole d'authentification statique : 1 contrôle de certificats
- Protocole d'authentification dynamique : 3 contrôles de certificats en cascade

Nécessite des cartes puissantes et des ressources

FINREAD : Pour sécuriser l’e-business

- Définition de normes et de spécifications techniques d'un nouveau standard européen.

- Lecteur avec une sécurité maximale pour les transactions à distance, idéal pc les paiements multi supports.

Les standards des télécoms

- GSM 11.11 et 11.14
  - Mobile subscriber identity module (SIM) and application toolkit
- CEN EN 726
  - Cartes et terminaux

Les spécifications PKCS

- Public Key Cryptography Standard (PKCS)
  - PKCS est un ensemble de spécifications développées par RSA Security et des développeurs de système dans le monde entier, dans le but d'accélérer le déploiement de la cryptographie à clé publique
  - PKCS est devenu un standard *de facto*
  - PKCS #7
    - Cryptographic Message Syntax Standard
  - PKCS #11
    - Cryptographic Token Interface Standard.
  - PKCS #15
    - Cryptographic Token Information Format Standard : ces spécifications définissent le format des fichiers et des répertoires abritant des certificats et des clés cryptographiques

La sécurité

- La sécurité est la principale qualité de la carte à puce. C'est d'ailleurs pour cette raison qu'elle a été choisie pour les transactions bancaires notamment en France.
- Cette sécurité accrue est rendue possible grâce à un ensemble de techniques variées
  - Une sécurité physique
    - Les cartes à puce disposent d'un bloc de sécurité qui vérifie que celle-ci est utilisée dans des conditions normales
    - Ce bloc intègre des systèmes de détection du voltage, de température, de luminosité, etc.
  - Le système d'exploitation
    - Le contrôle d'accès à la mémoire est assuré grâce à l'utilisation de clés de fabrication, de personnalisation, etc.
    - Il réalise aussi l'identification du porteur de la carte grâce au PIN composé de quatre chiffres.

La sécurité

- La mémoire
  - La politique de sécurité des données stockées en mémoire différencient trois granularités :
    - L'information en lecture seule,
    - L'information en lecture / écriture,
    - L'information en écriture seule.
  - Ces protections sont gérées par le masque (ou système d'exploitation)
- Carte à puce et cryptographie
  - Le rôle de la cryptographie dans une application utilisant la carte à puce est d'assurer la sécurité des transactions :
    - Authentification de la carte (ex : carte SIM)
    - Authentification du porteur (code PIN)
    - Génération et vérification des signatures électroniques

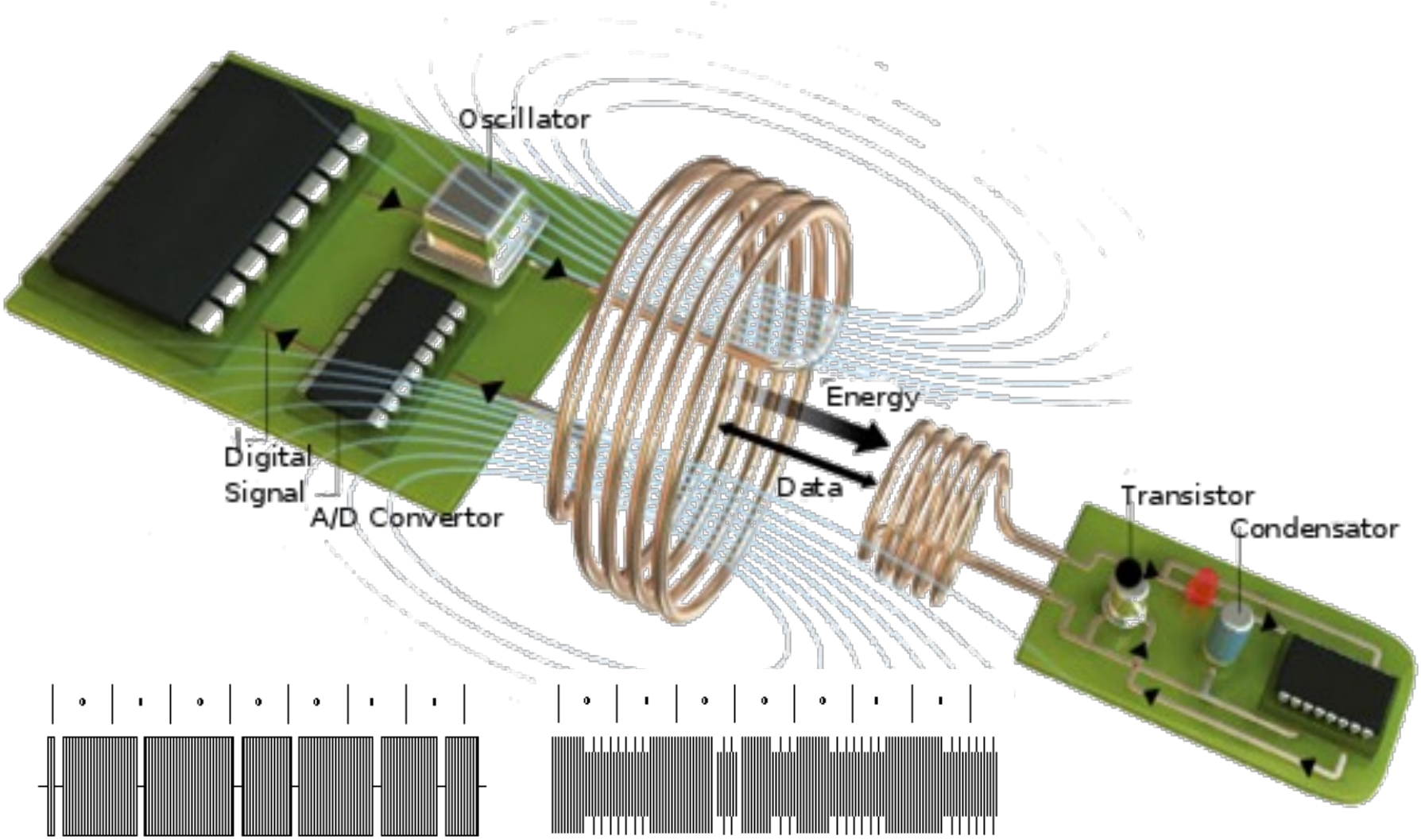
Niveaux d'assurance - Critères Communs

- Les EAL (Evaluation Assurance Level) sont des niveaux d'assurance de l'évaluation
  - Les EAL définissent une échelle pour mesurer l'assurance que l'on a dans une carte à puce contre des attaques (c.f. slide suivant)
  - Les EAL fournissent une échelle croissante qui permet d'obtenir un équilibre entre le niveau d'assurance obtenu et le coût et la faisabilité nécessaires pour parvenir à ce degré d'assurance
  - Les 7 niveaux d'assurance de l'évaluation
    - EAL1 - testé fonctionnellement
    - EAL2 - testé structurellement
    - EAL3 - testé et vérifié méthodiquement
    - EAL4 - conçu, testé et revu méthodiquement
    - EAL5 - conçu à l'aide de méthodes semi-formelles et testé
    - EAL6 - conception vérifiée à l'aide de méthodes semi-formelles et testé
    - EAL7 - conception vérifiée à l'aide de méthodes formelles et testé

Cartes sans contact / RFIDs

- Radio Frequency Identifiers
- Parfois des cartes
- Souvent plus petit
  - Etiquettes “intelligentes”
  - Concept de “poussière intelligente”
  - On peut intégrer plusieurs RFIDs dans un même produit
- parfois beaucoup plus gros!
  - Exemple: RFIDs pour le suivi des containers sur les ports

Technologie RFID : concept



Reader to tag signal
- Dropping field
- Modified Miller Encoding

Tag to reader signal
- Modulating field
- Manchester Encoding

RFID exxample: Mifare Classic

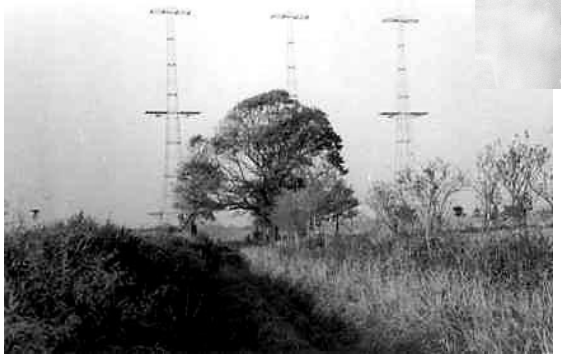
RFIDs: vers une identité diffuse

- Evolution naturelle du monde des tokens et cartes vers celui de l'informatique diffuse
  - Facteur de forme plus intéressant : La puce est intégrée aux objets
  - Vise tout type d'identité (utilisateur, produit …)
- Contraintes encore plus fortes en termes de capacités de calcul
- Lien logique-physique

- Papiers: passeport biométrique, carte d'identité numérique eID (Belgique notamment) …
- Transport aérien: billets électroniques, cartes d'embarquement mobiles, tags RFIDs sur bagages
- Fret (maritime not.) : RFIDs sur les containers

RFID Applications

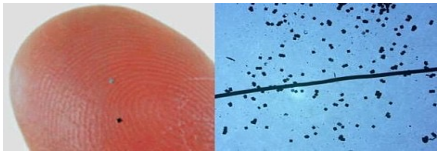
Identify friend or foe (1942)



Car keys

Public transport ticketing

Electronic passport

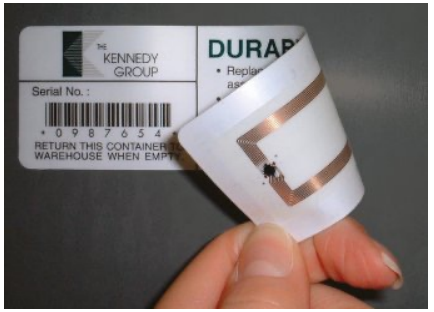


RFID Powder

Access control

Anti-theft

Event ticketing



Supply chain management

Les standards ISO 14443

- Les standards ISO 14443 sont pour les cartes à puce sans contact
  - Cette norme spécifie les caractéristiques applicables aux cartes d'identification, aux cartes sans contact à circuits intégrés et aux cartes de proximité
    - La partie 1 définit les caractéristiques physique
    - La partie 2 définit l'interface radio fréquence et des signaux de communication
    - La partie 3 définit les caractéristiques d'initialisation et anticollision
    - La partie 4 définit le protocole de transmission
  - Elle propose deux versions pour le codage numérique : type A et type B

	Type A	Type B
Lecteur vers carte	Modulation ASK 100% Codage Pulse Position Différentiel	Modulation ASK 10% Codage NRZ
Carte vers lecteur	Modulation d'impédance Sous-porteuse : 847 kHz Modulation sp : OOK Codage Manchester	Modulation d'impédance Sous-Porteuse : 847 kHz Modulation sp : BPSK Codage NRZ

- standard ISO 10536
  - Cette norme spécifie les caractéristiques applicables aux cartes d'identification, aux cartes sans contact à circuits intégrés et aux cartes à couplage rapproché
    - La partie 1 définit les caractéristiques physiques
    - La partie 2 définit les dimensions et emplacements des surfaces de couplage
    - La partie 3 définit les signaux électroniques et modes de remise à zéro

Mifare Classic

- Many standards for RFID
  - ISO14443A: Mifare (NXP)
  - ISO14443B: CryptoRF (Motorola/Atmel)
  - ISO14443C: Felica (Sony)
  - ISO14443D: (OTI)
  - ISO14443E: (Cubic)
  - ISO14443F: Legic (KABA)
  - ISO15693: Tag-IT (Texas Instruments)

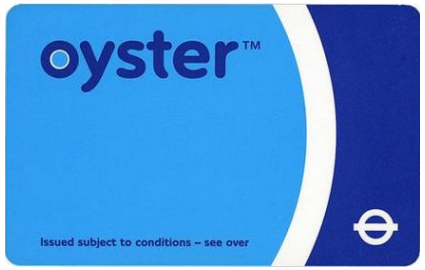
  - Typically describe physical and data-link layers (not cryptographic features)

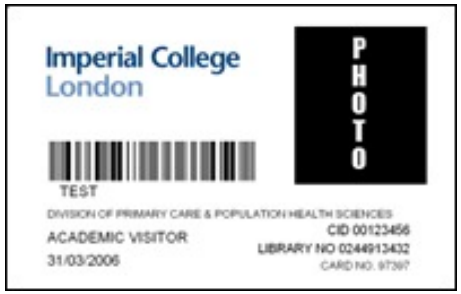
Mifare Classic

- Many chips in the Mifare (ISO14443A) family
  - Mifare Ultralight
  - Mifare Classic
  - Mifare DESFire
  - Mifare Plus
  - Mifare EV1
  - Mifare SMART MX
- Most popular: Mifare Classic
  - over 1 billion sold
  - over 200 million in use
  - 80% of contactless smartcard market

Mifare Classic Applications

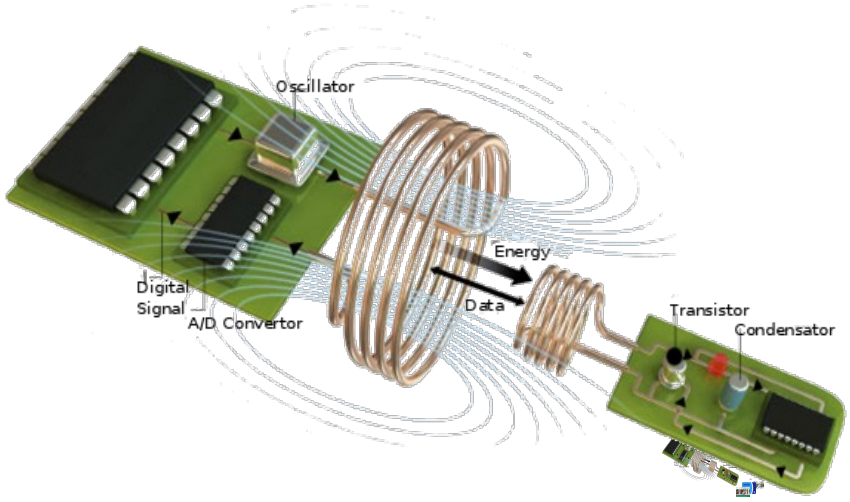
- Public transport ticketing systems
- Access control
- Wireless payment systems





RFID Security

- RFID = Radio Frequency Identification
- More properly authentication
- Contactless smartcards
  - data storage, computational capabilities
  - confidentiality
  - integrity



Common RFID Attacks

1. Relay attack
2. Replay attack
3. Cryptanalytic attack
4. Side-channel attack
5. Tracing attack
6. …

Mifare Classic is vulnerable to all of these.