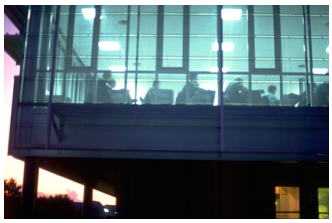


La carte à microprocesseur
De la carte à mémoire à Java Card
Un exemple de système embarqué

Pierre.Paradinas @ cnam.fr
Cnam/Cedric
Systèmes Enfouis et Embarqués (SEE)

Plan

- La carte à "mémoire" histoire d'une technologie
- La carte à microprocesseur
  - Architecture matériel
  - Normes et standards
  - Autre modèle d'OS (BasicCard, Multos, .Net,...)
  - Nouveaux modèles applicatifs
- Enjeux et perspectives de l'industrie
- Java Card

L'invention de la carte...

- Les origines sont multiples :
  - Les années 70...
  - Brevets : japonais (Arimura), allemand (Juergen Dethloff), Rolland Moreno (France), USA,...
  - 1974 : mémoire protégée par code d'accès (Innovatron/Moreno),
  - Roman de R. Barjavel "La nuit des temps"
  - L'implication d'industrielle de Bull et Schlumberger

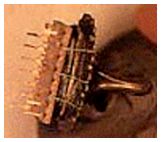
- Voir : http://www.cardshow.com/musee_carte.php

La nuit des temps

- *Chaque fois qu'un Gonda désirait quelque chose de nouveau, des vêtements, un voyage, des objets, il payait avec sa clé. Il pliait le majeur, enfonçait sa clé dans un emplacement prévu à cet effet et son compte, à l'ordinateur central, était aussitôt diminué de la valeur de la marchandise ou du service demandés.*
- René Barjavel, in "La nuit des temps", cité dans le n° 176 de "La Recherche", avril 1986, "Les cartes à puce", Michel UGON, Louis GUILLOU, p.470

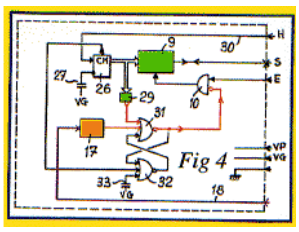
Et des implémentations...

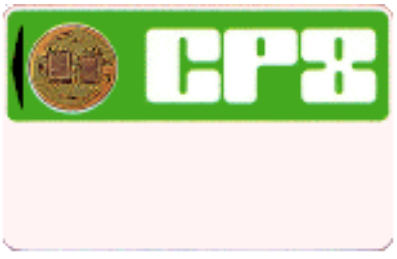
- On retrouve aussi cette forme dans un prototype de R. Moreno, le Java Ring de Sun Microsystem Inc, et le iButton de Dallas Semiconductor



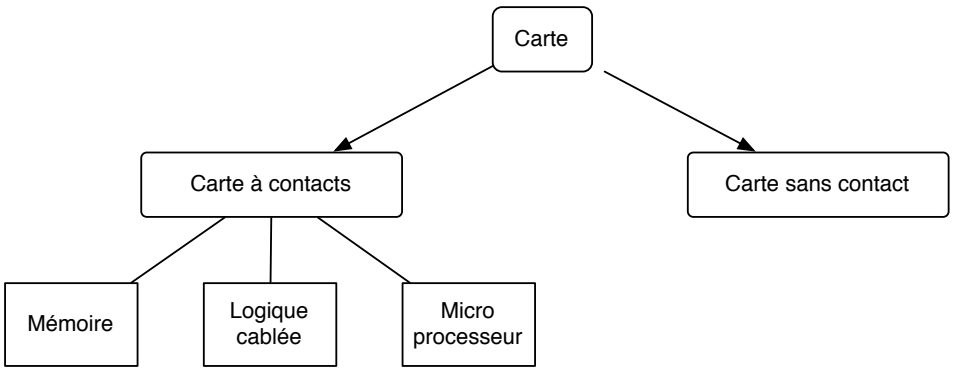
Premiers prototypes/produits

- 1978 : appel d'offre des banques françaises,
- 3 familles de produit apparaissent :
  - carte mémoire,
  - carte logique cablée,
  - carte à microprocesseur (SPOM/MAM).

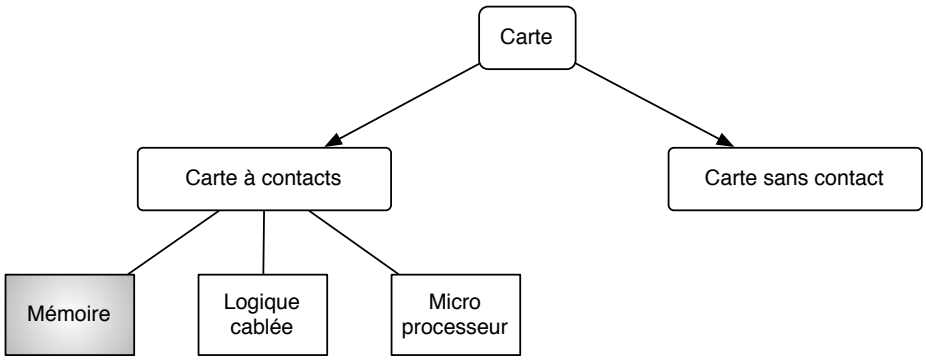




Les familles de produit



La carte à mémoire



La carte mémoire

- 1ère génération : fonction logique de stockage de données, pas de CPU.
  - notion de zone:
    - zone à valeur fixe, non modifiable [identifiant émetteur],
    - zone pour l'écriture, modifiable [compteur d'unité],
  - notion de fusible, cycle de vie de la carte [par exemple la zone à valeur fixe devient non modifiable après que le fusible soit grillée : OTP (One Time Programing)].
- Exemple la télécarte
  - (mémoire de 256 bits = ZP (96) + ZL (150))
- Pros : coût très bas. Cons : "clonage" simple.

La carte à mémoire

- Pour pallier à la faiblesse de résistance au clonage, introduction d'algorithme d'authentification dynamique de la carte.
  - En effet, avant une partie de la mémoire (EPROM) est inscrite en pré-perso chez les fabricants :
  - état vierge :

0	0	0	0

  - état après pré-personnalisation de toutes les cartes :
    - Télécarte :

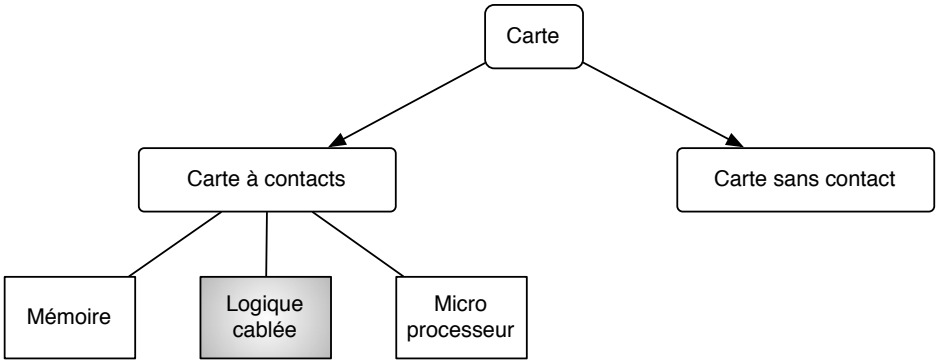
0	0	1	1

    - Pas une "télécarte" :

1	1	0	0

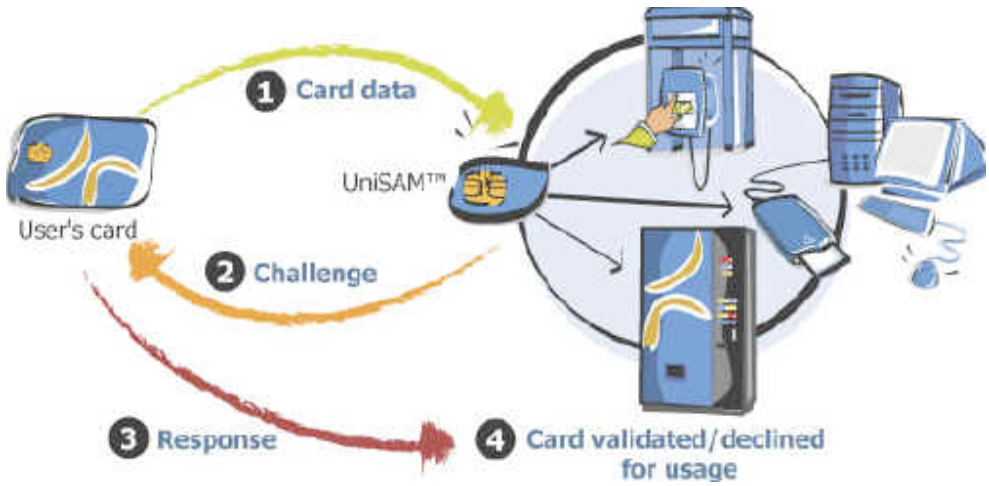
  - Pour pallier à cette faiblesse on introduit une authentification dynamique.

Carte à logique cablée



T2G (Télécarte de deuxième génération)

- Principe : (d'après http://gemplus.com)



Caractéristiques des cartes mémoires

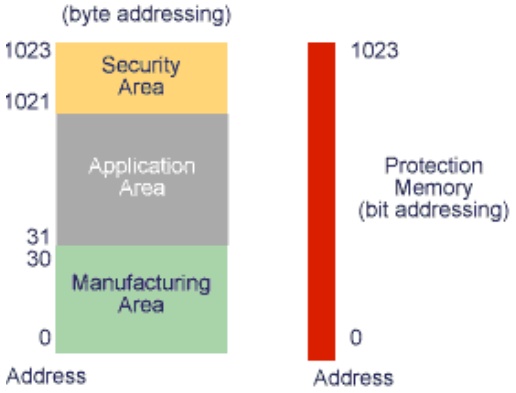
- Plusieurs produits "génériques" :
  - Eurochip II,
  - T2G (Protocole allemand).
- Caractéristiques (cas GPM 375, T2G) :
  - Le passage de l'EPROM à l'EEPROM a permis l'introduction de compteur (ici 32,767 unités).
  - Algorithme dynamique d'authentification (vérifié par un SAM = Security Access Module), procédure CBC (Cipher Block Chaining) pour lier authentification et signature de transaction.
  - Tension 5v, Protocole synchrone (5 contacts).
  - Durée de rétention , protection contre l'ESD > 4,000 volts.

Organisation de la mémoire

Adresse	Contenu	Rôle
0-15	Card manufacturer area	Identifies chip & card manufacturer
16-23	Issuer reference	Identifies issuer or application
24-63	Card identification area	Contains card serial number, secret key index, initial face value...
64-103	Abacus counter area	Holds balance of the card (units)
128-191	Authentication key	Contains card secret key
288-319	Pull-out flags	Enables to restore final counter value if transaction interrupted
320-375	56-bit user defined area	Erasable

Autres cartes de ce type

- Carte de plus grande capacité, le contrôle d'accès et la logique d'accès sont "cablés".
- d'après http://gemplus.com
- Produit GPM 2K ou 8K :
  - Protection par code secret,
  - 5v,
  - Utilise aussi le protocole 7816-3, partie synchrone



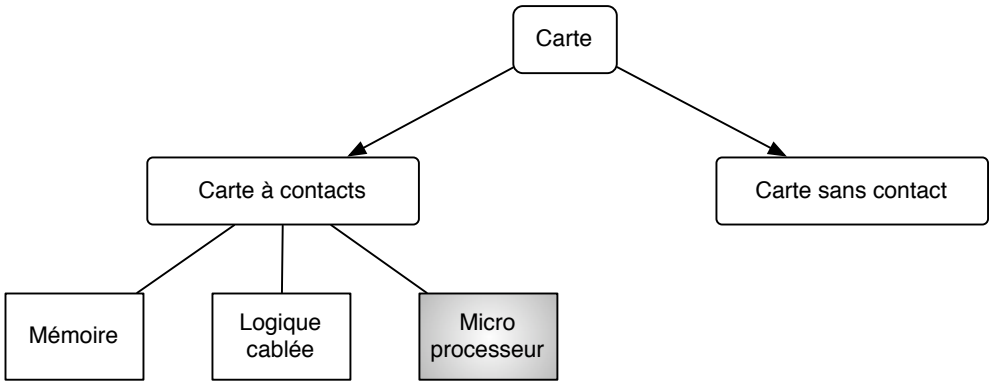
Autres Aspects

- Coût ≈ 0.2$ (en quantité...)
- Production annuelle en baisse, néanmoins 600 M unités ?
- Tendance du marché :
  - Après les années de déferlement (199x)
  - Marché en stagnation :
    - Dans les pays émergents le GSM à beaucoup baissé en prix les autorités passent plus directement aux réseaux mobiles (avec pré-paiement si nécessaire),
    - Dans les pays plus riches tout le monde à un téléphone mobile donc le besoin en téléphonie public est plus faible.
- Carte avec matière recyclable, carte de collection, etc... sont des moyens de diversification.

La carte à logique câblée

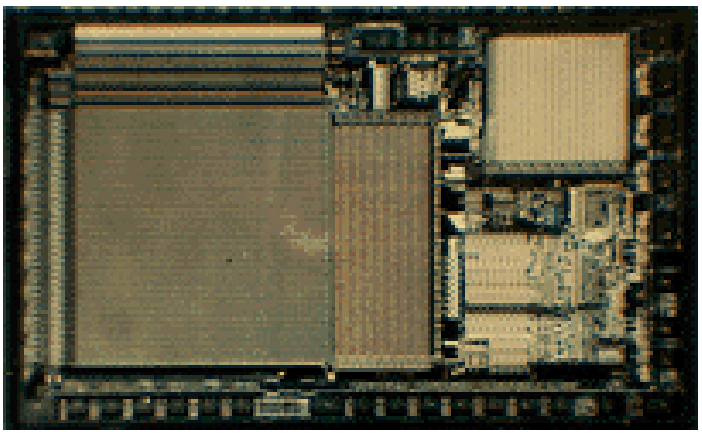
- Fonction : la carte comporte de la mémoire et des règles d'utilisation de celle-ci.
- La logique des règles est implantée de manière physique dans le silicium du composant de la carte.
- Pros : simple à définir,
- Cons :
  - Pas de souplesse, d'évolutivité de la carte : une caractéristique correspond à un ensemble de porte logiques,
  - Un silicium <=> une fonctionnalité, T2M plus long qu'avec une approche microcontrôleur et programme.
- Conduit à la carte à microprocesseur.

La carte à microprocesseur



Carte à microprocesseur

- 1978 brevet SPOM, Bull, Michel Ugon
  - Self Programming Once Memory (ou MAM : Microcalculateur Autoprogrammable Monolithique)
    - CPU + bus : permettant l'exécution de programmes, contrôlant l'accès à des mémoires, et la programmation d'une mémoire.
- 1ère implémentation de la "smart card" (CP8)
  - RAM : 36o
  - EPROM : 1ko
  - ROM : 1,6 ko



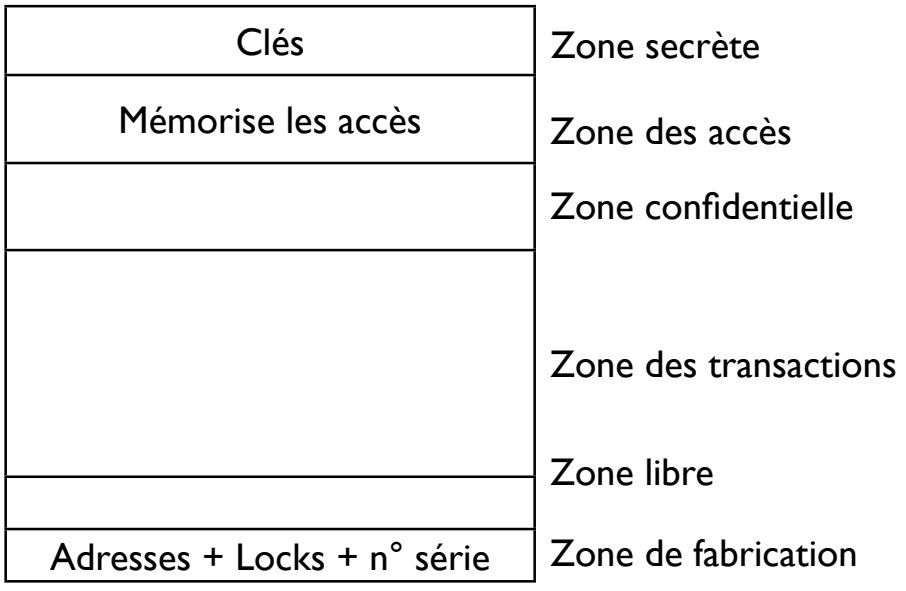
Architecture logicielle

- Gestion protocole d'E/S
- Gestion de la mémoire
- Fonction cryptographique
  - "Telepass" algorithme secret : Telpass (Data, Key)

Particularité du "système d'exploitation"

- SE et application sont imbriqués (de manière inextricable) :
  - Pas de notion de SE.
- Modèle absent ou rudimentaire :
  - Une structure de données = plan mémoire avec des zones et valeurs comme indicateurs de statut ou avancement dans le cycle de vie de la carte.
    - *On parle de "mapping" carte.*
  - Une suite de fonction = activable ou pas en fonction des valeurs de verrous (locks) qui agissent plus ou moins directement sur la mémoire.
    - *On parle de "jeu de commandes".*

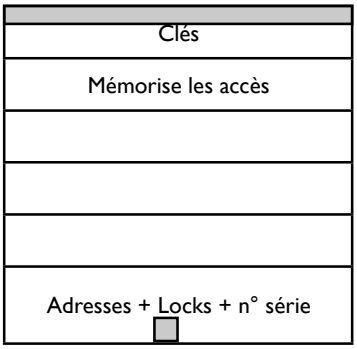
Exemple de "mapping" (carte M4)



A la préperso (à l a sortie de l'usine) : clé d e fabrication

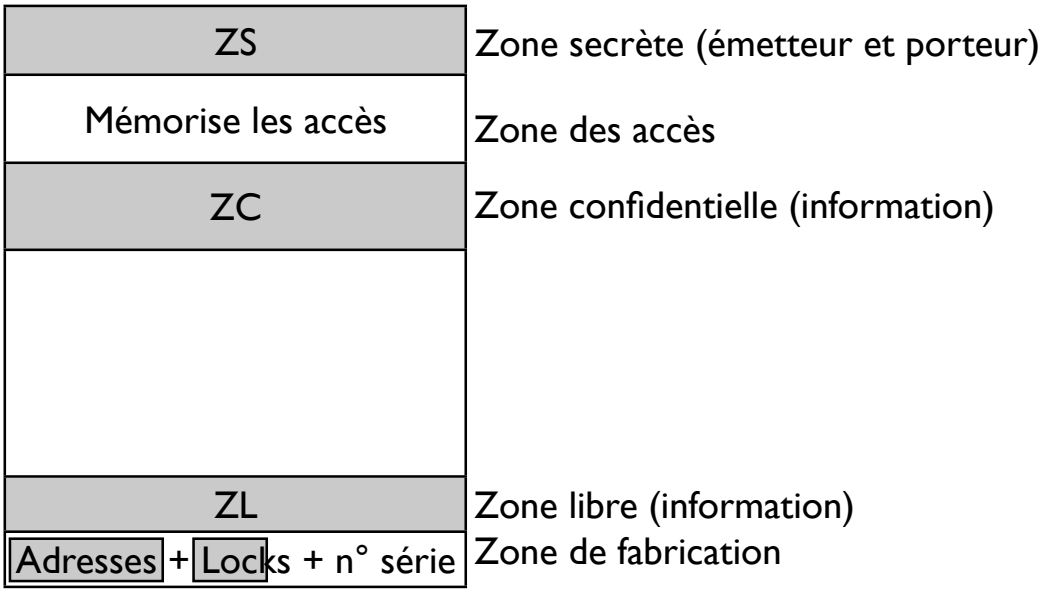
Fonctionnement (1)

- A la préperso (à la sortie de l'usine) : clé de fabrication



Fonctionnement (2)

- "Personnalisation"



Fonctionnement (3)

ZS	Zone secrète (émetteur et porteur)
Mémorise les accès	Zone des accès
ZC	Zone confidentielle (information) : *Lecture après présentation de code*
ZT	Zone transaction (information) : *Lecture & Écriture en fonction des protections*
ZL	Zone libre (information) : lecture possible
Adresses + Locks + n° série	Zone de fabrication

Fonctionnement (4)

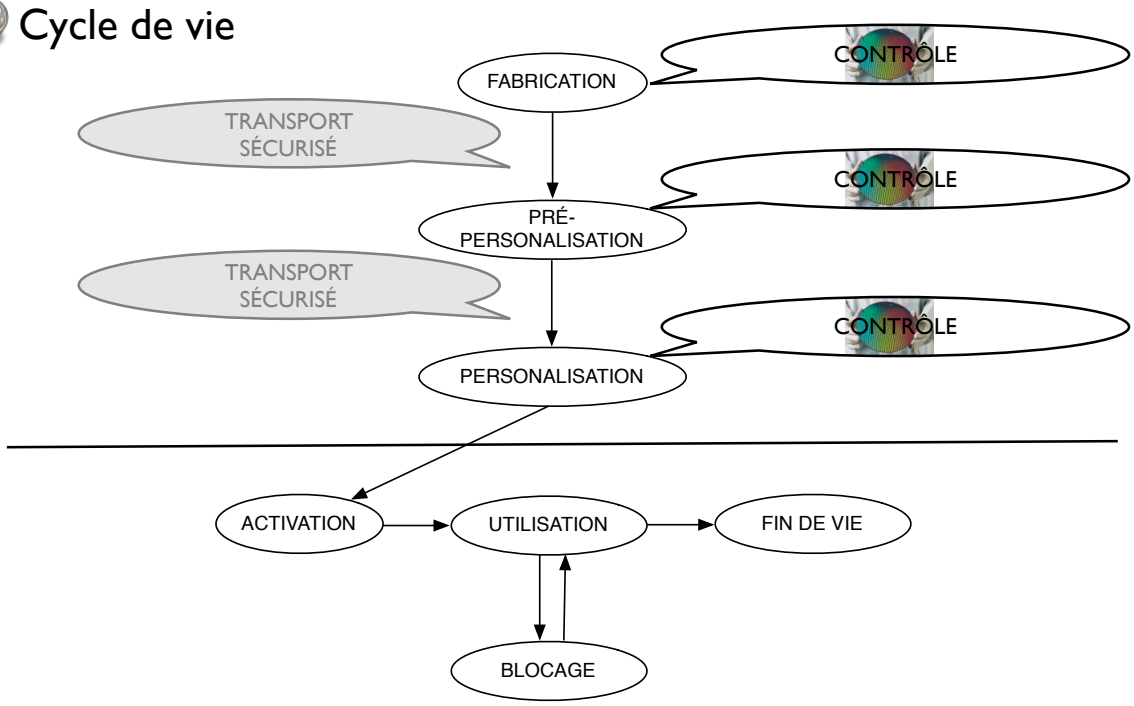
- Format du mot de 32 bits :

V	C	CA	_ _ _ _ _			

- Avec rôle particulier pour V, C et CA.

Fonctionnement (3)

- Cycle de vie

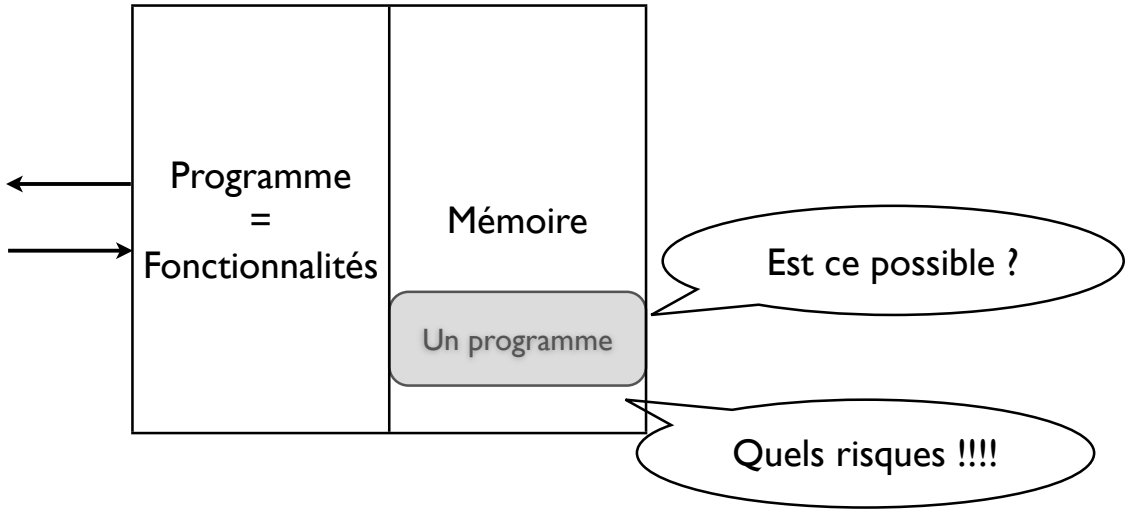


Les grands familles de SE

- Les prémisses (avant 1990):
  - M4, BO, COS,...
    - Mono-application
    - Plus ou moins figé dans les fonctions et structures
    - COS : possibilité d'ajouter des fonctions
- Les évolutions (1990-1995) :
  - MP, MP100, MCOS
  - Multi-application (répertoire ?)
- CQL (1993), Basic Card,....
- En avant vers l'ouverture...

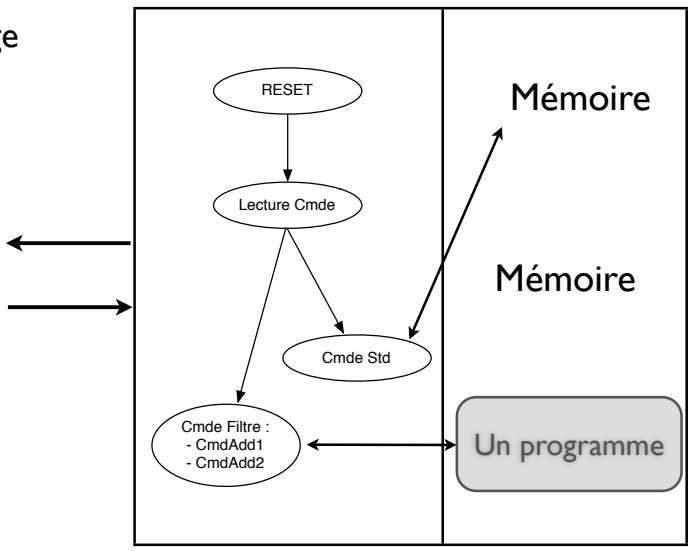
A propos du COS...

- et de l'ajout de fonctions...



Exercices

- Dans quelles conditions on peut réaliser ce type d'ajout de fonction ?
  - Le RESET doit être non contournable (pourquoi ?)
  - Table d'aiguillage



Architecture matérielle aujourd'hui

- 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

A propos de la mémoire

- 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

A propos des accès et gestion mémoire

- 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,...)

Performance des co-processeurs

- En cryptographie :

Algo	Fonction	Tps (horloge interne à 33Mhz)
RSA (1024)	Signature avec CRT	79 ms
RSA (2048)	Signature	485 ms
DES	Simple	18 µs
	Triple	8 µs
AES	avec calcul sous clés	85 µs

Détecteur de sécurité

- Horloge (haute/basse)
- Tension
- Température
- Glitch sensor
- Lumière

- Voir aussi cours sécurité et cartes (MASTER SEM & DLS)

Les standards

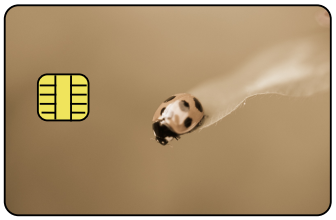
- Les normes liées à la carte :
  - ISO,
  - ETSI,
  - EMV,
  - ICAO,
  - Santé,
  - ...

Les standards ISO

- SC 17,WG4...
  - XXX
- **ISO/IEC 7816-1**
  Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics
  Cartes d'identification - Cartres à circuit(s) intégré(s) à contacts - Partie 1 : Caractéristiques physiques
  Published on 1998-10-15 (First Edition)
  The approved new title, Identification Cards - Integrated circuit cards Part 1: Cards with contacts: Physical characteristics, (see SC 17 resolution 499), will replace the current one at the next revision.
- **ISO/IEC 7816-1:1998/AM 1**
  Identification cards – Integrated circuit cards - Part 1 – Cards with contacts: Physical characteristics -- Amd 1 Maximum height of the IC contact surface
  FPDAM Ballot **17n2070** 2002-01-30 to 2002-05-31
  FPDAM Ballot Results **17n2127** 2002-06-05
  FDAM text sent to ISO/CS for FDAM ballot **17n2179** 2002-09-20
  FDAM Ballot **17n2317** 2003-05-08 to 2003-07-08
  FDAM Ballot Results **17n2335** 2003-07-16
  FDAM Disposition of Comments **wg4n1764.pdf** 2003-10-28
  Published on 2003-11-15 (First Edition)

Partie 1 : caractéristique physique

- Dimension :
  - 85.60 x 53.98 x 0.76 mm
- Contraintes : flexion et torsion
- AMD 1 (Amendement 1) : décalage maximum des contacts de la puce par rapport à la surface 0.1 mm (voir exposé sur la normalisation...)



Les standards ISO

ISO/IEC 7816-2
Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 2: Dimensions and location of the contacts
Technologies de l'information - Cartes d'identification - Cartres à circuit(s) intégré(s) à contacts - Partie 2 : Dimensions et emplacements des contacts
Published on 1999-03-01 (First Edition)
The approved new title, Identification Cards - Integrated circuit cards Part 2 – Cards with contacts: Dimensions and location of the contacts, (see SC 17 resolution 499), will replace the current one at the next revision.
Systematic Review Ballot 2004-02-12 to 2004-08-12
Systematic Review Results : 17n2683 2005-02-01

ISO/IEC 7816-2:1999/AM 1
Identification cards – Integrated circuit cards - Part 2 – Cards with contacts: Dimensions and location of the contacts -- Amd 1 Assignment of contacts C4 and C8
PDAM Ballot Results **17n2078** 2002-02-20
PDAM Disposition of Comments **WG 4 N 1637** 2002-05-16
FPDAM Ballot : **17n2191** 2002-09-20 to 2002-12-18
FPDAM Ballot Results : **17n2256** 2002-12-20
FPDAM Disposition of Comments **wg4n1708** 2003-07-10
FDAM Ballot 2004-02-26 to 2004-04-26
FDAM Ballot Results **17n2509**

Partie 2 : dimensions et positions des contacts

Les 8 contacts :

C1	VCC (Supply voltage)	Gnd	C5
C2	RST (Reset)	VPP (SPU :standard or proprietary use)	C6
C3	Clock	I/O	C7
C4	RFU	RFU	C8

- Plus de VPP depuis 1990

Evolution

- C6 : connexion d'une antenne
- C4 + C8 : utilisation pour le protocole USB

Les standards ISO

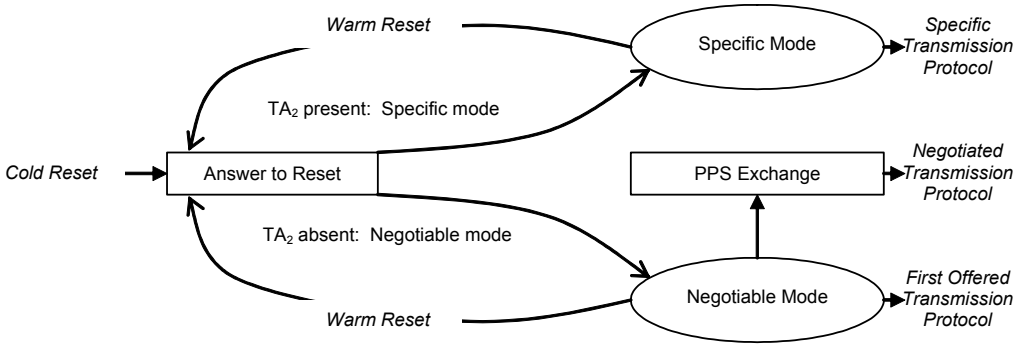
- Public :
  - ISO/IEC 7816-3:1997
    Part 3: Electronic signals and transmission protocols
    Partie 3 : Signaux électroniques et protocoles de transmission
  - ISO/IEC 7816-3:1997/Amd 1:2002
    Amendement 1 : Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V
- En chantier :
  - ISO/IEC 7816-3
    Part 3: Electronic signals and transmission protocols
    Partie 3 : Signaux électroniques et protocoles de transmission

La partie 3

- Voltage, 3 classes :
  - 5 V for class A, 60 mA,
  - 3 V for class B, 50 mA,
  - 1,8 V for class C, 30 mA.
- 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 désactiver électriquement.

Le RESET

- Le RESET va permettre de stabiliser les paramètres d'utilisation :
  - RESET à froid, en fonction de la réponse de la carte le terminal pourra présenter une autre classe (l'ordre n'est pas précisé),
  - Après le choix de la classe, et à l'aide RESET à chaud la carte et le terminal pourront s'entendre sur d'autres paramètres comme une vitesse de communication supérieur.



Les protocoles

- PPS (Protocol and Parameter Selection) permet d'ajuster les paratmètres dans la phase de RESET :
  - Type de protocole, vitesse,
  - Actuellement de 9 600 Bds à 115 000 Bds
- Les protocoles :
  - T = 0 à T = 15
  - T = 0 : Protocole par "caractères" half duplex
  - T = 1 : Protocole par "blocs" half duplex

Les autres protocoles réservés

- T=2, and T=3 sont réservés pour le full-duplex; T=4 pou half-duplex caractères,
- T=5 to T=13 réservé pour l'ISO/IEC JTC 1/SC 17,
- T=14 pour protocole propriétaire,
- T=15 pas un protocole, mais pour interface octet.

Le T=0

- Le lecteur initialise la communication par la transmission de 5 octets de commande entrante ou sortante :

CLA	INS	P1	P2	P3

- P1 et P2 paramètres;
- P3 nombre d'octets échangés dans la commande.
  - si cmde sortante P3 = 0 => 256 octets,
  - si cmde entrante P3 = 0 => pas de données.
- Après réception des 5 octets la carte répond avec un procédure byte :

Le procédure byte

- Trois types de réponse :
  - NULL c'est l'octet '60', pas d'action attente...
  - SW1 : dans ce cas la valeur est '6x' ou 9x', attendre l'octet suivant qui est le SW2 (valeur 'xy'),
  - ACK :
    - Transport des données restantes (INST, sauf '6x' et '9x')
    - Transport d'un packet de données (INST est INS $\oplus$ 'FF')
  - Les autres valeurs sont impossibles.

La réponse SW1/SW2

- La réponse SW1/SW2 indique la fin de la commande exécutée par la carte.
- Les valeurs de SW1/SW2 :
  - '9000' indicates that the command is normally completed.
  - '6E00' indicates that the class of commands is not supported.
  - '6D00' indicates that the instruction code is not programmed or is invalid.
  - '6B00' indicates that the instruction parameter is incorrect, though the card supports the instruction.
  - '6700' indicates that the number of data bytes is incorrect, though the card supports the instruction.
  - '6F00' indicates that no precise diagnosis is given, though the card supports the instruction.
  - The values where SW1 = '61', '62', '63', '64', '65', '66', '68', '69', '6A' and '6C' shall be as specified in ISO/IEC 7816-4.

Le protocole T=1

- Sous forme d'exposé ?
- Des volontaires

La commande APDU

- La paire commande/réponse :
  - Commande

CLA	INS	P1	P2	[Lc field] [Data field] [Le field]

  - Réponse

[Data field]	SW1	SW2

  - Quel est la longueur maximum des champ de données et de réponses ?
- Plusieurs cas : en fonction des valeur de C[5], C[6] et C[7], la longueur des champs peut aller jusqu'à 65535 octets.

La 7816-4

- Quelle bataille :
  - **ISO/IEC 7816-4**
    Identification cards – Integrated circuit cards - Part 4 – Organisation, security and commands for interchange
    CD Ballot : **17n2060** 2002-01-21 to 2002-04-21
    CD Ballot Results : **17n2112** 2002-04-26
    CD Disposition of Comments **WG 4 N 1649** 2002-07-19
    CD2 Ballot : **17n2155** 2002-07-22 to 2002-10-22
    CD2 Ballot Results : **17n2234** 2002-11-13
    CD2 Disposition of Comments **WG 4 N 1675** 2003-01-10
    FCD Ballot : **17n2268** 2003-01-17 to 2003-05-17
    FCD Ballot Results : **17n2319** 2003-05-22
    FCD Disposition of Comments **WG4N1726** 2003-09-29
    FCD 2 Ballot : **17n2383** 2003-09-30 to 2004-01-30
    FCD 2 Ballot Results : **17n2466** 2004-02-11
    FCD 2 Disposition of Comments **wg4n1806** 2004-06-27
    Text sent to SC 17 Secretariat ready for FDIS ballot **wg4n1805** 2004-06-27
    Notification that the revised text has been sent to ISO/CS for FDIS ballot **17n2537** 2004-07-02
    FDIS Ballot 2004-09-16 to 2004-11-16
    FDIS Ballot Results **17n2643.pdf** 2004-11-22
    Published on 2005-01-15 (Second Edition)

7816-4 (1)

- L'interchange est bâtit sur les points suivants :
  - La paire Commande-Réponse :
    - Chaînage de commande,
    - Canaux logique.
  - Data objects :
    - Les objets sont codés sur le principe TLV (tag lenght and value) et BER (basic encoding rules) de l'ASN.1 (voir ISO/IEC 8825-1)
  - Structures for applications and data
  - Security architecture

Structure des données dans la 7816-4

- MF : Master file
- DF : Dedicated file
- EF : Elementary file (internal or working) :"plat binaire", enregistrement (fixe ou pas, circulaire, tlv structure)
  - Internal : à usage de la carte
  - Working : utilisé par le monde extérieur

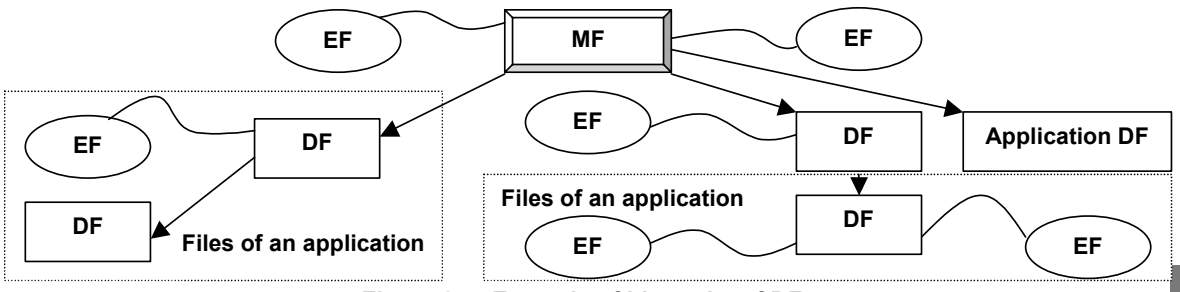


Figure 2 — Example of hierarchy of DFs

Mais aussi

Figure 3 — Example of independent application DFs

Accès aux objets

- L'accès aux objets se fait par désignation (nom DF, nom EF, nom d'objet via les tags,...) : SELECT
- Descripteur de fichier, cycle de vie

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information given
0	0	0	0	0	0	0	1	Creation state
0	0	0	0	0	0	1	1	Initialisation state
0	0	0	0	0	1	-	1	Operational state (activated)
0	0	0	0	0	1	-	0	Operational state (deactivated)
0	0	0	0	1	1	-	-	Termination state
Not all zero				x	x	x	x	Proprietary
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

Les commandes

- Binary (read, write, search, erase)
- Record (read, write, update, append, serach, erase)
- Get/Put Data

L'architecture de sécurité

- Statut de sécurité :
  - Etat atteint après l'achèvement de fonction de sécurité comme :
    - Présentation d'un code secret (VEIFY Command),
    - Connaissance d'une clé (GET CHALLENGE puis EXTERNAL AUTHENTICATE ou d'un SECURE MESSAGING.
- Les statuts :
  - Global (sur le MF),
  - Relatif à une application (DF), lors d'une (dé)sélection le statut sera modifié en fonction de règle de l'application,
  - Spécifique à un fichier,
  - Spécifique à une commande.

L'architecture de sécurité

- Les attributs de sécurité quand ils existent définissent les actions (commandes) autorisées et dans quelles conditions. Plus particulièrement :
  - Le statut de la carte avant un accès en lecture,
  - Restreindre l'usage de fonction en fonction du statut,
  - Précise comment atteindre un statut de sécurité en définissant les fonctions à activer.

Les fonctions de sécurité

- Authentification par mot de passe
- Authentification par clé à l'aide des fonctions (GET CHALLENGE suivi de EXTERNAL AUTHENTICATE, regroupées aussi dans GENERAL AUTHENTICATE)
- Authentification de données :
  - La carte compare des données reçues à celles dont elle dispose en utilisant des données qui lui sont propres (clé secrète ou clé public),
  - ou la carte calcule des données (avec des CRC cryptographique ou des signatures digitales), qu'elle peut ensuit écrire.
  - Intérêt pour le "provider".
- Chiffrement de données.

Exemple

Table 15 — Channel security attribute

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	-	-	1	Not shareable
0	0	0	0	0	-	1	-	Secured
0	0	0	0	0	1	-	-	User authenticated
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

Secure messaging

- Objectif : Protéger les échanges, dans la paire commande/réponse (tout ou partie ainsi que dans les commandes chaînées) par :
  - confidentialité des données, et
  - authentification des données.
- Attention

Command header	Command body
CLA INS P1 P2	[L_c field] [Data field] [L_e field]

Response body	Response trailer
[Data field]	SW1-SW2

Figure 5 — Command-response pair

Command header	Command body
CLA* INS P1 P2	[New L_c field] - {[Secured data field] = [T-N_c-Data bytes] - [T-'01' or '02'-L_e]} - [New L_e field]

Response body	Response trailer
[Secured data field] = [T-Nr-Data bytes] - [T-'02'-SW1-SW2]	SW1-SW2

Figure 6 — Secured command-response pair

Les commandes de la partie 4

Command name	INS	See
ACTIVATE FILE	'44'	Part 9
APPEND RECORD	'E2'	7.3.7
CHANGE REFERENCE DATA	'24'	7.5.7
CREATE FILE	'E0'	Part 9
DEACTIVATE FILE	'04'	Part 9
DELETE FILE	'E4'	Part 9
DISABLE VERIFICATION REQUIREMENT	'26'	7.5.9
ENABLE VERIFICATION REQUIREMENT	'28'	7.5.8
ENVELOPE	'C2', 'C3'	7.6.2
ERASE BINARY	'0E', '0F'	7.2.7
ERASE RECORD (S)	'0C'	7.3.8
EXTERNAL (/ MUTUAL) AUTHENTICATE	'82'	7.5.4
GENERAL AUTHENTICATE	'86', '87'	7.5.5
GENERATE ASYMMETRIC KEY PAIR	'46'	Part 8
GET CHALLENGE	'84'	7.5.3
GET DATA	'CA', 'CB'	7.4.2
GET RESPONSE	'C0'	7.6.1
INTERNAL AUTHENTICATE	'88'	7.5.2
MANAGE CHANNEL	'70'	7.1.2
MANAGE SECURITY ENVIRONMENT	'22'	7.5.11
PERFORM SCQL OPERATION	'10'	Part 7
PERFORM SECURITY OPERATION	'2A'	Part 8
PERFORM TRANSACTION OPERATION	'12'	Part 7
PERFORM USER OPERATION	'14'	Part 7
PUT DATA	'DA', 'DB'	7.4.3
READ BINARY	'B0', 'B1'	7.2.3
READ RECORD (S)	'B2', 'B3'	7.3.3
RESET RETRY COUNTER	'2C'	7.5.10
SEARCH BINARY	'A0', 'A1'	7.2.6
SEARCH RECORD	'A2'	7.3.7
SELECT	'A4'	7.1.1
TERMINATE CARD USAGE	'FE'	Part 9
TERMINATE DF	'E6'	Part 9
TERMINATE EF	'E8'	Part 9
UPDATE BINARY	'D6', 'D7'	7.2.5
UPDATE RECORD	'DC', 'DD'	7.3.5
VERIFY	'20', '21'	7.5.6
WRITE BINARY	'D0', 'D1'	7.2.4
WRITE RECORD	'D2'	7.3.4

INS	Command name	See
'04'	DEACTIVATE FILE	Part 9
'0C'	ERASE RECORD (S)	7.3.8
'0E', '0F'	ERASE BINARY	7.2.7
'10'	PERFORM SCQL OPERATION	Part 7
'12'	PERFORM TRANSACTION OPERATION	Part 7
'14'	PERFORM USER OPERATION	Part 7
'20', '21'	VERIFY	7.5.6
'22'	MANAGE SECURITY ENVIRONMENT	7.5.11
'24'	CHANGE REFERENCE DATA	7.5.7
'26'	DISABLE VERIFICATION REQUIREMENT	7.5.9
'28'	ENABLE VERIFICATION REQUIREMENT	7.5.8
'2A'	PERFORM SECURITY OPERATION	Part 8
'2C'	RESET RETRY COUNTER	7.5.10
'44'	ACTIVATE FILE	Part 9
'46'	GENERATE ASYMMETRIC KEY PAIR	Part 8
'70'	MANAGE CHANNEL	7.1.2
'82'	EXTERNAL (/ MUTUAL) AUTHENTICATE	7.5.4
'84'	GET CHALLENGE	7.5.3
'86', '87'	GENERAL AUTHENTICATE	7.5.5
'88'	INTERNAL AUTHENTICATE	7.5.2
'A0', 'A1'	SEARCH BINARY	7.2.6
'A2'	SEARCH RECORD	7.3.7
'A4'	SELECT	7.1.1
'B0', 'B1'	READ BINARY	7.2.3
'B2', 'B3'	READ RECORD (S)	7.3.3
'C0'	GET RESPONSE	7.6.1
'C2', 'C3'	ENVELOPE	7.6.2
'CA', 'CB'	GET DATA	7.4.2
'D0', 'D1'	WRITE BINARY	7.2.6
'D2'	WRITE RECORD	7.3.4
'D6', 'D7'	UPDATE BINARY	7.2.5
'DA', 'DB'	PUT DATA	7.4.3
'DC', 'DD'	UPDATE RECORD	7.3.5
'E0'	CREATE FILE	Part 9
'E2'	APPEND RECORD	7.3.6
'E4'	DELETE FILE	Part 9
'E6'	TERMINATE DF	Part 9
'E8'	TERMINATE EF	Part 9
'FE'	TERMINATE CARD USAGE	Part 9

– In the interindustry class, any valid INS code not defined in ISO/IEC 7816 is reserved for future use by ISO/IEC JTC 1/SC 17.

Les valeurs de SW1/SW2

	SW1-SW2	Meaning
Normal processing	'9000'	No further qualification
	'61XX'	SW2 encodes the number of data bytes still available (see text below)
Warning processing	'62XX'	State of non-volatile memory is unchanged (further qualification in SW2)
	'63XX'	State of non-volatile memory has changed (further qualification in SW2)
Execution error	'64XX'	State of non-volatile memory is unchanged (further qualification in SW2)
	'65XX'	State of non-volatile memory has changed (further qualification in SW2)
	'66XX'	Security-related issues
Checking error	'6700'	Wrong length; no further indication
	'68XX'	Functions in CLA not supported (further qualification in SW2)
	'69XX'	Command not allowed (further qualification in SW2)
	'6AXX'	Wrong parameters P1-P2 (further qualification in SW2)
	'6B00'	Wrong parameters P1-P2
	'6CXX'	Wrong L_e field; SW2 encodes the exact number of available data bytes (see text below)
	'6D00'	Instruction code not supported or invalid
	'6E00'	Class not supported
	'6F00'	No precise diagnosis

Les autres parties de la 7816

- Part 5: Registration of application providers
- Part 6: Interindustry data elements for interchange
- Part 7: Interindustry commands for Structured Card Query Language (SCQL)
- Part 8: Commands for security operations
- Part 9: Commands for card management
- Part 10: Cards with contacts: Electronic signals and answer to reset for synchronous cards
- Part 11: Personal verification through biometric methods
- Part 12: Cards with contacts: USB electrical interface and operating procedures
- Part 15: Cryptographic information application

La norme 24727

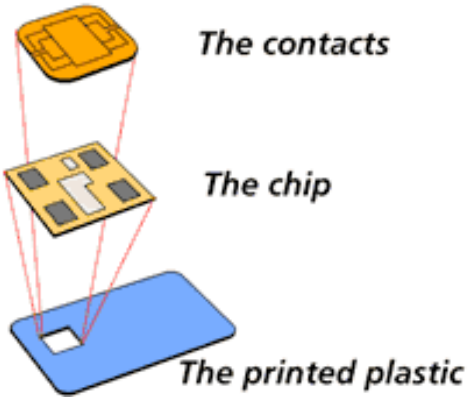
Les standards ETSI

La norme EMV

Cycle de vie d'une carte

- Fabrication du support ou corps de carte
  - Plastique laminé, ABS coulé, autre facteur de forme

- Fabrication du composant (galette de silicium ou "wafer")
- Fabrication du module :
  - Découpage/Sciage,
  - Contact/Binding,
  - Protection dans le module,
  - Collage.



Cycle de vie d'une carte (suite)

- Personnalisation : la carte comporte généralement le SE (il est inscrit en ROM)
- La personnalisation consistera :
  - à finir de paramètrer le SE
    - taille des mémoires utilisateur !
    - limitations de fonction
  - Renseigner les informations de l'application par rapport aux :
    - émetteur et ses services
    - porteur et ses services
    - de manière électrique et graphique

Cycle de vie d'une carte (suite)

- Distribution.
- Vie de la carte :
  - Utilisation,
  - Perte, fin de vie.

Contraintes de fabrication et de personalisation

- Les cartes sont potentiellement de l'argent, un moyen d'accès à un services
  - Besoins de sécuriser l'accès physique aux locaux
  - Besoins de contrôler les "composants" utilisés ou pas !
    - Suivi complet/ traçabilité des produits

Avantages & propriétés des cartes

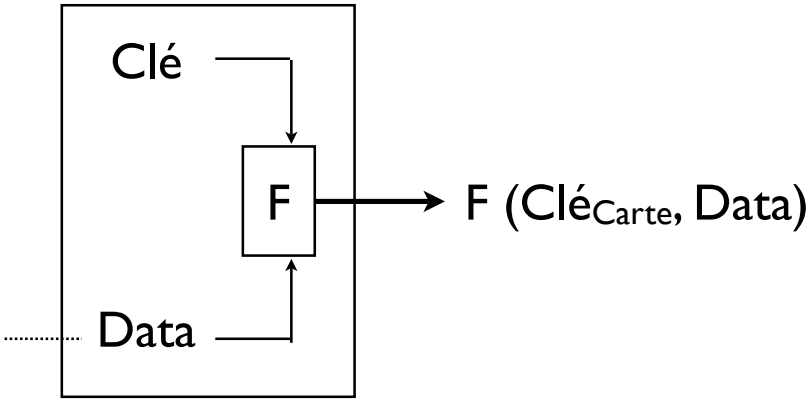
- Un dispositif de mémorisation sécurisé(e) :
  - Écriture et lecture se font sous contrôle
    - Porteur (Pin Code) et/ou partenaire de la carte
    - Émetteur

Autre travaux

- Approche SGBD étendu par rapport à la 7816-7 par les équipes Pucheral & Bouganim (XXX)
- Extension de la zone mémoire de la carte (voir article de P. Bigett sur gemplus.com)

Avantages & propriétés des cartes

- Dispositif de protection de clé(s) cryptographiques
  - Des mots (zones) mémoires peuvent être utilisés pour mémoriser des clés cryptographiques :
    - Confidentialité de la clé (personne ne peut *lire*)
    - Intégrité de la clé et du calcul de la fonction F (personne ne peut *modifier*)



Ecriture du logiciel pour la carte

- Les langages et méthodes :
  - Assembleur au début :
    - PLACE, PLACE, PLACE... et rapidité
      - et retour aujourd'hui vers ce langage pour d'autres raisons !
        - *(voir cours de sécurité).*
  - Début des années 1990 arrivée de C/Pascal interprété (gain de place au niveau du code, prototypage facile) mais manque d'efficacité et sur le petits codes l'approche est pas "rentable".
  - Puis langage C, processeur plus gros et plus adaptés
    - Pros : proche des machines, efficace, disponibles,
    - Cons : un peu "bidouille".

Ecriture du logiciel pour la carte

- Puis "Java Card Technology", la raison du passage à Java n'est pas liée au langage et à ses bonnes propriétés...
  - C'est lié à un besoin des applications qui avait besoin d'adaptabilité de leurs services.
- Les challenges et enjeux aujourd'hui sont liés :
  - L'augmentation de la **complexité** des codes qui font plusieurs 100 ko, même si celà reste "petit" au regard d'autres industries, les contraintes sont fortes :
    - T2M, taille/efficacité/sécurité, QUALITE, QALITE, QUALITE, QUALITE
    - Arrivée de nouveaux concepts.

Les nouveaux concepts émergents

- La carte va vivre dans les 3 à 5 ans une nouvelle vague d'innovations dans le domaine du logiciel :
  - Nouveau composant (aujourd'hui sous utilisé) : MMU/MPU, mode user/super user,
  - Multi-tâche,
  - Nouvelle pile de protocole (SLIP, IP, TCP-IP,...)
  - Les contraintes industrielles vont aussi pousser à une meilleure modularité et ré-utilisabilité des codes.
- Ceci va générer une réelle mise en place d'un système d'exploitation pour carte. (www.inspired.org).

Aspects développement du DES

- DES 3 étapes dans son développement :

faire rentrer

optimiser

protéger

Le code a augmenté sa taille.
Le code a augmenté son temps d'exécution.
Aujourd'hui réalisé par matériel...

Développement ?

- NON ce n'est pas le plus important.

Qualité du Logiciel

Qualité du logiciel

- Par évitement des fautes à la construction,
- Par la qualité du développement,
- et par le test...
- Quel est la part du test dans le coût de développement ?
  - Etapes :

Conception	Développement	Test

  - Coût/temps :

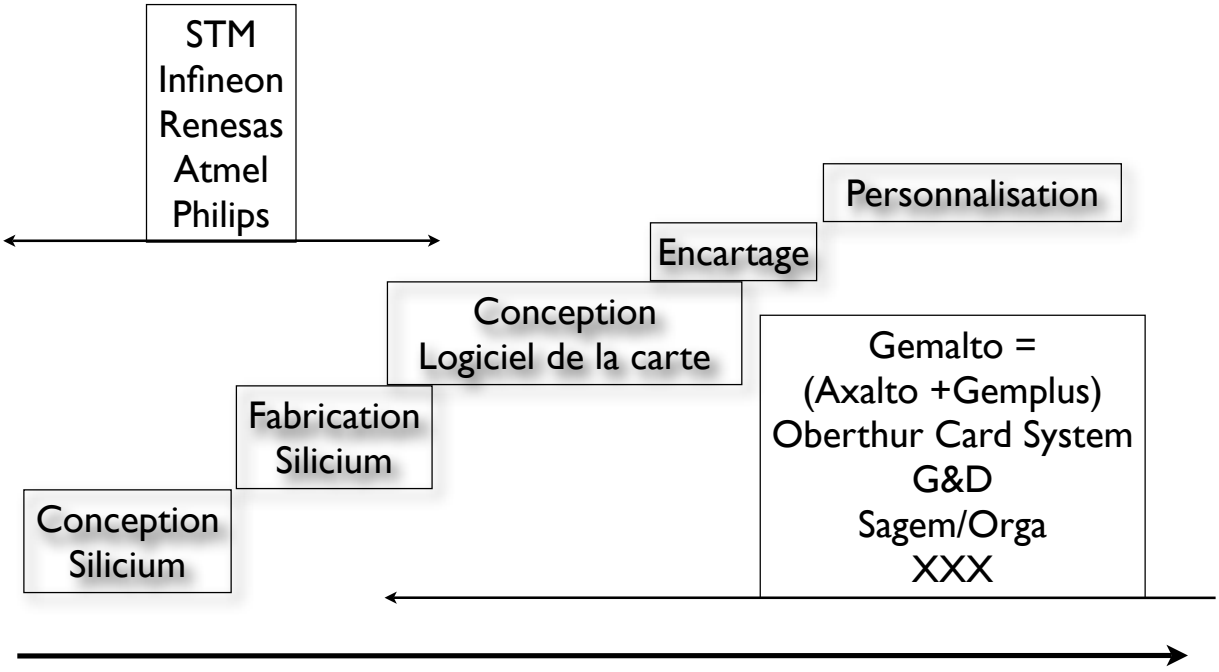
Conception	Développement	Test

  - Temps : peut être le frein au lancement du produit.

Etapes du développement de l'industrie

- La carte à microprocesseur et les grandes étapes de développement (marché et technique) :
- Les pionniers (1975-1985) : de(s) idées aux premiers produits, les bases technologiques sont établies,
- 1985-1995 : les marchés et les déploiement importants sont là, la technologie du départ est améliorée et renforcée, des limites apparaissent (besoin de flexibilité qui an- nonce Java Card)
- 1995-2005 : explosion du marché, qui s'accompagne d'un nouveau paradigme les cartes évolutives

La chaîne de la valeur



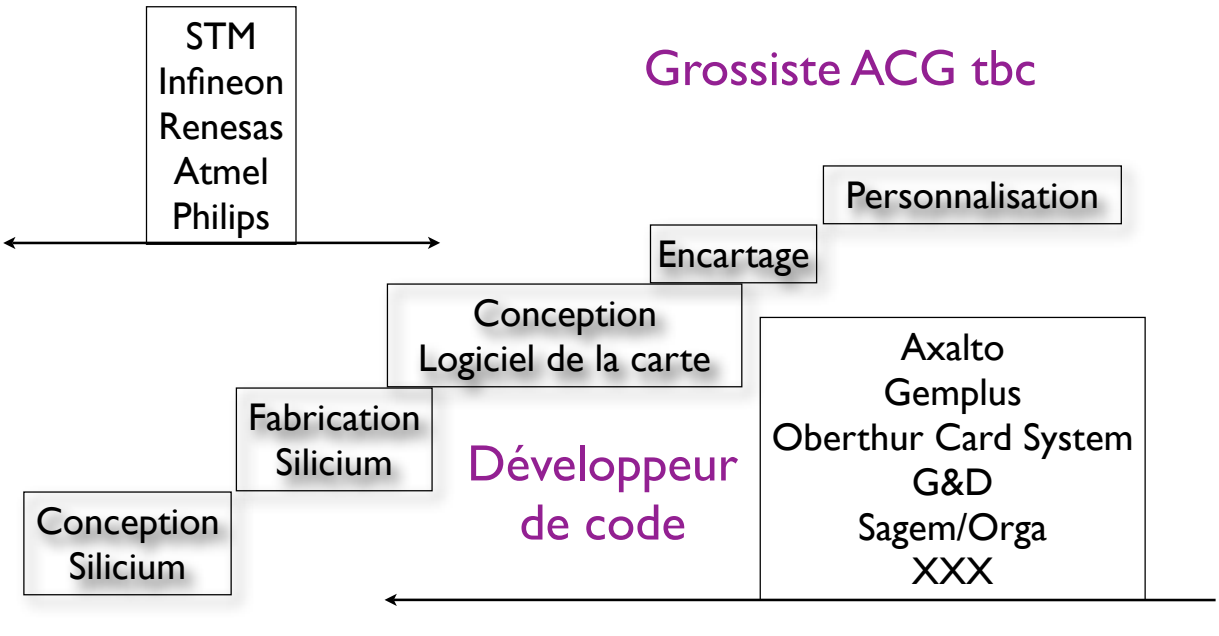
L'origine des fabricants

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

Nouveaux acteurs

- Dans un métier ou une brique "classique" :
  - Sagem est entré à la fin des années 90.
- Avec une technologie, standard de fait et une "vision" :
  - Sun et Java Card Technology (1996),
  - Windows for SC (W4SC) après l'arrivée de Sun.
- Avec une approche système complet et acteurs du domaine (IBM).
- "Grossiste de la fabrication".
- Réalisateur de logiciel : système d'exploitation pour carte (Aspect Software, Trusted Logic, ...).

Nouveaux acteurs



Nouveaux défis

- Concentration encore plus forte :
  - Sagem + Orga
  - Axalto + Gemplus = Gemalto
  - (Microelectronica absorbé par mSystem) absorbé par SanDisk !
  - RSA absorbé par EMC
- Prix des cartes en chute libre régulière (20% par an !)
- Arrivée des fabricants chinois

Les volumes d'après http://www.eurosmart.com/index.htm

EUR SMART THE VOICE OF THE SMART CARD INDUSTRY

2006 Worldwide Shipments

	Smart Cards (Millions of units - Mu)		
	Memory	Microprocessor	
			Growth From 2005
Telecom	510	1650	18,7%
Financial Services - Retail - Loyalty	30	400	20%
Government -Healthcare	25	85*	42%
Transport	85	25	25%
Pay TV	-	60	9%
Corporate Security	10	20	33%
Others	10	15	-
TOTAL	670	2255	20%
TOTAL 2006 Forecast	2925*		

* : not including China ID Smart Card

Exercice

- Donnez les grandes lignes des fonctions d'une application "carte d'entreprise".
  - Expliciter les données contenues dans la carte, listez les fonctions mettant en oeuvre ces données (aspects in-card et off-card).
  - Expliciter les fonctions exécuter par les lecteurs ou points de "contacts" des cartes.
- Donnez et listez les contraintes qui sont celles d'un système de personnalisation du badge d'entreprise décrit précédemment.

Bibliographie

- http://www.cardshow.com/musee_carte.php
- http://{axalto, gemplus, gemalto}.com, Obertur Card System, Sagem Orga,...
- http://www.eurosmart.com/index.htm