http://membres-liglab.imag.fr/donsez

La Carte à Microprocesseur

communément denommé

carte à puce

Un système mobile en plein essor

Didier Donsez (Univ. Joseph Fourier, Grenoble 1)

En collaboration avec

Gilles Grimaud (Univ. Lille 1)

Sébastien Jean (Univ Pierre Mendés France, Grenoble 2)

Sylvain Lecomte (Univ. Valenciennes)

Sommaire

- Sur la carte elle-même :
  - 1. Historique
  - 2. La fabrication de la carte et cycle de vie
  - 3. La normalisation
- Sur son architecture :
  - 1. Communication Carte Lecteur
  - 2. La norme 7816-4
  - 3. La sécurité

Définition de la carte à microprocesseur

support électronique de données

- doté d'une capacité de traitement,
- qui se présente sous la forme d'une carte à format réduit
- possédant un microprocesseur et son environnement (mémoires, entrées/sorties).

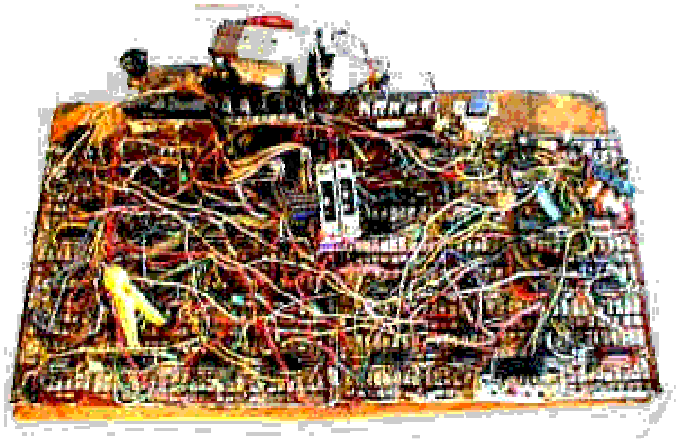
Un peu de vocabulaire

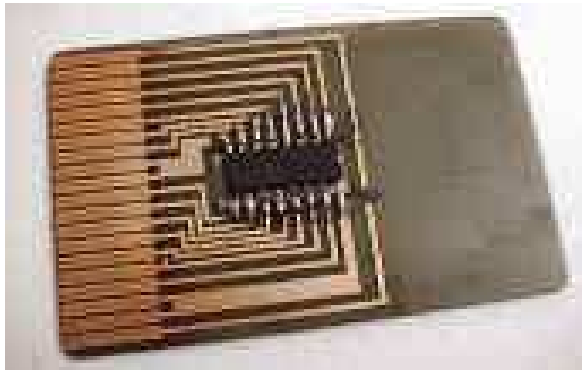
- Carte à mémoire :
  - Mémoire de 256 à 1024 bits
  - R/W sans protection, mais possibilité d ’utiliser des « fusibles »
    - Ex : Télécarte, carte de stationnement, cinéma
- Carte à logique câblée :
  - Mem : 4600 bits protégés par des circuits
  - Contrôle de code du porteur
    - ex : carte d ’accès physique
- Carte à microprocesseur
  - Processeur encarté
  - possibilité de calculs algorithmiques

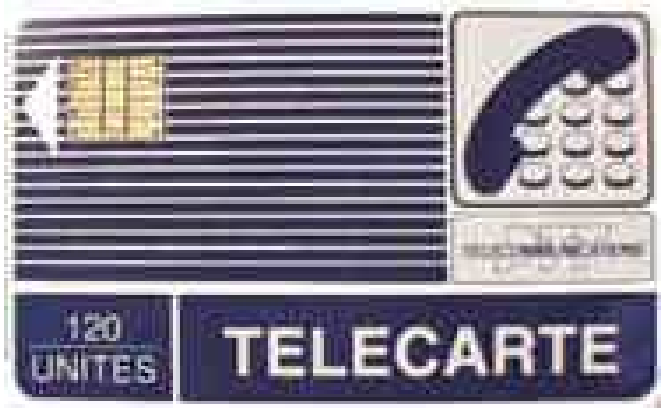
Historique

- 1951 :
  - Carte plastique Diners Club (Frank McNamara)
- 1970 :
  - La carte à mémoire connaît un succès grandissant
- 1974-1975 :
  - Roland Moreno remplace l'enregistrement magnétique par un composant électronique et crée la société INNOVATRON
- 1981 :
  - Premier Microcalculateur Auto Programmable Monolithique.
- 1984 :
  - Lancement de la télécarte
- 1986 :
  - Apparition des cartes bancaires "haut de gamme" VISA
- 1989 :
  - Première version du GSM

Quelques spécimens de mon Zoo

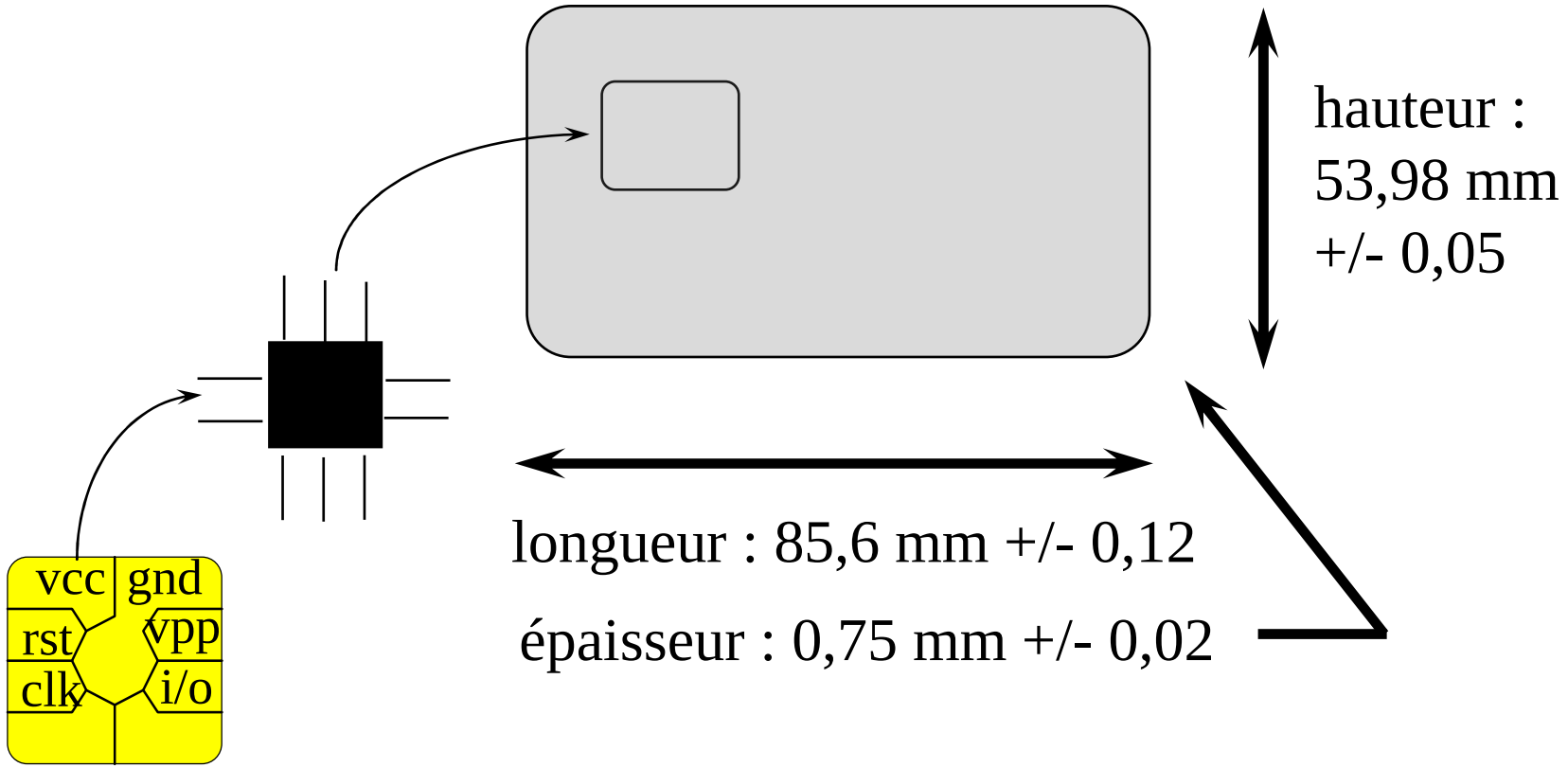






Coté matériel

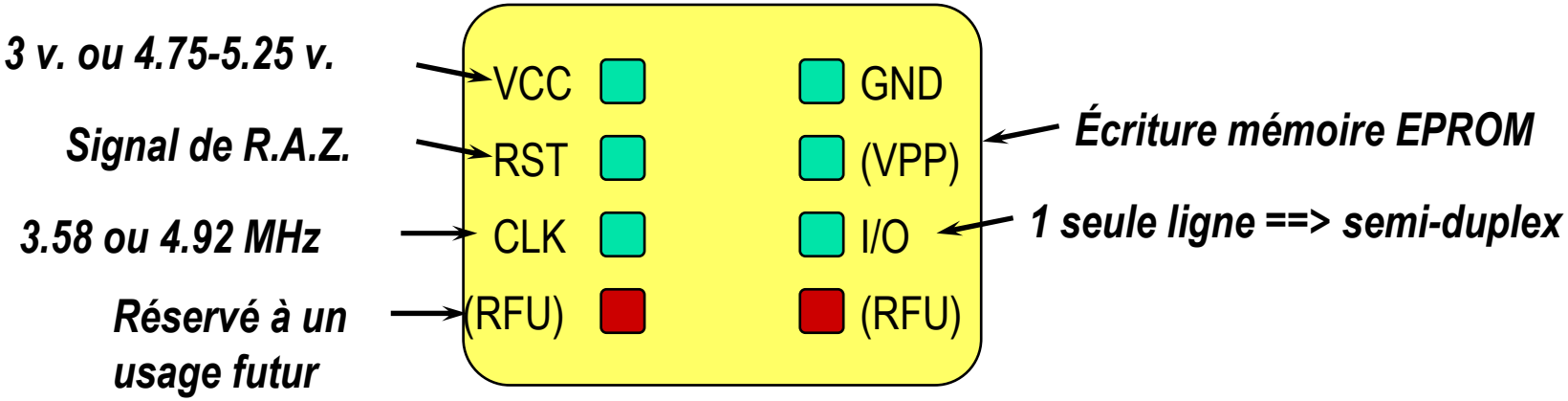
Caractéristiques de la carte



- Norme ISO 7810 : Caractéristiques physiques (1ère partie)
- Norme ISO 7816-1 : Caractéristiques physiques (2ème partie)
- Norme ISO 7816-2 : Caractéristiques électriques

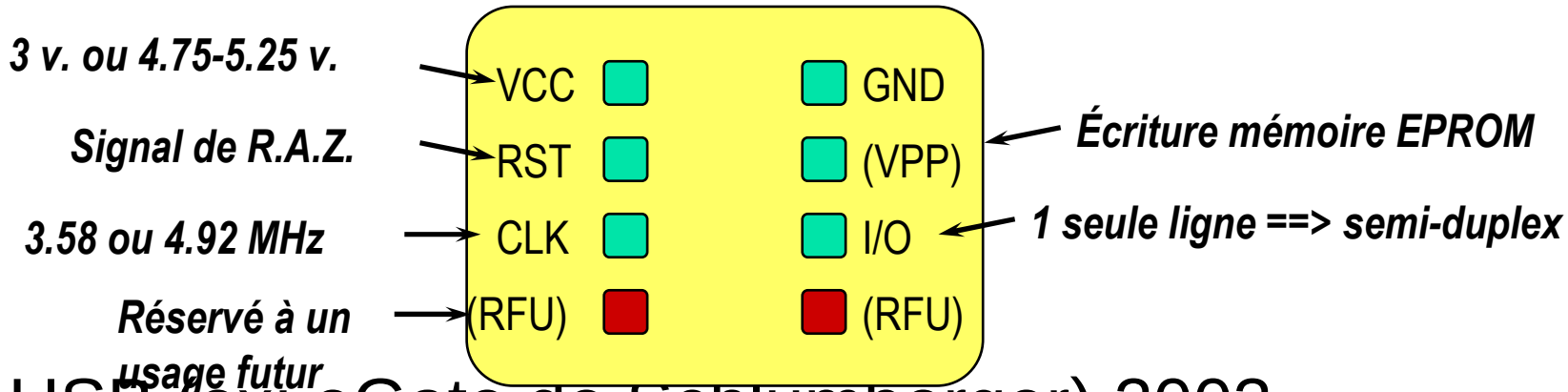
La carte avec contact (i)

- ISO 7816-2

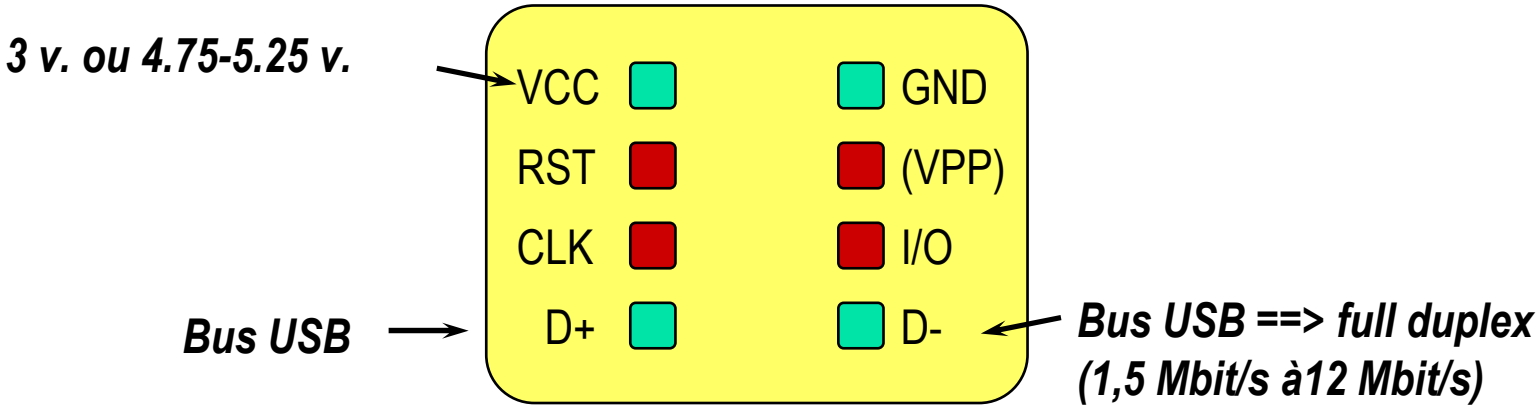


La carte avec contact (ii)

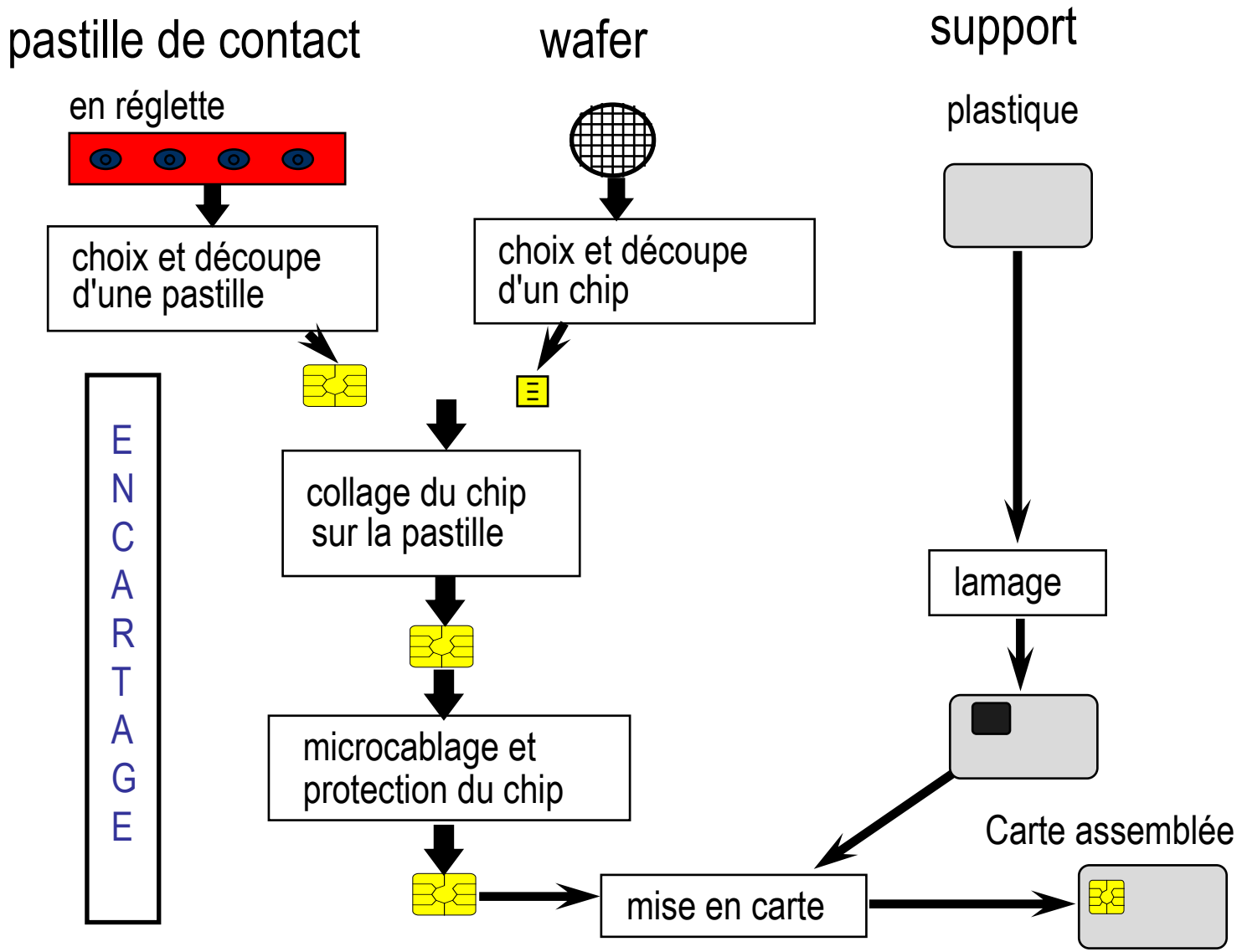
- ISO 7816-2



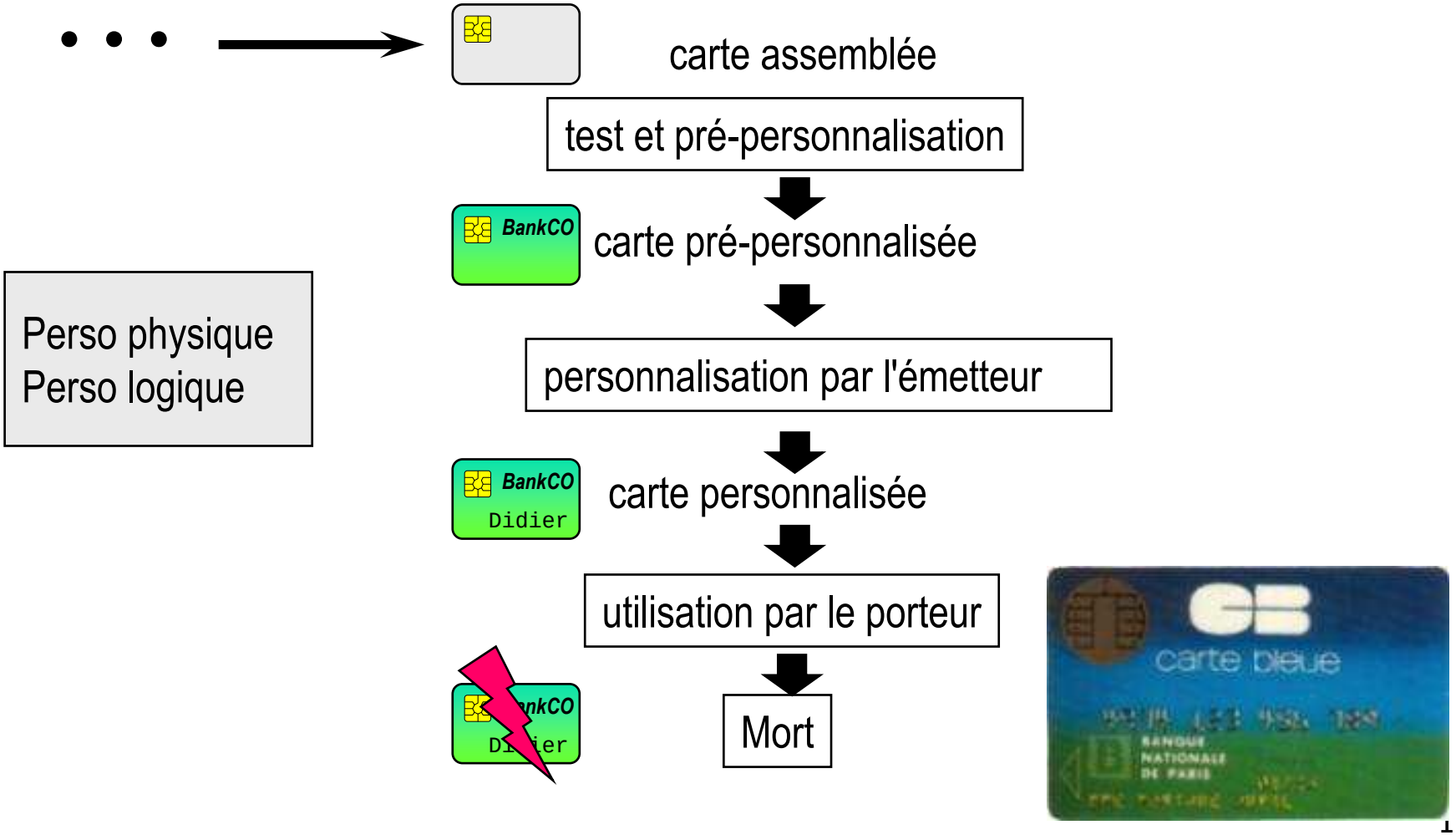
- USB (ex: eGate de Schlumberger) 2003



Fabrication et Personnalisation d'une carte (i)

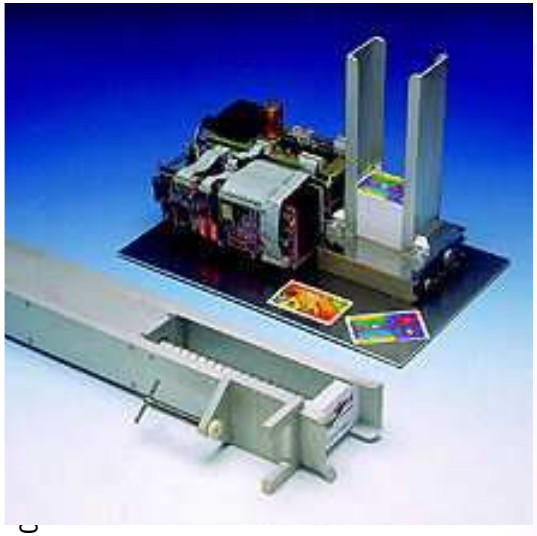


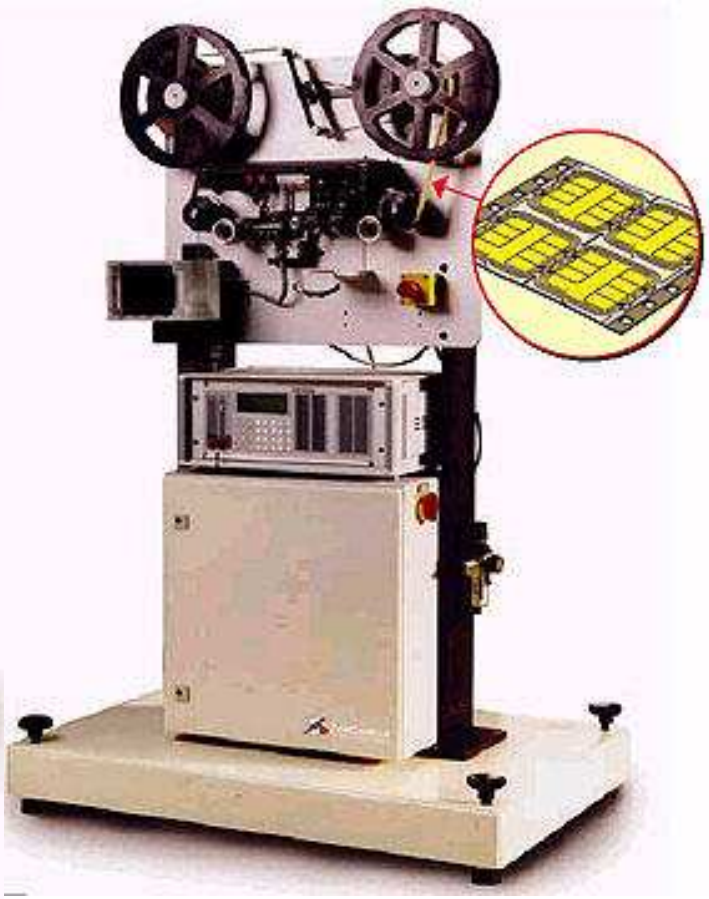
Fabrication et Personnalisation d'une carte (ii)



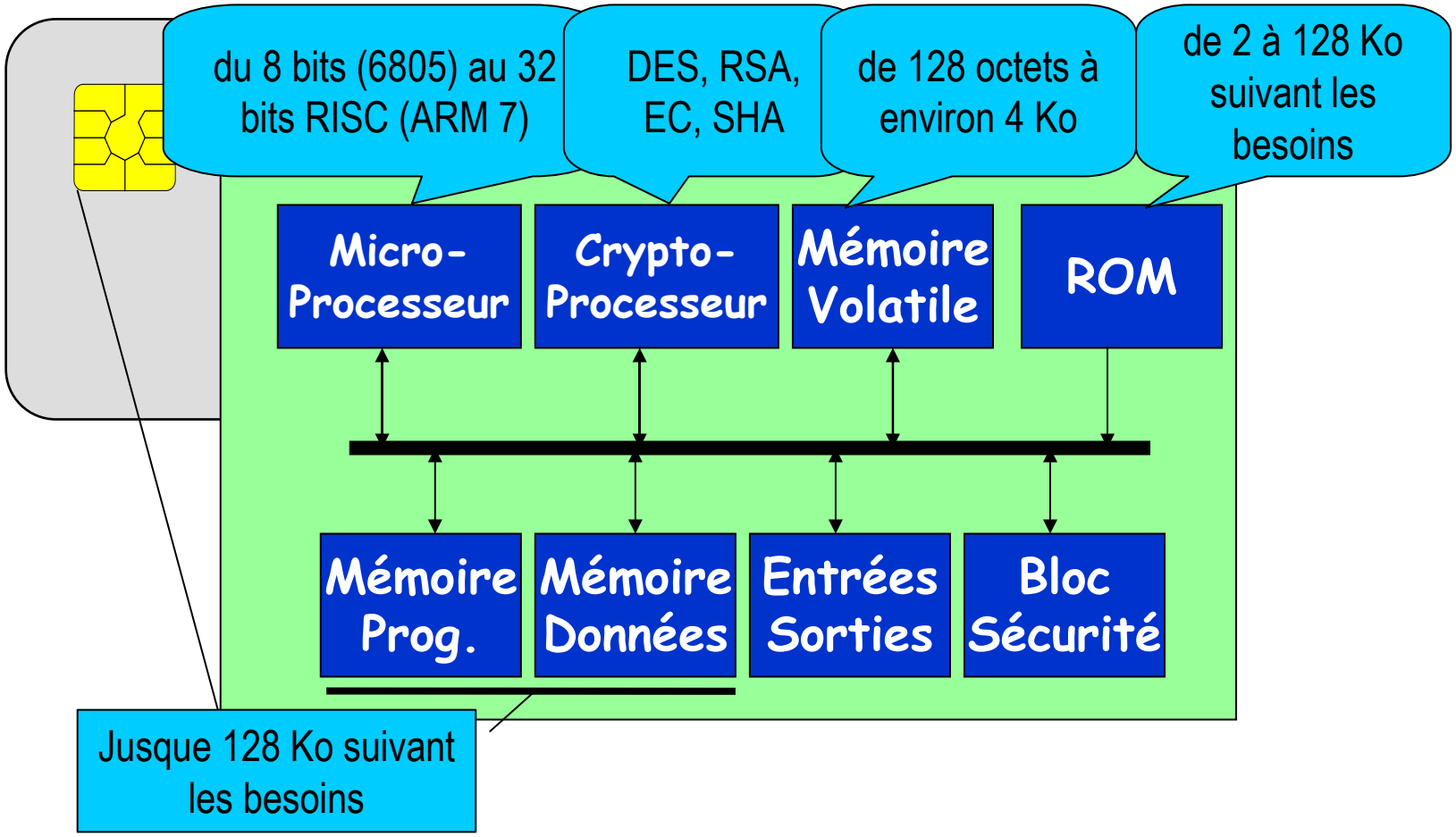
Fabrication et Personnalisation d'une carte (iii)

Station de personnalisation





Architecture matérielle



Types de mémoire dans la Carte

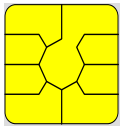
	RAM Statique	EEPROM	Flash-RAM	Fé-RAM (expérimentale)
Persistance	Volatile	Non Volatile	Non Volatile	Non Volatile
Tps Accès Read	0.1 µs	0.15 µs	0.15 µs	0.1 µs
Tps Accès Write	0.1 µs	10 µs	10 µs	0.4 µs
Tps Effacement (Reset)	**Sans**	5 000 µs	100 000 µs	**Sans**
Granularité Effacement	Sans	4 Octets	64 Octets	Sans
Nombre de Cycles garanti	Très grand	10^5 en Ecriture	10^5 en Ecriture	10^{10} en Ecriture/Lecture
Taille du point mémoire	> 100 µm²	> 30 µm²	< 10 µm²	< 10 µm²

Comparaison Architecture

	Smart Card	Personal Computer	Ratio
RAM	1 kbyte	128 Mbytes	130000
Storage	64 kbytes	6 Gbytes	100000
Baud Rate	192 kbits	100 Mbits	500
CPU Speed	20 Mips	500 Mips	25

Les différentes formes et interfaces de communication

- Cartes avec contact (Module SIM GSM)
  - ISO 7810, 7816-1, 7816-2
  - USB ou OTG (USB pour mobile)



- Cartes sans contact
  - Plusieurs normes

- Cartes Hybrides
  - combinaison contact et sans contact
- Boutons
  - Produits iButton (bus DS 1-Wire)
  - JavaRing (iButton monté sur bague)

- Dongle
  - Série, parallèle, USB

Les terminaux carte

- Contact / sans contact
- Simple / complexe (keypad,LCD, multi-slot, biometrie …)

La normalisation

- Les normes ISO:
  - 7816-1 et 2 : caractéristiques physiques des cartes
  - 7816-3 : Signaux électroniques et protocole de transmission
  - 7816-4 : Echange d ’information et système de fichier
  - 7816-7 : spécification d ’un carte contenant des tables SQL
- Norme Europ Telecom Standard Institut:
  - GSM 11.11 : définition de la carte SIM
  - TE 9 : spécification de cartes et terminaux
- Comité Européen de Normalisation:
  - TC 224 : Cartes et équipements associés : des caractéristiques physiques, à la spécification d ’applications (santé, transport, voyage aérien)

L'évolution matérielle *D'après Bertrand du Castel*

- 2004 100Mhz E2+ & FullDuplex 1MB RSA2048 en 50ms
- 2006 200Mhz Bluetooth/UWB 4MB RSA2048 en 10ms
- 2008 400Mhz Bluetooth/UWB 16MB
- 2010 800Mhz Dynamic Display 50MB
  - Microphone
  - Battery (2003 : CEA Grenoble 500µm d'épaisseur)
  - FingerPrint Sensor
  - Pad
  - Rock-n-roll interface (scrolling avec la gravité)

L'évolution matérielle : Exemple : Java-Powered iButton

- *http://www.ibutton.com*
- Packaging : capsule étanche en métal
  - Peut-être monté sur bague (Java Ring)
    - *« Chaque fois qu'un Gonda désirait quelque chose de nouveau, des vêtements, un bagage, des objets, il payait avec sa clef. Il pliait le majeur, enfonçait sa clef 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 demandé. » La Nuit des Temps, René Barjavel*
- Communication : 1-Wire
  - Un fil pour les échanges et l'alimentation
  - Débit : 16,6 Kbit/s et 144 Kbit/s
- Horloge temps réel (Secure timestamping)
- Mémoire
  - 64Ko de ROM (OS+JVM)
  - 6Ko à 135Ko de NV-RAM à 100 ns (Non Volatile RAM : 10 ans)
- API JavaCard 2.0
  - Entiers 32 bits
  - javacardx.crypto : Crypto SHA-1, RSA DES, 3DES
- Coté terminal
  - OCF, OneWireContainer
  - PKCS#11, MS CSP, X509, Win2000 log on

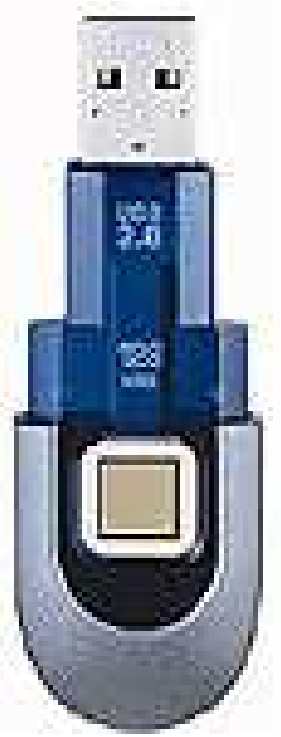
Joli concept
mais
concept abandonné

L'évolution matérielle : Exemple: Cyberflex eGate

- Axalto (ex Schlumberger)
- Brevet WO0016255
- Capacité
  - 32 de FlashRAM
- Format
  - ISO7816-1, GSM11.11
- Interface
  - USB/OTG (de 1.5 MBits/s à 12 Mbits)
  - TCP/IP+USB pour la couche physique (bulk mode)
  - Full duplex
- Crypto :
  - RSA, DES, AES (très haut débit)
- Programmation
  - JavaCard
  - Mini-Serveur HTTP et SOAP

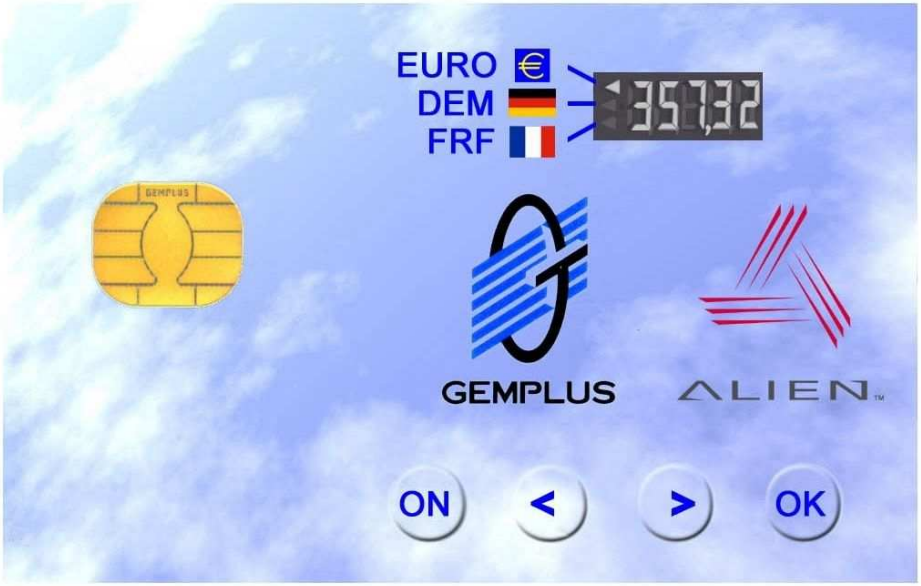
L'évolution matérielle : Exemple: la clé MicroVault

- Clé USB Micro Vault
  - clé USB à reconnaissance d'empreinte digitale.
  - 8 identifications biométriques différentes sur le MicroVault.
- Fonctions
  - File and Folder Encryption/Decryption
  - Screen Saver Lock
  - ID / Password Auto Login
  - Access to Favourites



L'évolution matérielle : Exemple

- Un afficheur, un clavier
  - protection contre les terminaux trafiqués
- Une horloge
  - éviter les attaques temporelles
- Une batterie
  - la mémoire volatile est plus dure à observer !
  - Le processeur peut être réveillé pour rappeler des événements au porteur



source Alien Technology http://www.alientechnology.com/

Les Acteurs (2011)

- Gemalto (Mariage Gemplus+Axalto 7 Décembre 2005)
- Oberthur Card Systems
- Delarue
- Giesecke & Devrient
- Sagem Orga
- …

Chiffres du marché

Nombre de cartes vendues en Million
(source: Eurosmart www.eurosmart.com)

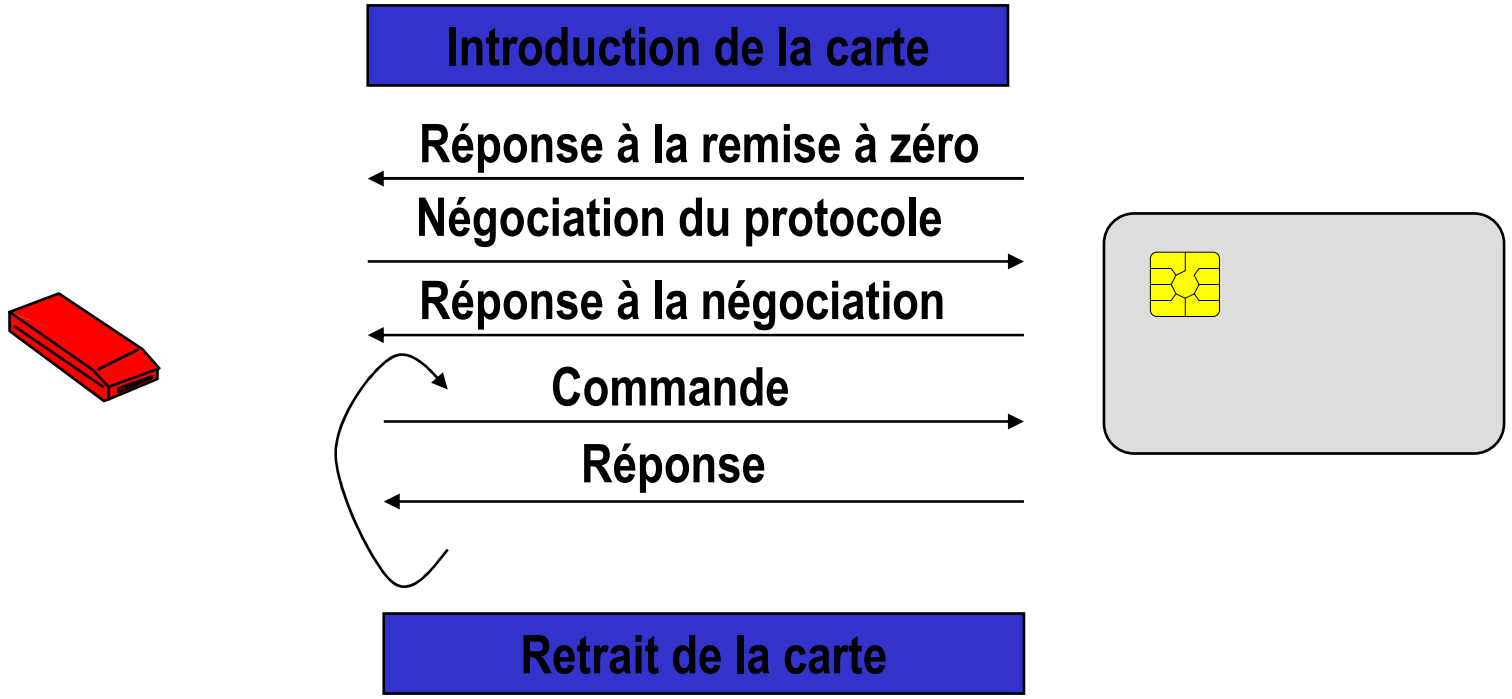
	2005	2006	2007	2008	2009	2010
Telecommunications	1390	2040	2650	3200	3600	4000
Financial/retail/loyalty	336	410	510	650	700	880
Government/HealthCare	60	90	105	140	160	190
Transport	20	20	30	30	40	65
Pay TV	55	65	85	100	100	110
Other usages	27	30	65	65	70	75
Total	1 888	2 655	3 445	4 185	4 660	5320

Selon EuroSmart, les prévisions pour 2011 sont de 13% de croissance pour les cartes à contact et de 28% de croissance dans le domaine du sans contact.

La communication Carte-Terminal

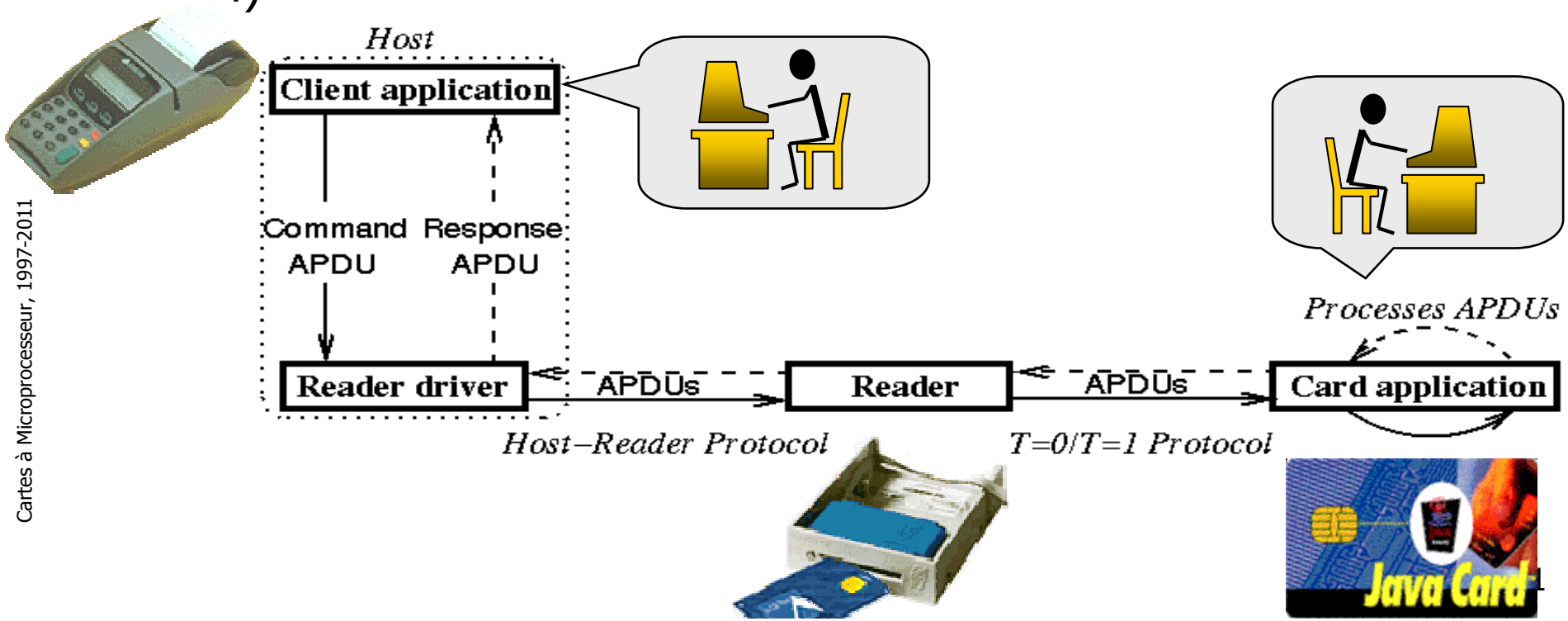
Communication Carte / Lecteur

- La carte n'est jamais l'initiateur de la communication



Architecture d'application carte

- Schéma général
  - Le terminal contrôle, la carte est passive
  - Dialogue terminal-carte de type requête/réponse
  - Format de messages standard : APDUs (ISO 7816-3 & 4)



Les normes ISO 7816-3 et

- Norme 7816-3
  - http://www.cardweb.com.tw/card/iso/ISO7816-3.htm

- Norme 7816-4
  - Une structure de message
  - Des commandes de bases
  - Le transport des données
  - *Un système de fichier*
- But
  - indépendance des applications par rapport aux couches physique et liaison

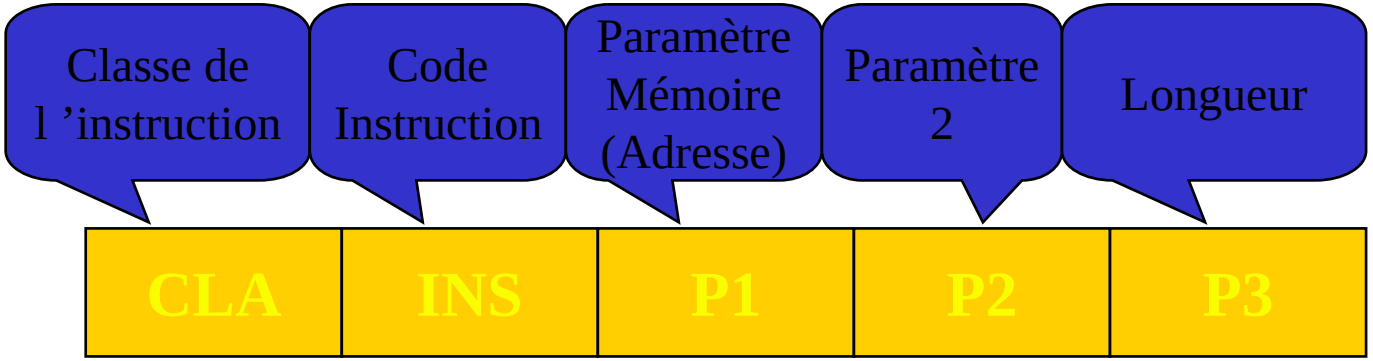
Remise à Zéro (ATR)

- Mise en route du prog ROM de la carte
  - Max. 33 caractères et 5 champs
- Permet de fixer :
  - Les conventions de codage des octets
  - le temps de transmission d ’un bit
  - La valeur de la tension de programmation
  - Le protocole de communication
  - Un historique qui s ’affichera à la mise sous tension de la carte (ex: version de l ’OS)
- Détails
  - page 164 du livre « Smart Card Handbook » de Rankl & Effing
  - Section 7.2 du manuel de programmation BasicCard

Exemple d'ATR

- Carte Santé Vitale
  - ATR = 3F 65 25 00 2C 09 69 90 00
- Carte Bancaire CB
  - ATR = 3F 65 25 08 36 04 6C 90 00
- Carte Verte Monéo
  - ATR= 3B E6 00 FF 81 31 42 45 19 16 01 01 27 B1 37
- Carte Cinema (perimé)
  - ATR = 3B 23 00 35 13 96
- Carte GSM Itineris
  - ATR=3F 2F 00 30 AF 59 02 01 02 80 00 17 0A 0E 83 1E 9F 16
- GXP211_PKIS
  - ATR = 3F 6D 00 00 80 31 80 65 B0 05 01 02 5E 83 00 90 00
- GemSafe
  - ATR= 3B A7 00 40 18 80 65 A2 08 01 01 52
- Schlumberger Palmera
  - ATR= 3B 65 00 00 9C 02 02 06 01
- Cyberflex Access e-gate 32K
  - ATR=3B 75 94 00 00 62 02 02 00 80

T=0 : Structure de l 'ordre



- Commande
  - CLA 00 pour ISO, AA pour GSM, …
  - INS pair pour l'ISO
- Réponse
  - SW1/SW2

    90 00

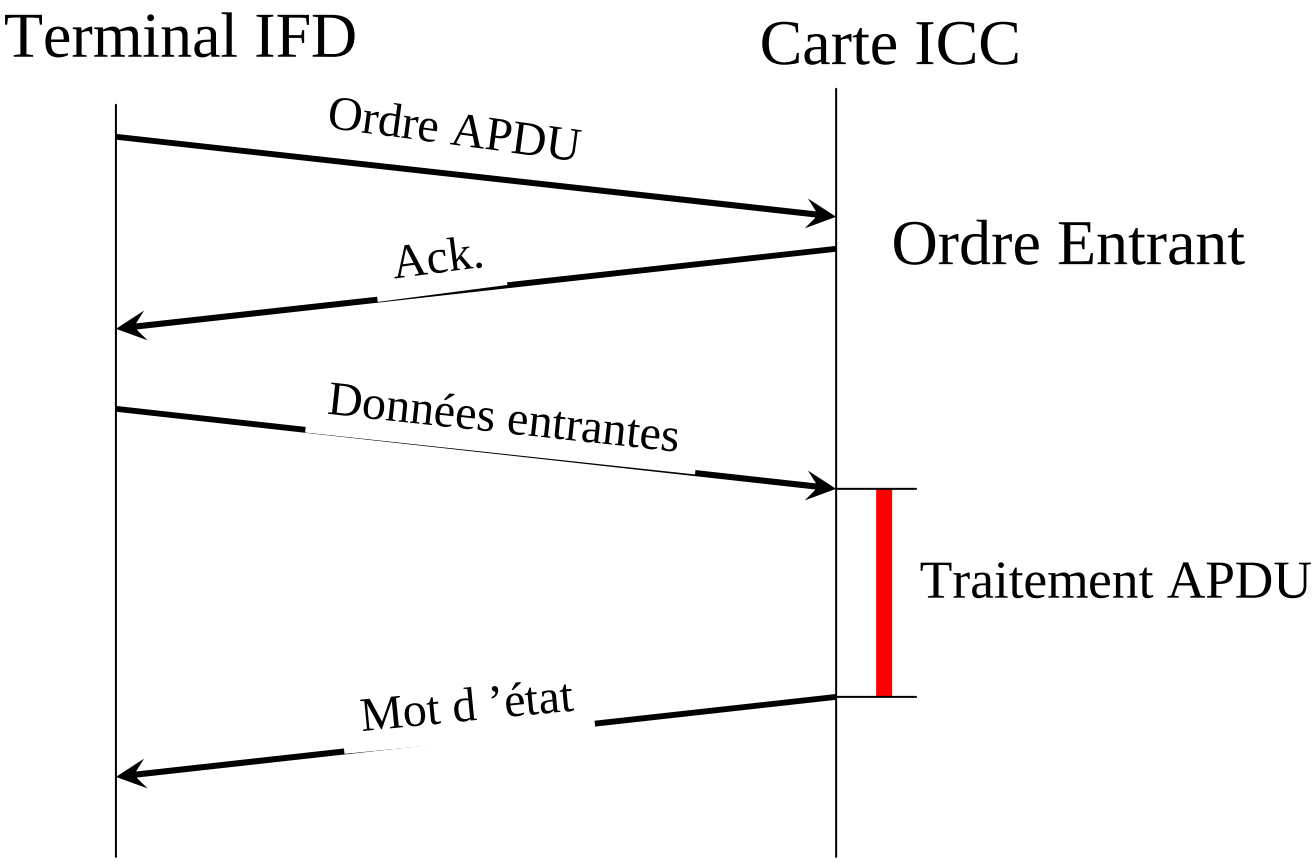
    6E XX: Classe inconnue

    6D XX: instruction inconnue

    9X XX: Erreur applicative

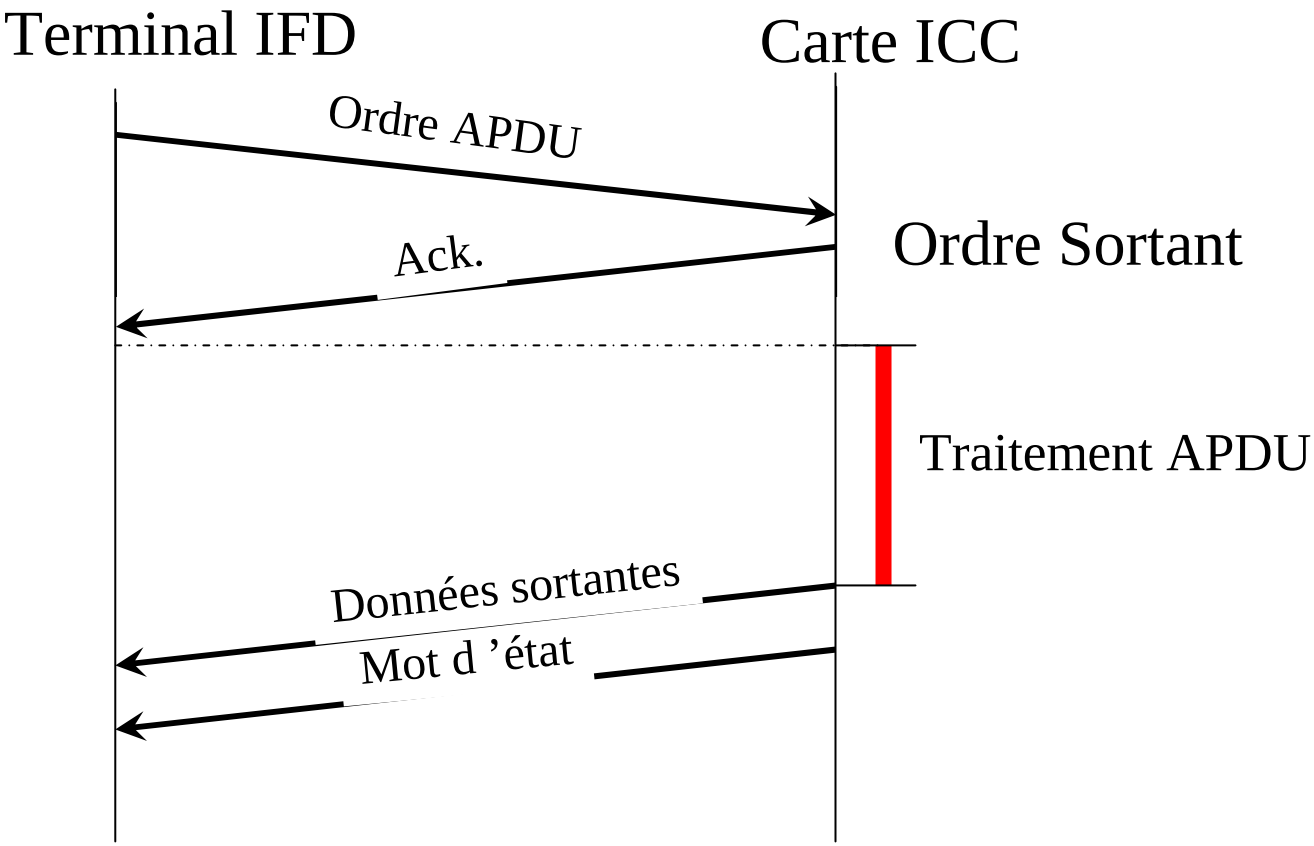
Echange de Données : T=0

Transmission de caractères asynchrones



Echange de Données : T=0

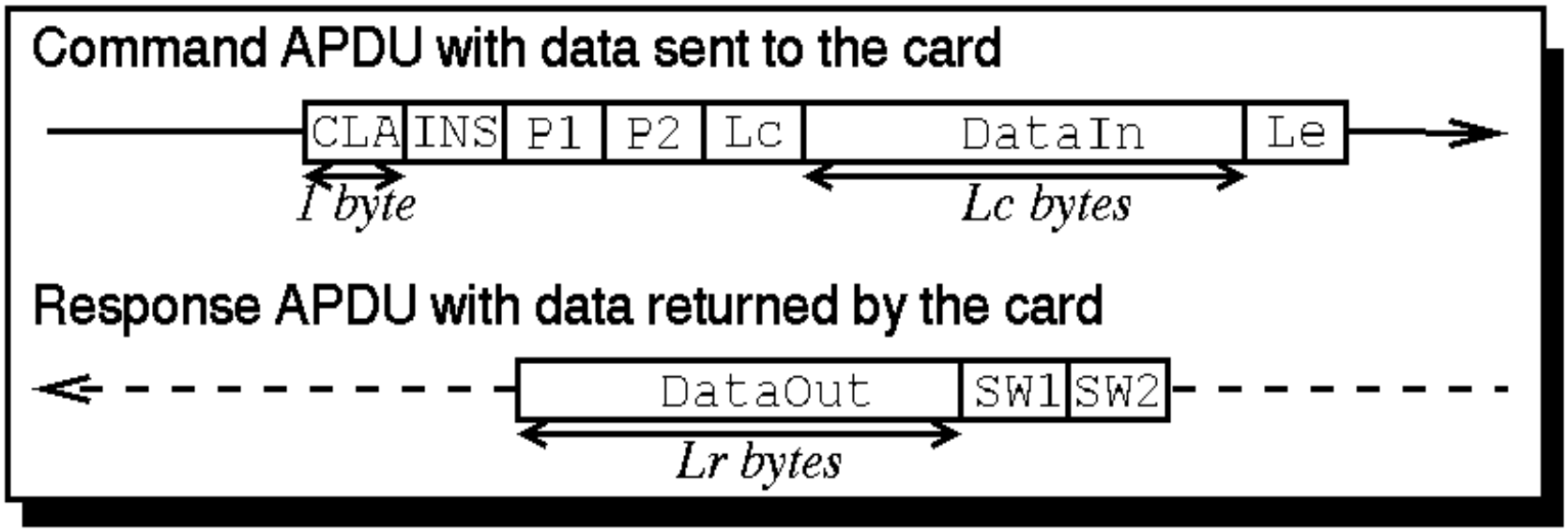
Transmission de caractères asynchrones



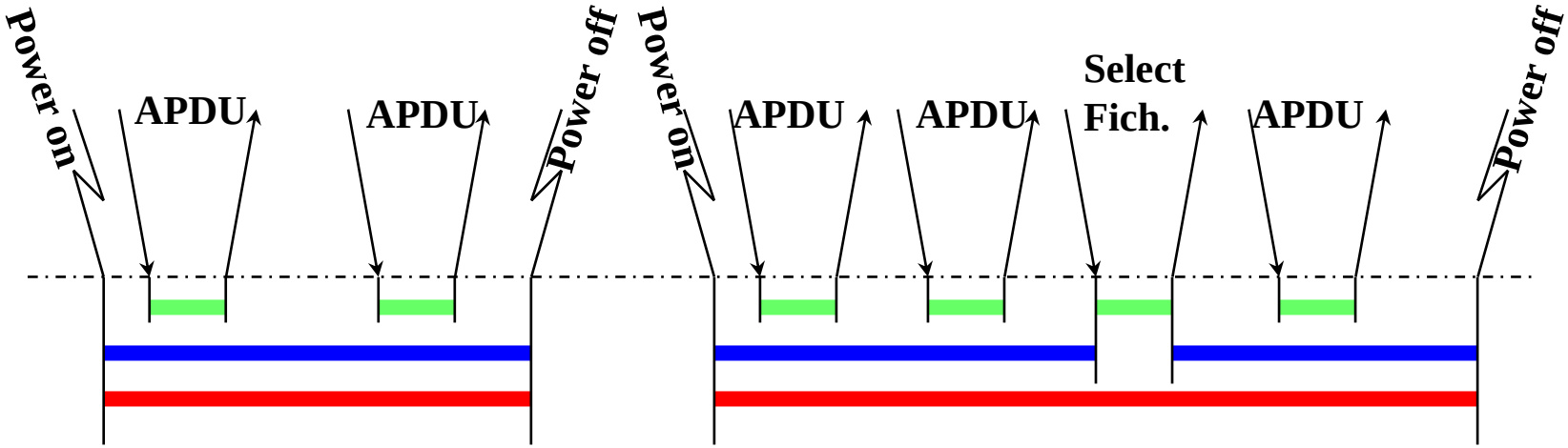
Commandes et Réponses APDU

- APDU :
  - permet tous les types de transfert de données

Cas	Commande	Réponse
1	Pas de données	Pas de données
2	données	Pas de données
3	Pas de données	données
4	données	données



Déroulement d ’une session



Durée d’une APDU

Durée d’une session

Durée d’une connexion

Cartes et sécurité

Sécurité

- Objectifs du fraudeur
  - Obtenir l'accès à une information
  - Corrompre des informations
  - Réfuter l'envoi ou la réception d'une information
  - Provoquer la méfiance vis à vis d'un système
- Attaques :
  - Se faire passer pour quelqu'un d'autre
  - Empêcher le fonctionnement correct d'un système
  - Corrompre un protocole pour obtenir des secrets
  - S'insérer dans le système comme relais actif

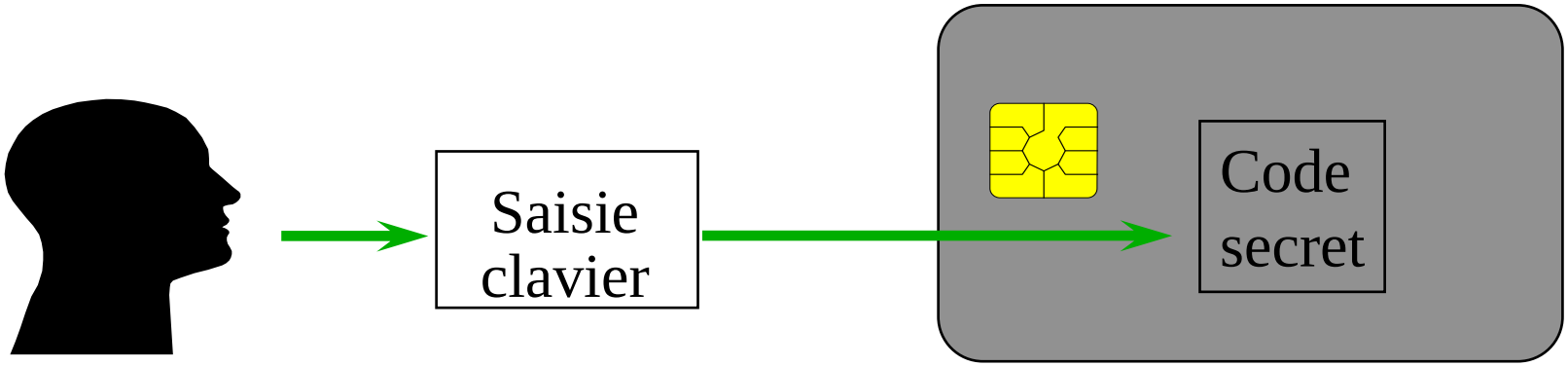
Sécurité intrinsèque de la carte

- Attaques
  - Lecture au microscope électronique
  - Insertion de sondes
  - Provoquer des dysfonctionnements
- Mécanismes
  - Détecteurs de lumière, de passivation, de température, de tension, de fréquence
  - Couche de passivation, bus enterré (inaccessible de l'extérieur)
  - Brouillage des adresses
  - Logique sauvage des circuits
  - Mode test - protection par fusibles
  - Matrice de sécurité physique (RAM, ROM, EEPROM)

Conclusion Sécurité Physique

- La sécurité physique
  - Le micromodule est monolithique
    - difficile de distinguer ses différents composants
  - Présence d'un bloc de sécurité
    - détection de tension
    - détection de fréquence
    - détection de lumière
  - Le système d'exploitation est en ROM et ne peut donc être ni remplacé, ni altéré.

La sécurité logique



- L' Identification
- L' Authentification
- La Certification
- L' Intégrité
- La Confidentialité

Première Conclusion

- Avantages des CAM :
  - Support d ’exécution sécurisé
  - Support mobile
  - Support personnel
- Désavantages
  - Lent, Coûteux, faible capacité de stockage

Applications

Applications

- Paiement
  - Carte de Crédit, Carte de Débit
  - Porte Monnaie Electronique, Carte Prépayée
- Sécurité
- Billettique
  - Transports, Parc à Thèmes, Remontées Mécaniques
- Fidélité
  - Mono ou Multi-partenaires
- Jeux (d'argent) offline
- Dossier Portable
  - La carte regroupe des informations sur un porteur
  - Carte d 'assurance Maladie, Dossier médical portable, …
  - Carte Portail Web
    - configuration des serveurs mails et news, liste des signets, liste des mots de passe

Applications de paiement (1/3)

- Cartes de Crédit
  - Somme débité sur le compte du titulaire avec un taux d ’intérêt fixé
- Cartes de Débit
  - Compte débité qqs jours après l ’achat
- Techniques :
    - Authentification mutuelle carte et terminal commerçant
    - Signature Électronique
    - Contrôle du NIP
    - Contrôle (régulier ou systématique) du solde bancaire (en ligne)
  - Ex : Carte Bancaire française (GIE Cartes Bancaires)
    - 1 DAB pour 900 hab en France
    - 317 G€ de transactions en 2003
      - 260 M€ de fraudes du à la piste magnétique contrefaite et utilisée depuis l’étranger.

Plan de Migration de VISA vers les SC

Feb 1998	Launch of Chip Migration program
Jan 1999	New Visa and Electron chip cards to be EMV and VIS compliant
Jan 2001	All new Visa Cash programmes to be CEPS compliant
Oct 2001	All Acquirer hosts certified to EMV, All new Terminals EMV+VIS compliant (POS, EPOS, ATM)
Jan 2002	Regional review to assess EMV and PIN readiness
July 2002	Visa, Electron and Visa Cash to be EMV, VIS and CEPS compliant
Jan 2005	All Visa Electron terminals to be EMV and PIN enabled, Proposed Intra regional liability shift

Applications de paiement (2/3)

- Carte Prépayée
  - Cas particulier du PME : la carte contient des jetons (et non de l'argent)
  - Ex : Abonnement autoroute (Marseille), Places de cinéma, …
  - Une réussite : la Télécarte
    - Fin du vandalisme des cabines téléphoniques
    - Temps de communication +50%
    - Support publicitaire, Avance de trésorerie

Applications de paiement (3/3)

- Porte-Monnaie Electronique (e-Purse)
  - Remplace pièces et petites coupures de billets
  - Carte rechargeable dans des guichets (ou chez le commerçant)
  - Permet de régler des petites sommes (fraction d'euros à quelques dizaines)
  - Mode de paiement sûr, pratique, rapide, anonyme ???
    - Mais en cas de perte, l'argent est perdu
  - Exemple
    - SIBS (Portugal), Proton (Belgique), Monéo & Modeus (France), GeldKarte (Allemagne), CEPS
  - Avantages
    - Pour la banque :
      - Absence de fraude, contrôle des facilités de crédit, coût de transaction faible, diminution des liquidités
    - Pour le commerçant :
      - Garantie de paiement, rapidité d 'encaissement, absence de liquidité
    - Pour le porteur :
      - Paiement rapide, rechargement simple, protection par mot de passe, Etat des différentes transactions sur demande

Applications d ’identification

- Identification d ’une personne :
  - dans une entreprise (contrôle horaire),
  - sur un réseau informatique (login),
  - sur un réseau téléphonique (carte SIM),
  - ou dans la société (carte d ’identité)
- Ex: Le GSM et la carte SIM
  - Abonné localisé par la carte (le terminal utilisé devient celui du porteur)
  - Facturation directe de l ’abonné
  - Sécurité physique (carte)+logique (NIP)
  - Stockage de données personnelles (agenda)
  - 1,22 milliards de cartes SIM livrés en 2005

Applications de sécurisation

- Sécurité physique :
  - Accès à des locaux : ouverture et fermeture de porte (suivi de passages)
    - ex : Ministère des finances, Gemplus
- Sécurité logique :
  - Contrôle d 'accès logique à un serveur
    - Identification, Authentification
  - Protection de messagerie électronique
    - Signature électronique et chiffrement des messages
  - Renforcement de la sécurité des transactions sensibles
    - Ordres de virements internationaux (chiffrement de code porteur)
  - Vote électronique

Applications de Dossier Portable

- Principe :
  - La carte regroupe des informations sur un porteur
- Carte d ’assurance Maladie
  - Remplace les formulaires
  - Accélère le paiement et le remboursement
- Carte dossier médical portable
  - Dossier médical stocké sur une carte
- Carte de médecine ambulatoire
  - Carte de suivi des soins dans un hôpital

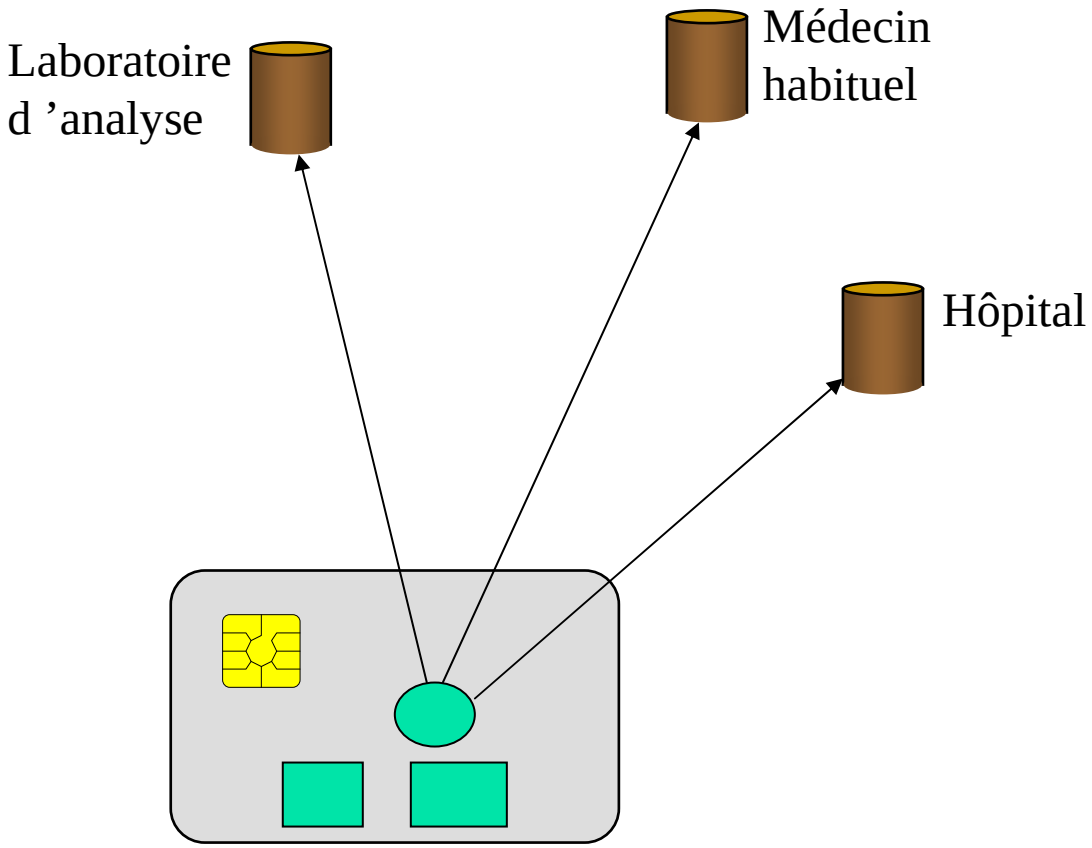
Applications Actuelles des Cartes

- Différents secteurs porteurs
  - Les Télécommunications : Cartes Pré-payées, carte SIM
    - Recherche tj + de services, ∀ le coût
  - Les Banques : Porte-monnaie Électronique, Carte Bancaire
    - Recherche de coût de fonctionnement le plus faible
  - La Santé : Carte patient, carte professionnels de santé
    - Recherche la sécurité d ' informations sensibles
- Sous l 'impulsion du GSM,
  la carte doit offrir de + en + de services

Futures Applications

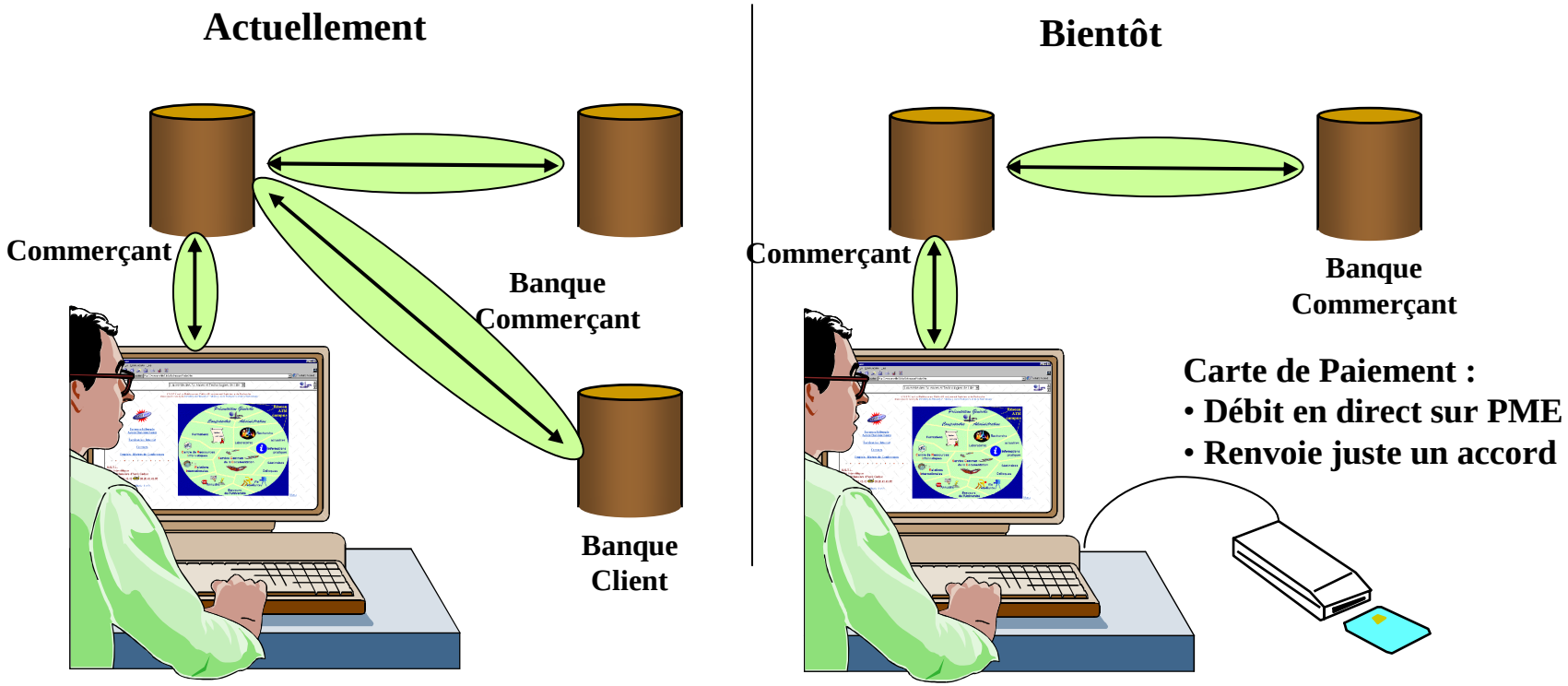
- La Carte « bookmark » ou Portail
  - Toutes les informations propres à l ’utilisateur sont stockées dans la carte
  - configuration des serveurs mails et news,
  - liste des signets
  - Liste des mots de passe
- La Carte à Mémoire Etendue
  - La carte contient des liens vers des informations stockées sur des serveurs anonymes
  - Permet de laisser les informations sur le réseau sans problème de sécurité
  - L ’information peut être cryptée, et la carte est utilisée pour décrypter
- La Carte pour personnaliser un terminal générique
  - CESURE
  - Déploiement des composants de l’application terminal

Ex: une nouvelle carte santé



Futures Applications

- La carte et les paiements distribués



API Carte

Phases de Dev. D 'une appli carte

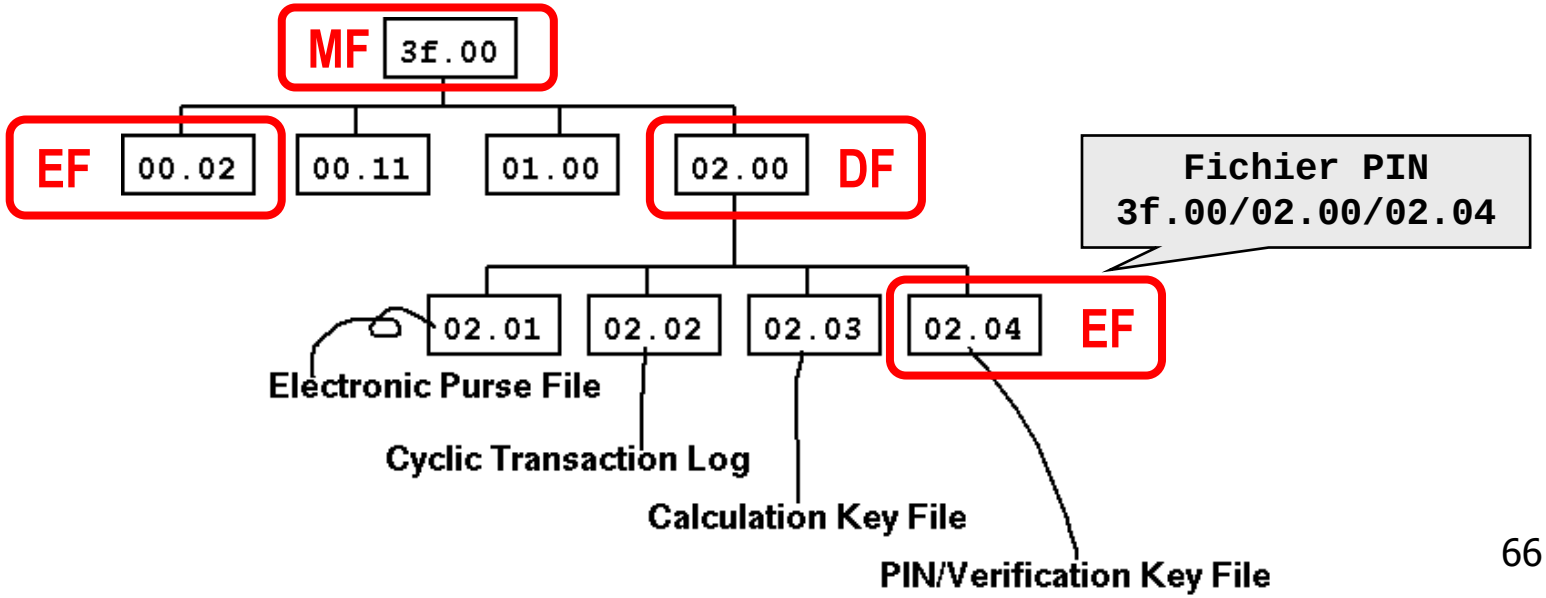
- Choix de la carte :
  - Puissance du processeur
  - Types et tailles des mémoires
  - Respect (ou non) des normes
- Choix du masque
  - Caractéristiques des « ROM » de la carte
    - OS + fonctions applicatives
  - Ecriture du masque
    - directement en assembleur
  - Dev. D 'une application carte spécifique
    - Utilisation d 'un masque « générique » + filtres
- Initialisation+personnalisation de la carte
  - Chargement des fonctions spécifiques
    de l 'application, de l 'émetteur, des utilisateurs et du porteur
- Environnement de l 'application

Systèmes d ’exploitation carte

- Masque dédié : une seule application figée
  - B0 (CB, Sesame Vitale, CPS)
  - Monéo
- Mono Application
  - ISO 7816-4
    - Système de fichier sur carte
    - Authentification du porteur et contrôle d’accès
  - ISO 7816-7
    - Moteur de base de données
  - *BasicCard*
- Multi Applications
  - Multos
  - JavaCard
  - .NET SmartCard

Système de Fichier ISO 7816-4

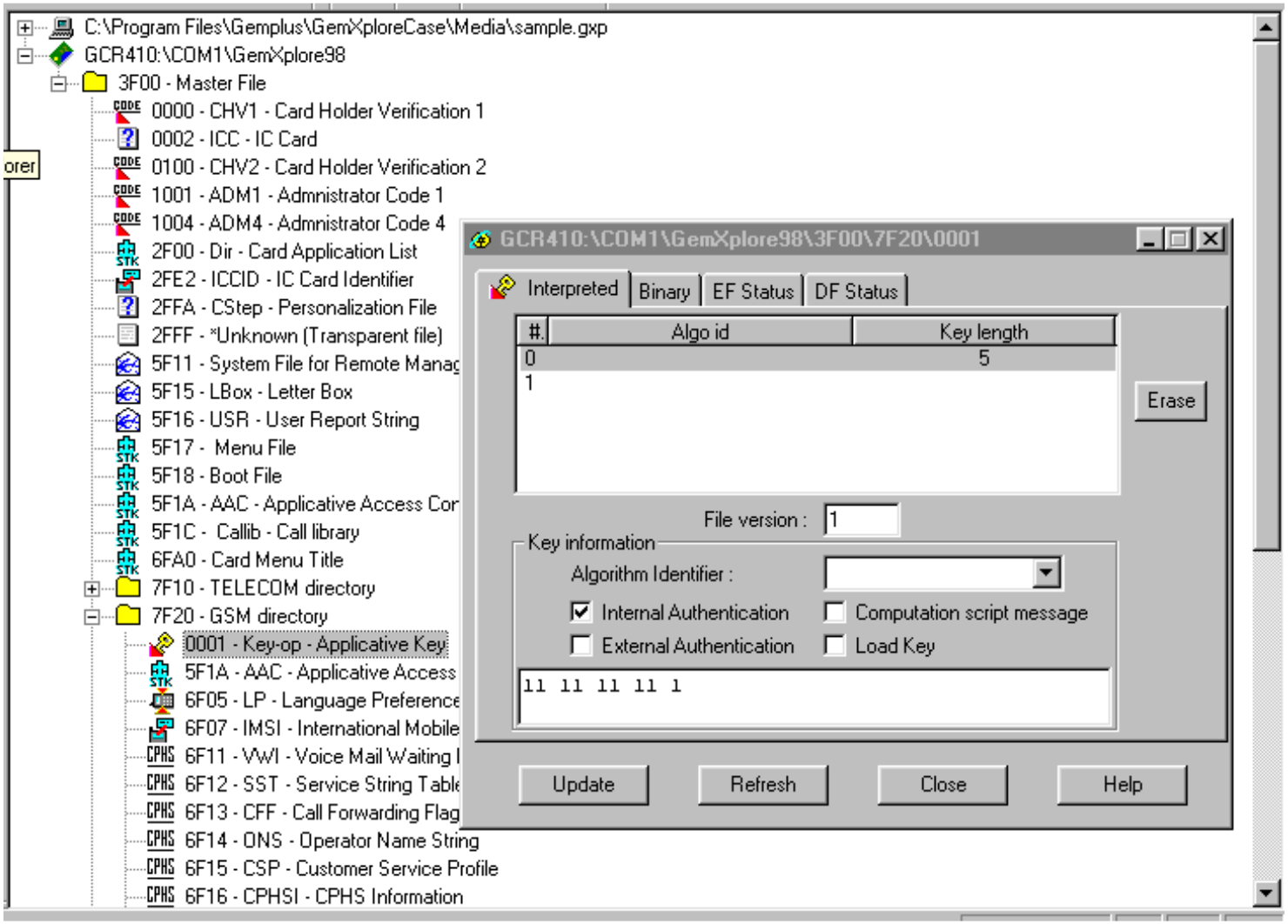
- Structure hiérarchique (MS-Dos, Unix)
  - MF : Fichier Maître : Obligatoire (Racine) **3F.00**
    - Contient un fichier de contrôle d 'information et de mémoire allouée
  - DF : Fichier Dédié :
    - contient des mots de passe pour accéder aux EF
  - EF Fichier Elémentaire :
    - contient des données ou des informations de contrôle



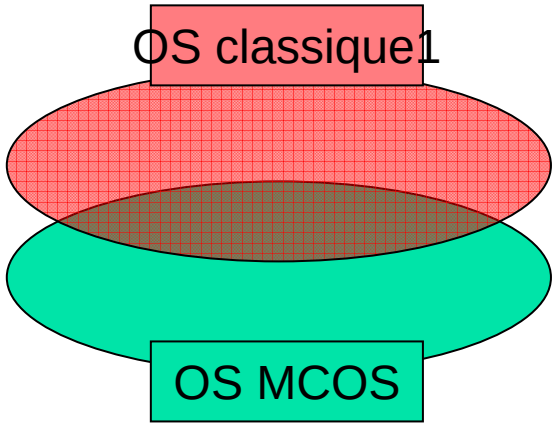
Système de Fichier ISO 7816-4

- 4 types d ’EF :
  - Fichier de travail :
    - Données de l ’application
  - Fichier Public :
    - sans contrôle
  - Fichier de contrôle d ’application :
    - accessible en lecture
  - Fichier de secrets internes :
    - non accessibles
- 4 structures de données
  - fichiers binaires (données accessibles par adresse)
  - Enregistrements séquentiels (longueur fixe)
  - Enregistrements séquentiels (longueur variable)
  - Enregistrements cycliques

Exemple de système de fichier d'un module SIM GSM



Système d ’exploitation des 7816-4



- Il manque :
  - La notion de programme utilisateur
  - Pas de gestion mémoire
  - Pas de parallélisme

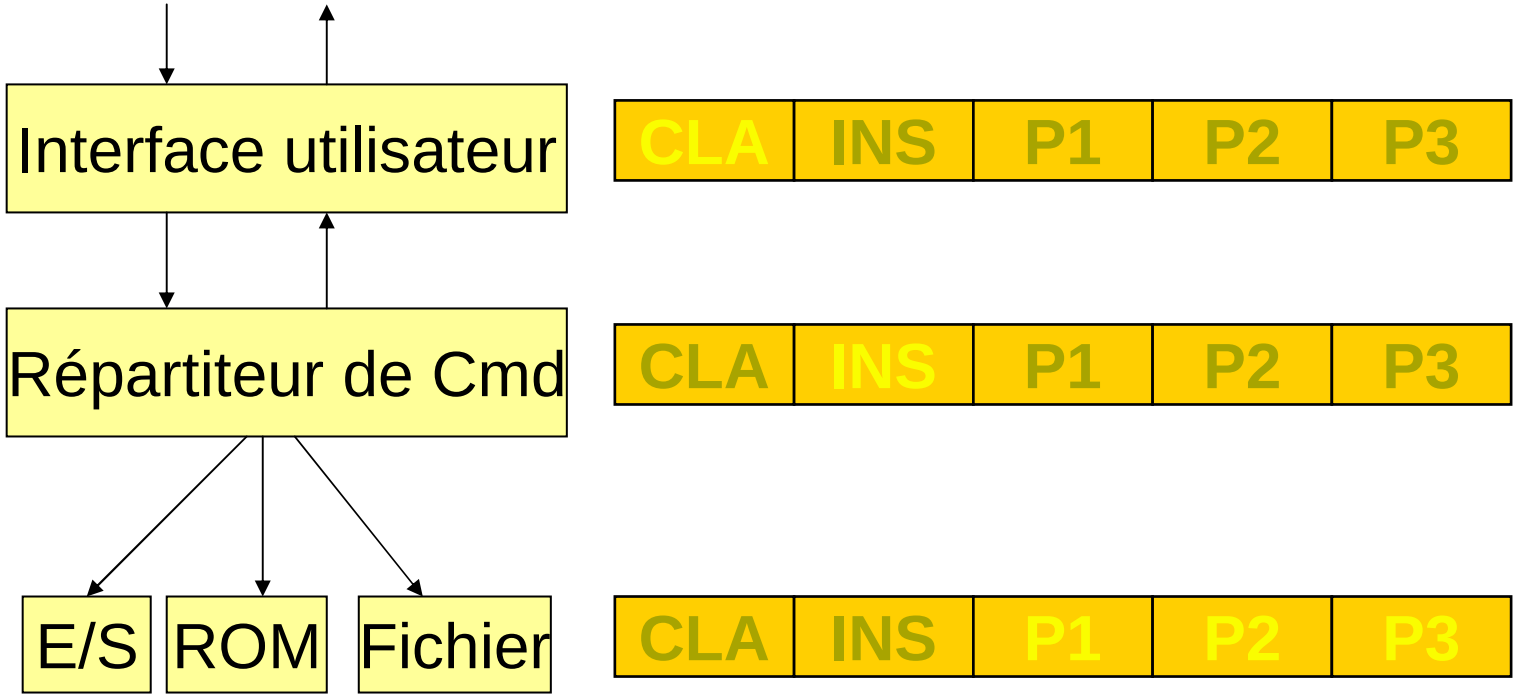
Il reste :

Protection
Le système de fichier
des routines utilitaire

On y trouve :

La def. d’un cycle de vie propre, la cryptographie et la notion de filtre

Système d ’exploitation des 7816-4



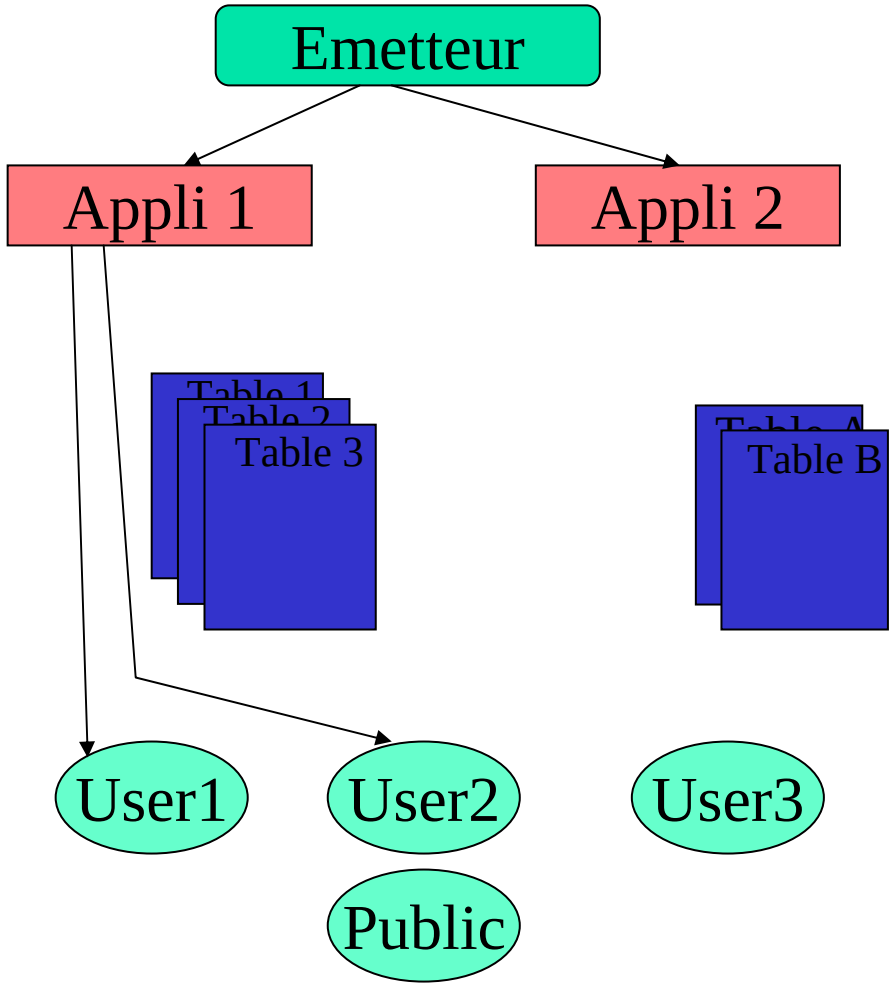
Système d ’exploitation des 7816-4

- Avantage de la 7816-4 :
  - Pas chère
  - Facile à utiliser
  - Possibilité de définir des ordres non standards
- Inconvénient :
  - Impossible d ’exécuter du code
  - Carte figée après la personnalisation
  - Uniquement orientée données

La norme ISO 7816-7

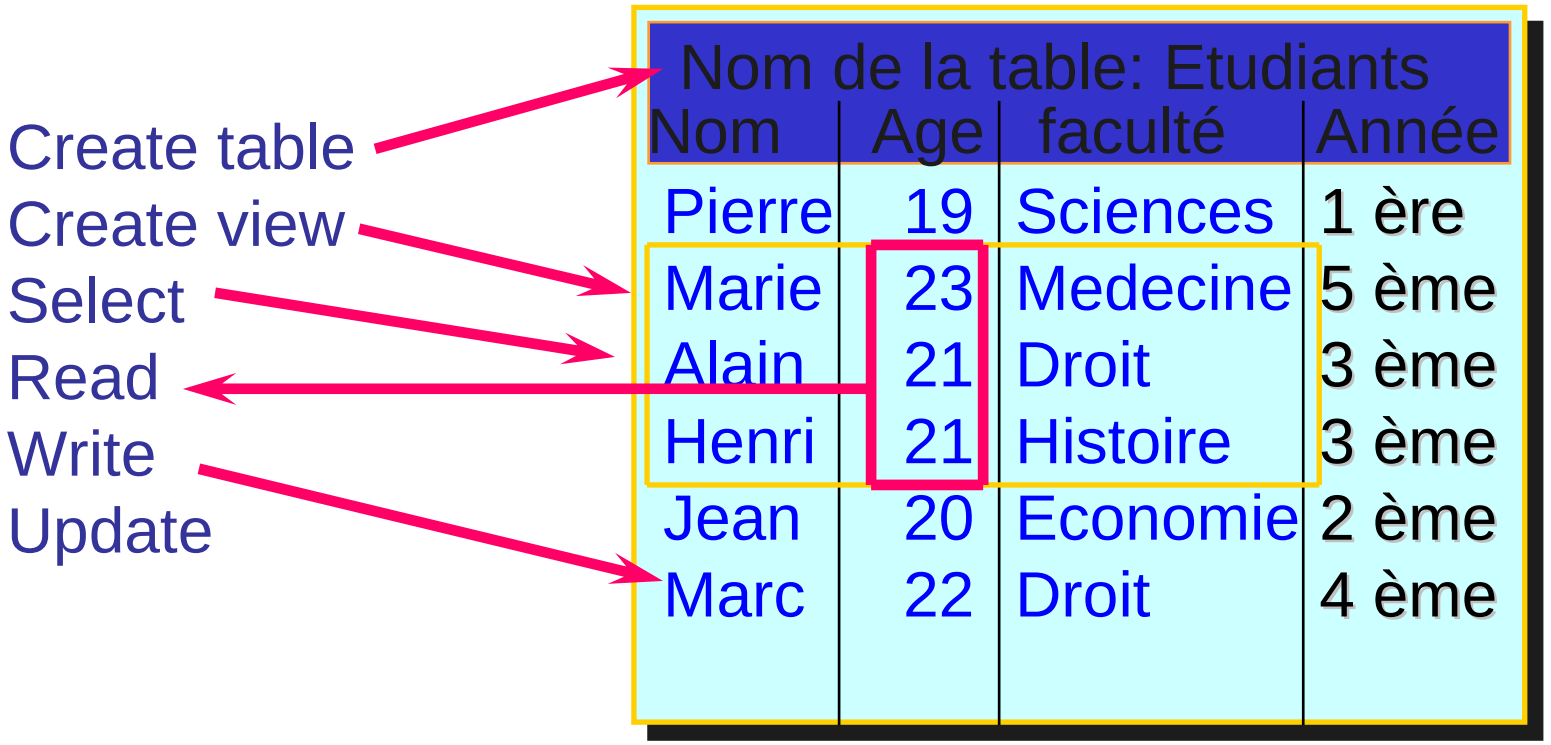
- Organisation des données
  basées sur les concepts des bases de données
  - Données sous forme de tables relationnelles
  - Possibilité de définir des VUES sur les tables
  - 4 ordres de bases : SELECT INSERT UPDATE et DELETE
  - Schéma de sécurité
    - 3 types d ’utilisateur
    - Emetteur, Gestionnaire d ’application, Utilisateurs
    - Règles
    - Un utilisateur (ou E, ou GA) est propriétaire des objets qu’il créé (il peut seul effectué des traitements sur cet objet)
    - Un propriétaire peut accorder ou retirer des privilèges (SELECT, etc…) sur des objets (Tables ou vues)

La norme ISO 7816-7 : Gestion des Applications



Ordre « CQL » :
present E ‘ code ’;
create application app1 ‘ sec_app1 ’;
create application app2 ‘ sec_app2 ’;
present app1 ‘ sec_app1 ’
create user user1 ‘ sec_us1 ’
create user user2 ‘ sec_us2 ’
….

La Carte ISO 7816-7 : Manipulation de données relationnelles



GSM 11.11

- TODO

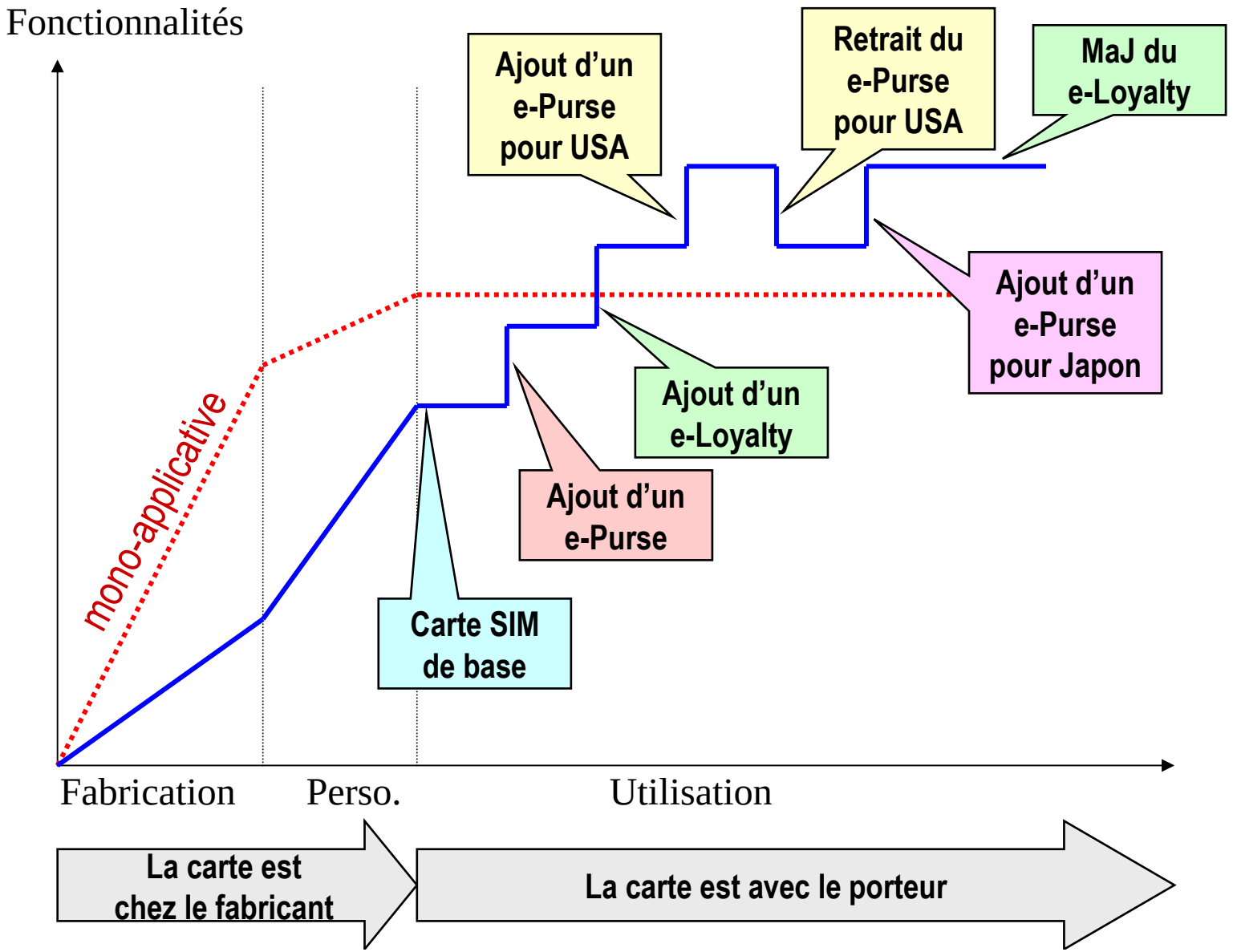
Une notion importante : Le time2market

- Temps entre la décision et le lancement d ’un produit
  - Phase très longue si ré-écriture d ’un masque (peut atteindre 1 an)
  - Peu adapté aux besoins du marché :
    - La téléphonie mobile est très concurrentiel
    - Les coûts de développement sont très important
- Apparition d ’un nouveau type de carte : les cartes génériques
  - Disposent d ’un véritable OS
  - Peuvent charger des applications au cours du cycle d ’utilisation

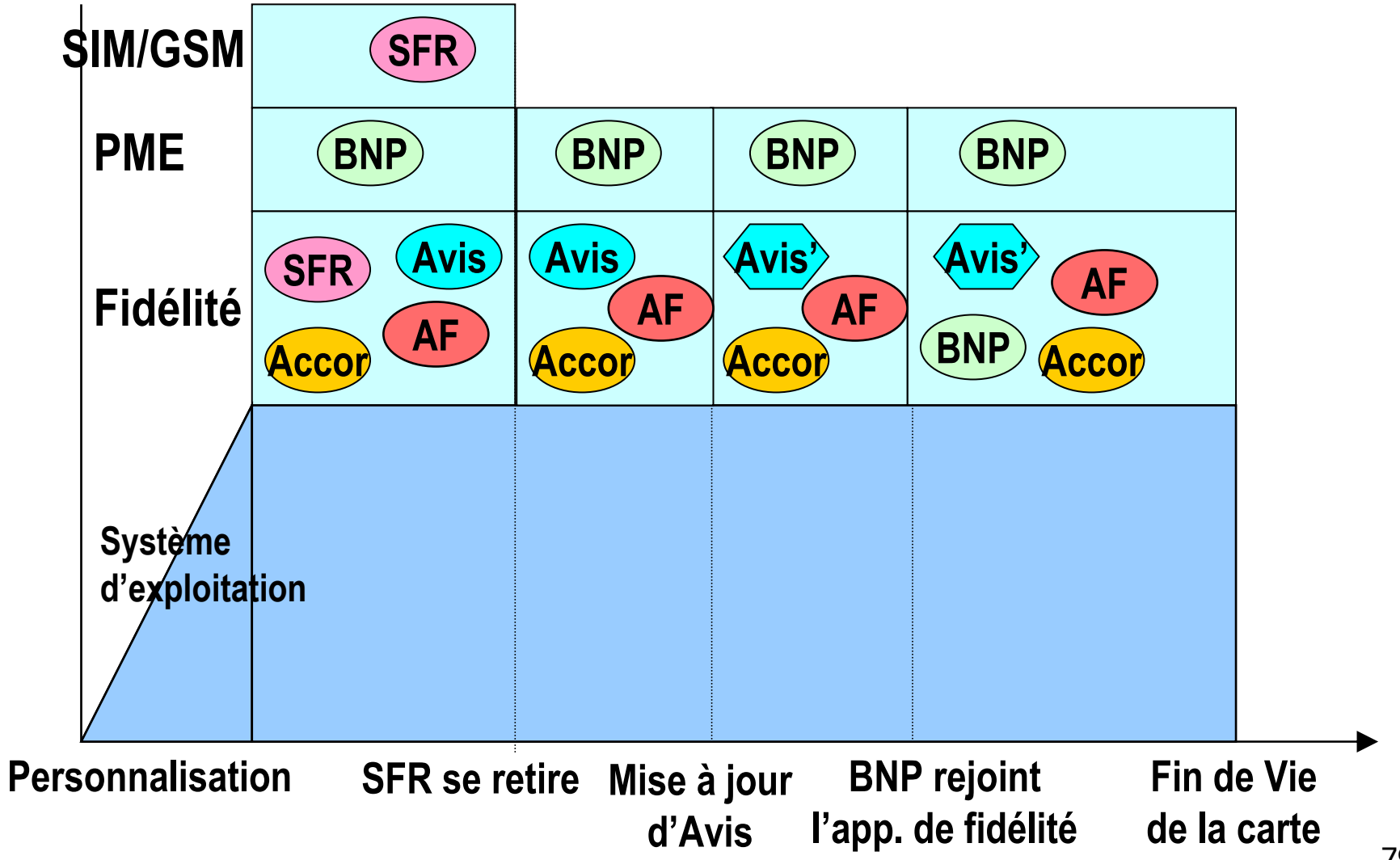
Une nouvelle génération : Les cartes multi-services

- But :
  - Permettre à plusieurs applications de coexister
  - Partager des données entre plusieurs applications (non redondance d 'information)
  - Possibilité de charger/décharger des applications en cours de vie de la carte
- Avantages
  - une seule carte pour l 'utilisateur
  - Possibilité d 'évolution des cartes
- Inconvénients
  - Peur des partages
  - Tailles réduite de la place / application

Le cycle de vie des cartes multi applicative



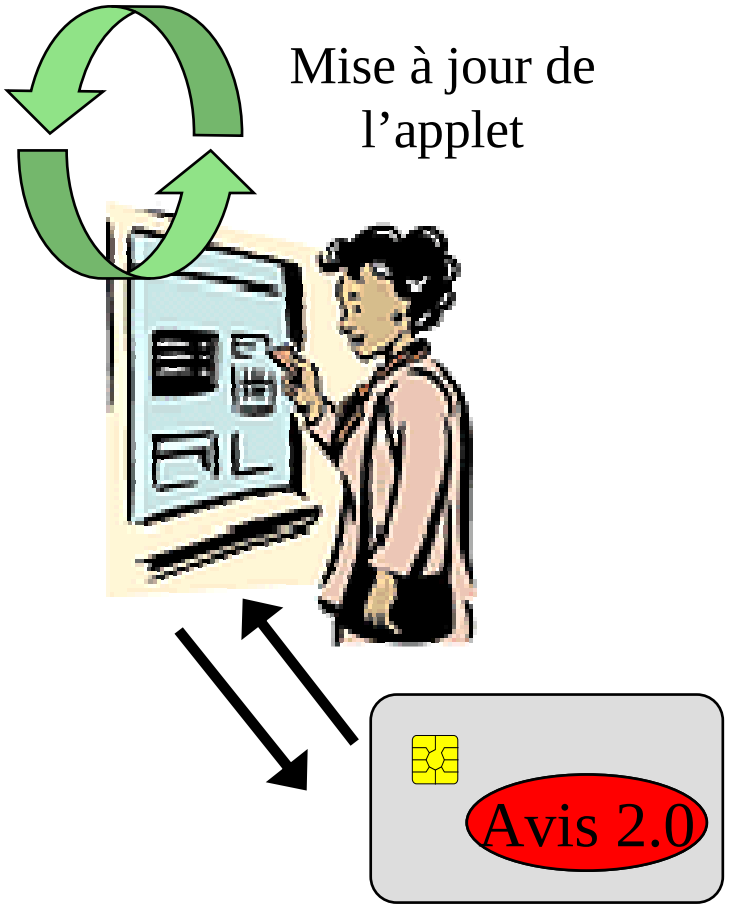
Cycle de vie d'une carte multi-partenaires



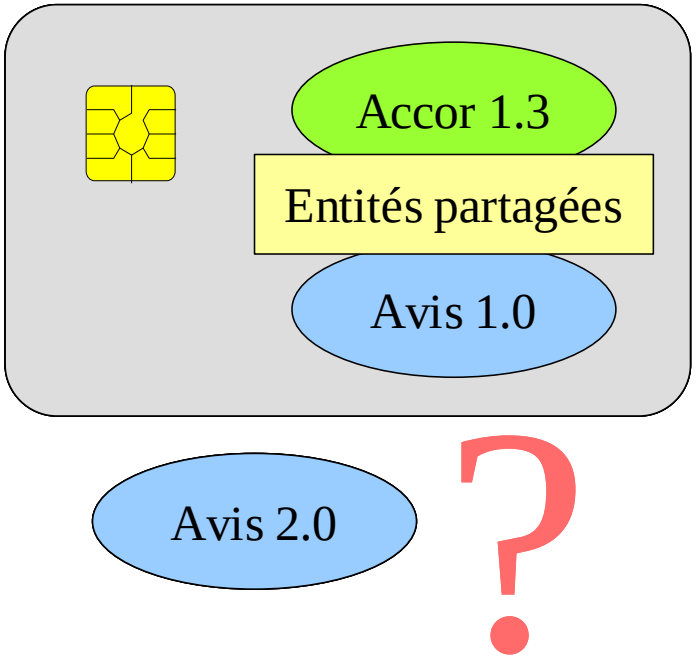
Évolution d'applications
Cartes multi-applications

Cas mono-partenaire

Mise à jour de l'applet



Cas multi-partenaires



Besoins des développeurs

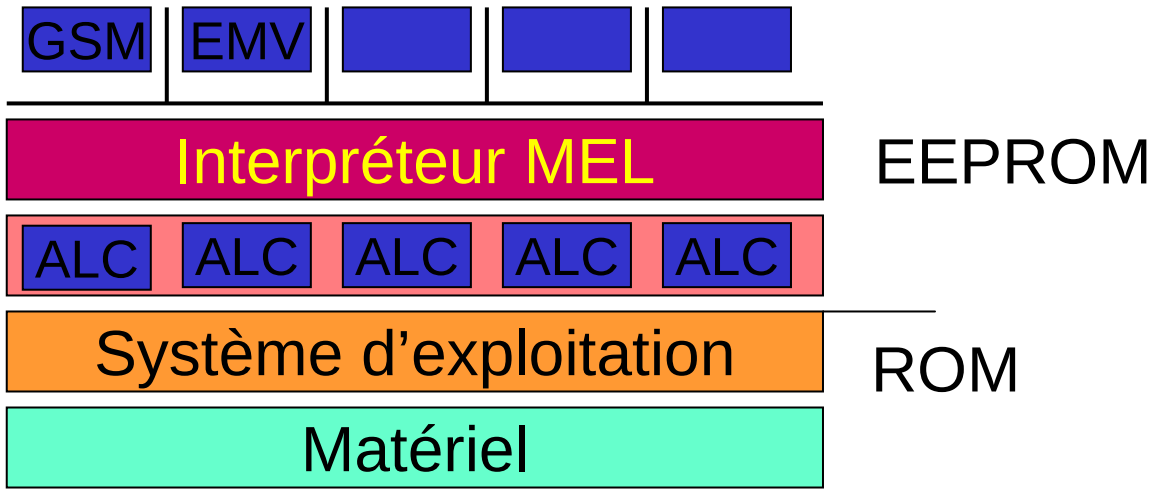
- Sortir la carte d ’une programmation «élitiste » :
  - Seul les programmeurs de longue date savent correctement écrire une application carte
  - Solution : utiliser des langages de programmation courants en informatique (C, Java, Visual Basic)
- Permettre de tester des solutions :
  - portage sur carte plus rapide => possibilité de test

Besoins des utilisateurs

- Se simplifier la vie :
  - utiliser la même carte pour toutes les applications
    - Plusieurs applications sur une même carte
  - Pouvoir changer de prestataire sans avoir à recommander une carte
    - Chargement / déchargement d ’application

Multos

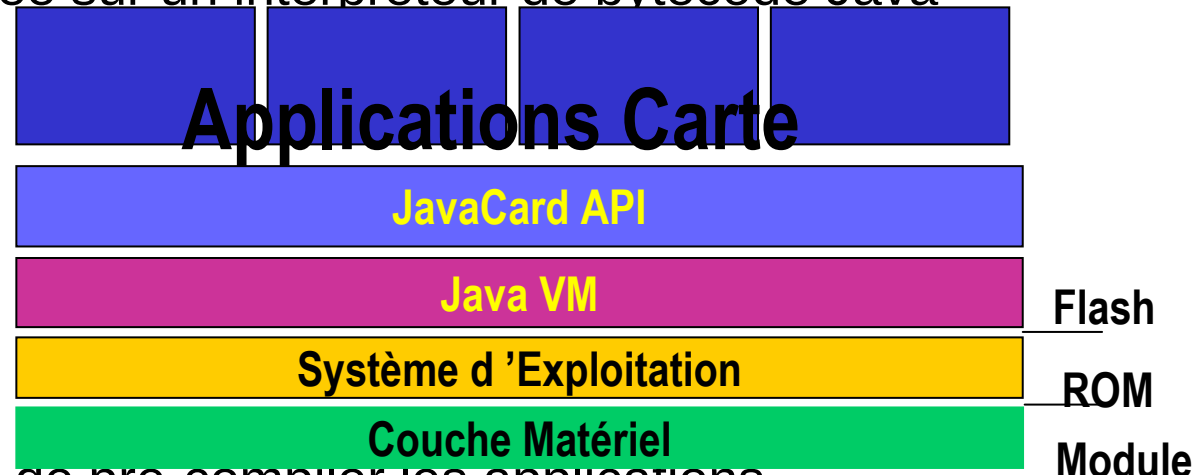
- Carte basée sur un interpréteur MEL (Multos Executable Language)



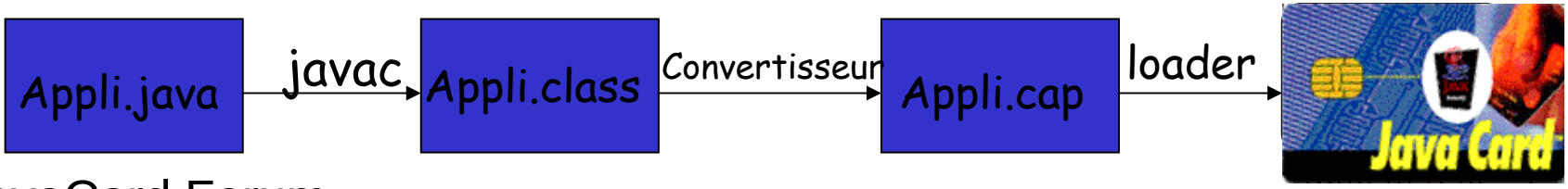
- Carte limitée par la norme 7816-4
- Plus d 'info : http://www.multos.com

JavaCard

- Carte basée sur un interpréteur de bytecode Java



- Nécessité de pré-compiler les applications



- JavaCard Forum
- Marché
  - 300 millions de JavaCard vendues depuis 2002
  - 121 millions de Contactless Javacard en 2004

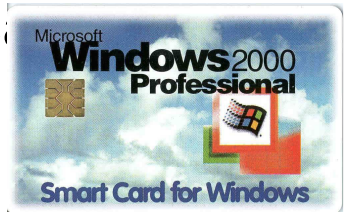
BasicCard

- Développement d'applications carte en langage Basic
  - Coté Carte
    - interpréteur de « bytecode » P-Code
    - Système de fichier DOS-like
  - Coté Terminal
    - Interpréteur de « bytecode » P-Code
    - Remarque : l'application terminal peut être écrite aussi
      - en C/C++/C# avec un driver PS/SC ou MUSCLE
      - en Java avec OCF
- Avantages
  - Aux applications en très petites séries (club de tennis, …)
  - Pour une première approche pédagogique de la carte
- Inconvénients
  - Propriétaire (http://www.zeitcontrol.de/)
  - Pas de soutien des *Majors*

.NET SmartCard

http://www.hiveminded.com/

- Récent (2003)
  - Effet d'annonce ?? Souvenez vous de Windows SmartC
- Caracteristiques
  - Implémentation de la CLI adapté à la carte
  - Multi-applications
  - Développement Multi-langage : C#, J#, VB, Jscript, Perl, …
  - Isolation
    - Application Domain de .NET
  - Transactions
    - Multi-niveaux ?
  - Garbage Collector
    - Mark and Sweep (sans marquage en EEPROM)
  - Communication
    - Inter-applications
      - Channel : flux d'octets bidirectionnel
    - Terminal-Application : APDU, .NET Remoting, Javacard 2.2 RMI



.NET SmartCard

- Motivations
  - Implémentation de la CLI adapté à la carte
  - Multi-applications
  - Développement Multi-langage : C#, J#, VB, Jscript, Perl, …
  - IDE : Visual Studio
- *Produits*
  - *HiveMinded http://www.hiveminded.com/*
    - Caractéristiques
    - Isolation
      - Application Domain de .NET
    - Transactions
      - Multi-niveaux ?
    - Garbage Collector
      - Mark and Sweep (sans marquage en EEPROM)
    - Communication
      - Inter-applications via des Channels : flux d'octets bidirectionnel
      - Terminal-Application : APDU, .NET Remoting, Javacard 2.2 RMI
  - GemAlto http://www.NETsolutions.gemalto.com

.NET Smartcard

L'évolution fonctionnelle

D'après Bertrand du Castel

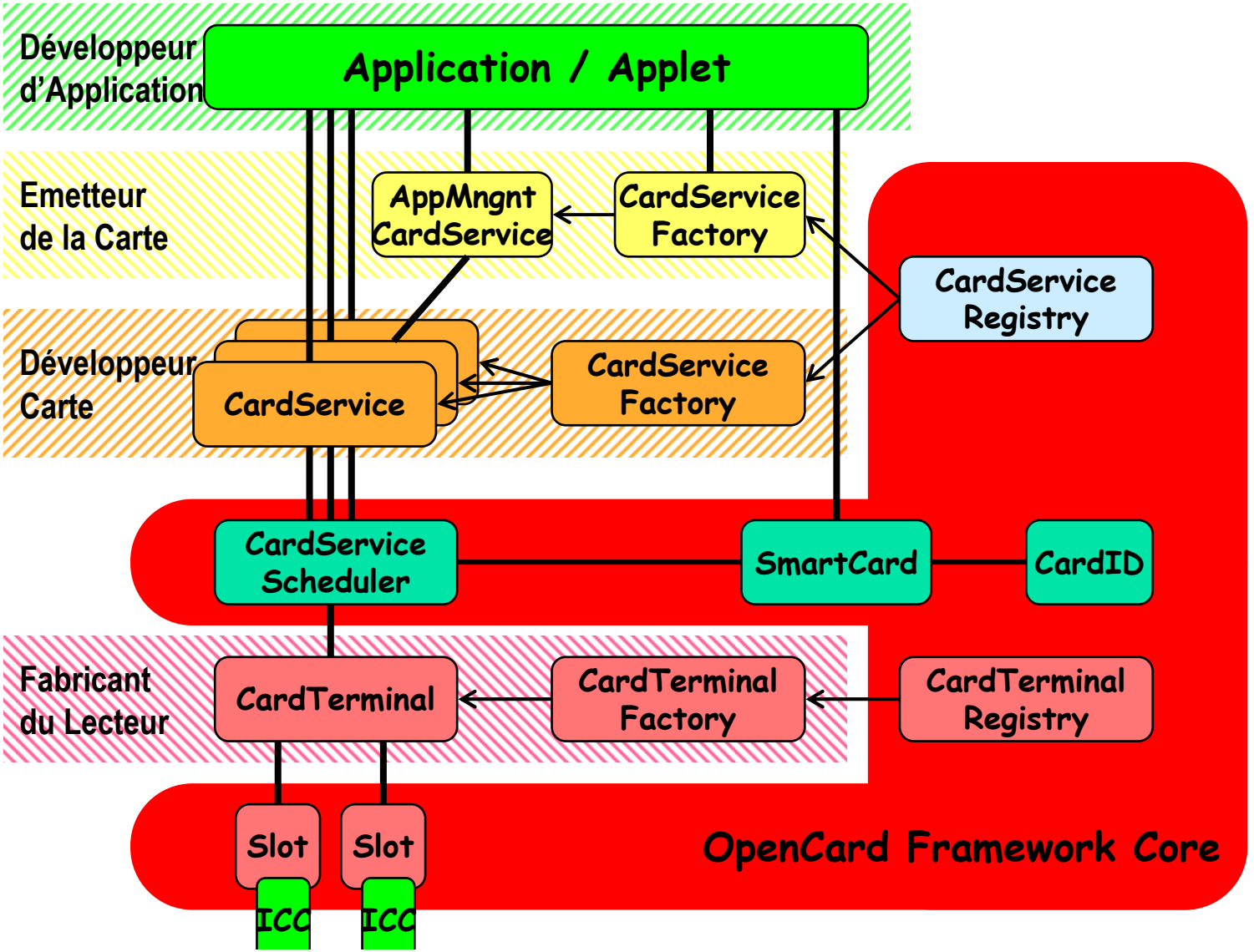
- *1997 JavaCard*
- *1998 JavaCard+GSM SIM*
- *1999 JavaCard+RSA*
- *2000 WAP MicroBrowser*
- *2001 Biometric (FingerPrint)*
- *2002 RMI*
- *2003 .NET Card*
- 2004 TCP/IP Full Duplex
- 2005 Linux
- 2006 Multi-Channel (STIP)
- 2007 Streaming (full TV sattelite)
- 2008 Spontaneous networking (JINI)
- 2009 GRID

API Terminal

OCF : Open Card Framewo

- Consortium lancé par IBM
  - En sommeil depuis plusieurs années ;-(
- Framework standard d'accès à des cartes et des lecteurs depuis un environnement Java
  - orientée objet, extensibilité, réutilisabilité, *etc.*
- 2 notions
  - CardTerminal
    - Drivers Terminal fournis par chaque fabricant
  - CardService
    - représente un type de cartes ou d'applet carte fournit par l'émetteur d'une carte ou d'une applet carte
- eOCF : Embedded OCF
  - adaptation aux hôtes contraints par la mémoire (*e.g.*, terminaux de paiement, téléphones mobiles, …)

Architecture OCF



JSR-268 Java Smart Card I/O API

- APIs for APDU-based communication with Smart Cards
  - in Java Platform 6.0
- Package javax.smartcardio
  - TerminalFactory, TerminalFactorySpi, CardTerminal
  - Card, CardChannel
  - CardException, CardPermission
  - ATR, CommandAPDU, ResponseAPDU
- Comments
  - JC-RMI proxy generators based on 268 ???

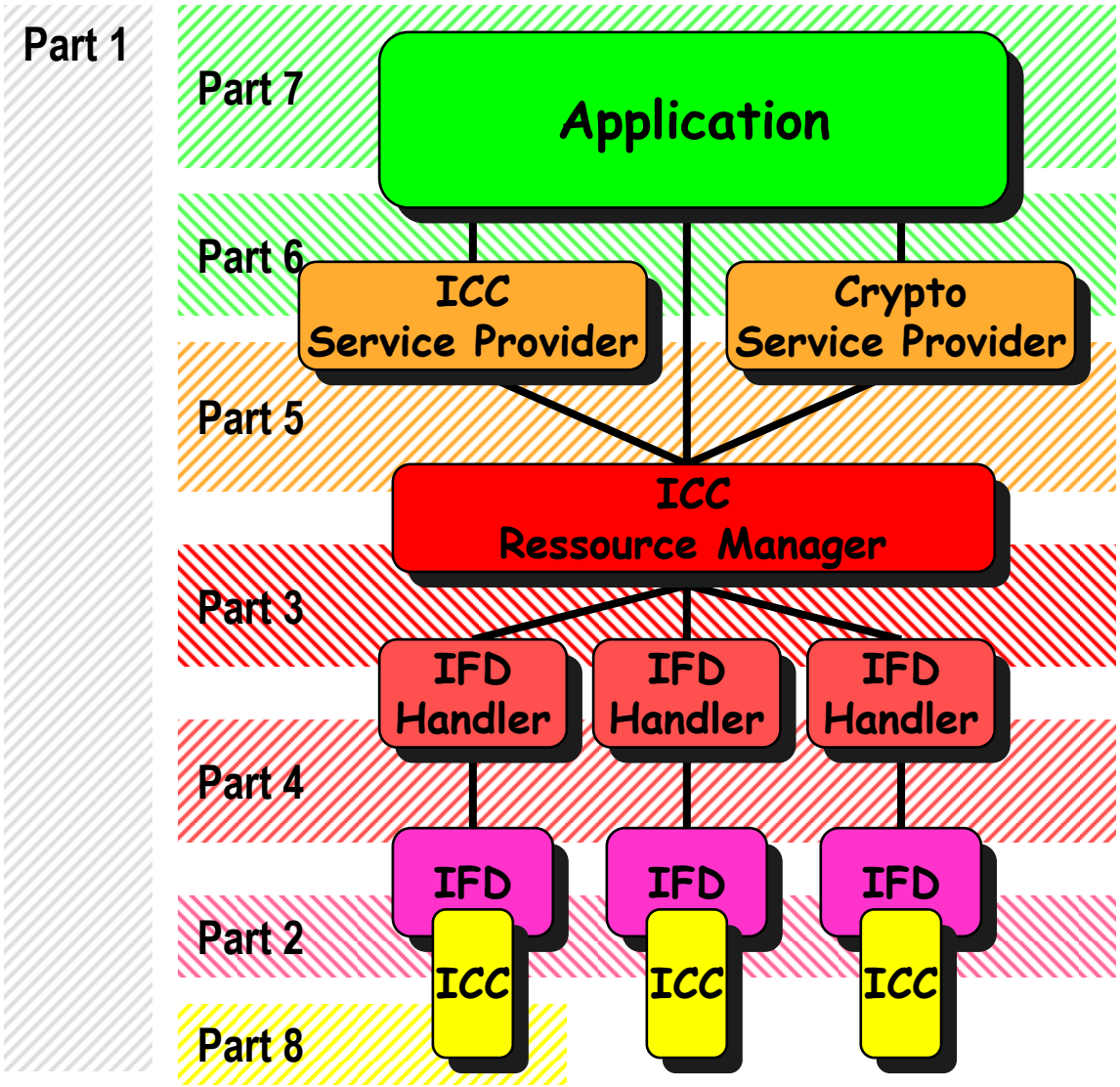
JSR-268 Java Smart Card I/O API Usage sample

```
// show the list of available terminals
TerminalFactory factory = TerminalFactory.getDefault();
List<CardTerminal> terminals = factory.terminals();
System.out.println("Terminals: " + terminals);
// get the first terminal
CardTerminal terminal = terminals.get(0);
// establish a connection with the card
Card card = terminal.connect("T=0");
System.out.println("card: " + card);
CardChannel channel = card.getBasicChannel();
ResponseAPDU r = channel.transmit(new CommandAPDU(c1));
System.out.println("response: " + toString(r.getBytes()));
// disconnect
card.disconnect(false);
```

PC/SC

- Define Specifications
  - Platform and OS independent
    - Windows
    - Linux, Apple (MUSCLE)
  - Compliant with ISO7816, support and endorse industry specifications (EMV, GSM…)

Architecture et Spécifications PCSC



Terminaux Carte

- Contraintes de l'informatique embarqué et enfouie
  - Faible coût (µp 16bits@8Mhz, <256KB (RAM+ROM+EEPROM)
- Spécifications
  - STIP (Small Terminal Interoperability Platform)
  - FINREAD
  - OPTF (Open Platform Terminal Framework)
  - EMV (EuroCard MasterCard Visa)
  - J-Consortium

STIP (Small Terminal Interoperability Platform)

- Objectives
  - Secure transaction applications
    - Banking, Loyalty, e- purse, Security / ID application, Digital Rights Management (MP3, video), Gambling, Games (scores collection, …), eBilling, eVoucher
  - Range of Terminal
    - EFT/ POS terminals, Payphones, Mobile Phones, Palmtops/ PDAs, Stand- alone readers, Home banking terminals, Vending Machines, PC connected card readers, Mass transit terminals, Parking Meters, Utility Meters, Set top boxes
  - Interoperability
  - Application life cycle management
  - Smart card accepting devices
  - Platform with limited resources
  - Coexistence with legacy applications
  - Multi- applications
- Acteurs (www. stip.org)
  - Gemplus, Schlumberger Sema, Schlumberger CP8, Thales, VeriFone, Ingenico, Rambler, Cardsoft, Texas Instruments
- Technologies
  - J2ME (KVM)

FINREAD

- Scope
  - Intelligent Smart card Readers with display and keyboard (pinpad) connected to PC for home- banking and e- commerce
- Specifications
  - •Java API based on STIP 2.0
    - http: //www.cenorm.be/isss/workshop/finread/documents/default.htm
- •Objective
  - Provide security in financial transactions (PIN processing,amount validation) by running program on a secure attached device, not on PC. Remove insecurity that blocks development of e- commerce.
- Actors
  - European Payment Systems (Visa EU, Europay, Interpay, GIE Cartes Bancaires) and Banks

Global Platform *www.globalplatform.org*

- Motivations
  - Global Platform is establishing standards for smart card related industries (smart cards, card acceptance devices,related infrastructures and systems) .
- Actors
  - The main payment schemes are member of Global Platform
- Specification
  - OPTF (Open Platform Terminal Framework)
  - Based on STIP/FINREAD

Conclusion #1 : Les cartes d ’aujourd’hui

- Grand décalage entre les cartes « annoncées » et les cartes « utilisées »
  - La plupart des cartes actuelles sont des 7816-4
  - Peu de JavaCards commercialisées
  - Actuellement la carte est surtout un support de données sécurisées
- De plus en plus de cartes vendues
  - Malgré le surcoût, le gain de sécurité est grand

Conclusion #2
Nouvelles Technologies et cartes

- Internet et Terminaux anonymes
  - Transport de bookmark
  - Identification/Authentification pour accès à un site
- Internet et paiement sécurisé
  - Solution du numéro de CB = le pire
  - Paiement On-line via un PME
  - Utilisation d ’un intermédiaire de confiance

Bibliographie

- Livres carte
  - La Carte à Puce, Coll Que Sais Je ?, n°3492, Ed PUF, 1999
  - Henry Dreifus & J. Thomas Monk, *smartcards -- A guide to building and managing smart card applications*, ISBN: 0-471-15748-1, New York: John Wiley & Sons, 1998.
  - Scott B. Guthery & Timothy M. Jurgensen, *SmartCard Developer's Kit*, ISBN: 1-57870-027-2, Indianapolis, Indiana: Macmillan Technical Publishing, 1998.
    - http://ww.scdk.comm
- Ressources
  - Ressources du site CITI
    - http://www.citi.umich.edu/projects/smartcard/
  - FAQ
    - http://www.scdk.com/atsfaq.htm
  - Google
    - http://directory.google.com/Top/Computers/Hardware/Systems/Smartcards/

Bibliographie

- Articles introductifs
  - "The smart card primer," Rinaldo Di Giorgio (JavaWorld, December 1997)
    - http://www.javaworld.com/jw-12-1997/jw-12-javadev.html
  - How to write a Java Card applet: A developer's guide
    - http://www.javaworld.com/javaworld/jw-07-1999/jw-07-javacard_p.html
  - Sun's Java Card page contains the specifications of the Java Card APIs, the Java Card Virtual Machine, and the Java Card Runtime Environment:
    - http://java.sun.com/javacard
  - "Get a jumpstart on the Java Card," Rinaldo Di Giorgio (JavaWorld, February 1998):
    - http://www.javaworld.com/javaworld/jw-02-1998/jw-02-javadev.html
  - "Understanding Java Card 2.0," Zhiqun Chen with Rinaldo Di Giorgio (JavaWorld, March 1998):
    - http://www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev.html

Bibliographie

- API d'accès aux cartes
  - Uwe Hansmann, Martin S. Nicklous, Thomas Schäck, Frank Seliger, Smart Card Application Development Using Java, Ed Springer, 2000, ISBN: 3-540-65829-7,
    - http://www.opencard.org/SCJavaBook
    - Orienté OCF et livré avec une carte pour les tests
  - Open Card Framework (OCF)
    - http://www.opencard.org/
    - http://www.gemplus.fr/developers/technologies/opencard/index.htm
  - PC/SC
    - http://www.smartcardsys.com/
    - http://www.microsoft.com/smartcard/
    - http://www.pcscworkgroup.com/
  - MUSCLE pour Linux
    - http://www.linuxnet.com/

Bibliographie

- Jack M. Kaplan, *SmartCards -- The Global Information Passport*, ISBN: 1-850-32212-0, Boston, Massachusetts: Thomson Computer Press, 1996.
- Mike Hendry, *Smart Card Security and Applications*, ISBN: 0-89006-953-0, Norwood, Massachusetts: ARTECH House, Inc., 1997.
  - Présentation des concepts de la sécurité et des principales applications de la carte
- W. Rankl & W. Effing, *Smart Card Handbook*, ISBN: 0-47196-720-3, New York: John Wiley & Sons, 1997.
- Chuck Wilson, *Get Smart*, 338 pages (June 1, 2001), Mullaney Corporation; ISBN: 0967446058
  - Orienté décideurs (pas de programmation)
- Damien Deville, Antoine Gall, Gilles Grimaud, Sébastien Jean, « Smart Card Operating Systems: Past, Present and Future » (2003), Proceedings of the 5 th NORDU/USENIX Conference

Webographie

- Une page pleine de références
  - http://paroissien.free.fr/

Autres cours ou présentations

- Jean-Pierre Tual (Axalto), Introduction à la carte à puce, 2004
- …

Bibliographie

- Conférences:
  - CARDIS
  - GDC
  - ESmart
  - CFSE (parfois des articles)
  - …
- Salons et exhibitions professionnels
  - Cartes http://www.cartes.com
  - JavaOne
  - …
- Concours
  - SIMagine

Remerciements à

- Jean-Jacques Vandewalle (Gemalto R&D)
- Pierre Paradinas (CNAM- INRIA)
- Alain Rhelimi (Gemalto)

Vos suggestions et vos remarques

- Merci de me les retourner à
  - Didier DONSEZ, didier.donsez@ieee.org
- Avez vous trouvé ce cours instructif ?
  - Est il complet ?
  - Qu 'est qu 'il manque ?
  - Qu 'est que vous auriez aimé voir plus développé ?
  - Est il bien organisé ?
  - ...
- Quels sont votre fonction et votre domaine d'activité ?