

La carte à puce

Damien Sauveron
damien.sauveron@unilim.fr
<http://damien.sauveron.fr/>

(et tous les auteurs cités en bibliographie)

1

Intervenants dans le module

Damien Sauveron (Cours, TD et TP) :

- Membre de l'équipe « Smart Secure Devices » (Périphériques Sécurisés Intelligents)
- Thème de recherche : sécurité des cartes à puce et des réseaux ad hoc

Pour me contacter :



Damien Sauveron
XLIM UMR 6172 CNRS -- Université de Limoges
123 avenue Albert Thomas
87060 Limoges Cedex, FRANCE

Email: Damien.Sauveron@unilim.fr
Web: <http://damien.sauveron.fr/>
Phone: +33 (0) 5 87 50 67 93

MCF à l'Université de Limoges depuis septembre 2006

Visite postdoctorale au Smart Card Centre de l'Information Security Group du Royal Holloway University of London

Thèse au LaBRI – Université Bordeaux 1 sur la Sécurité de la Technologie Java Card

Ingénieur R&D dans le CESTI de SERMA Technologies (Pessac)

Organisateur de WISTP2007 (Héraklion) et WISTP2008 (Séville)

Vice président du groupe de travail de l'IFIP : Pervasive System Security

2

Plan

La carte à puce et les concepts de base

Qu'est-ce qu'une carte ?

Historique

Deux classifications:

- Par technologie pour la puce
- Par technologie de communication

Standard ISO 7816

- Protocole de communication

Chaîne de fabrication

Acteurs

Applications

Les sécurités

Au niveau physique

Au niveau logicielle

Au niveau de l'environnement de production

Méthodes formelles & Test

Évaluation sécuritaire et certification

Les attaques

Non invasive

Invasive

Les cartes du futur

Bibliographie

Rendez vous

Java Card Grid Projet

3

Et si on se commençait par une vidéo ?

On ne rit pas !!!!

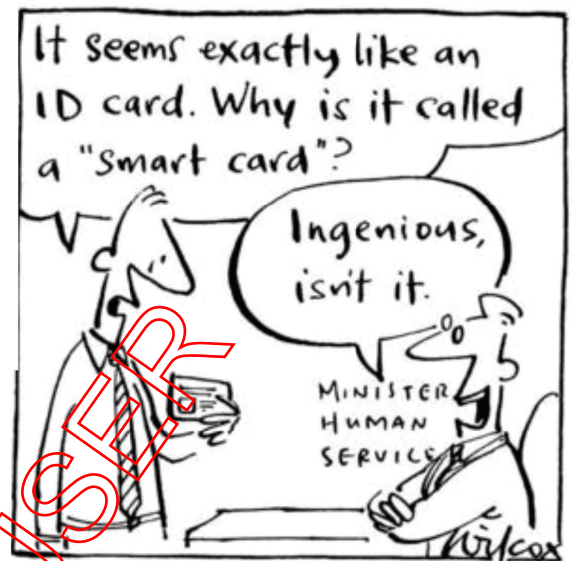
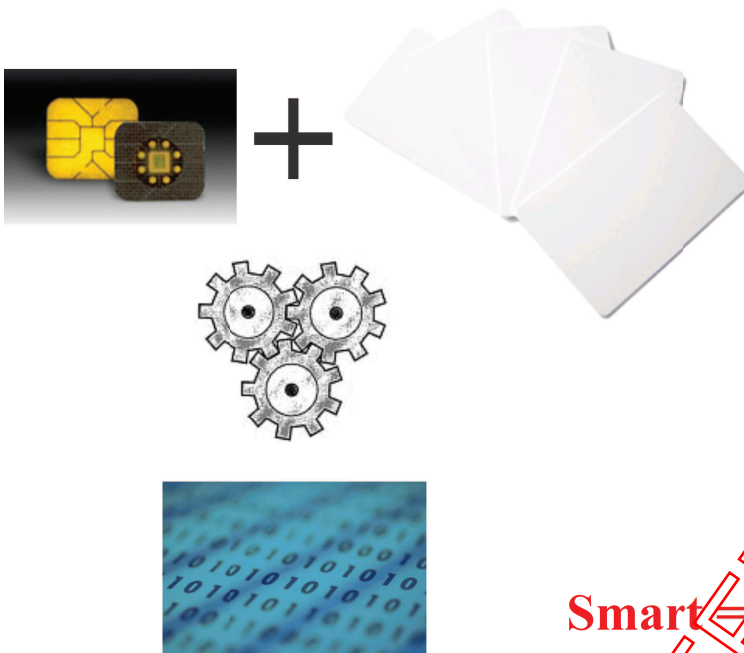
Roland Moreno La carte a puce (prod Le sabre).flv

4

Qu'est ce qu'une carte à puce

un morceau de plastique de la taille d'une carte de crédit

un circuit électronique capable de manipuler (stocker, calculer, etc) des informations



Smart = intelligente !
Pourquoi ?

5

Historique



La carte à puce,
une innovation française ?

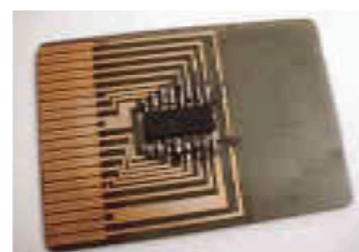
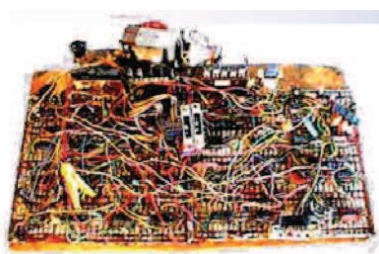
En France : OUI

Dans le reste du monde : NON

En 1967-1968, deux ingénieurs Allemands **Jürgen Dethloff** et **Helmut Grötrupp** introduisent un circuit intégré dans une carte plastique (déposent un brevet en 1969)

En mars 1970, Kunitaka Arimura au Japon dépose un brevet sur la carte à puce.

En 1971, Paul Castrucci de IBM dépose aux USA un brevet intitulé *Information Card*



6

Historique

Entre 1974 et 1978, le français Roland Moreno, le père de la carte à puce dépose 47 brevets dans 11 pays.
(crée ensuite la société **Innovatron**)

Implication industrielle de Bull et Schlumberger

Prototype de puce portable imaginé par Moreno :



En 1968, René Barjavel dans la "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. »

Mise au point de moyens inhibiteurs (par Moreno) logés sur la puce

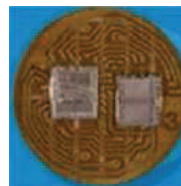
- comparaison interne du code confidentiel ;
- compteur d'erreurs, qui provoque l'autodestruction de la puce en cas de soumission répétée d'un code faux ;
- moyens de traitement ;
- lecture impossible de zones prédéterminées, notamment code confidentiel, clés, etc. ;
- écriture, modification, effacement impossibles de zones prédéterminées de la mémoire.

En 1997, Roland Moreno est entré au National Museum of American History.

7

Historique

En 1977, le Français Michel Ugon (de la compagnie Bull) propose de mettre les moyens inhibiteurs sur un micro-processeur.



Mars 1979, CII Honeywell Bull et Motorola :

Deux puces: une mémoire 2716 EPROM et un microprocesseur 8 bits 3870.

Octobre 1981, puce monolithique CII-Honeywell Bull
(CP8 : Circuit Portatif des années 80)

Historique

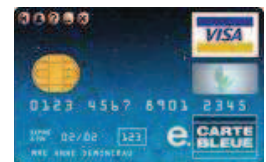
En 1979, la première carte est créée par Bull CP8 (1Ko de mémoire programmable et cœur à base de microprocesseur 6805).



En 1983, apparition des premières cartes téléphoniques à mémoire (commercialisation des premières télécartes par France Télécom fabriquées par Schlumberger)



En 1984, adoption par le G.I.E carte bancaire de la « carte bleue » (carte à microprocesseur)

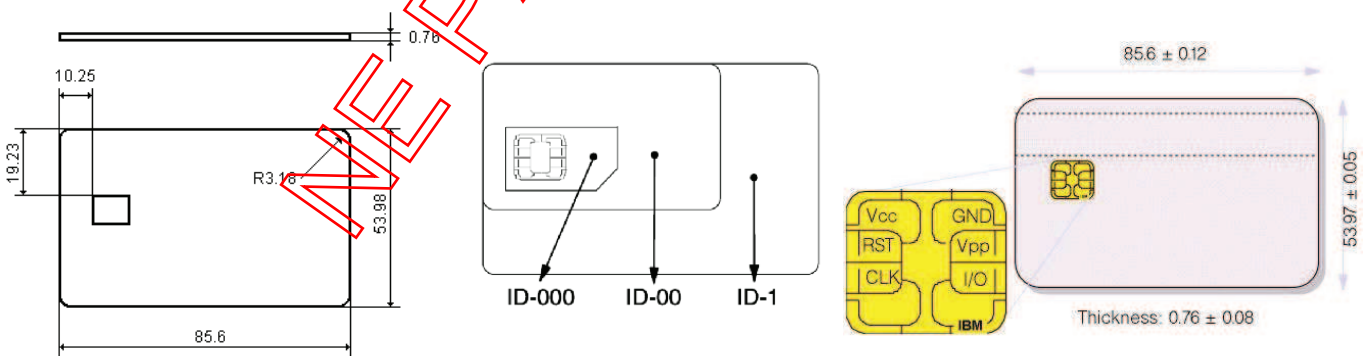


9

Historique

Entre 1984 et 1987, normes ISO 7816 (carte à puce à contact)

- **Objectif** : Permettre aux cartes de fonctionner partout dans le monde !



En 1997, apparition des premières Java Cards

- 30 ans après des nouveautés dans le monde de la carte. Enfin !!!



Premières entreprises de la carte

- La société Innovatron créée par Moreno pour exploiter ses brevets.
- En 1979, Schlumberger (géant des services pétroliers) entre au capital d'Innovatron, pour 34 %.
- Schlumberger devient le numéro 1 mondial de la carte à puce (cartes, lecteurs, cabines téléphoniques, systèmes),
- En 1997, Schlumberger acquiert le concurrent français : SOLAIC.
- En 2001, Schlumberger acquiert le concurrent français Bull CP8.
- En 1981, le GIE « Carte à Mémoire » lance trois expérimentations de la carte à puce avec: Bull, Phillips, et Schlumberger.
- En 1984, le GIE devient « Cartes Bancaires ».
- Fin des années 80, GIE « CB » commande 10 millions de cartes CP8, généralisant l'utilisation de la carte à puce en France en 1992.

Vers les géants de la carte à puce

- En 1988, Marc Lassus crée Gemplus en France
- En 2001, l'activité « Cartes à puce » est cédée à Schlumberger qui externalise cette activité à Axalto
- En 2004, Schlumberger qui veut se recentrer sur les métiers du secteur pétrolier, se sépare d'Axalto en l'introduisant à la bourse de Paris.
- En 2006, fusion de Axalto et de Gemplus =>
Gemalto (numéro 1 mondial de la carte à puce)
- Exemples d'entreprises concurrentes aujourd'hui : Oberthur Technologies, Sagem Orga

Quelques dates/1

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

13

Quelques dates/2

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

14

**les cartes à mémoire
versus
les cartes à microprocesseur**

**les cartes à contact
versus
les cartes sans contact
versus
les cartes dual-interface**

15

La carte à mémoire

Premier modèle de cartes à puce

Majorité des cartes vendues dans le monde en 1999 (on va voir quelques chiffres plus récents)

Elle possède :

- une puce mémoire de 1 à 16 Ko
- une logique câblée non programmable

Avantages :

- sa technologie simple
- son faible coût (1€)

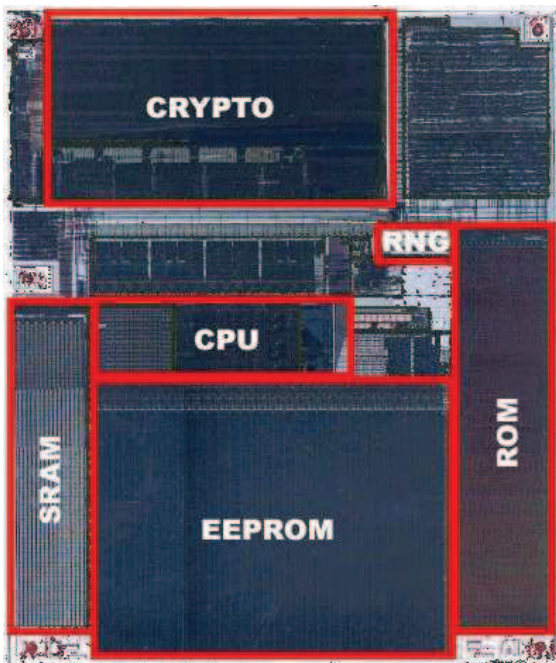
Inconvénients :

- sa dépendance vis-à-vis du lecteur de carte
- « assez » facile à dupliquer

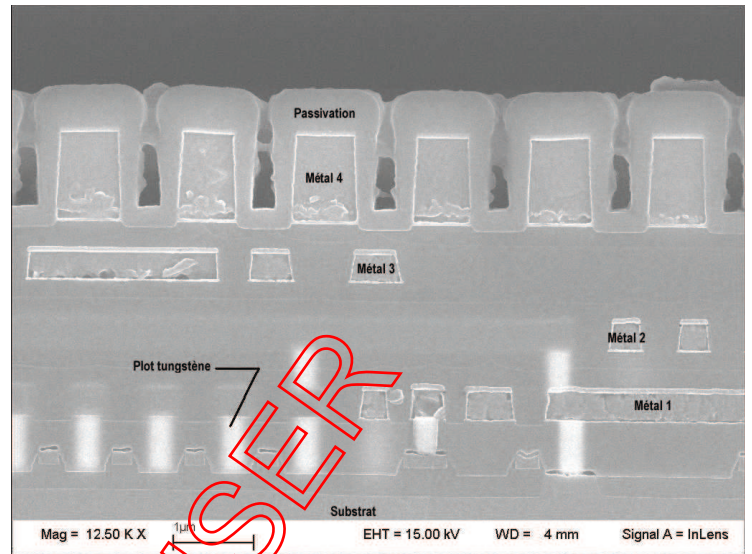
16

La carte à microprocesseur

Taille de la puce : $25\text{mm}^2 * 200\mu\text{m}$ ($6\mu\text{m}$)



Vue de dessus



Vue en coupe

Coût : entre 1€ et 20€ (acceptable pour tant de sécurité).

17

La carte à microprocesseur

Microprocesseur : 8, 16 ou 32 bits (à architecture CISC ou RISC)

ROM : 32 à 256 Ko

Stocke le système d'exploitation et des données permanentes
Figée en usine

EEPROM : 32 à 256 Ko

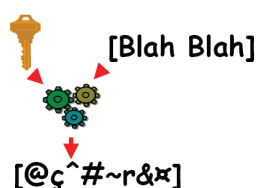
Mémoire persistante => stocke les données applicatives
Problèmes : durée de vie limitée et temps d'accès lent

RAM : 1 à 4 Ko

Mémoire de travail

Avantages : durée de vie illimitée et temps d'accès rapide

Coprocasseur cryptographique



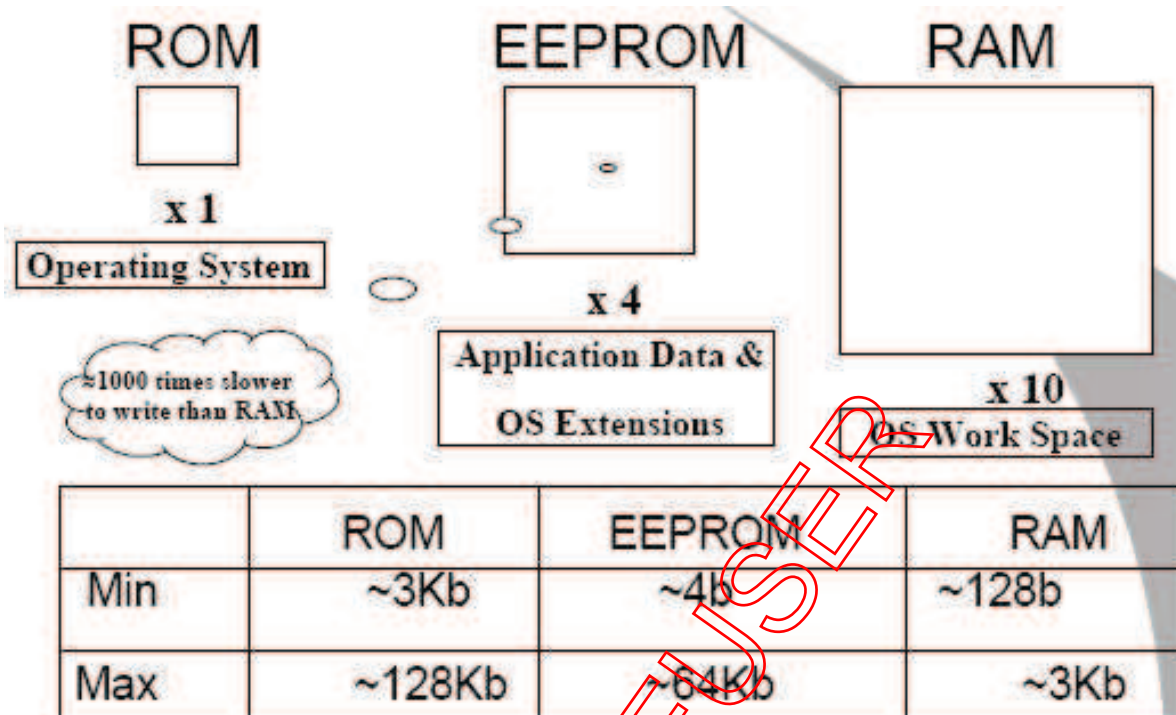
Générateur de nombres aléatoires (RNG)

Vers de nouvelles mémoires (+ rapide, + grosse) : FeRAM, Flash, MRAM



18

Les différents types de mémoires



19

Les différents types de mémoires

	RAM Statique Volatile	EEPROM	Flash-RAM	Fé-RAM (expérimentale)
Persistance	Non Volatile	Non Volatile	Non Volatile	Non Volatile
Tps Accès Read	0.1 μ s	0.15 μ s	0.15 μ s	0.1 μ s
Tps Accès Write	0.1 μ s	10 μ s	10 μ s	0.4 μ s
Tps Effacement (Reset)	Sans	5 000 μ s	100 000 μ s	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 μ m ²	> 30 μ m ²	< 10 μ m ²	< 10 μ m ²

20

Comparatif entre la carte et ...

L'ordinateur de pilotage d'Apollo 11 (1969)

- 2 Mhz CPU
- 16 bits
- 2 Ko de RAM
- 36 Ko de ROM

Un PC de la fin des années 90



	Carte à puce	PC	Ratio
RAM	1 Ko	128 Mo	130000
Stockage	64 Ko	6 Go	100000
Connectivité	192 Kbits	100 Mbits	500
Microprocesseur	20 Mips	500 Mips	25

21

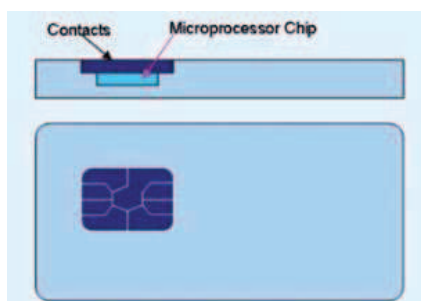
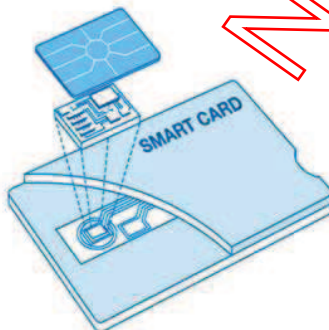
Carte à contact

Suit le standard ISO 7816

Communication série via huit contacts => insertion dans un lecteur de carte

Problèmes :

l'insertion et le retrait sont des facteurs d'usure de la carte
orientation de la carte dans le lecteur

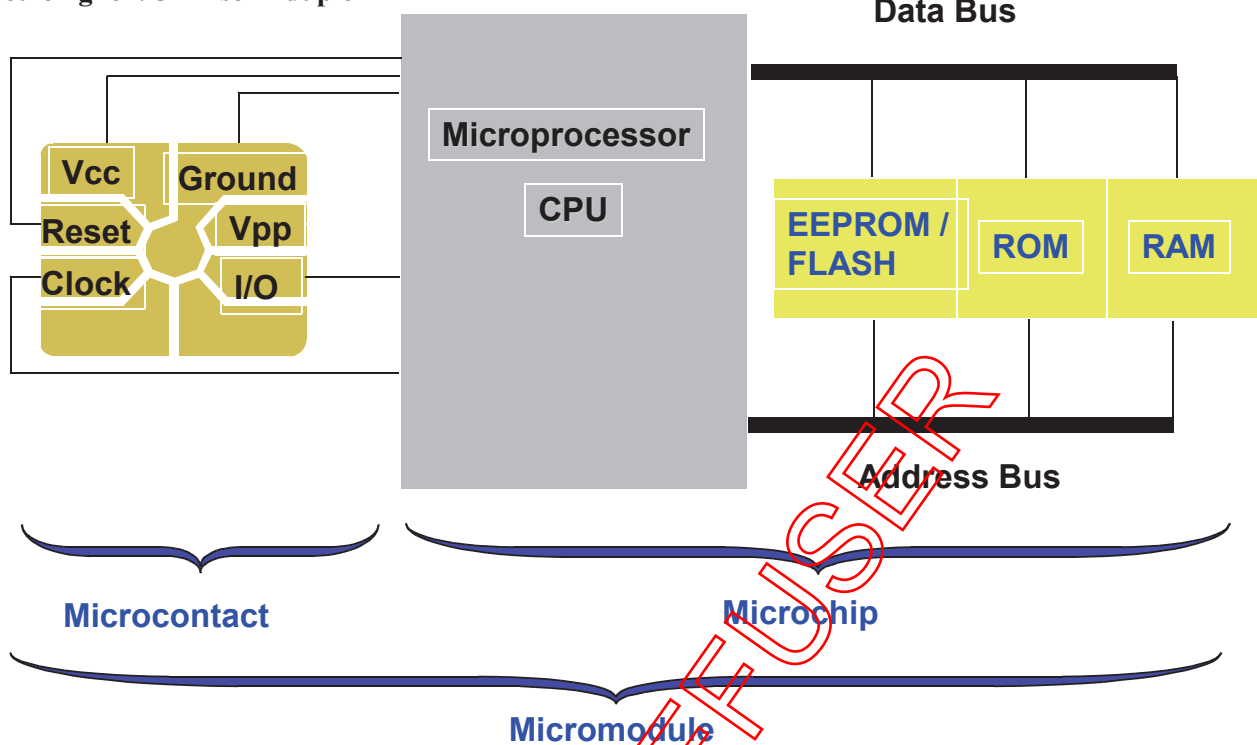


22

La carte à contact

Son fonctionnement, l'oblige à être insérée dans un lecteur de carte.
Elle utilise une communication série via huit contacts.

1 seule ligne I/O => semi duplex



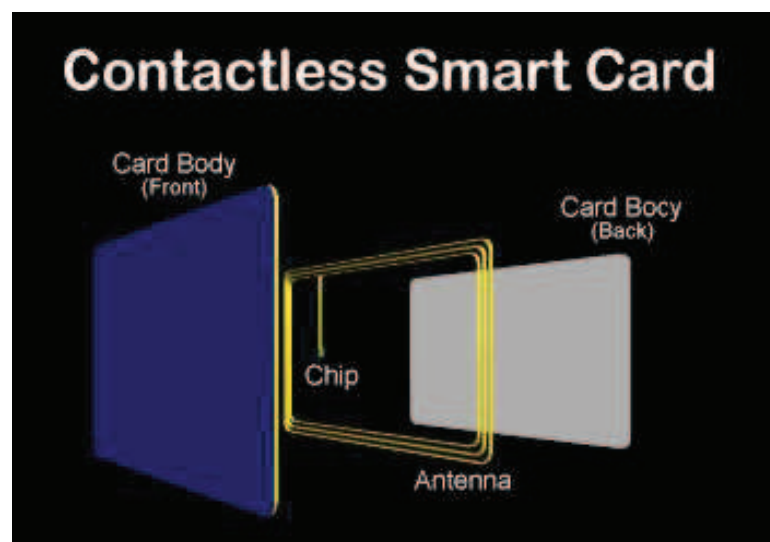
23

Carte sans contact

Communication via une antenne dans la carte
Récupère son énergie d'un couplage capacitif ou d'un couplage inductif
Suit le standard ISO 14443

Problèmes :

distance de communication limitée (environ 10 cm)
temps de transaction est de l'ordre de 200 ms => limite les données à échanger
le coût élevé



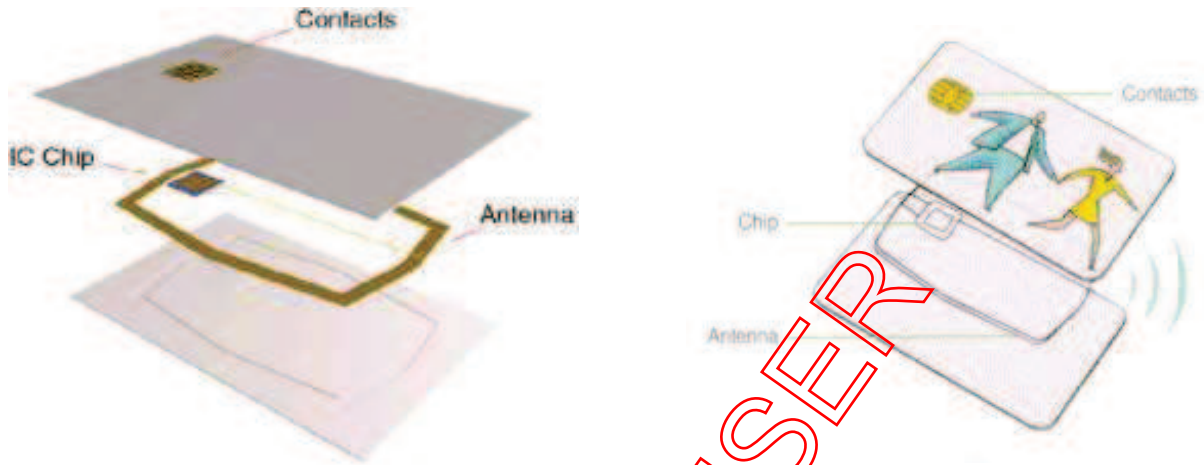
24

La carte combi

C'est une combinaison entre :

- la carte à contact
- et la carte sans contact

Ces deux possibilités de communication en font une carte « idéale ».



25

Quelques spécimens de mon Zoo



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 cartes

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

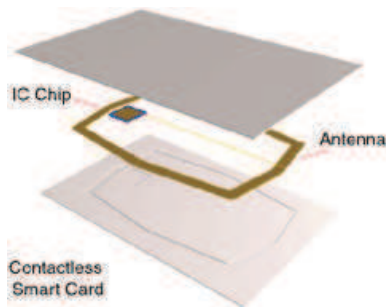


Quelques périphériques pouvant intégrer une puce sécurisée



Anneau Java

IButton



Dongles : Série, parallèle, USB

29

Quelques chiffres

1999 Card Shipments figures per sector

- Strong increase in microprocessor cards (+60%)
- Slight progression of memory cards (+14%)

	Memory (MU)	Microprocessor (MU)
Banking		108
Healthcare	27.5	30
Telecom	913	200
Transport	40.5	3
Pay TV / IT	1	29
Others	49	28
Total 1999	1031	398
	1429	

Worldwide Market 2004

Cards (Millions of units - Mu)			
By segments	Memory (MU)	Microprocessor	
			Growth % From 2003
Telecom	710	1050	57%
Financial services / Retail / Loyalty	35	280	37%
Government/ Healthcare	20	45	12%
Transport	60	15	25%
Pay TV	-	55	57%
Corporate Security	10	12	72%
Others	10	12	20%
Total H1 2004	845	1469	50%
Total 2004	2314		

30

Quelques chiffres

Cards (Millions of units - Mu)			
Sectors	Memory (Mu)	Microprocessor	
			Growth % From 2004
Telecom	580	1390	32,38%
Financial services / Retail / Loyalty	30	336	20%
Government/ Healthcare	25	60*	33,33%
Transport	73	20	-
Pay TV	-	55	-
Corporate Security	20	15	-
Others	10	12	-
Total	738	1 888	28,52%
Total 2005	2626		

Shipments by Region 2005

Cards %		
Geographical Zones	Memory (Mu)	Microprocessor
EMEA	44%	48%
ASIA	32%	36%
AMERICAS North and South	44%	16%
Total 2005	100%	100%

Quelques chiffres

Smart Card shipments Global 2007

Cards (Millions of units - Mu)		
Sectors	Memory	Microprocessor
Telecom	440	2 600
Financial services / Retail / Loyalty	30	500
Government/ Healthcare	300	105
Transport	160	15
Pay TV	-	70
Corporate Security	20	20
Others	10	15
Total 2007	960	3325
Total 2007	4285	

Quelques chiffres

2007 Secure Contactless market overview (excluding access control and ticketing)

	Secure Memory Contactless (Mu)	Secure Microprocessor Contactless (Mu)
Financial Services	-	45
Government - Health care	250	45
Transport	160	15
Others	-	28
TOTAL 2007	410	133

33

Quelques chiffres

Worldwide Smart Secure Device shipment - 2011 and 2012 forecasts Millions of Units (Mu)

	2011 forecast	2012 forecast	2012 vs 2011 % growth
Telecom	4,600	5,100	11%
Financial services	1,010	1,200	19%
Government - Healthcare	240	300	25%
Transport	80	95	19%
Pay TV	125	140	12%
Others	80	90	13%
Total	6,135	6,925	13%

Telecom: including NFC secure elements (SWP UICC, μ SD, embedded SEs)

Secure Contactless market figures – 2010 and 2011 forecasts Millions of Units (Mu)

	2011 forecast	2012 forecast	2012 vs 2011 % growth
Financial services	225	290	29%
Government - Healthcare	125	160	28%
Transport	80	95	19%
Others	30	35	17%
Total	460	580	26%

34

Quelques chiffres

Eurosmart estimated worldwide Smart Secure Devices (microprocessors)
Millions of Units

	2012	2013 forecast	2013 vs 2012 % growth
Telecom	5.100*	5.350	5%
Financial services	1.200	1.480	23%
Government - Healthcare	310	360	16%
Transport	135	160	19%
Pay TV	135	145	7%
Others	90	100	11%
Total	6.970	7.595	9%

Eurosmart estimated worldwide Smart Secure Contactless Devices (microprocessor)
Millions of Units

	2012	2013 forecast	2013 vs 2012 % growth
Financial services	295	455	54%
Government - Healthcare	170	210	24%
Transport	135	160	19%
Others	60	70	17%
Total	660	895	36%

35

ISO 7816 : le standard !

Partie 1 : Caractéristiques physiques

Partie 2 : Dimensions et position des contacts

Partie 3 : Signaux électroniques et protocoles de transmission

Partie 4 : Commandes inter-industrie pour l'échange

Partie 5 : Identificateur d'application

Partie 6 : Eléments de données inter-industrie

Partie 7 : Commandes inter-industrie pour SCQL (Structured Card Query Language)

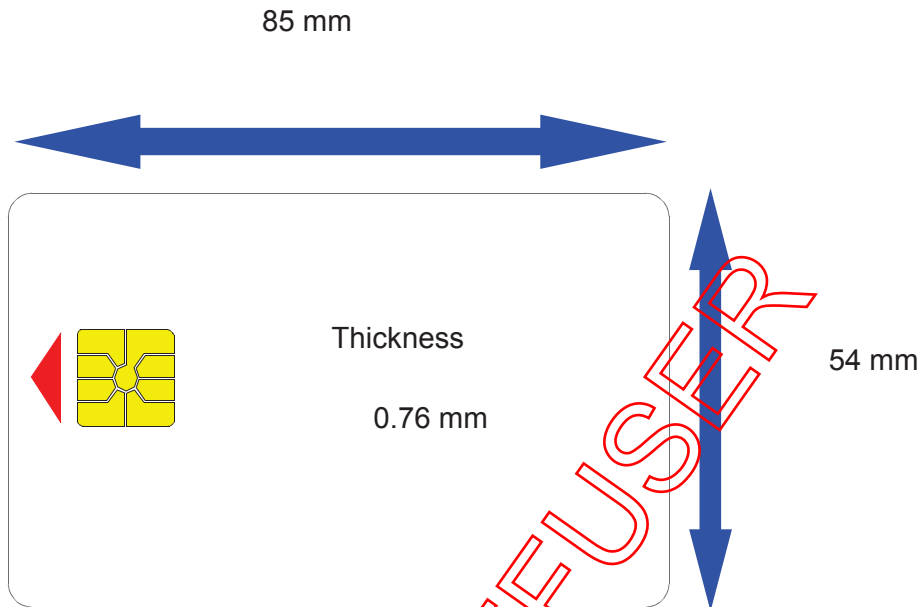
Partie 8 : Sécurité de l'architecture et des commandes inter-industrie

36

ISO 7816-1

Définit les caractéristiques physiques : dimensions, flexibilité, résistivité.

Définit aussi les formats plus petits (SIM)



37

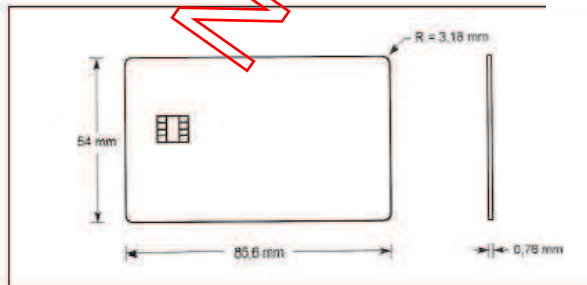
ISO 7816-1

Formats normalisés des cartes à puce

- Même si on connaît en général deux formats de la carte à puce
 - ✓ Celui de la carte bancaire
 - ✓ Celui de la carte SIM

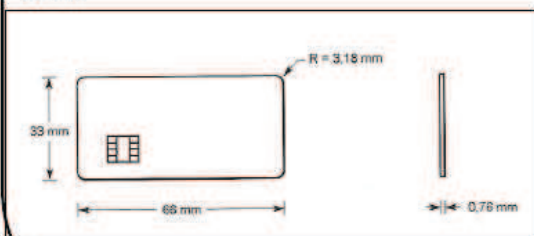
Les 3 formats

- 3 formats normalisés : ID1, ID00 et ID000

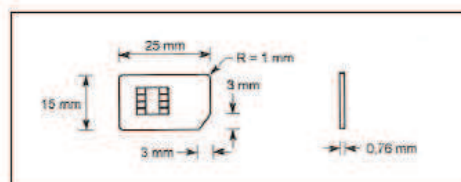


ID 01

ID 00



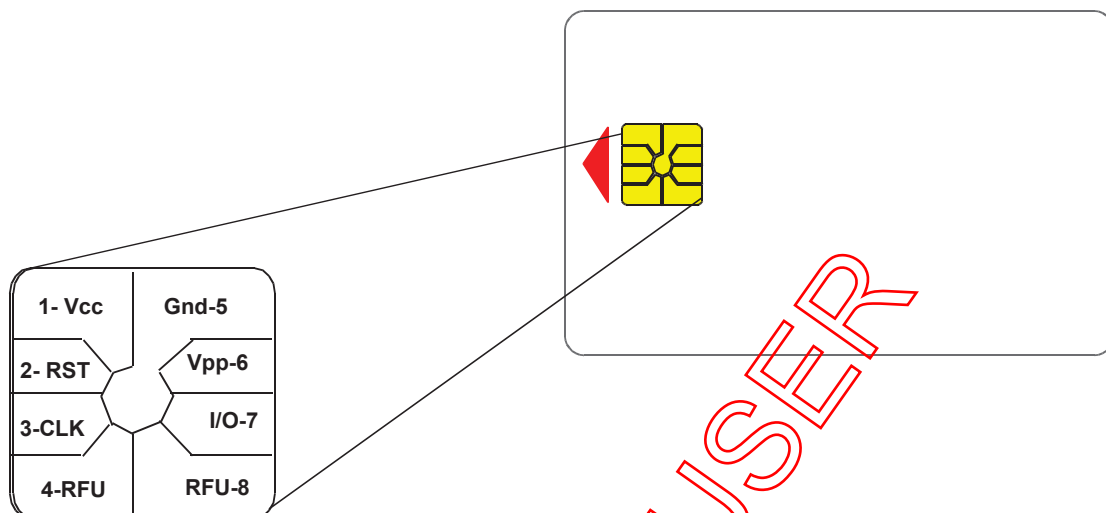
ID 000



38

ISO 7816-2

Définit les aspects électriques et la situation des contacts sur la carte.



39

ISO7816-2

Normalisation AFNOR / ISO

La position des contacts : position AFNOR et position ISO



Carte ISO

Carte AFNOR

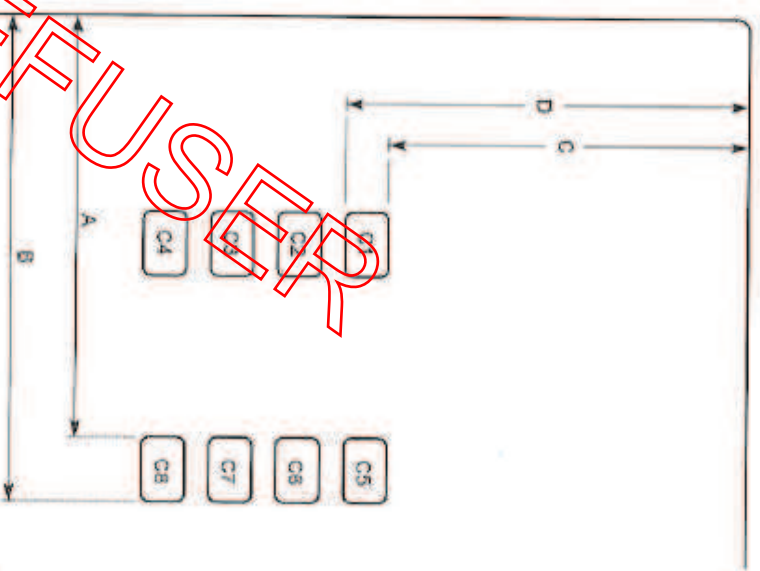
40

Position de la puce % au support plastique

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

Position ISO 7816

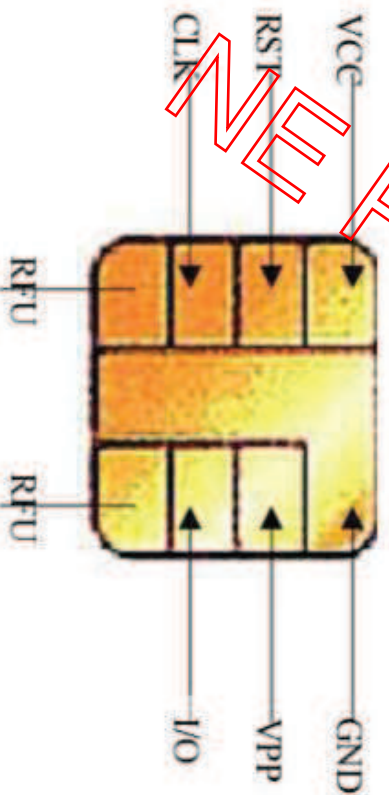
Valeurs en mm



ISO 7816-2



Les différents contacts



Vcc: tension électrique (3 à 5 V)

RST: c'est le « reset », initialise le microprocesseur (warm reset)

cold reset = coupure et rétablissement de l'alimentation

CLK: signal d'horloge car pas d'horloge sur la carte

GND: masse

Vpp: utilisé dans les anciens modèles pour avoir une autre source d'alimentation

I/O: utilisé pour le transfert des données et des commandes entre la carte et le lecteur.

ISO 7816-3

Cette partie normalise :

les caractéristiques électriques comme :

- la fréquence d'horloge (entre 1Mhz et 5Mhz)
- la vitesse des communications (jusqu'à 115200 bauds)

les protocoles de transmission (TPDU : Transmission Protocol Data Unit) :

- T=0, protocole orienté octet
- T=1, protocole orienté paquet
- T=14 réservé pour les protocoles propriétaires

la sélection du type de protocole (PTS : Protocol Type Selection)

la réponse au reset (ATR : Answer To Reset)

Correspond à la mise en route du prog ROM de la carte

- Max. 33 caractères et 5 champs
- Permet de fixer :

Les conventions de codage des octets

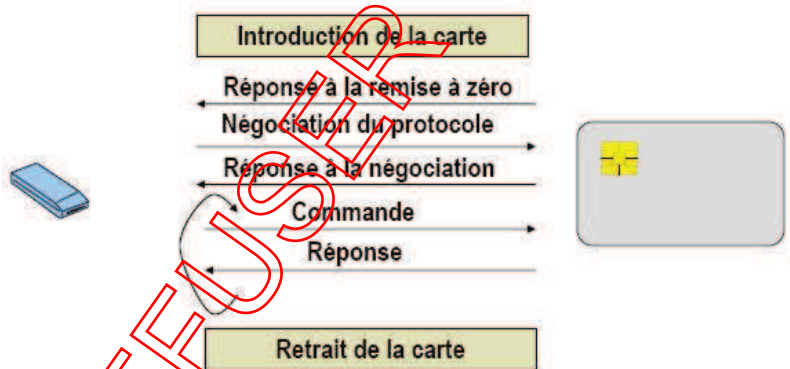
Le temps de transmission d'un bit

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)

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



Exemples 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

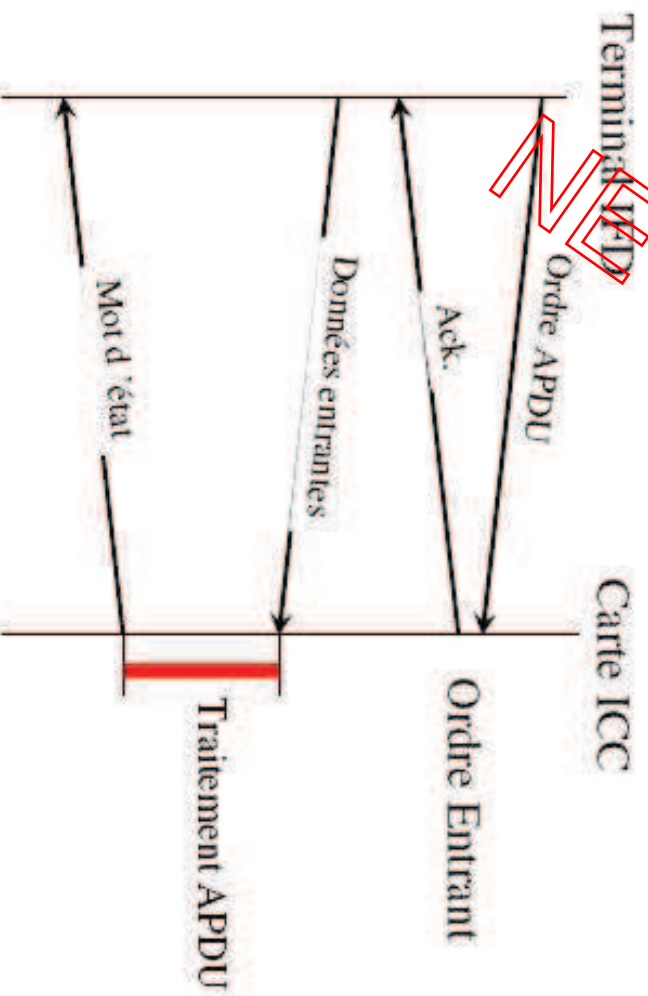
T=0 : Structure de l'ordre



- 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

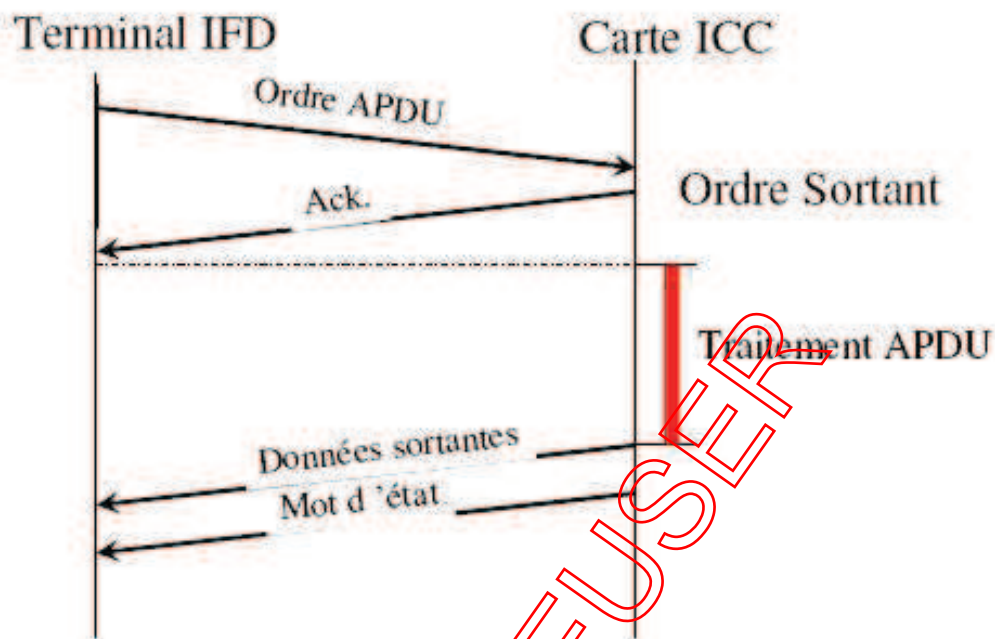
Echange de données : T=0

Transmission de caractères asynchrones



Echange de Données : T=0

Transmission de caractères asynchrones



47

ISO 7816-4

ISO 7816-4 vise à assurer une interopérabilité.

But : indépendance des applications par rapport aux couches physique et liaison

Il spécifie :

le contenu des messages entre la carte et le lecteur

- les commandes
- les réponses

les structures des fichiers et de données :

- l'accès à ces données
- l'architecture de sécurité
- la sécurisation des communications

Le protocole APDU

Protocole de niveau application.

- La commande APDU (C-APDU) : émise par le CAD vers la carte

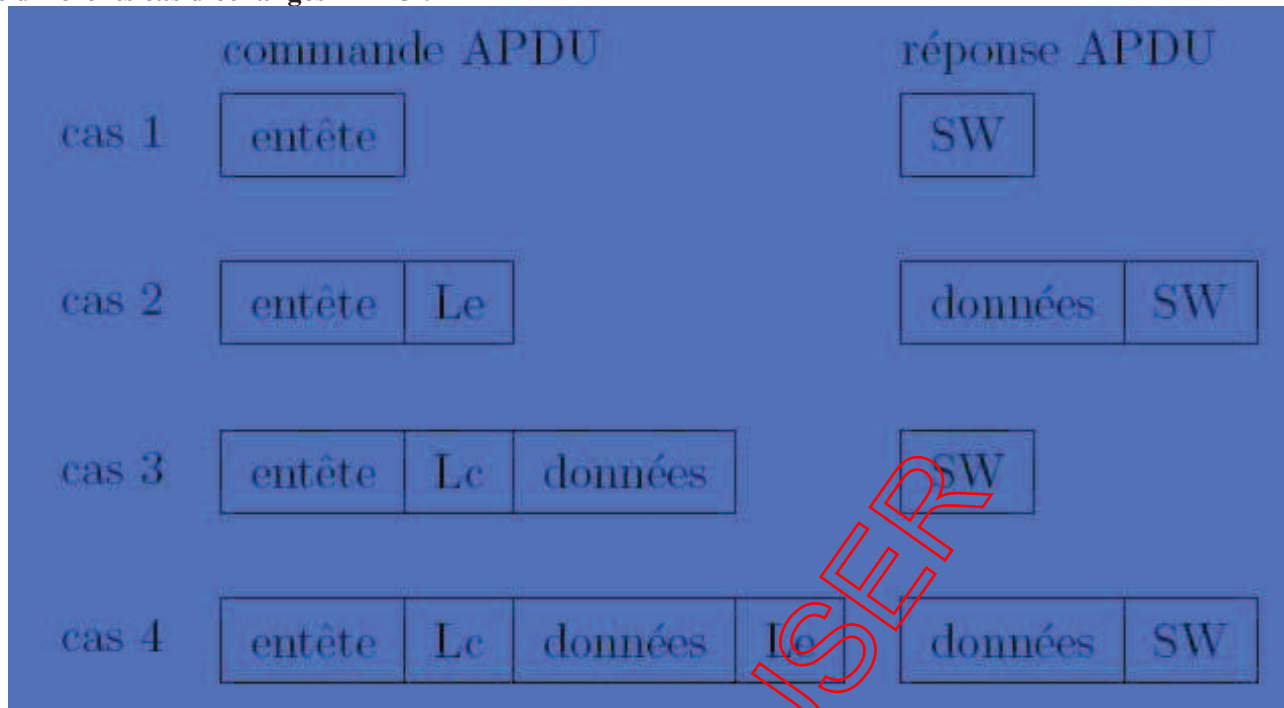
Entête obligatoire				Corps optionnel		
CLA	INS	P1	P2	Lc	Champ de données	Le

- La réponse APDU (R-APDU) : transite de la carte vers le CAD

Corps optionnel		Enqueue obligatoire	
Champ de données	SW1	SW2	

48

Les différents cas d'échanges APDU :



Standardise différents codes de réponse SW1/SW2

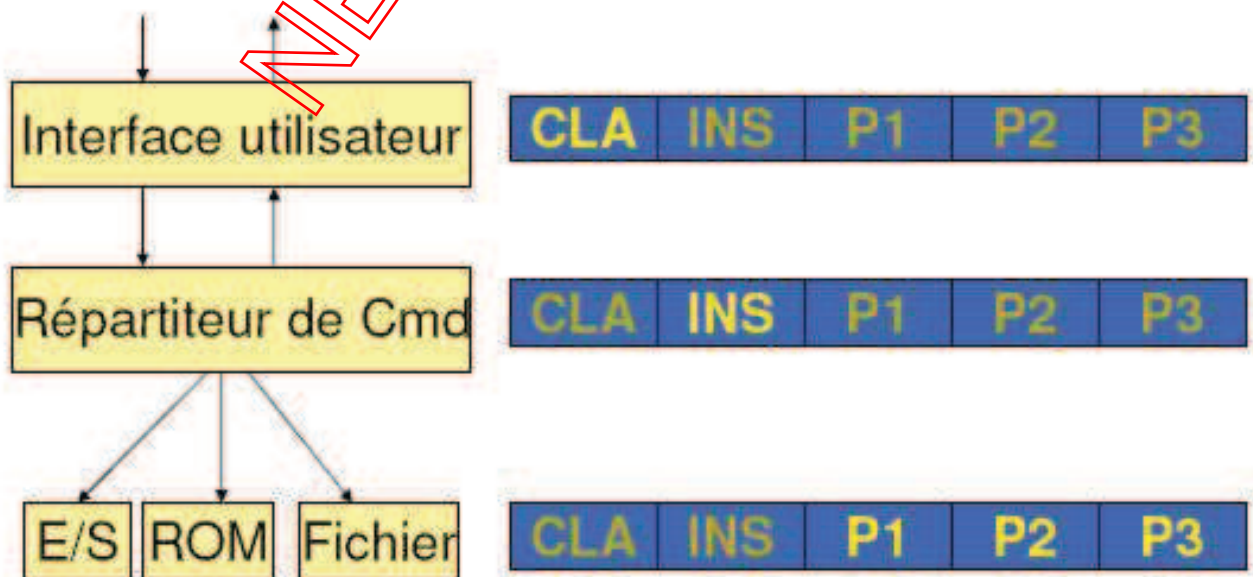
90 00

6E XX: Classe inconnue

6D XX: instruction inconnue

9X XX: Erreur applicative

49

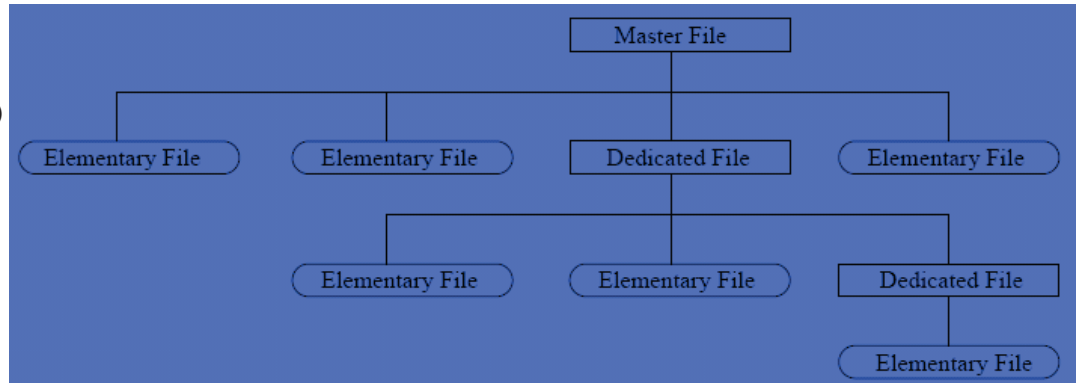


50

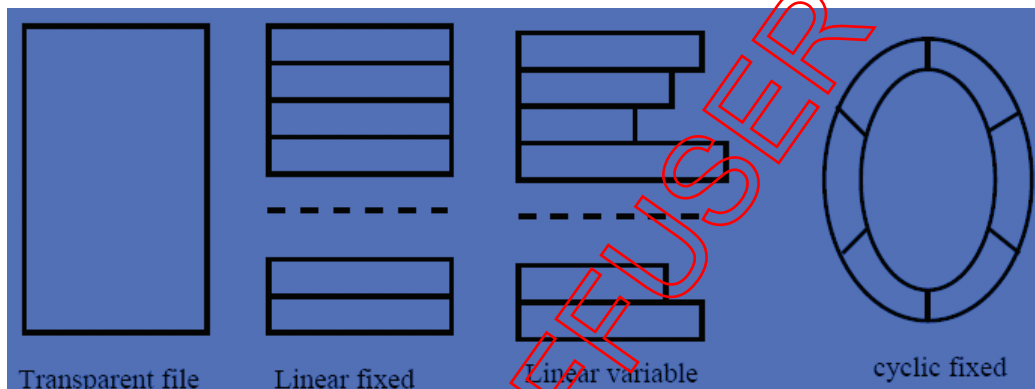
ISO 7816-4

Le système de fichiers des cartes à puce supporte un système de fichiers hiérarchique qui peut contenir trois types de fichiers :

- "Master File" (MF)
- "Dedicated File" (DF)
- "Elementary File" (EF)



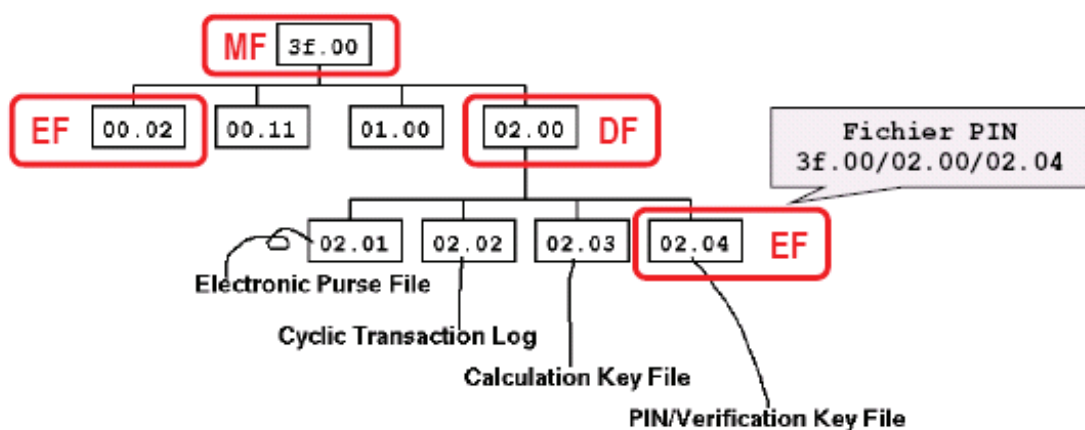
Les différents types de « Elementary File » (EF)



51

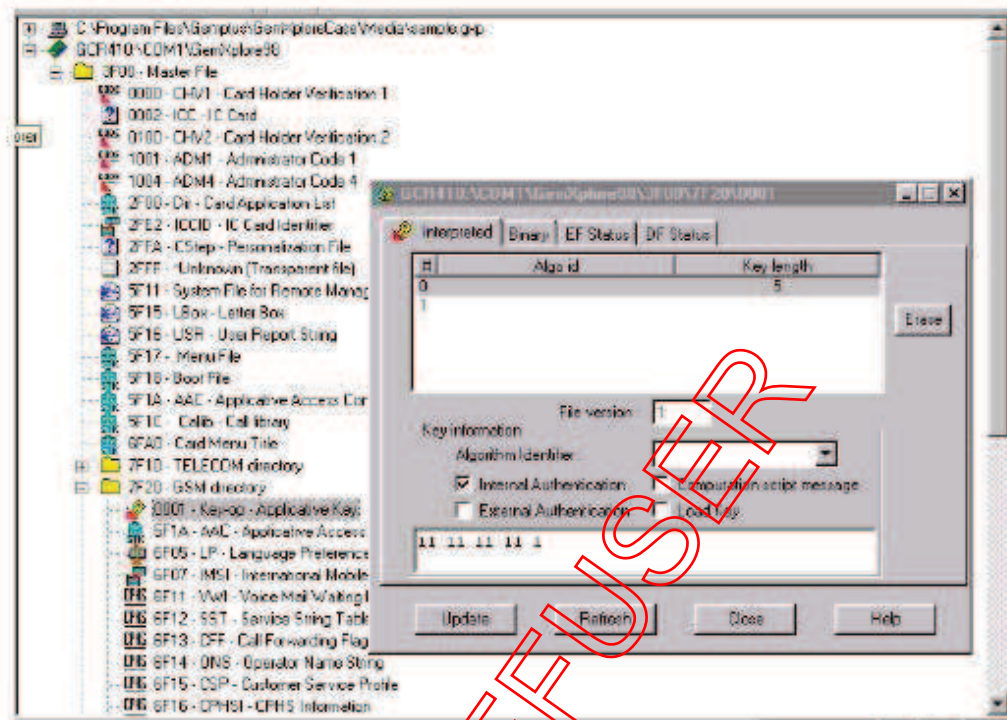
Système de Fichier ISO 7816-4

- 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



2

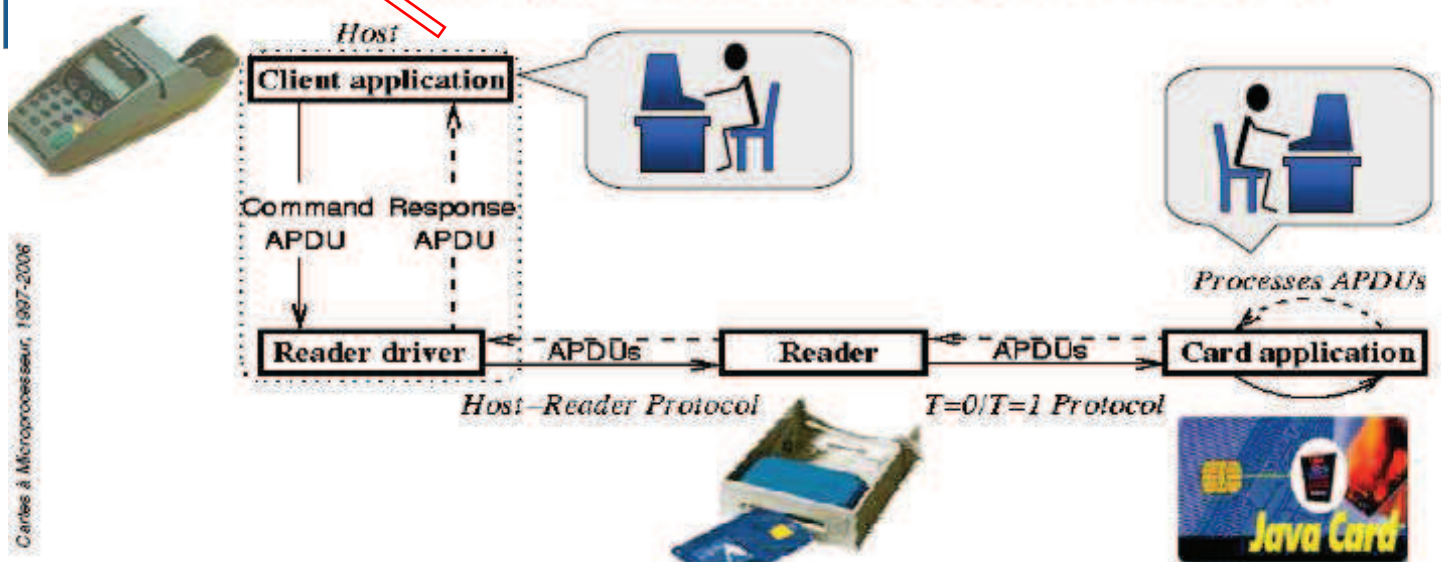
Exemple de système de fichier d'un module SIM GSM



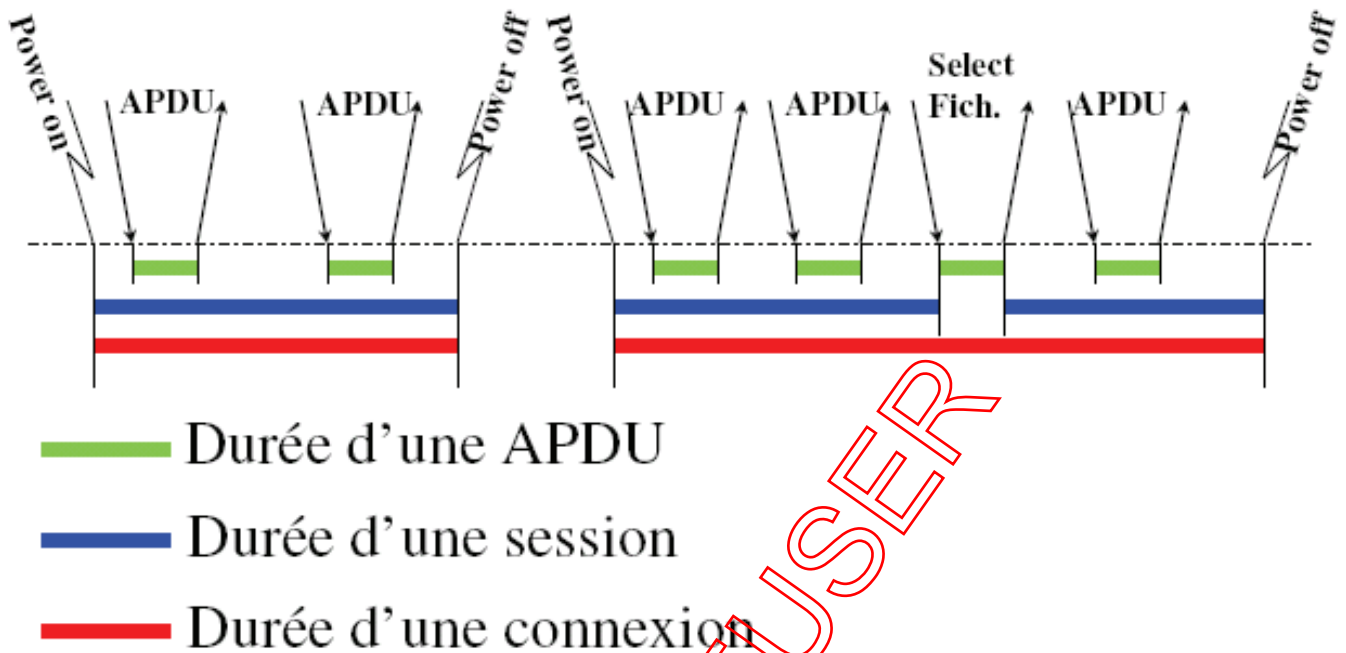
53

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)



Déroulement d'une session



55

ISO 7816-5

Spécifie le système de numérotation et les procédures d'enregistrement des identifiants d'applications (AID pour Application Identifier).

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

Un AID se compose de deux parties :



Ressource Identifier

Proprietary Identifier eXtension

56

ISO 7816-6

Spécifie les éléments de données inter-industrie tels que le nom du porteur de carte, de la date d'expiration, etc.

Etiquette	Longueur	valeur
-----------	----------	--------

Exemple :

Tag	L	Value	Applies to
'80'	2	Number of data bytes in the file, excluding structural information.	Transparent EFs
'81'	2	Number of data bytes in the file, including structural information if any	Any file
'82'	1	File descriptor byte (see table 3)	Any file
'82'	2	File descriptor byte followed by data coding byte (see table 86)	Any file
'82'	3 or 4	File descriptor byte followed by data coding byte and maximum record length.	EFs with record structure
'83'	2	File identifier	Any file
'84'	1 to 16	DF name	DFs
'85'	var.	Proprietary information	Any file
'86'	var.	Security attributes (coding outside the scope of this part of ISO/IEC 7816)	Any file
'87'	2	Identifier of an EF containing an extension of the FCI	Any file
'88' to '9E'		RFU	
'9FXY'		RFU	

57

ISO 7816-7

Propose des commandes inter-industrie pour SCQL.

Create table	Nom de la table: Etudiants
Create view	Nom
Select	Age
Read	faculté
Write	Année
Update	
	Pierre 19 Sciences 1 ère
	Marie 23 Medecine 5 ème
	Alain 21 Droit 3 ème
	Henri 21 Histoire 3 ème
	Jean 20 Economie 2 ème
	Marc 22 Droit 4 ème

58

ISO 7816-8

Concerne la sécurité de l'architecture et des commandes inter-industrie.

59

ISO 7816-9, ISO 7816-10, ...

A vous de chercher !

60

Des normes ... encore des normes !

Norme Europ Telecom Standard Institut:

GSM 11.11 : définition de la carte SIM

TE 9 : spécification de cartes et terminaux

EMV, (cartes de paiement)

ICAO, (agence de l'ONU, biométrie, passeport)

Santé (ISO 21 549)

...

61

Pourquoi utiliser la carte à puce ?

Avantages :

- la sécurité
- la portabilité
- la facilité d'utilisation
- la personnalisation

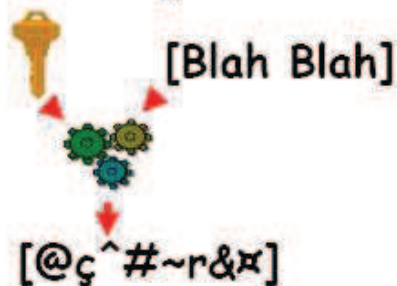
- Tamper resistance
 - Storage



- Portability



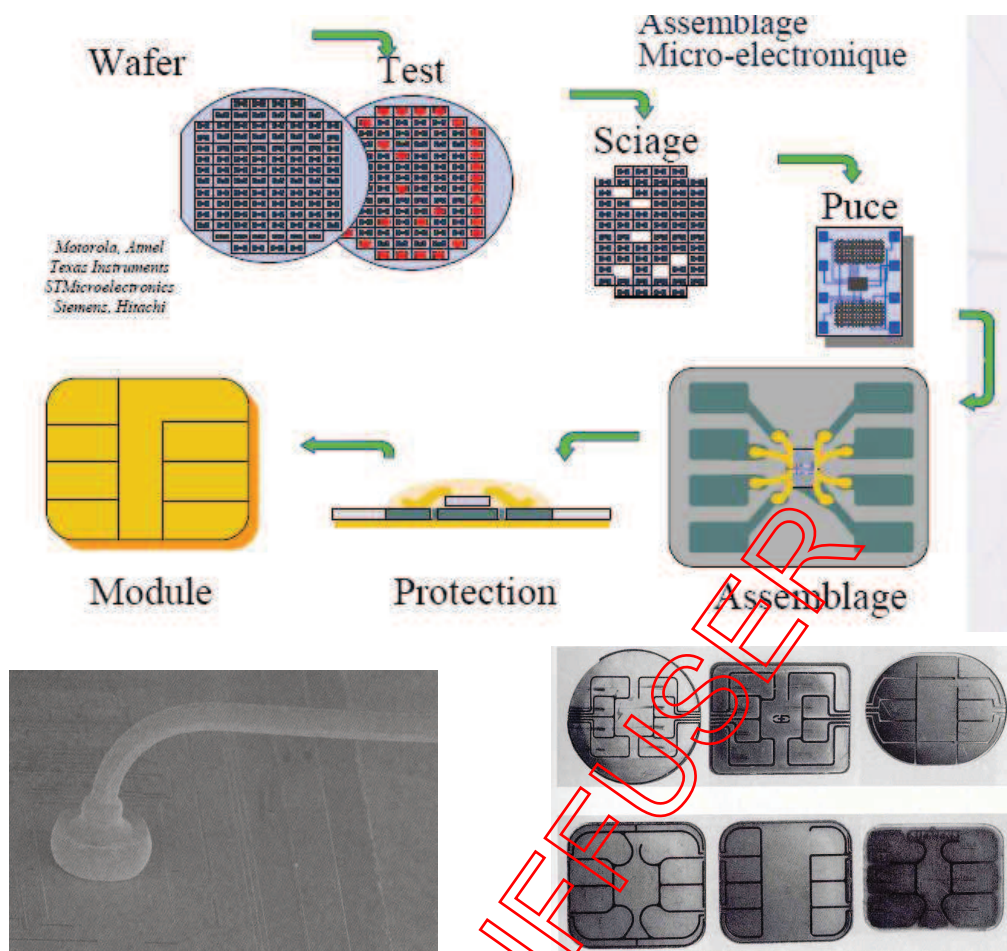
- Tamper resistance
 - Processing



- Ease of use
- Onboard key generation
- Cost

62

Cycle de fabrication



63

Cycle de fabrication



64

Cycle de fabrication

pastille de contact

en réglette



choix et découpe
d'une pastille

wafer



choix et découpe
d'un chip

support

plastique



lamage



Carte assemblée



...

E
N
C
A
R
T
A
G
E

collage du chip
sur la pastille

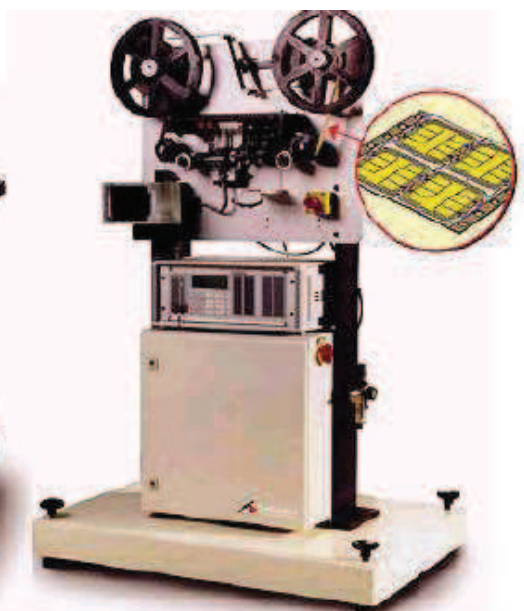
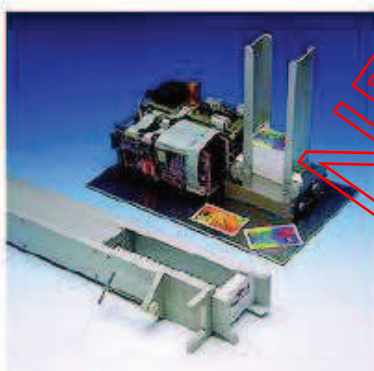


microcablage et
protection du chip

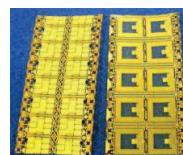
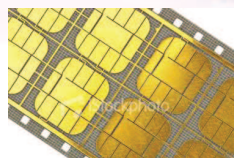
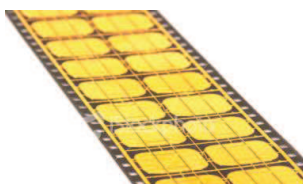


mise en carte

Machine pour la fabrication

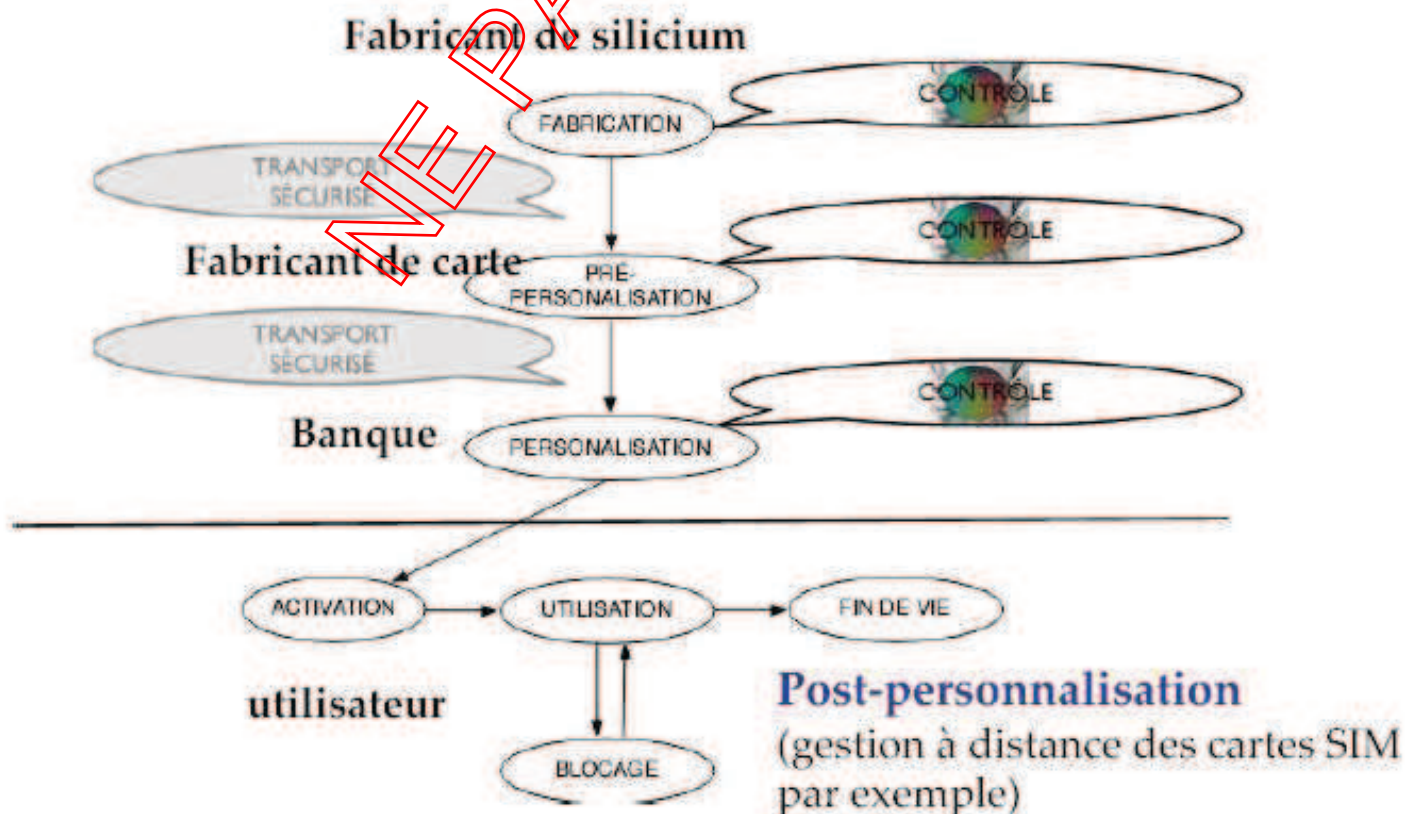


Cartes à Microprocesseur, 1997-2006





Cycle de vie (exemple de la carte bancaire)



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 » + *firmes*
- **Initialisation+personnalisation de la carte**
 - Chargement des fonctions spécifiques de l'application, de l'émetteur, des utilisateurs et du porteur
- **Environnement de l'application**

9

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

Applications

L'industrie des télécommunications

L'industrie bancaire et monétaire (B0', EMV)

Le porte-monnaie électronique (Monéo, Proton, CEPS)

Le secteur de la santé

L'industrie audiovisuelle avec la télévision à péage, ...

Les transports en commun.

Le contrôle d'accès physique de personnes à des locaux, ...

L'identification : à des sites sur l'Internet, ...

Les "e-services"

L'identification gouvernementale (carte d'identité, ...)

Les applications de fidélité



71

La carte à puce aujourd'hui

➤ Aujourd'hui : près de 7 milliards de cartes en circulation

➤ **Monétique :**

- Carte bancaire : Groupement Cartes Bancaires, nouvelles cartes EMV, etc.
- Porte-monnaie : **Octopus**, **Moneo** en France, **Proton** en Belgique, **Geldkarte** en Allemagne

➤ **Identification :**

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

➤ **Éducation** (comme carte d'étudiant et/ou de restauration)

➤ **Téléphonie mobile** (carte **SIM**)

➤ **Secteur médical** (carte **Vitale** en France, carte **SIS** en Belgique).

➤ **Titre de transport** (Passe Navigo à Paris, Oyster à Londres).

➤ **Sécurité informatique** (authentification forte et signature électronique): carte dotée d'un cryptoprocésseur pour la génération des clés et le stockage de la clé privée).

Exemples des Passeports

Depuis 2006 en France :

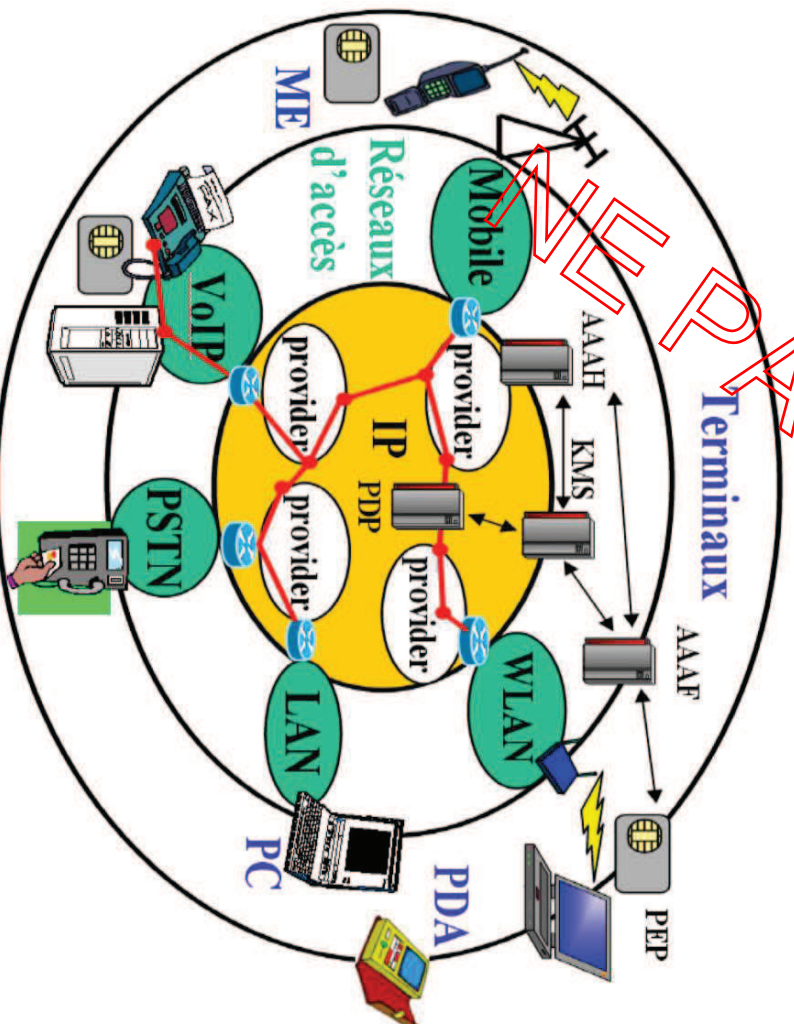
Passeport électronique comporte une puce électronique qui stocke les données personnelles du détenteur : (son nom, sa date de naissance, sa nationalité, son numéro de passeport et la photo numérisée du titulaire).

Depuis le 15 Juin 2009 :

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

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

La carte : omniprésente !

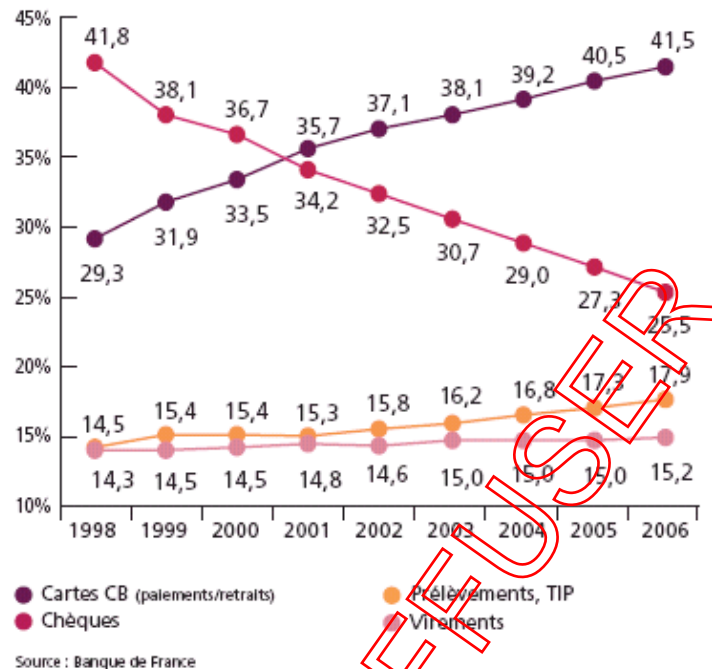


Applications de paiement

Cartes de Crédit : Somme débitée sur le compte du titulaire avec un taux d'intérêt fixé

Cartes de Débit : Compte débité quelques jours après l'achat

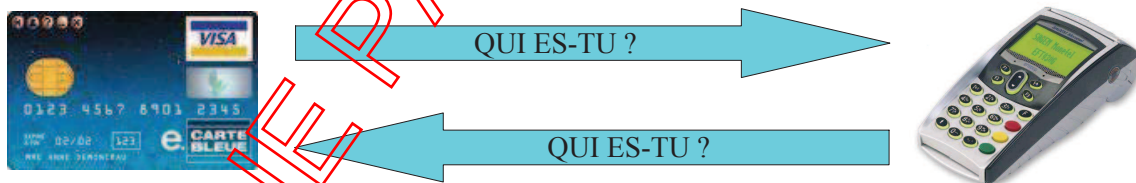
Poids relatif des moyens de paiement en nombre de transactions (%)



75

Applications de paiement : Techniques

Authentification mutuelle carte et terminal commerçant



Signature Électronique



Contrôle du PIN



Contrôle (régulier ou systématique) du solde bancaire (en ligne)

76

Applications de paiement (Exemple : GIE Cartes Bancaires)

53,6 millions de cartes

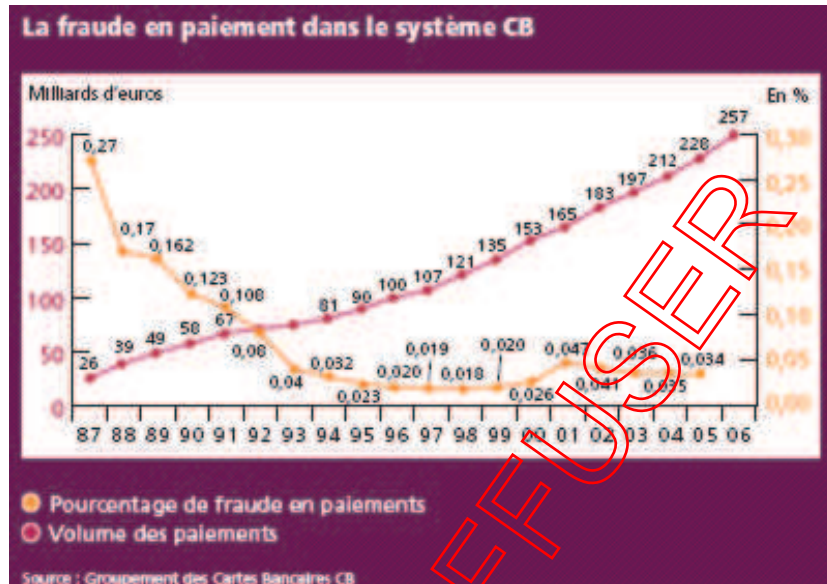
1,2 million de points d'acceptation :

- 950 000 terminaux de paiement dans les commerces
- 140 000 automates de vente
- 50 000 distributeurs de billets
- 75 000 commerçants à distance dont 15 000 sites Internet

1 Distributeur Automatique de Billets pour 1200 habitant en France

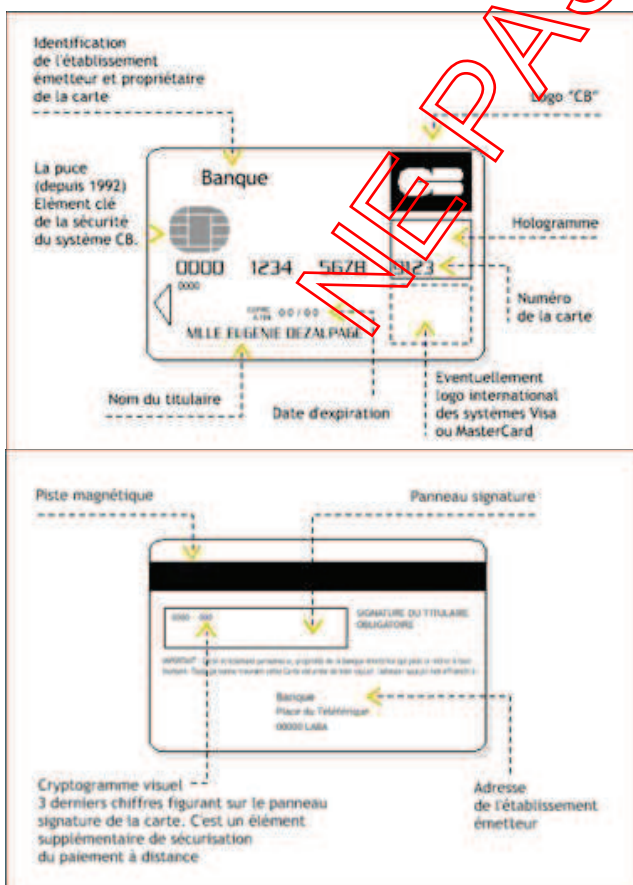
349,5 Mds€ de transactions en 2006 (257,3 Mds€ de paiements et 92,2 Mds€ de retraits)

260 M€ de fraudes du à la piste magnétique contrefaite et utilisée depuis l'étranger (en 2003)



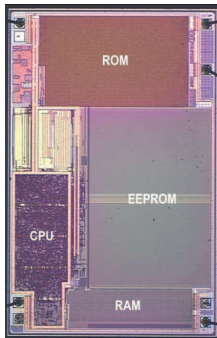
77

La carte bancaire



78

La carte à puce et sa sécurité



La Yescard : une carte « pirate » qui dit OUI à toutes les transactions !
Une remise en cause la sécurité de la carte à puce ?



NON
*Il s'agit d'une mauvaise utilisation de la carte dans un système plus large, ici, le système bancaire
Exemple : Utilisation d'un seul des différents verrous du coffre-fort*

Aujourd'hui on utilise « tous les » verrous et le système est à nouveau sécurisé.

79

Les risques

Sanitaire : à priori aucun !

Financier :

- Sur un chèque ou sur une demande de prélèvement automatique, **la signature apposée prouve l'identité de l'émetteur**
- Dans le cas de l'utilisation d'une carte bancaire, **la preuve est électronique et fournie par le PIN !**
- Dans certains pays qui n'utilisent pas le PIN la puce est interrogée

OU

la piste magnétique de la carte est lue

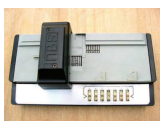
OU

l'empreinte physique de la carte est faite

ET

une signature est demandée sur le reçu émis
SAUF

dans les automates où on ne demande rien !
(voilà une source de fraudes)



- À distance : sur internet ou par téléphone

Le vendeur ne peut fournir aucune preuve irréfutable que l'acheteur est bien qui il prétend être.
Par conséquent si la banque le laisse se servir sur votre compte, il en relève de sa responsabilité.
La loi oblige d'ailleurs les banques à rembourser les sommes prélevées dans le délai d'un mois.

N'ayez plus peur de commander sur l'Internet !

80

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

Royaume Uni: PIN obligatoire depuis le 14/02/2006

81

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

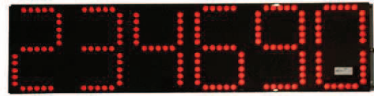
82

Analyse du succès de la télécarte

C'est une carte prépayée.
Elle contient des jetons (et non de l'argent)

Les raisons de sa réussite :

- Fin du vandalisme des cabines téléphoniques
- Temps de communication +50%
- Support publicitaire



83

Le porte-monnaie électronique (e-Purse)

Remplace les pièces et les petites coupures de billets

Carte rechargeable dans des guichets (ou chez le commerçant)

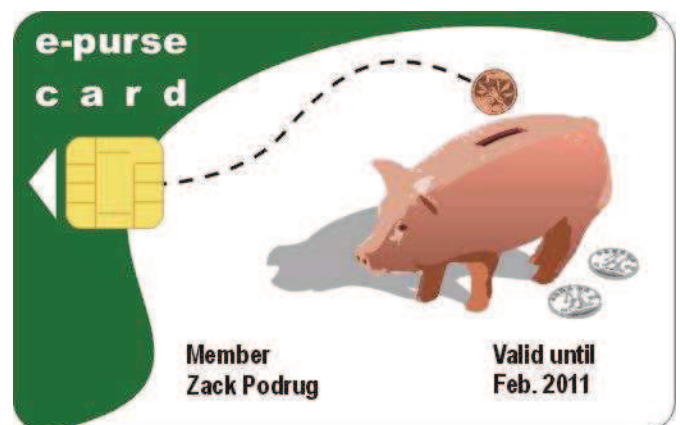
Permet de régler des petites sommes (fraction d'euros à quelques dizaines)

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



84

Le porte-monnaie électronique (e-Purse) : 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 PIN (optionnel)
- État des différentes transactions sur demande



85

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 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)

87

La carte SIM et le GSM

L'abonné est localisé par la carte (le terminal utilisé devient celui du porteur – personnalisation du mobile)

Facturation directe de l'abonné

Sécurité pour l'accès au réseau téléphonique : physique (carte) + logique (PIN)

Stockage de données personnelles (agenda)

1,22 milliards de cartes SIM livrés en 2005

Bientôt, le paiement ?



88

Applications Actuelles des Cartes

- Différents secteurs porteurs
 - Les Télécommunications : Cartes Pré-payées, carte SIM
 - Recherche tj + de services, $\forall$ 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

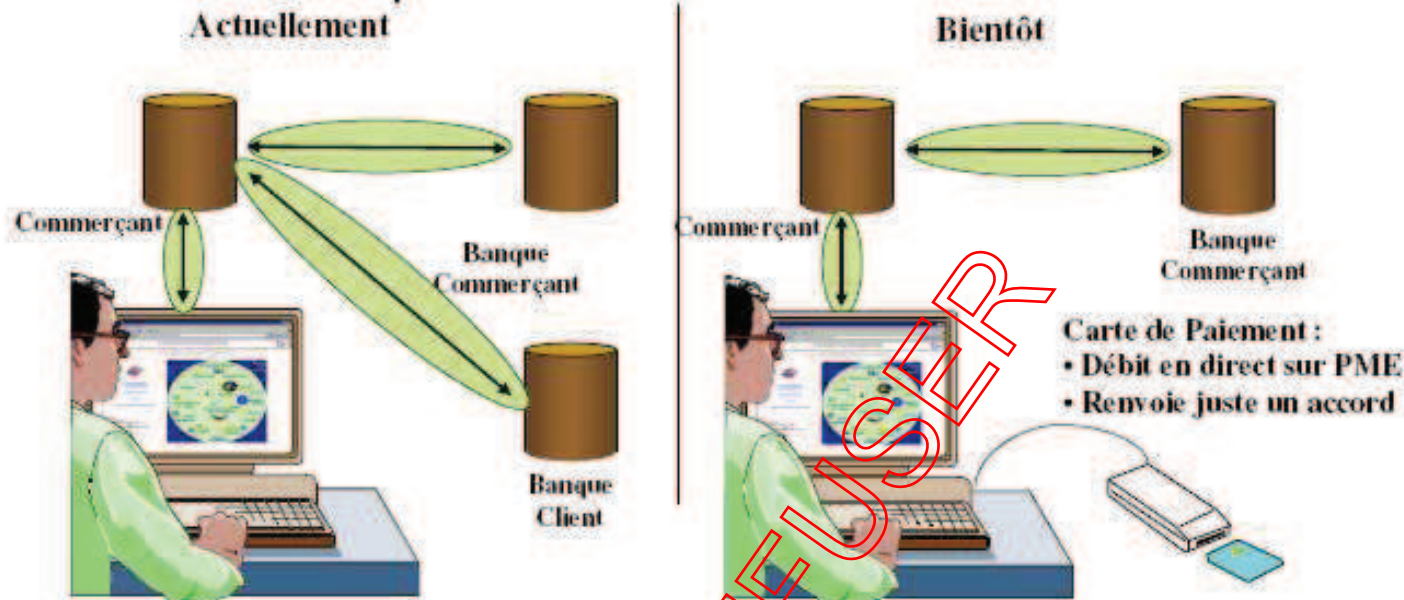
89

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

Futures Applications

• La carte et les paiements distribués



91

Quelques acteurs

Fondeur: Atmel, Infineon, Philips, Samsung, ST Microelectronics,

Encateur: Axalto, Gemplus, Giesecke & Devrient, Oberthur Card Systems, Orga

Bancaire: Carte Bancaire, Carte Bleue, EMV, MasterCard, Monéo, VISA

Téléphonie: Bouygues Télécom, France Telecom, Orange, SFR, Vodafone

TV: Canal+, CanalSat, TPS

Santé: Sécurité sociale

Evaluation/Certification: AQL, CEACI, CEA Leti, SERMA Technologies, SGDN -- DCSSI

Laboratoire: LaBRI, XLIM, INRIA, CNRS, CNAM, ...

92

Les Acteurs (2006)

- Bull CP8 (racheté par Schlumberger)
- Schlumberger
- Axalto (filiale mise sur le marché par Schlumberger) (#2)
- Gemplus (#1)
- Gemalto (Mariage Gemplus+Axalto) 7 Décembre 2005
 - 1,8 G€ de CA, 11000 employés, ~50 pays, 22 usines
 - 55% du marché mondial des cartes SIM avec plus de 600 millions de cartes livrées sur un total estimé de 1,22 milliards de SIM pour 2005. La nouvelle entité sera aussi un poids lourd sur le marché des services financiers et sur celui des lecteurs. Elle ne devrait toutefois contrôler "que" 16% du marché des cartes de sécurité
- Oberthur Card Systems
- Delarue
- Giesecke & Devrient (#3)
- Sagem Orga (#4)
 - 1,800 employés
- ...

NE PAS DIFFUSER

La carte à puce

—
Sa sécurité

La sécurité physique

techniques d'impression sophistiquées

- différentes couches d'impression
- hologramme
- Embossage

procédés d'encollage

matériaux plastiques

design du micro-contact

95

La sécurité hardware

Le micromodule est monolithique => difficile de distinguer ses différents composants

un numéro de série unique

l'utilisation de mémoire de type PROM

blindage physique du composant (grille, grille active, ...)

des détecteurs de conditions anormales (tension, fréquence, température, lumière, ...)

brouillage des informations dans le composant (mémoire, bus, ...)

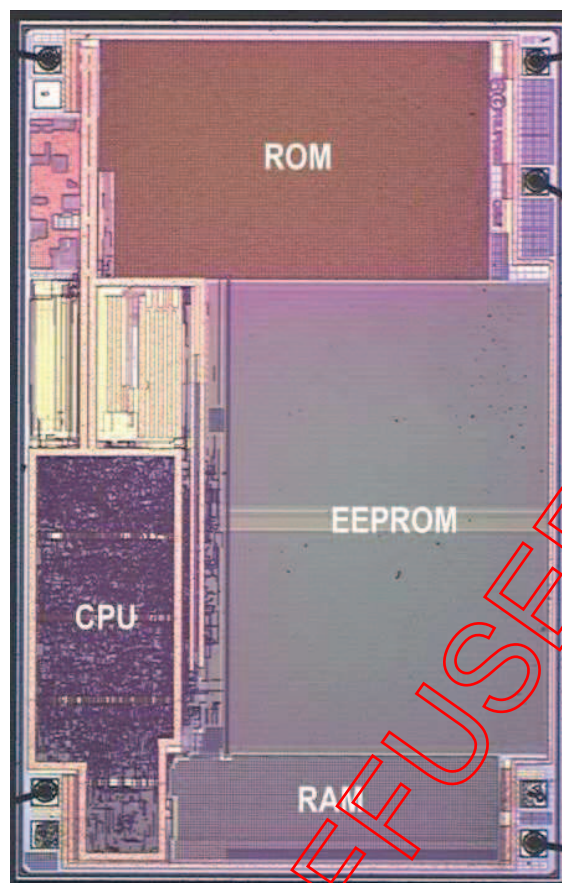
co-processeurs cryptographiques

pompe de charge pour le lissage de la consommation

Dual logic, circuit asynchrone

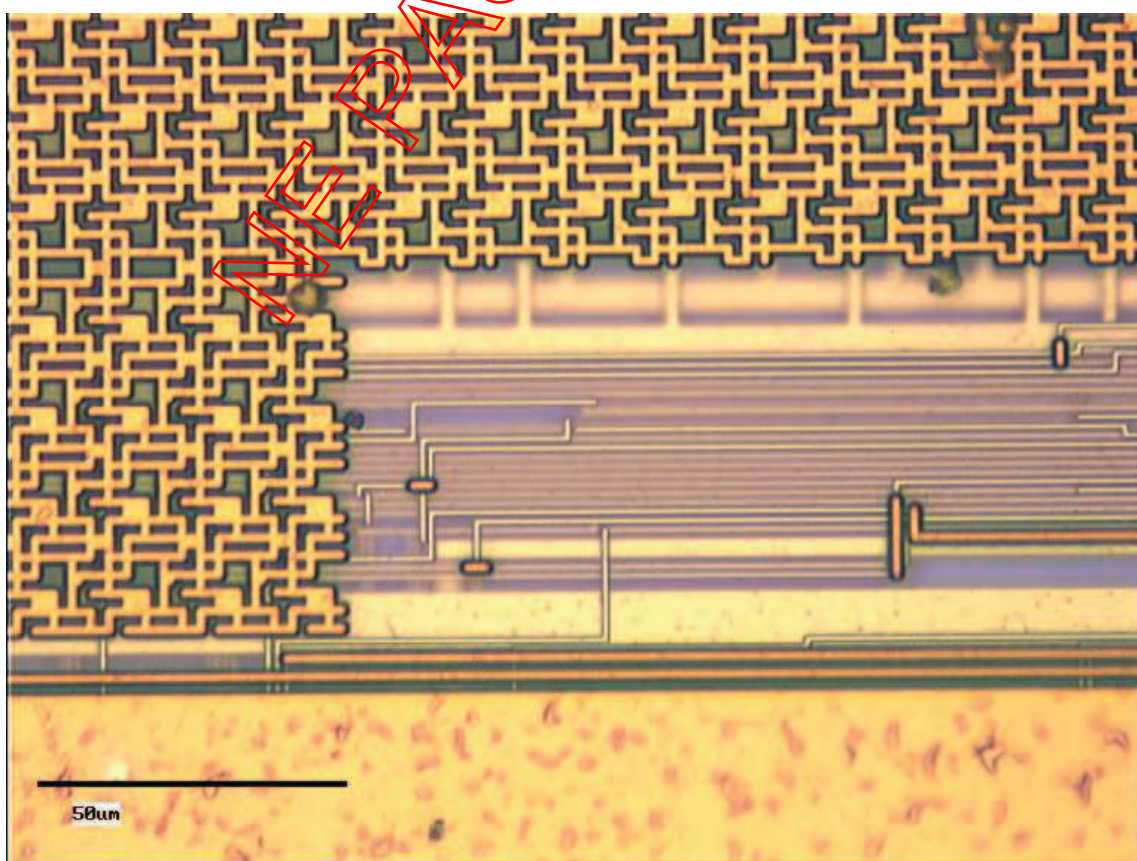
96

Une puce



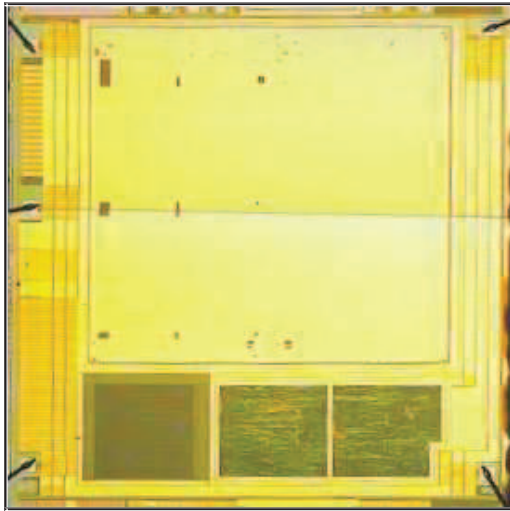
97

La grille de protection

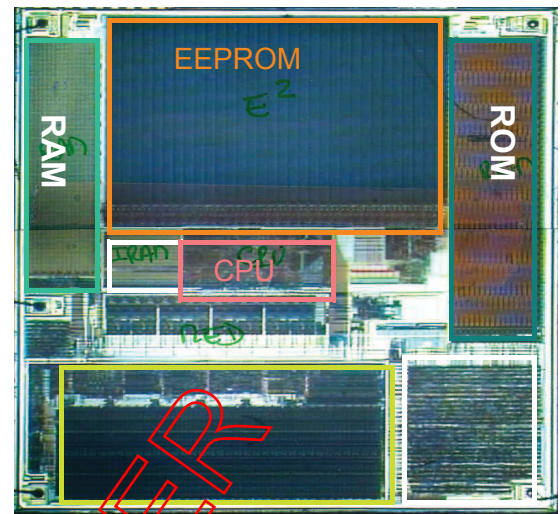


98

LESSON LEARNED: SHIELD IT!

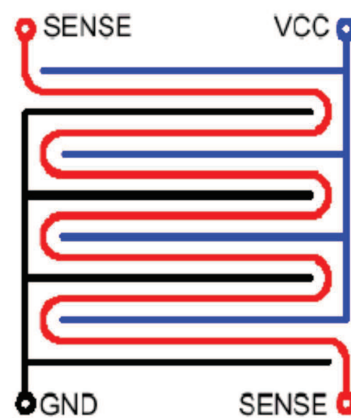
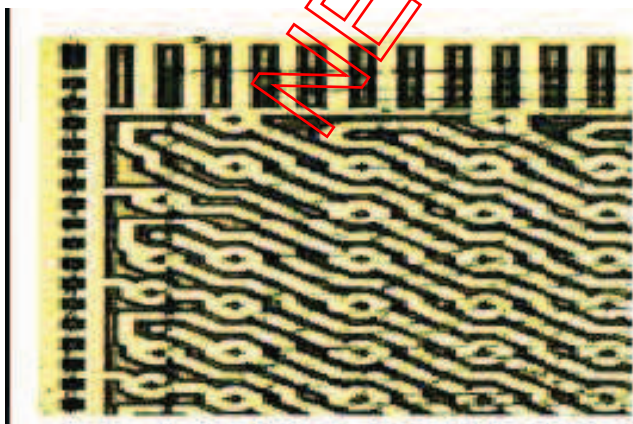


- Shield
- Scrambled glue logic
- No Buses visible

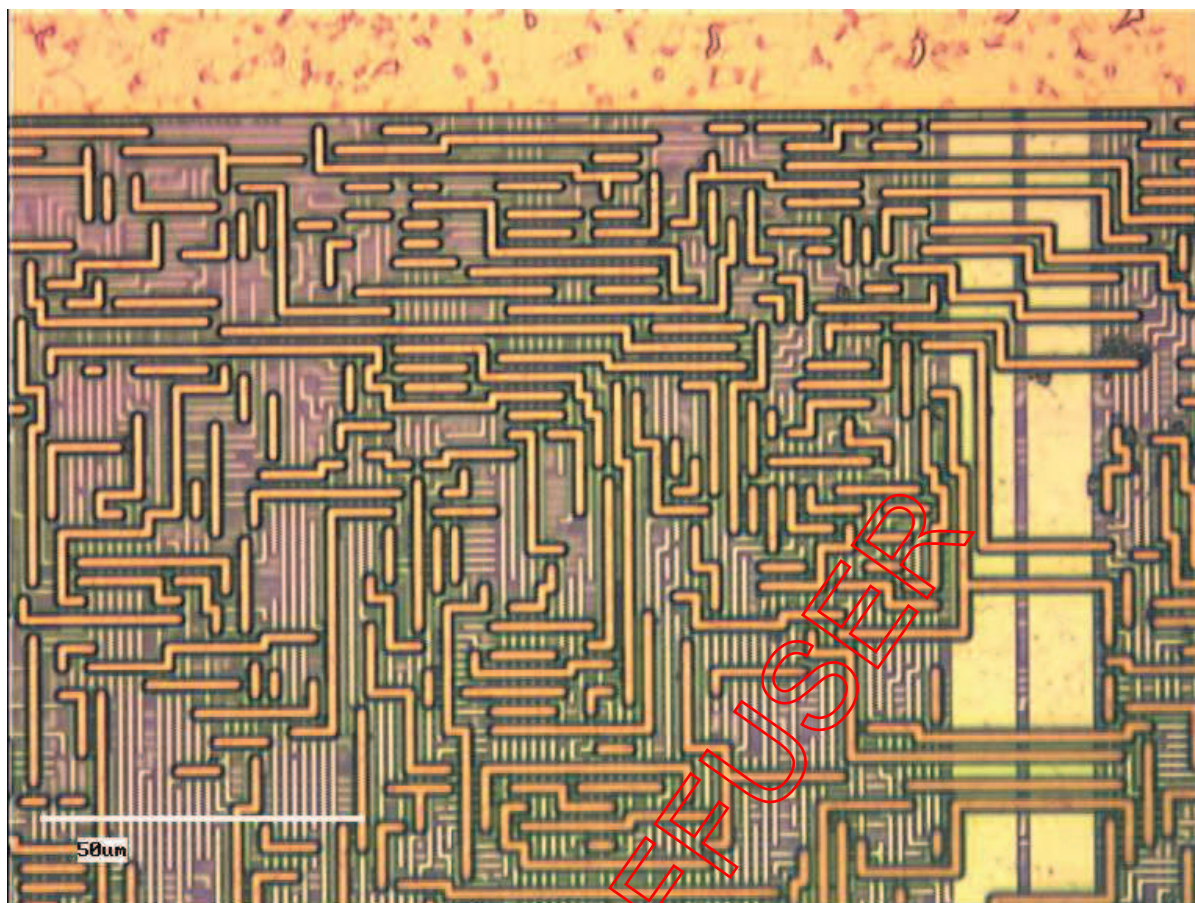


- Blocks easily identified
- No shield
- No glue logic
- Buses clearly visible

Grille active

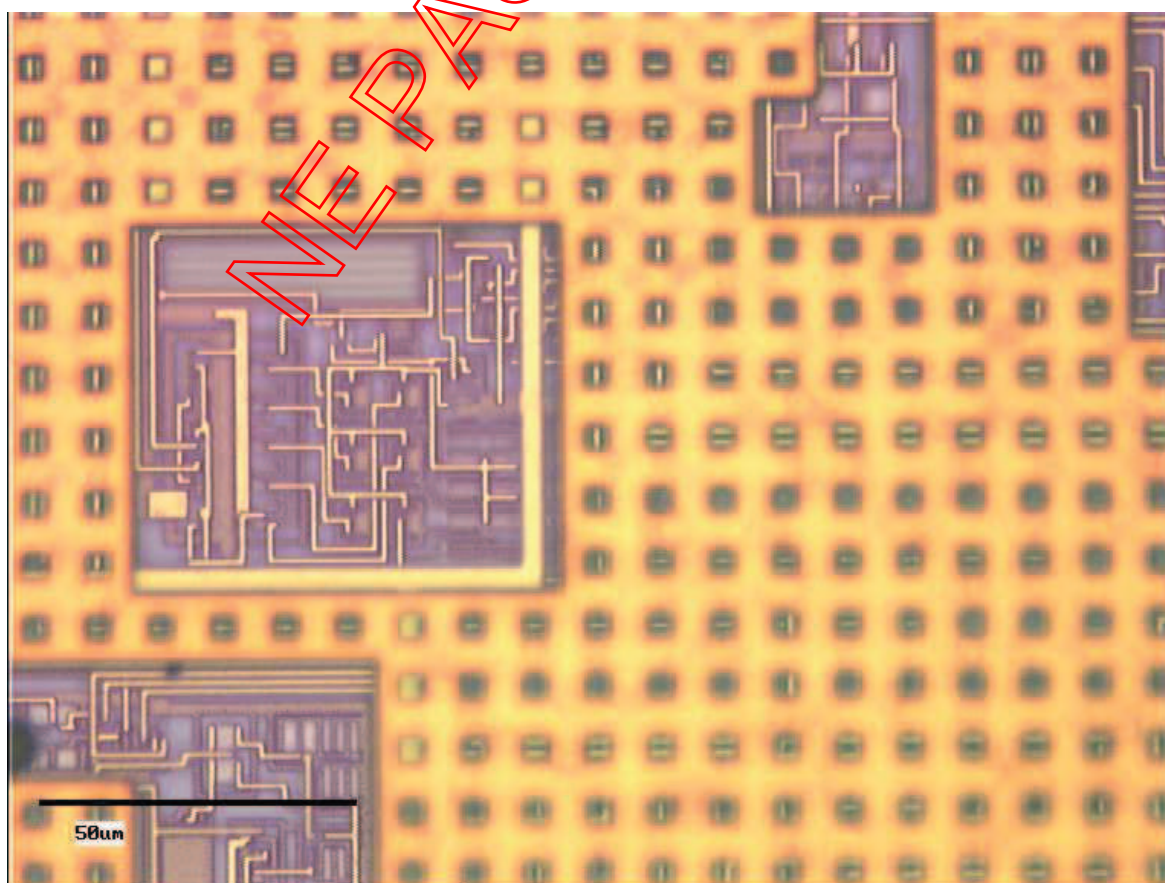


Le CPU



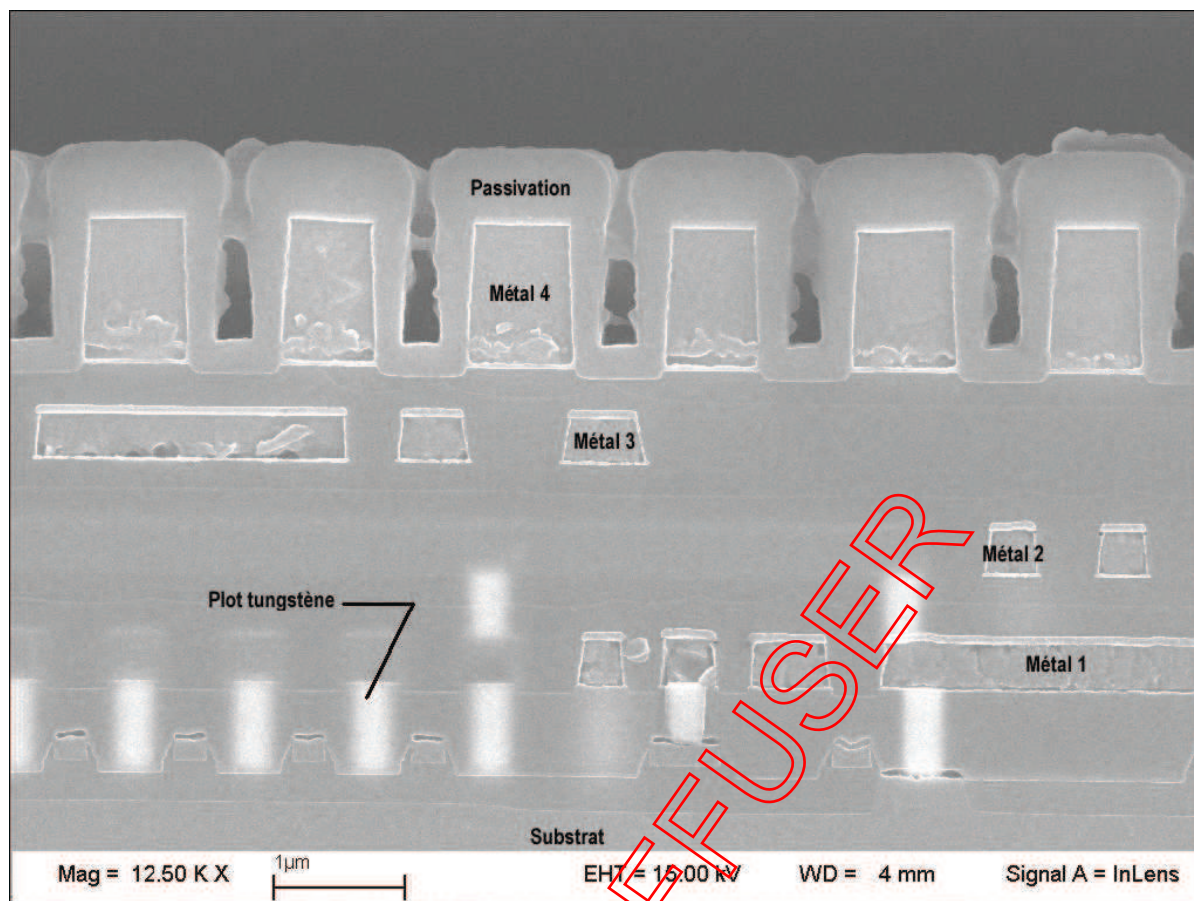
101

La partie analogique



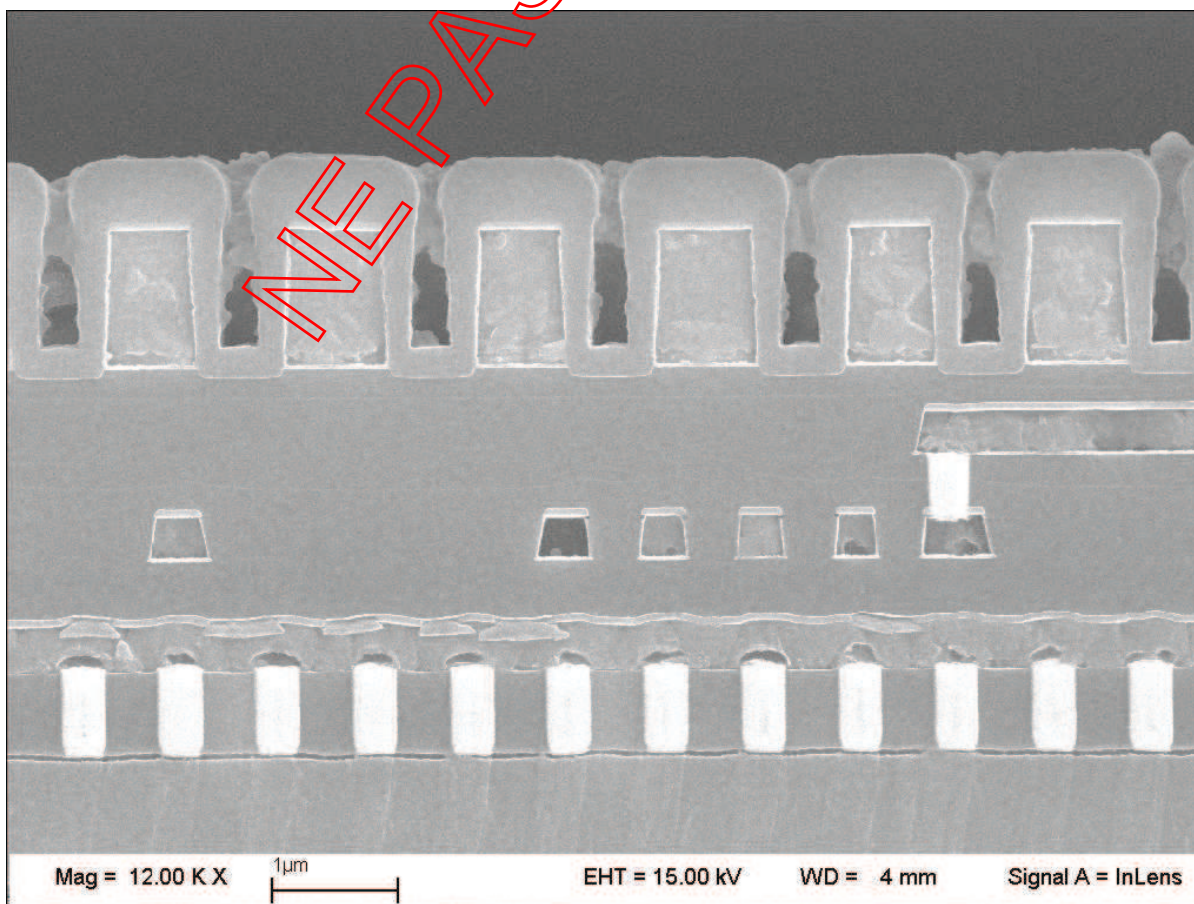
102

La coupe d'une puce



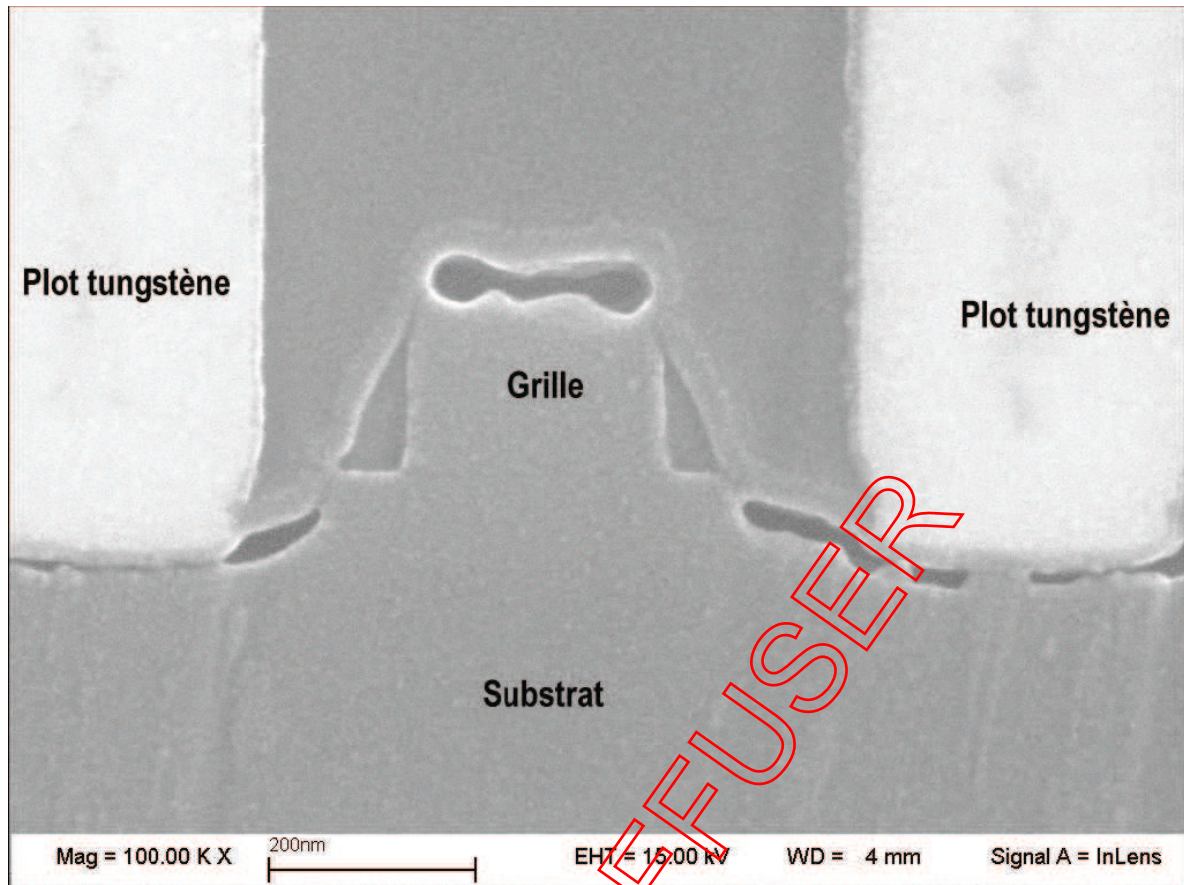
103

La coupe d'une puce



104

La coupe d'un transistor



105

La sécurité software

contrôles d'accès aux données

maintien de l'intégrité des données

entrées/sorties sécurisées

migration du code

106

La sécurité de l'env. de production

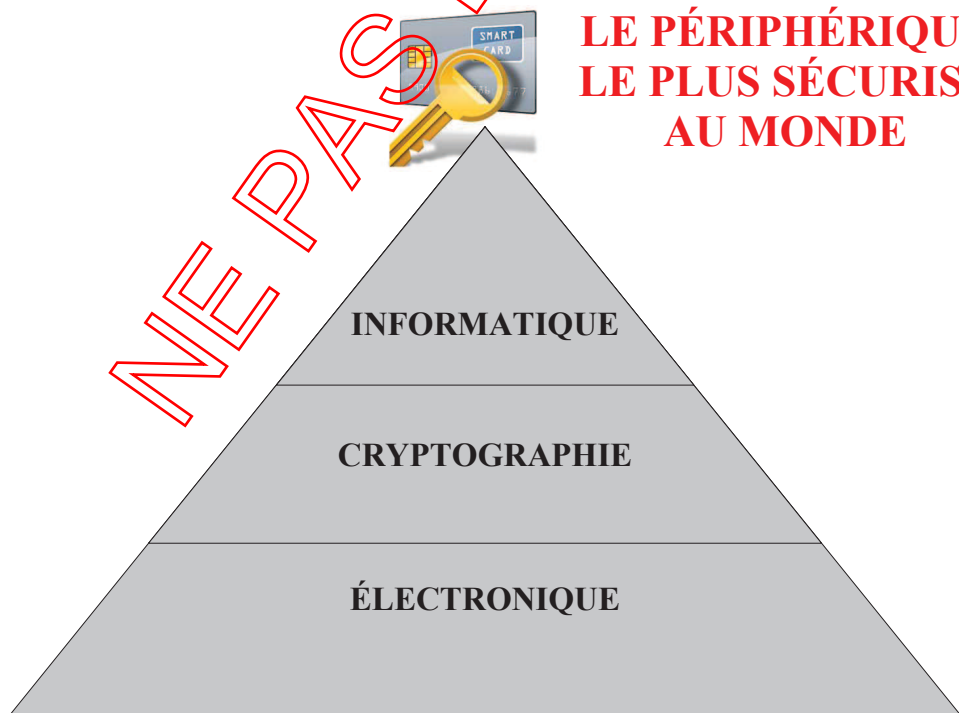
physiquement sécurisé

régulièrement audité

107

La sécurité

Pour résumer :



*La haut niveau de sécurité est assuré
par la triple alliance de l'électronique,
de l'informatique et de la cryptographie*

108

Les méthodes formelles et le test

Conception formelle de certains parties de l'OS (voire de l'OS complet)

Preuve formelle sur des aspects sécuritaire

Génération de jeux de tests associés aux spécifications

...

109

L'évaluation sécuritaire et la certification

La certification

Objectifs :

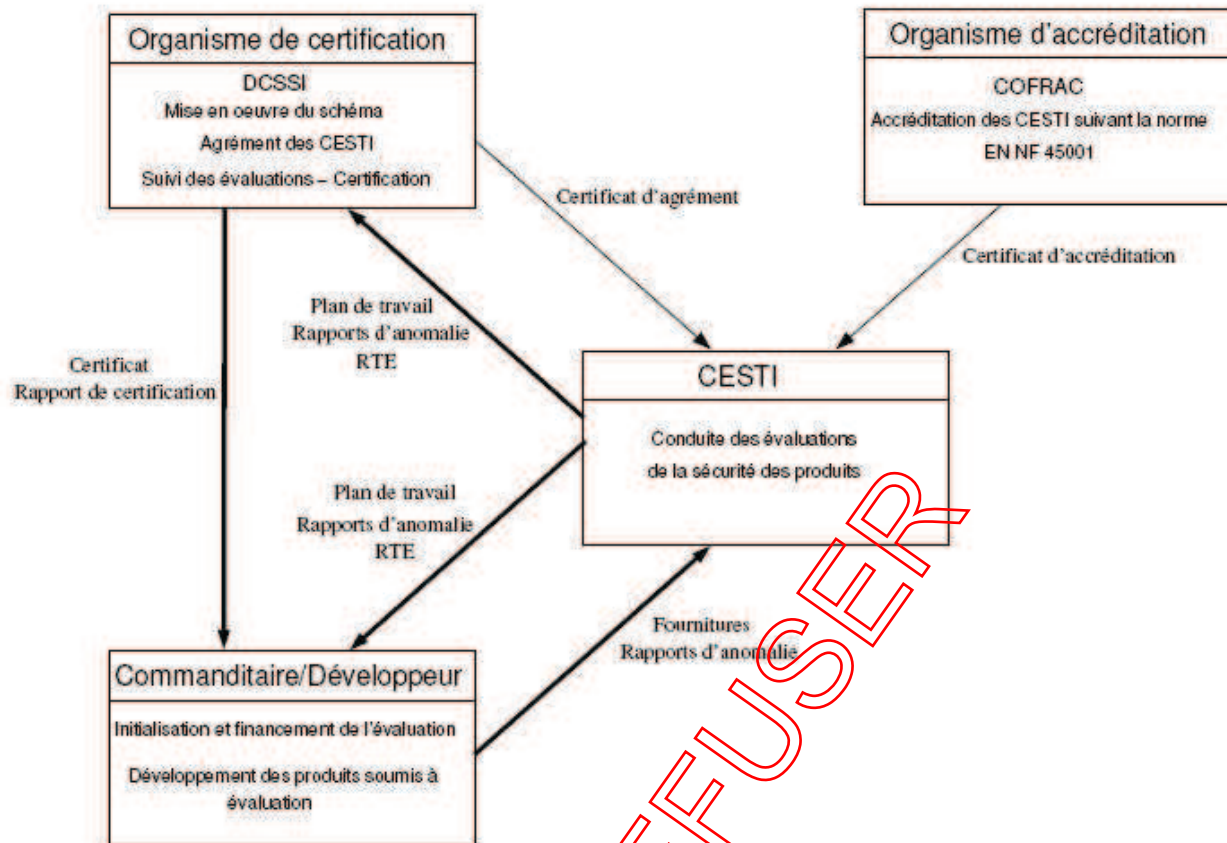
- Garantir le niveau de sécurité d'un produit TI (confidentialité, intégrité, disponibilité).
- Bénéficier des accords de reconnaissance mutuelle.

Avantages pour :

- les utilisateurs : comparer sur une base objectif ;
- les industriels : prouver leur compétence et d'étendre leurs marchés ;
- les autorités d'homologation : s'assurer que les objectifs de sécurité sont satisfaits et que leur pays ne court pas de risque majeur à utiliser des produits TI !

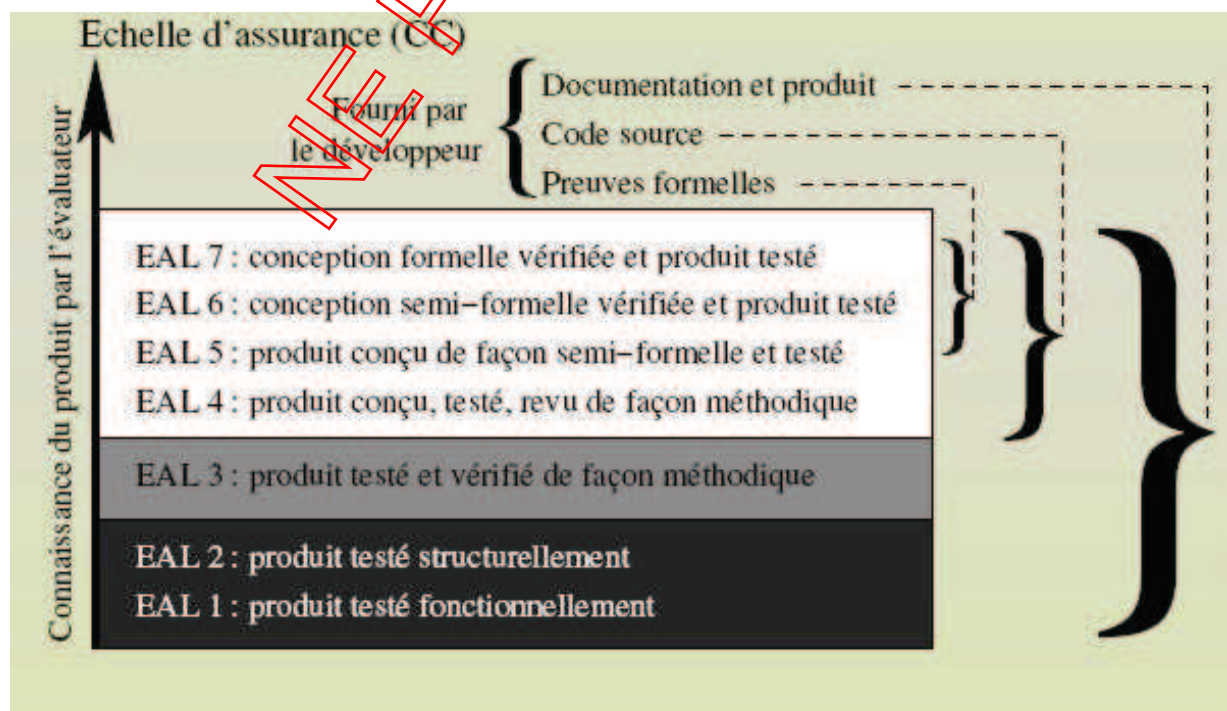
110

Le schéma Français



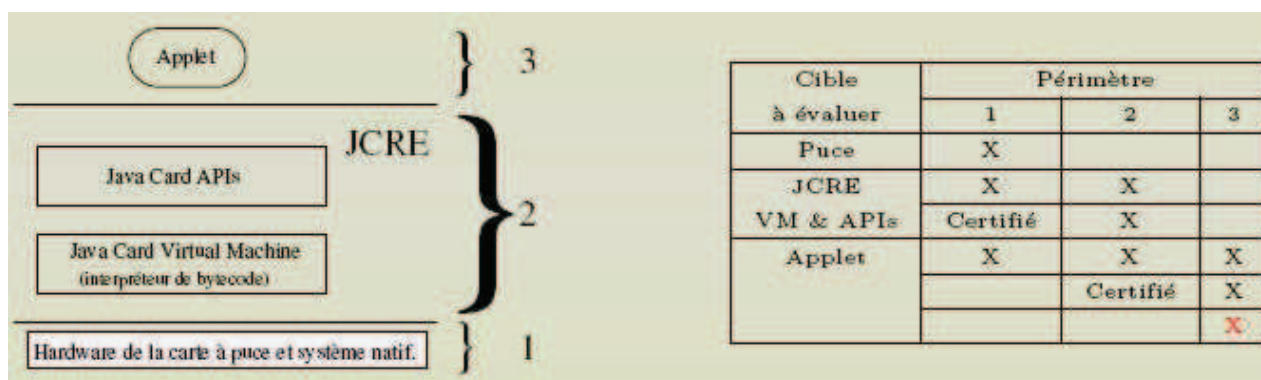
1

L'échelle d'assurance



Le périmètre d'évaluation

Défini dans la cible de sécurité dans la description de la cible d'évaluation.



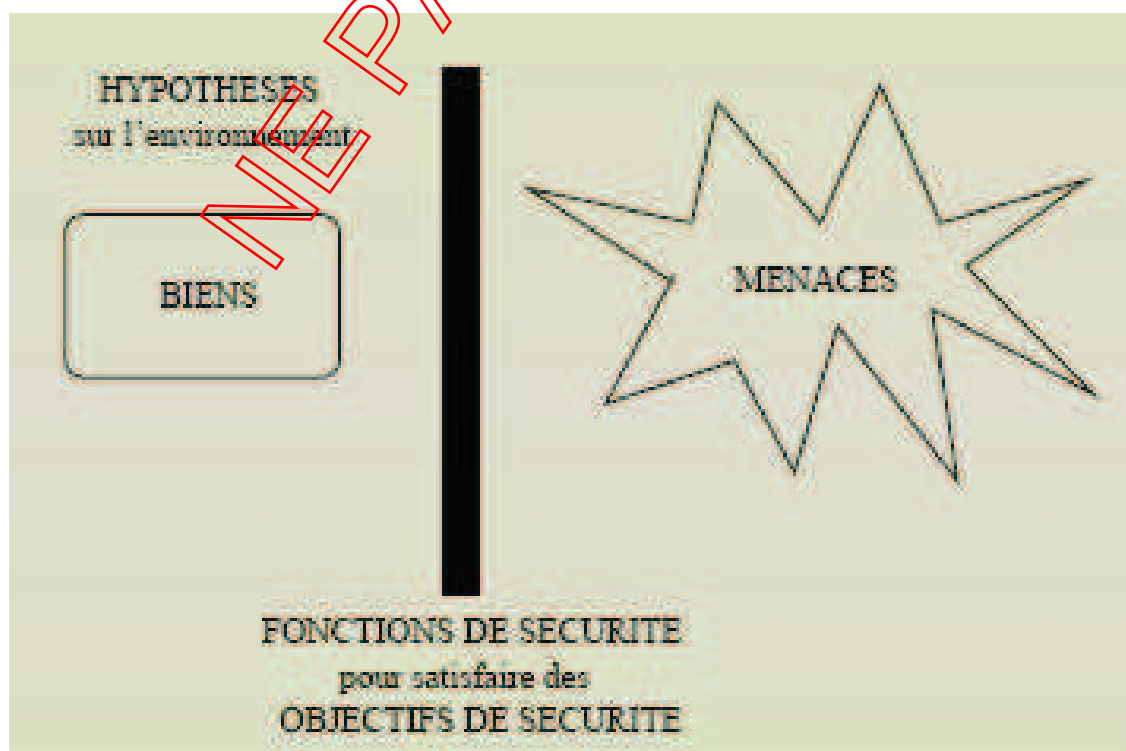
Nouveaux problèmes apportés par les applets Java Card :

- pas de définition précise du périmètre d'évaluation ;
- pas de méthodologie d'évaluation d'une applet ;
- la multi-application.

113

Les bases des critères communs

Critères Communs (ISO15408)



114

La carte à puce

Les attaques

115

Différentes catégories

Non invasives

Le produit reste fonctionnel

Invasives

Le produit est partiellement endommagé

116

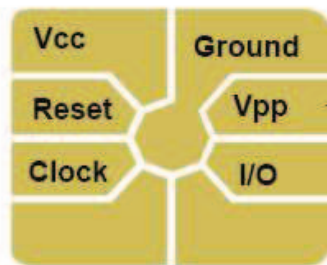
Non invasives

modification des conditions opérationnelles (Vcc, F)

modification de la température

modification des rayonnements lumineux (UV, rayon X, lumière blanche, IR, ...)

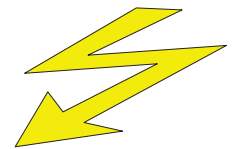
injection de fautes (glitches, rayonnements lumineux)



- Attack on VPP
- Using nail polish
- Card not debited...

(injection de fautes sur la JVM : <http://www.cs.princeton.edu/~sudhakar/papers/>)

attaques sur les canaux cachés



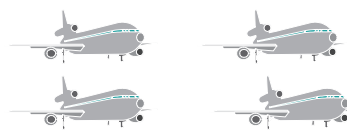
117

ARE WE DONE?

Broken toys are not charged to our clients



car = \$3



plane = \$5

Jack

How will you pay?

I'll send \$15
by postal order

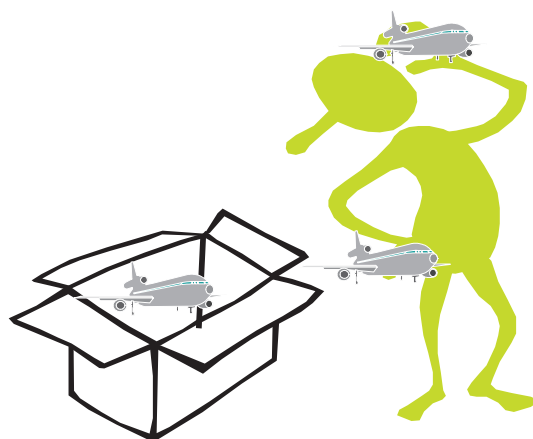
Dino

Dino buys toys from Jack

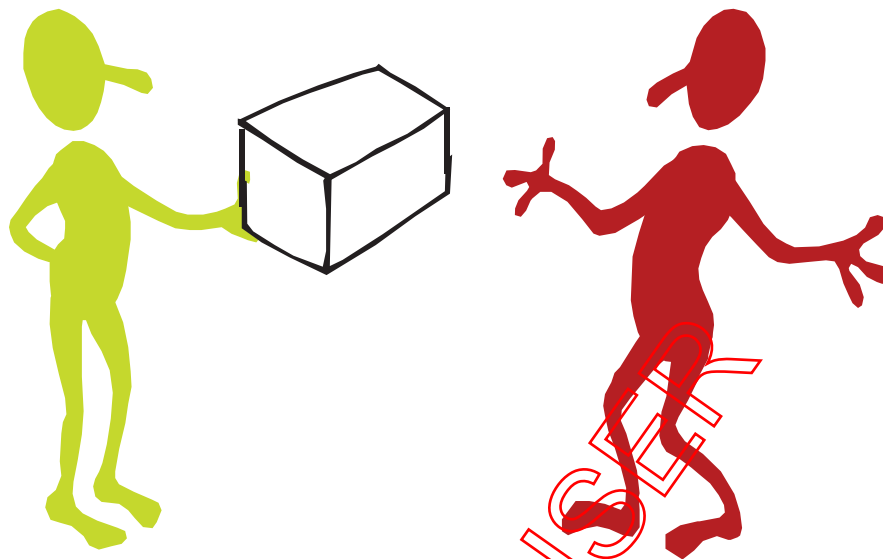
*The postman wants to know what
Dino bought for \$15*



*In the meanwhile Jack prepares
the DHL*



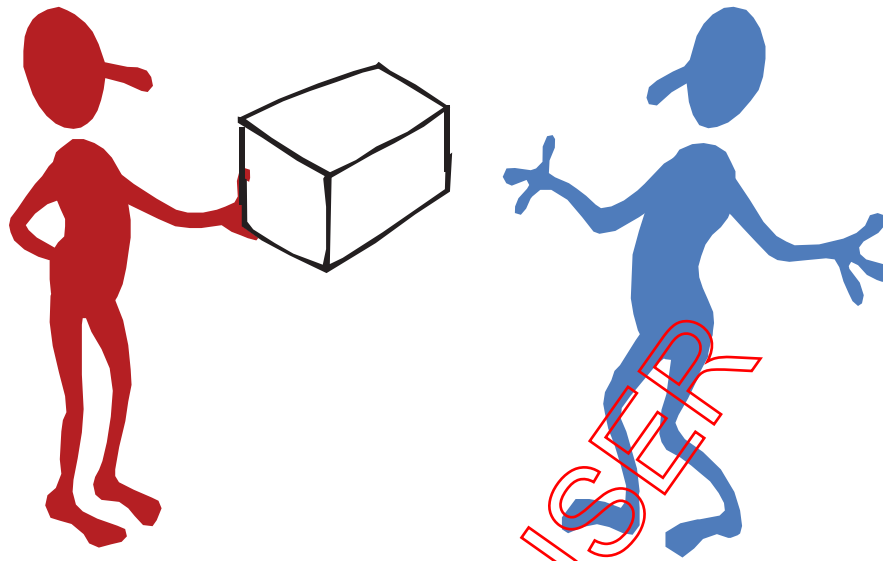
and gives it to the postman



*Who kicks it strong enough to
break one toy*



and gives it to Dino



*a week later he monitors Dino's
postal order...*

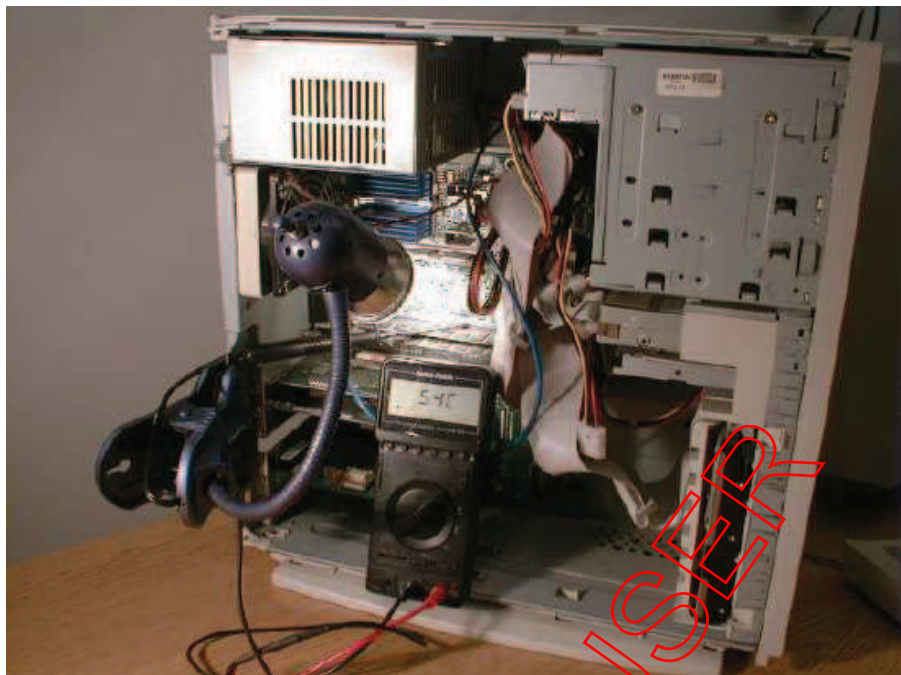


Lesson learned: **Fault attacks** can also extract secrets from tokens!

Hardware faults can have various sources:
voltage glitches, light beams, laser beams...

Attaques software/hardware

Pour forger des pointeurs et ensuite ...



<http://www.cs.princeton.edu/~sudhakar/papers/memerr-slashdot-commentary.html>

125

Les dernières news

Des détecteurs lasers embarqués sur les puces récentes !
(voir thèse d'Alexandre SARAFIANOS)

126

Les canaux cachés

le temps d'exécution

=> nombre de cycle d'une instruction ou d'un algorithme.

la consommation de courant

=> Les modifications rapides de la tension et de l'intensité du courant au sein du même composant sont à la base des émissions du circuit car ils conduisent des courants RF à l'intérieur et à l'extérieur du chip.

les émissions électromagnétiques

=> Les courants RF entraînent un rayonnement électromagnétique.

127

Le matériel

un oscilloscope numérique,

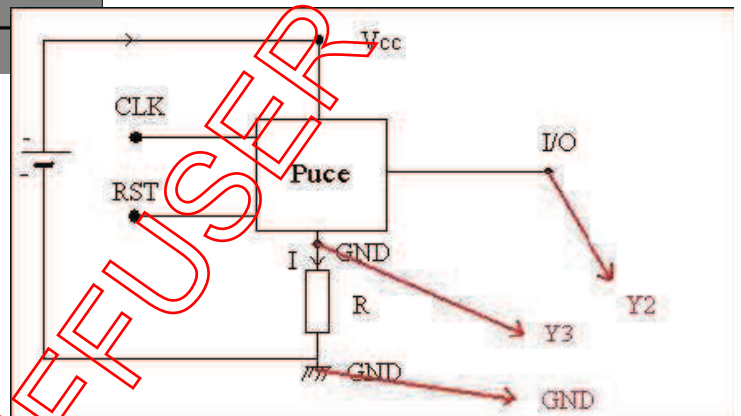
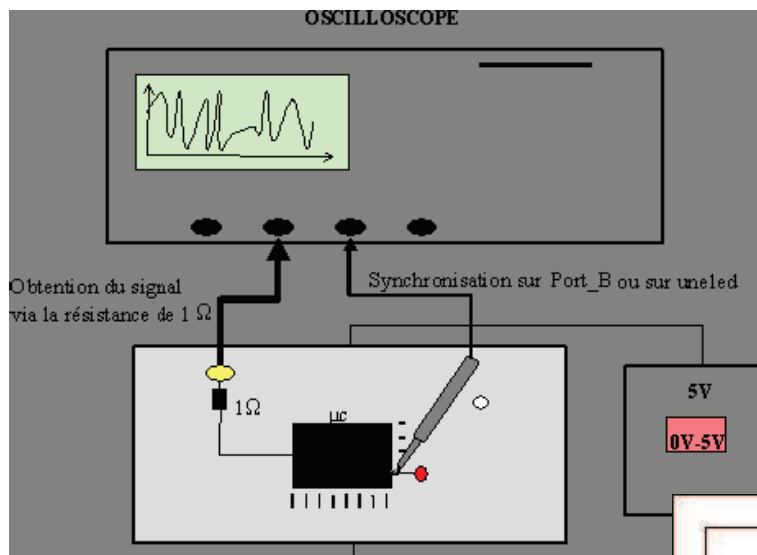
un lecteur de carte à puce,

un pc équipé de cartes d'acquisition et de logiciels mathématique pour le traitement des données,

une sonde CEM si on veut étudier les émissions électromagnétiques.



Le montage pour suivre la consommation en courant



La “timing attack”

Cette attaque consiste à mesurer le temps d'exécution d'un algorithme.

=> Révèle des informations sur les opérations et/ou les opérandes.

Nécessite souvent :

- un grand nombre d'exécution à messages choisis,
- un traitement statistique des résultats obtenus.

Exemple:

A GAME

- You put \$28 in one of the pots and \$10 in the other:



- I ask you to multiply the contents of the blue pot by 10 and the contents of the red pot by 7, add the two results and tell me if the sum is odd or even.
- Is your answer enough to reveal what's in each pot?

IS THIS A MEANINGFUL GAME?

- Well, normally not :

$$28 \times 7 + 10 \times 10 = 296$$

is an even number

and

$$10 \times 7 + 28 \times 10 = 350$$

is also even...

- However, just by monitoring the time it takes to give the answer (the mental calculation leading to 296 is more complicated than the one leading to 350) one can tell where each amount is!

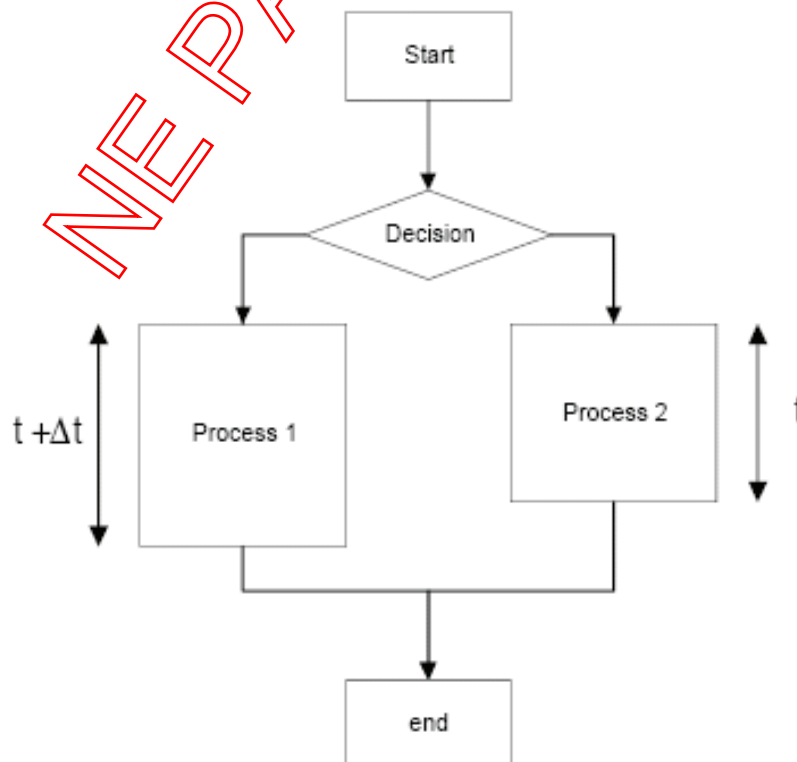
CONCLUSION

The external monitoring of the processing time of a card may leak secrets to the external world (e.g. credit keys, PINs etc).

Timing attacks were exposed in the early 1990's.

Lesson learned: **Current card software runs in constant time**

La “timing attack”



La “timing attack” sur le PIN (1/2)

```
for ( i = 0 ; i <= 7; i++)  
    if ( pinCarte [ i ] != pinPresente [ i ] )  
        return false ;  
return true ;
```

Présentons un PIN quelconque et déroulons le programme :

```
cas du premier octet FAUX  
i = 0  
i <= 7 ? NON  
( pinCarte [ i ] != pinPresente [ i ] ) ? OUI  
return false
```

```
cas du premier octet VRAI  
i = 0  
i <= 7 ? NON  
( pinCarte [ i ] != pinPresente [ i ] ) ? NON  
i++  
i <= 7 ? NON  
( pinCarte [ i ] != pinPresente [ i ] ) ? OUI  
return false
```

135

La “timing attack” sur le PIN (2/2)

```
for ( i = 0 ; i <= 7; i++)  
    if ( pinCarte [ i ] != pinPresente [ i ] )  
        return false ;  
return true
```

Présenter les n valeurs possibles de pinPresente[0] (256 valeurs) (n,0,0,0,0,0,0,0).

Mesurer la durée d'exécution de la commande T pour les n valeurs.

Calculer T[n0] le maximum des T

– $T[n0] = \max(T[n]); n = 0; \dots; 255$

n0 est la solution pour pinCarte[0]

Itérer sur tous les pinPresente[i]

Nombre d'essais : $8 * 256 = 2048$ (contre 256^8 en force brute)

136

Exemples de protection (1/2)

```
alea = random ( 0 , 7 ) ; // alea situe dans l'intervalle [0 ; 7]
for ( i = 0 ; i <= 7; i++ ) {
    octet = ( alea + i ) mod 8 ;
    if ( pinCarte [ octet ] != pinPresente [ octet ] )
        return false ;
}
return true ;
```

Nombre d'essais en moyenne : $8 * 2048$ (contre 256^8 en force brute)
Possibilité d'attaque de type MasterMind.

137

Exemples de protection (2/2)

```
boolean test = true ;
for ( i = 0 ; i <= 7; i++ ) {
    test = test ;
    if ( pinCarte [ i ] != pinPresente [ i ] )
        test = test && false ;
    else
        test = test && true ;
}
return test ;
```

équivalent à :

```
boolean test = true ;
for ( i = 0 ; i <= 7; i++ )
    test = ( pinCarte [ i ] == pinPresente [ i ] ) && test ;
return test ;

Et pas test = test && ( pinCarte [ i ] == pinPresente [ i ] );
```

138

La consommation de courant

Elle est surtout utilisée dans le domaine de la cryptographie.

Il existe différentes attaques :

la SPA (Simple Power Analysis)

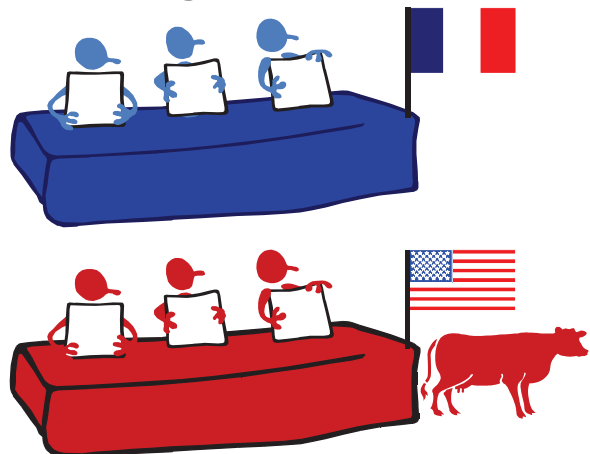
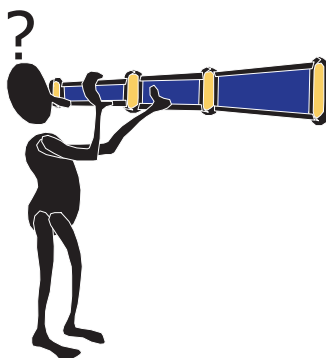
la DPA (Differential Power Analysis)

la HODPA (High Order Differential Power Analysis)

139

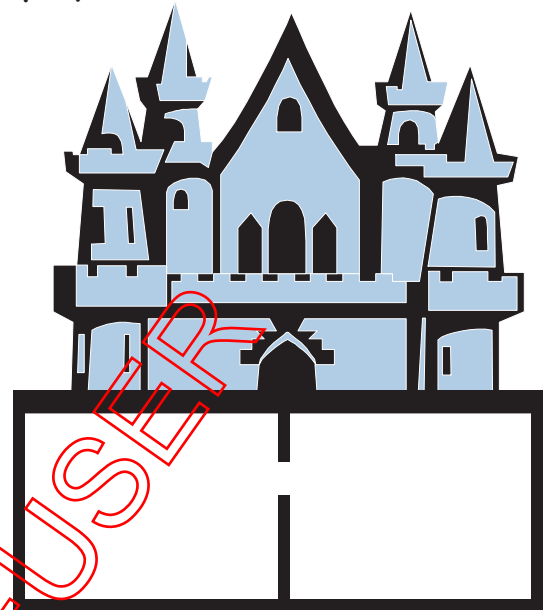
IMPORTING THE BEEF?

- Seattle, 1999.
- US and French delegates negotiate under which conditions beef could be imported to France.
- «The Sun» sends a journalist to investigate:



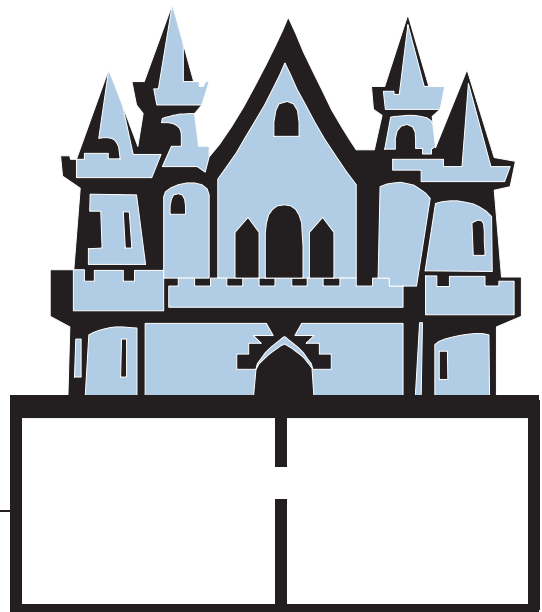
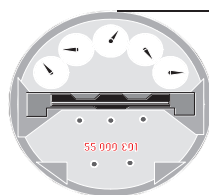
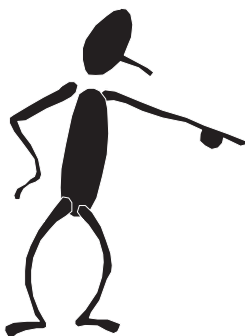
IMPORTING THE BEEF?

- But there is a technical problem: negotiations take place in a hotel which windows are opaque



POWER ATTACKS

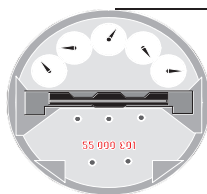
- Idea: look at the hotel's electricity meter!



POWER ATTACKS

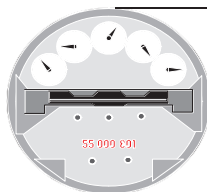
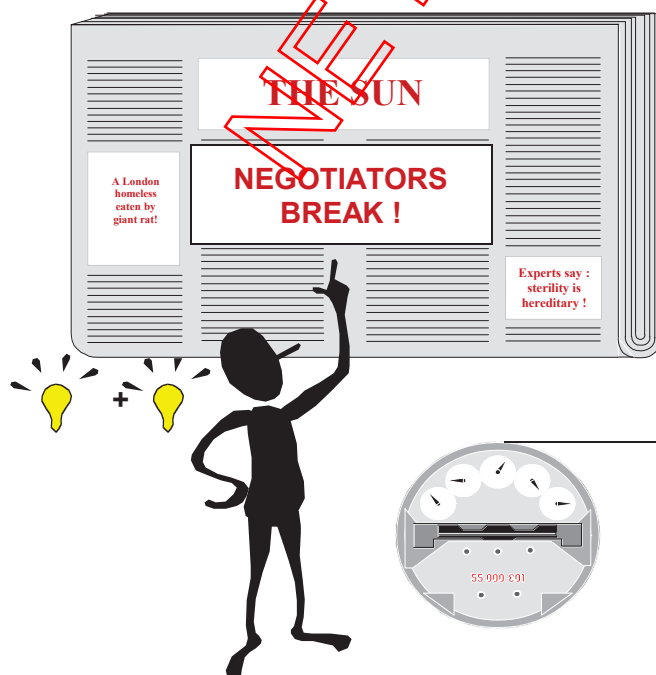
- disk is spinning slowly:

DEAL CONCLUDED



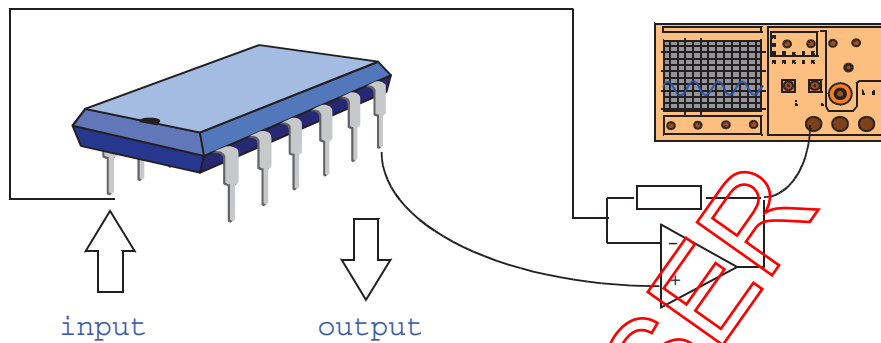
POWER ATTACKS

- But if the disk is spinning quickly:



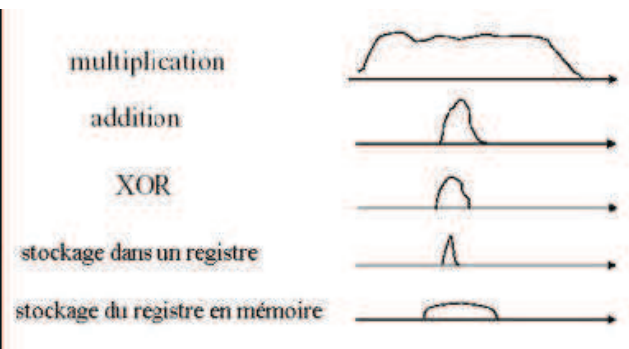
CONCLUSION

The card's current consumption may reveal secret information.

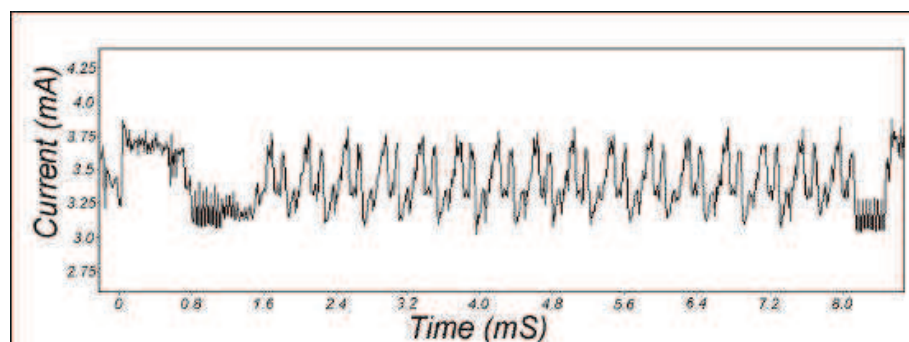


La SPA (Simple Power Analysis)

Principe : Des instructions différentes ont une trace différente.



Consommation en courant d'un DES. On peut voir la permutation initiale, suivie des 16 tours.



La SPA sur la signature RSA

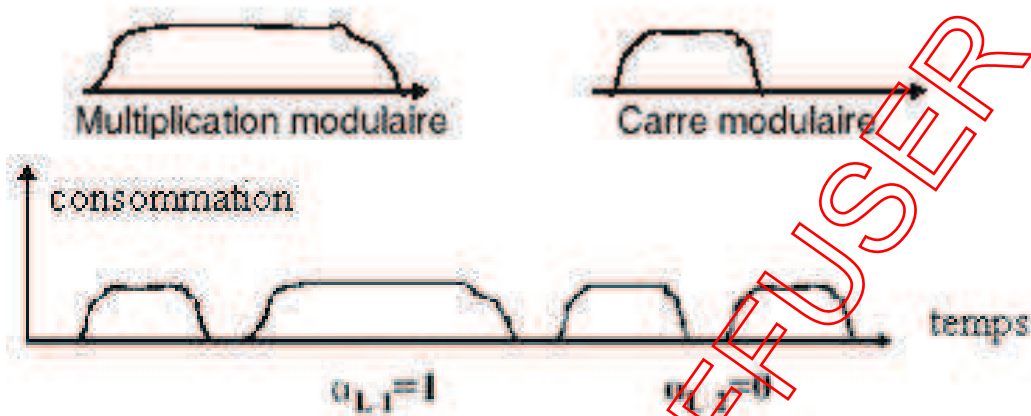
```
s = 1 ;  
for ( i = L - 1 ; i >= 0; i-- ) {  
    s = s*s mod n ;  
    if ( a [ i ] == 1 )  
        s = s*y mod n ;  
}
```

Signature RSA : $y^a \mod n$

y est le message à signer,

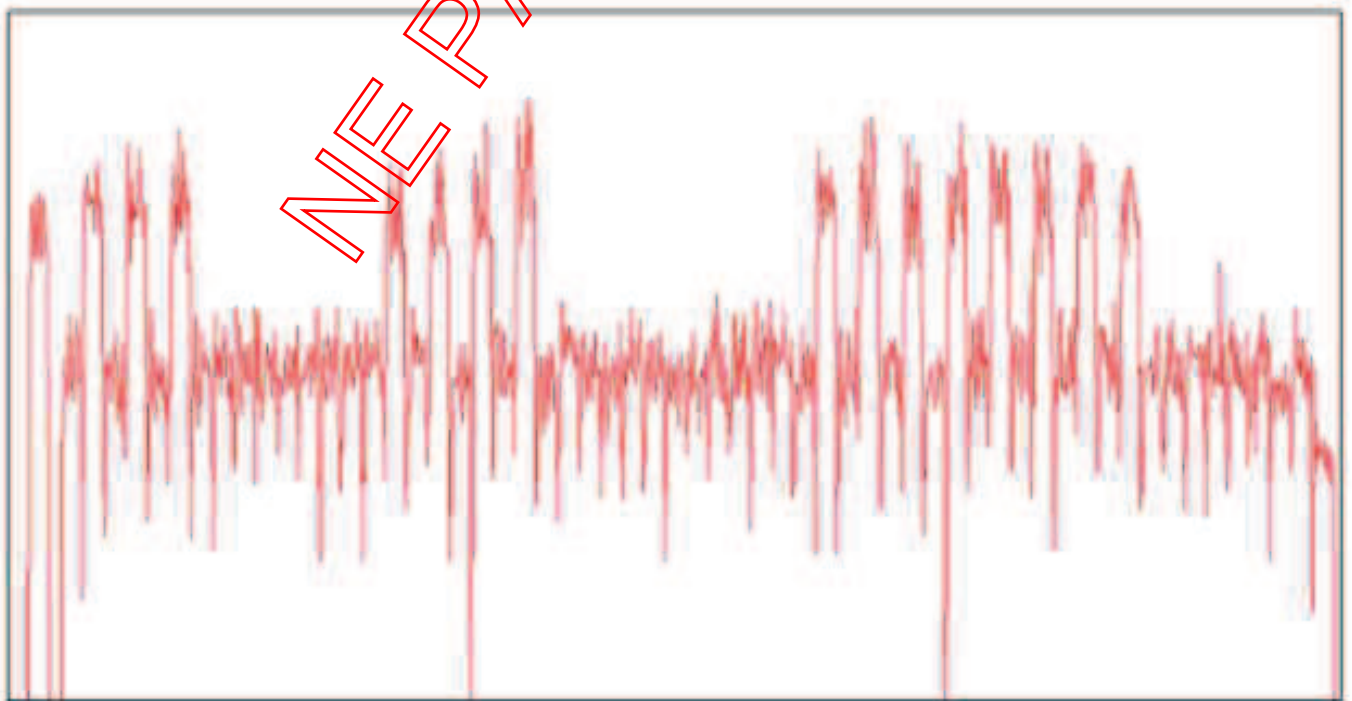
n est public,

a, l'exposant peut être considéré comme la clé secrète.



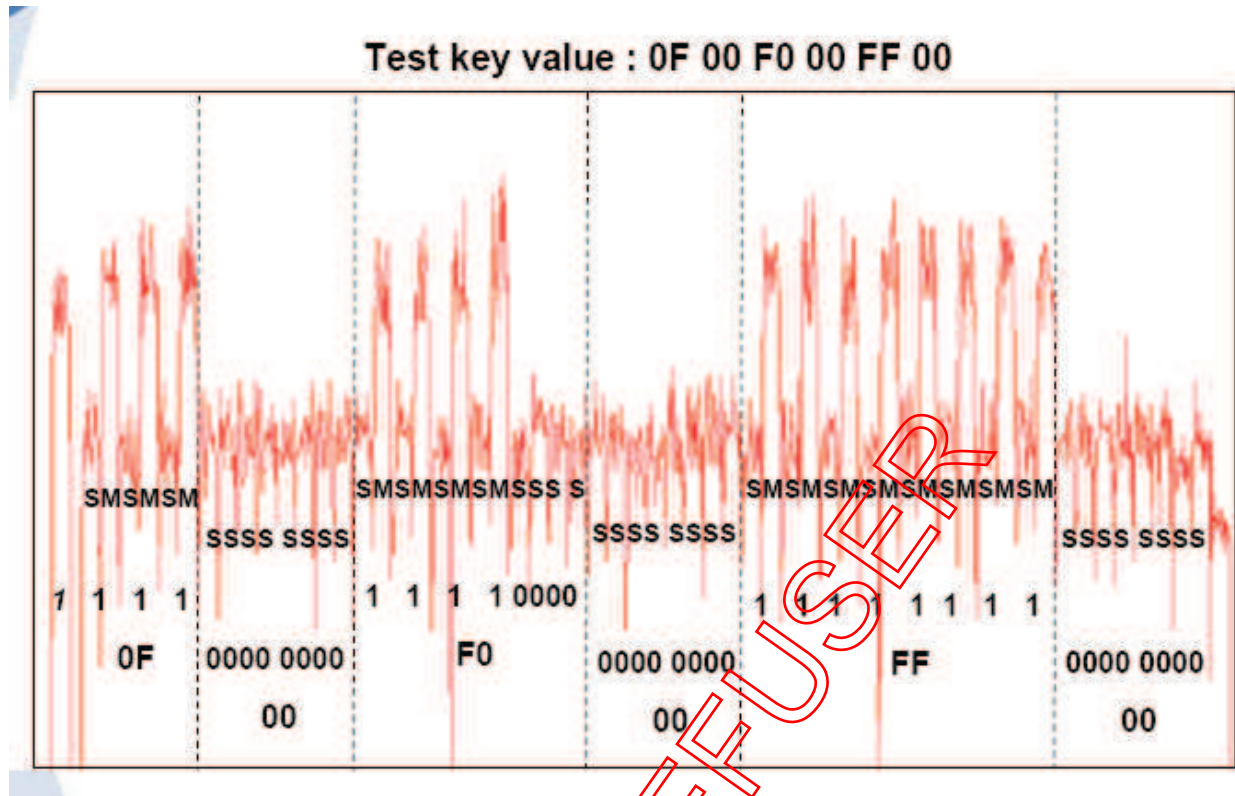
147

Exemple « réel »



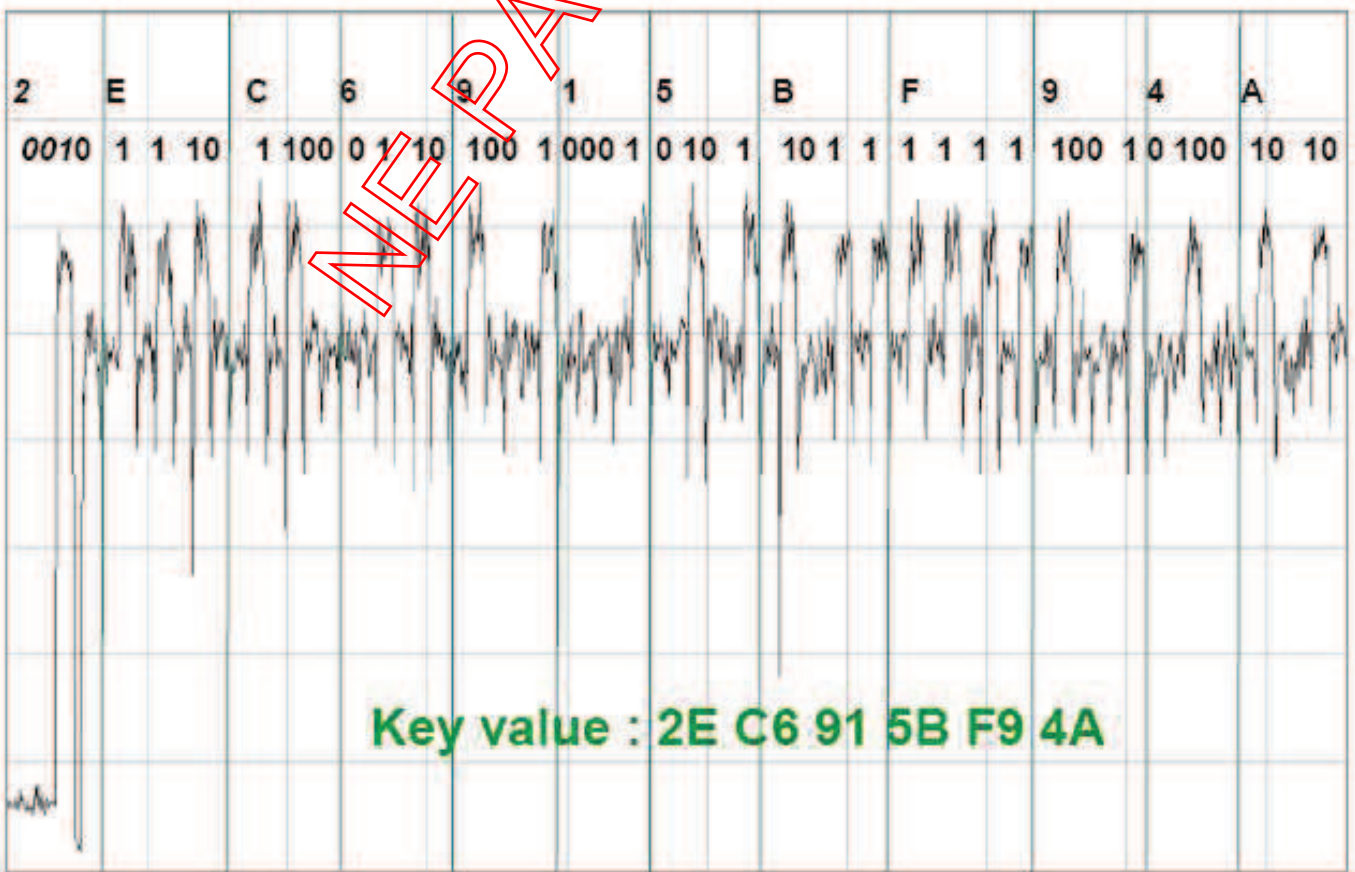
148

Exemple « réel »



149

Exemple « réel »

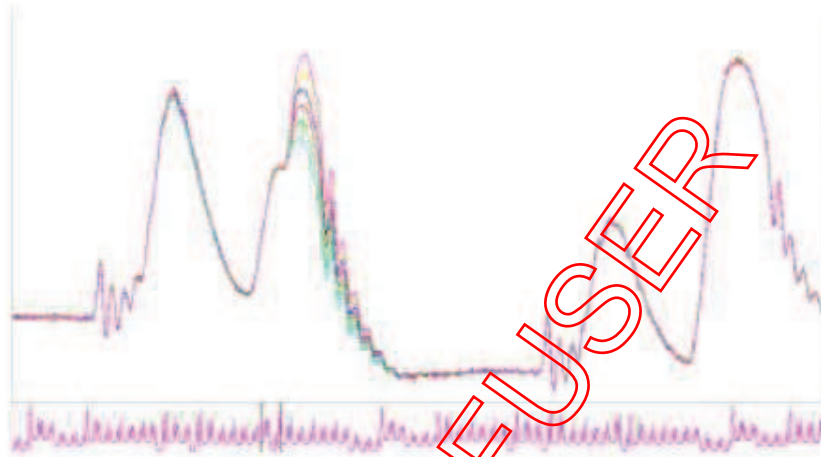


La DPA (Differential Power Analysis)

Principe : La consommation dépend des opérations effectuées (les instructions) mais aussi des opérandes.

Elle utilise des fonctions statistiques adaptées à l'algorithme visé qui font ressortir des corrélations entre un bit intermédiaire a (ne dépendant que d'un fragment Kr de r bits de la clé et du message d'entrée M) et la consommation de courant.

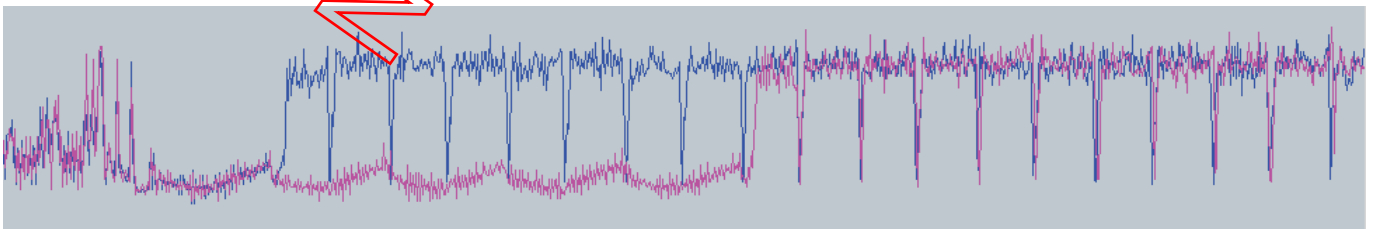
- Based on SPA
Adding the power of statistics to separate signal from noise



151

CONCRETE ATTACK ON CONCRETE KEYS

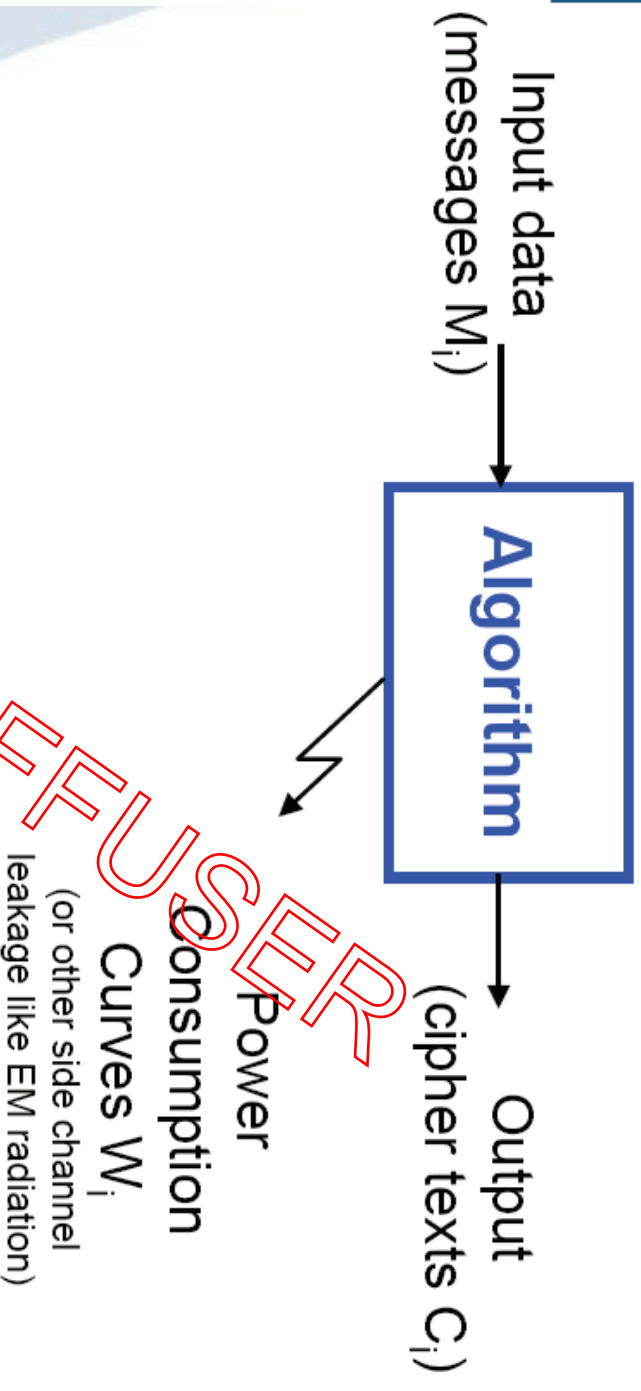
- Comparing:
 - decryption with key = 0000 1111 ...
 - decryption with key = 1111 1111 ...



token designed and manufactured in 1998...

DPA Hypothesis

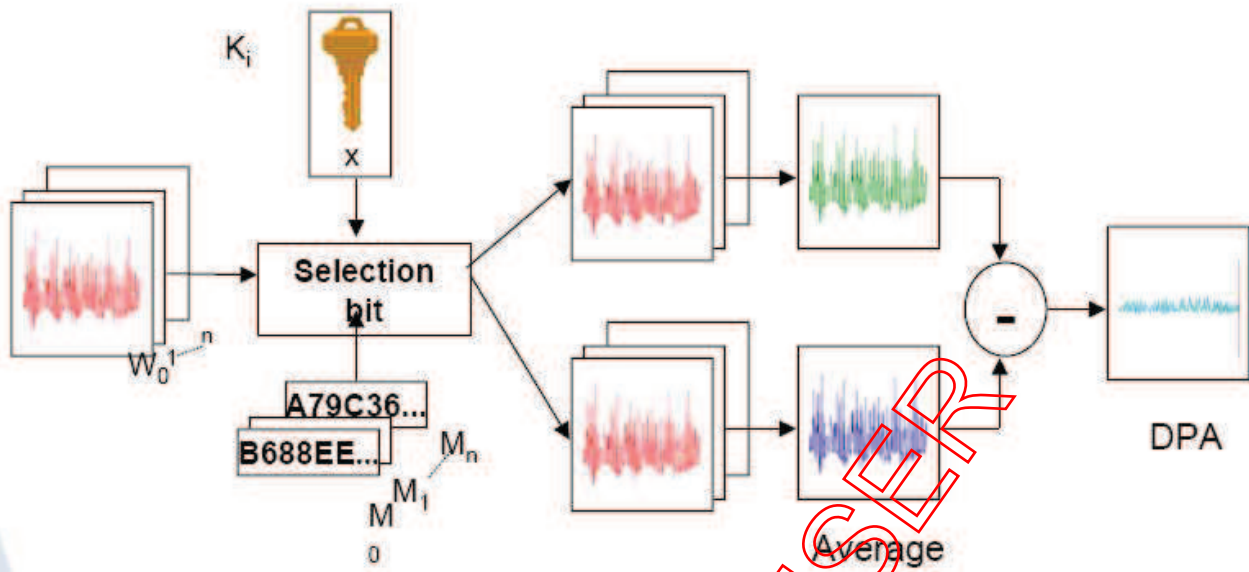
Play the algorithm N times
($100 < N < 100000$)



Acquisition procedure

- After data collection, what is available ?
 - N plain and/or cipher random texts
00 B688EE57BB63E03E
01 185D04D77509F36F
02 C031A0392DC881E6 ...
- N corresponding power consumption waveforms





La HODPA (High Order DPA)

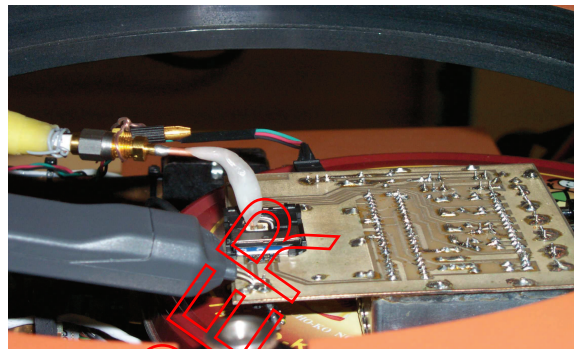
La HODPA ou DPA d'ordre n est aussi basée sur une étude statistique de la consommation de courant de la carte.

Différence : elle utilise des corrélations entre la consommation de courant et n variables intermédiaires ne dépendant que d'un fragment de la clé et du message d'entrée.

Elle est beaucoup plus difficile à réaliser, mais beaucoup plus puissante.

COUNTER-COUNTER MEASURE

- Against *adding noise to the power consumption signal*.
- Capture electromagnetic radiation at various chip locations!
- Equipment:



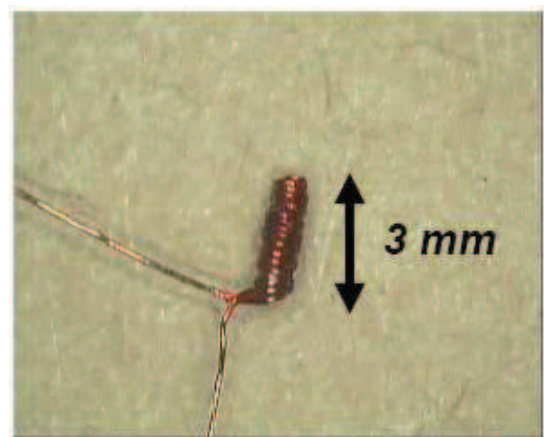
Les émissions EM

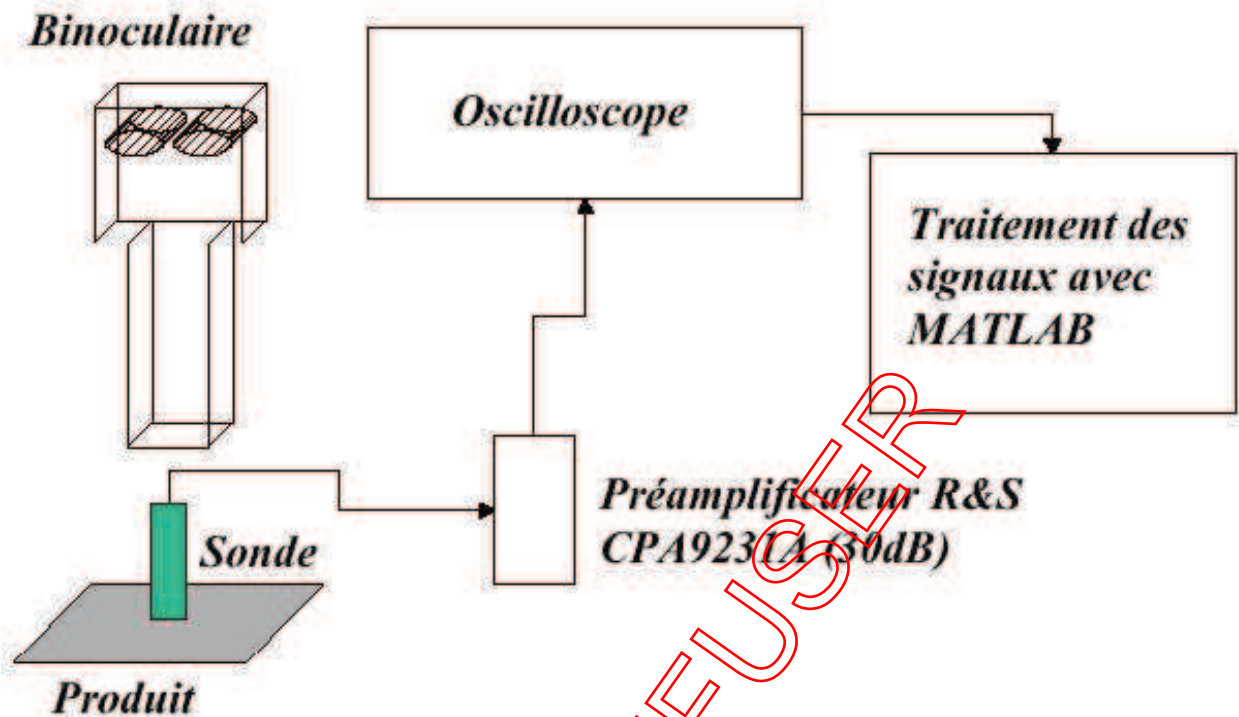
Principe : Les courants qui circulent dans la puce induisent des champs électromagnétiques qui sont susceptibles de donner le même type d'information que le courant.

Différence : L'information est plus locale. On peut déplacer la micro-sonde électromagnétique au dessus de la zone qui nous donnera le plus d'informations (exemple : co-processeur cryptographique).

Avantage : Insensible aux contre-mesures physiques tels que l'ajout de bruit en sortie ou le lissage de la consommation globale de courant.

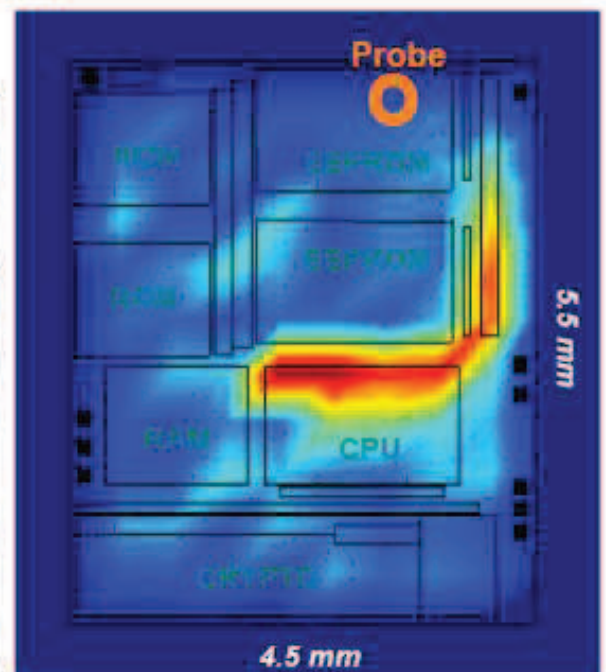
Inconvénient : La reproductibilité des mesures est difficile.





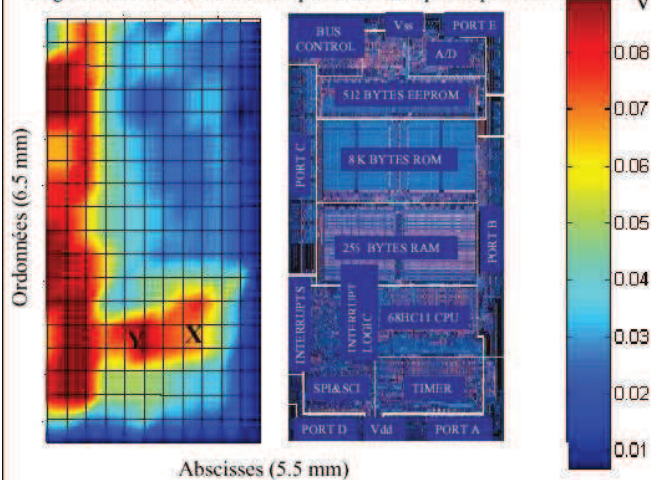
159

- Horizontal cartography (XY plane)
 - to pinpoint instruction related areas
 - better if automated

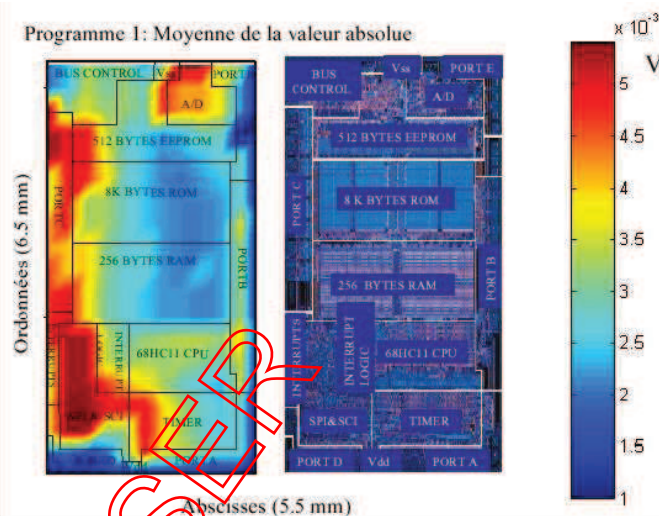


Cartographie pour l'algo 1

Programme 1: Maximum en amplitude de chaque acquisition



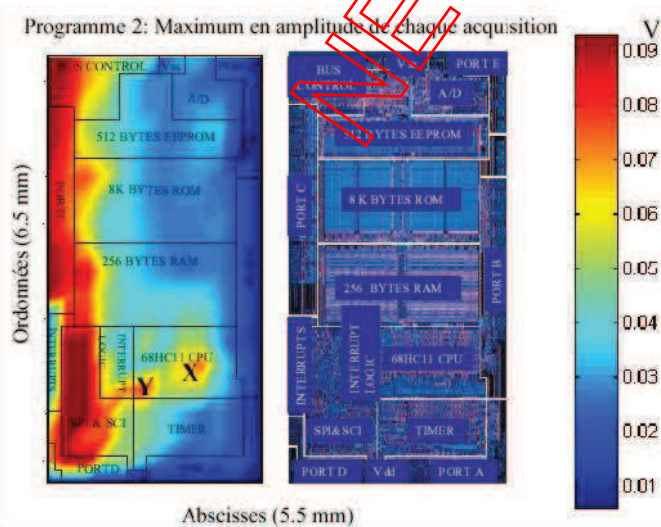
Programme 1: Moyenne de la valeur absolue



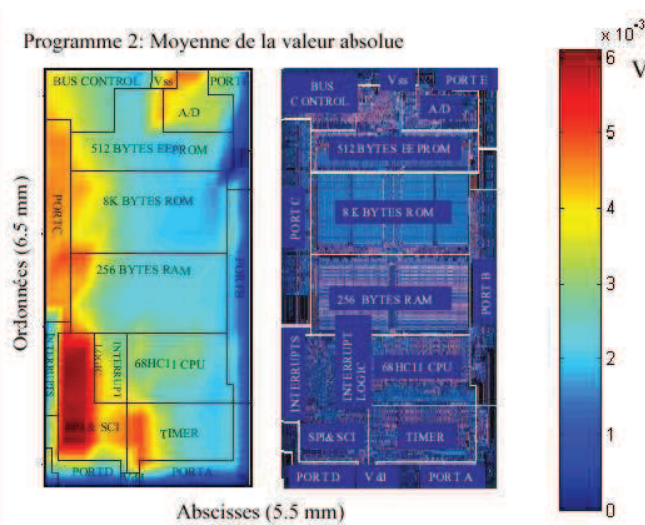
161

Cartographie pour l'algo 2

Programme 2: Maximum en amplitude de chaque acquisition



Programme 2: Moyenne de la valeur absolue

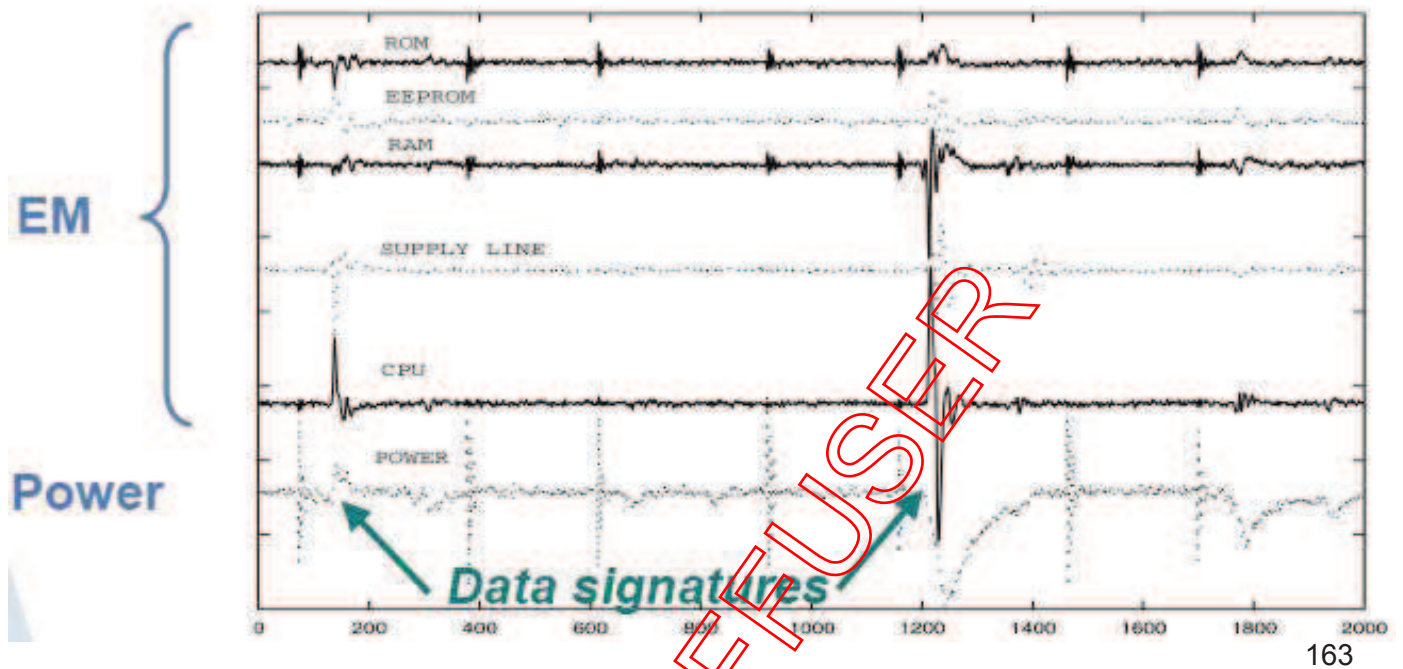


162

Différence EM/Power

- EM signals versus XY probe position

Differential traces between (00h $\oplus$ 00h) and (FFh $\oplus$ 00h) picked up at different locations



163

Attaques EM

la SEMA (Simple EM Analysis)

la DEMA (Differential EM Analysis)

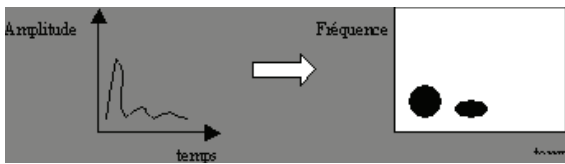
=> nécessite moins d'acquisitions

164

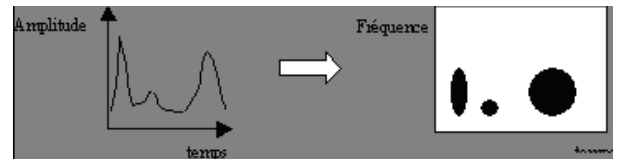
La rétro-conception logicielle

méthode du « dictionnaire » :

Une instruction :



Une autre instruction :



- La séquence des deux :



Utilisation possible de la consommation en courant ou des émissions EM

Statut : recherches en cours.

165

Invasives

micro-probing

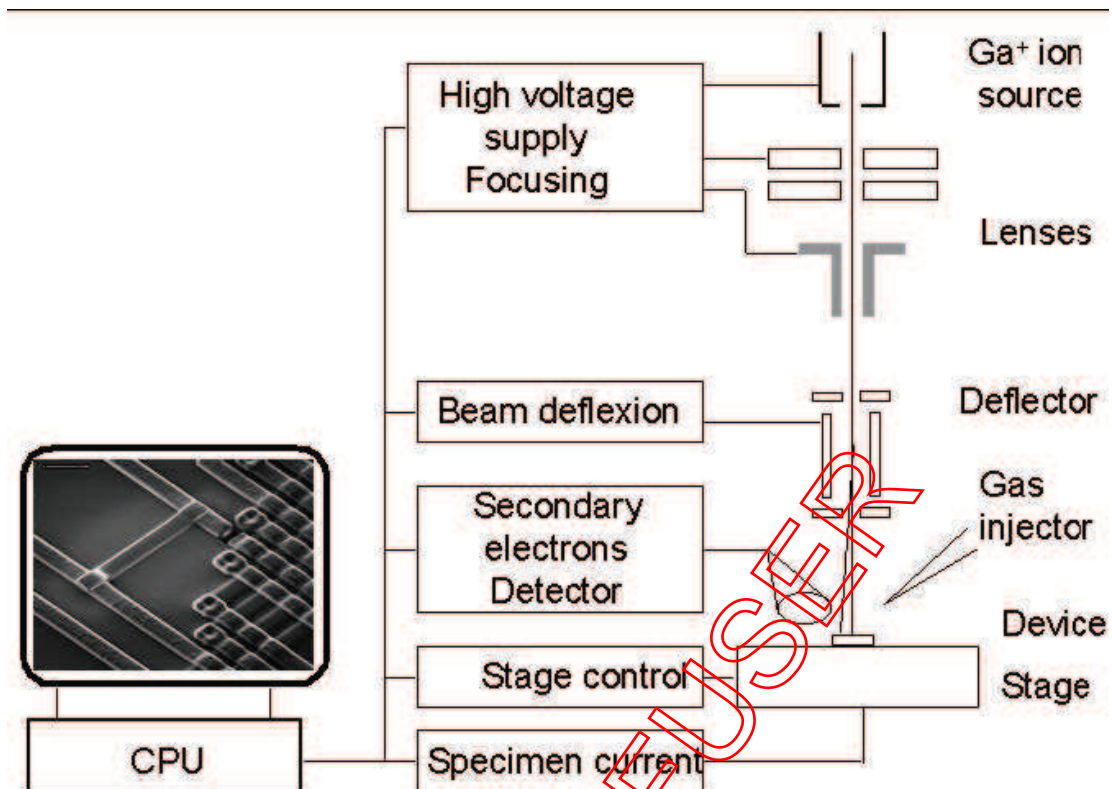
modification de circuit (FIB)

réetro-conception du circuit

NE PAS DIFFUSER

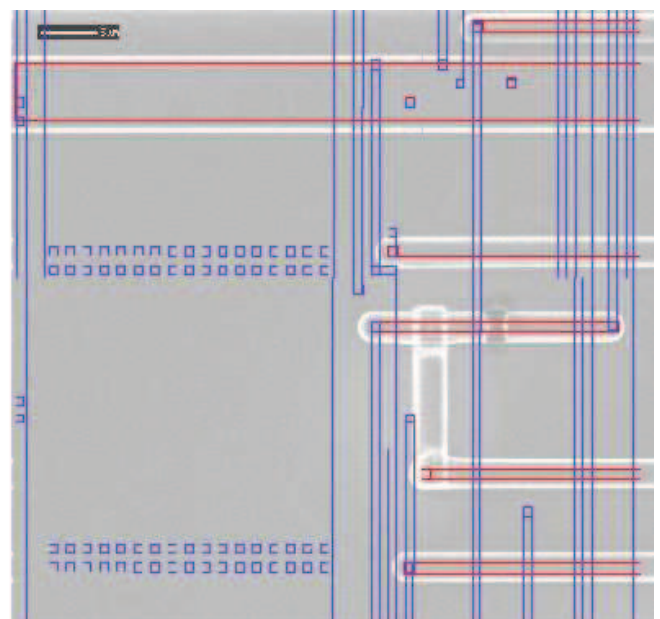
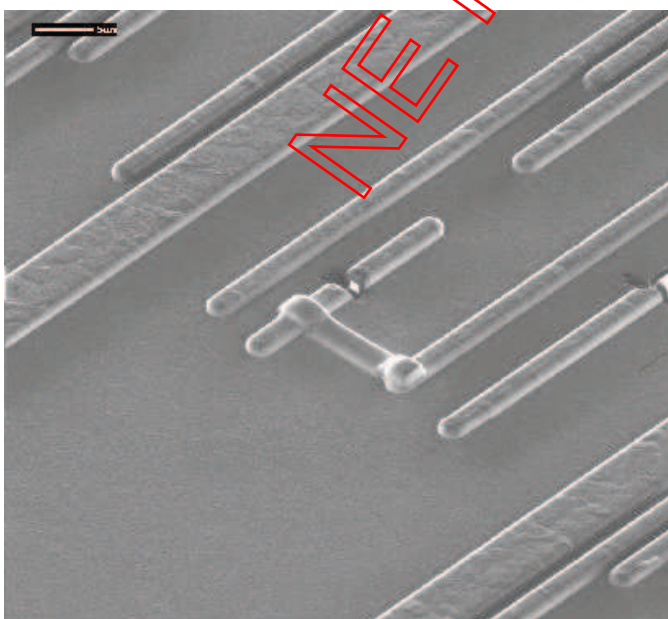
166

Le FIB (Focused Ion Beam)



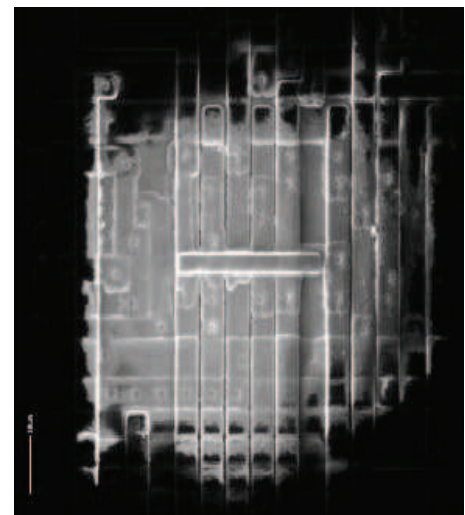
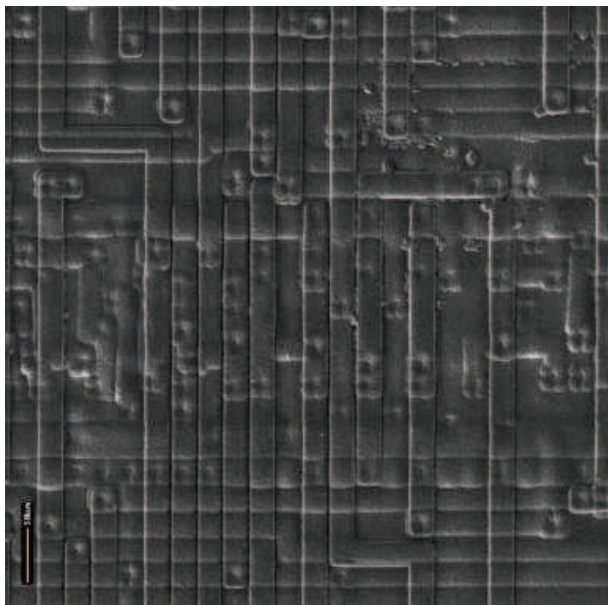
167

Modifications de circuits (1/2)



168

Chip Re-Wiring / Addition of a Track



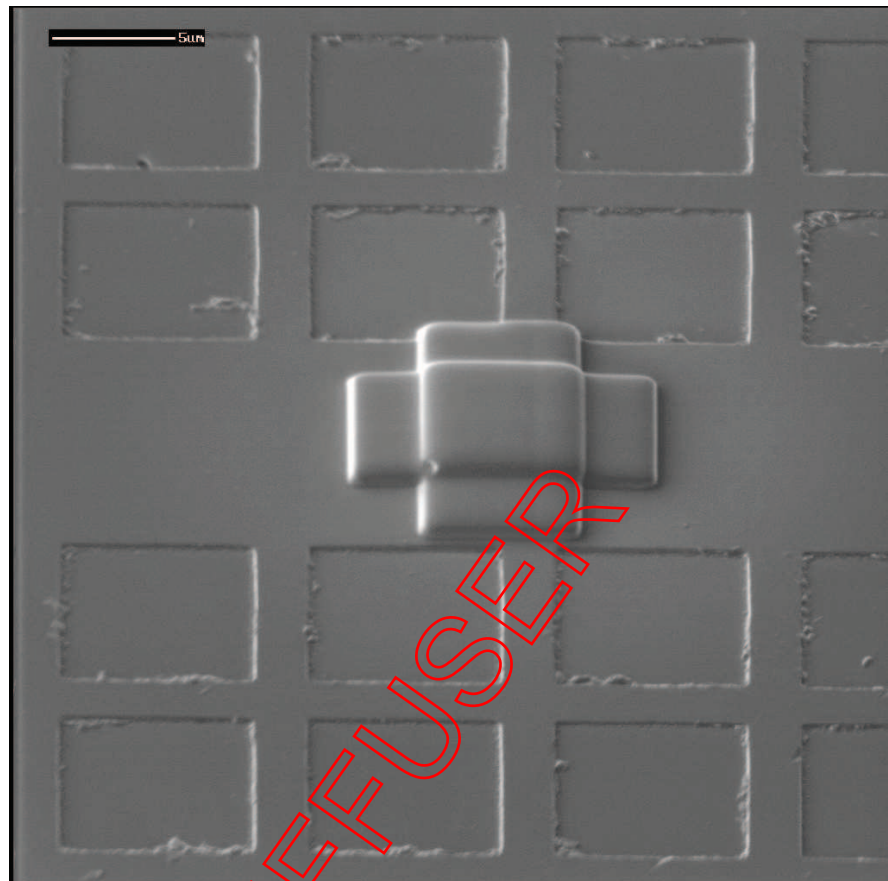
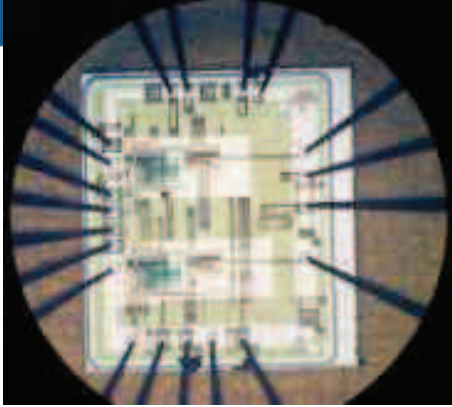
169

Modifications de circuits (2/2)



170

Micro-probing

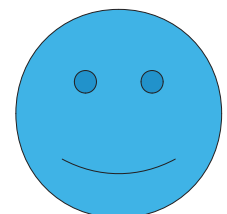


171

Coût

Très cher !

- If you have more money or if you are a student.



172

Côtation d'une attaque

Niveau d'expertise requise

Expert, ..., homme de la rue

Connaissance du produit

Information publique, diffusion restreinte, sensible, critique

Accès au produit

Nombre d'échantillon nécessaire : <10, <100, <1000, non praticable

Temps d'identification

<1 heure, 1 jour, 1 semaine, 1 mois, ...

Temps d'exploitation

<1 heure, 1 jour, 1 semaine, 1 mois, ...

Équipement

Aucun, standard, spécialisé, ...

...

=> La sécurité et le business s'opposent. Il faut donc trouver un juste compromis !

173

Le piratage facile en vidéos

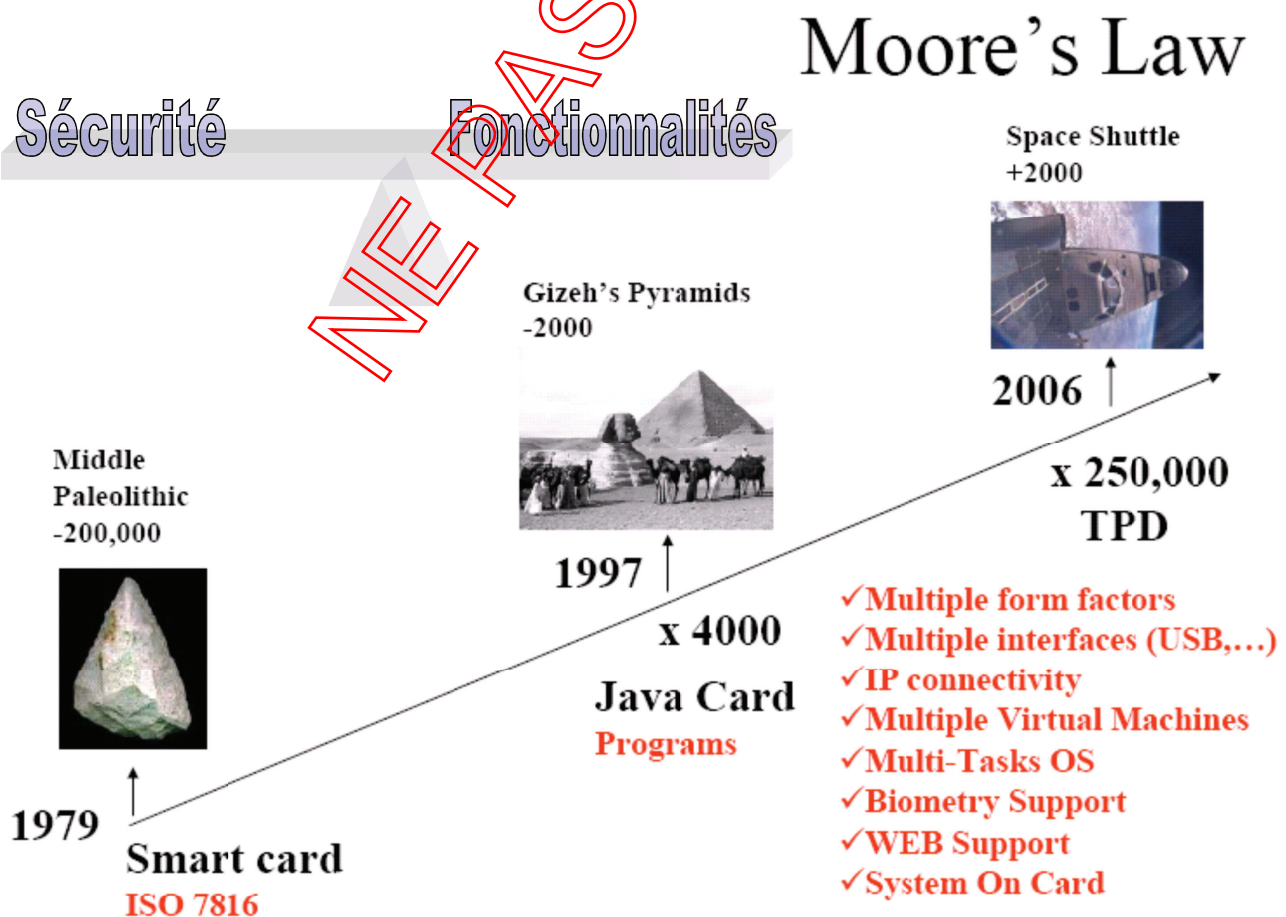
How to Reverse-Engineer a Satellite TV Smart Card.mp4

Mifare Hack.mp4

174

Le futur de la carte à puce

175



176

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 satellite)
- 2008 Spontaneous networking (JINI)
- 2009 GRID

177

Les cartes du futur

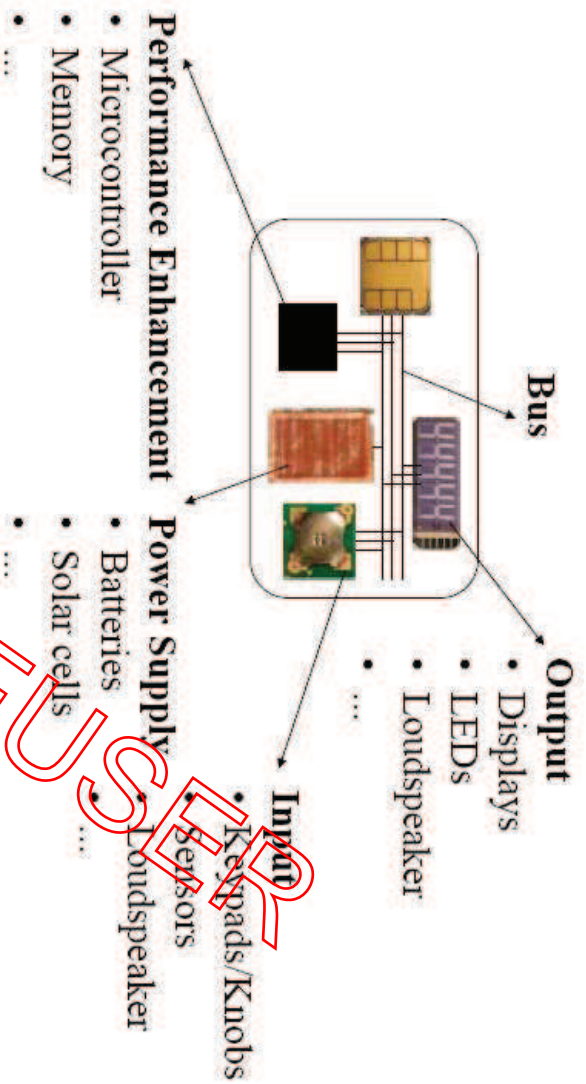
L'évolution matérielle

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)

178

About System on Card (Soc)



179

L'évolution matérielle :

Exemple : Java Powered iButton



• <http://www.ibutton.com>

• Packaging : capsule étanche en métal

- Peut-être montée sur baguette (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, enfonceait 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, X.509, Win2000 log on

Joli concept
mais
concept abandonné

L'évolution matérielle :

Exemple: Cyberflex eGate

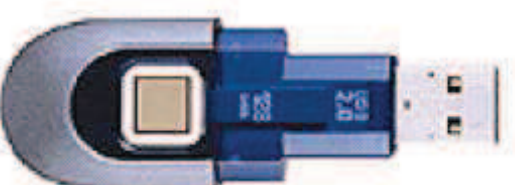
- Axalto (ex Schlumberger)
- Brevet WO0016255
- Capacité
 - 32 de FlashRAM
- Format
 - ISO7816-1, GSM11.11
- Interface
 - USB/OTG (de 1.5 Mbits/s à 12 Mbits)
 - TCP/IP+USB pour la couche physique (bulk mode)
 - Full duplex
- Crypto :
 - RSA, DES, AES (très haut débit)
- Programmation
 - JavaCard
 - Mini-Serveur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



L'évolution matérielle :

Exemple: la clé Micro Vault

- Clé USB Micro Vault
 - clé USB à reconnaissance d'empreinte digitale.
 - 8 identifications biométriques différentes sur le Micro Vault.
- 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 réveiller pour rappeler des événements au porteur



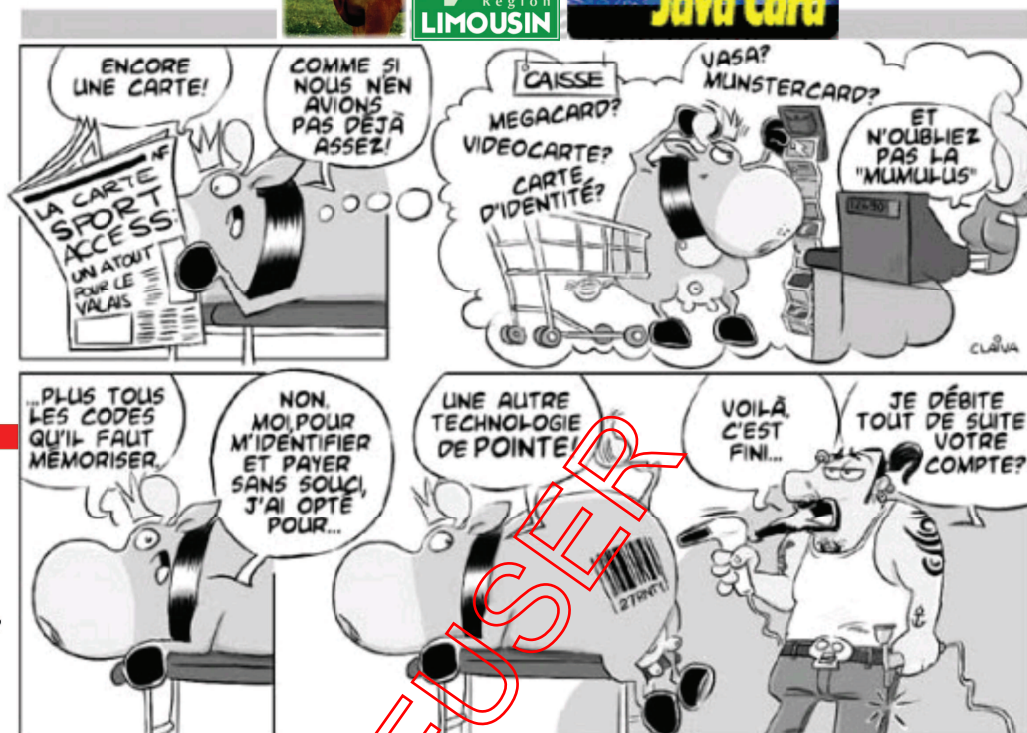
source Alien Technology <http://www.alientechnology.com/> ;

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 attendre 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

Les cartes à puce du futur

*Des cartes ... encore ... toujours ...
... toujours plus ...
... partout ...*



Comment résoudre ce problème ?

La carte multi-applicative

185

Oyster Card et Barclays

Oyster – Facile et pratique pour voyager pas cher dans Londres.
Chargement de crédits ou carte d'abonnement.
C'est une fonctionnalité totalement séparée du compte associé à la carte de crédit



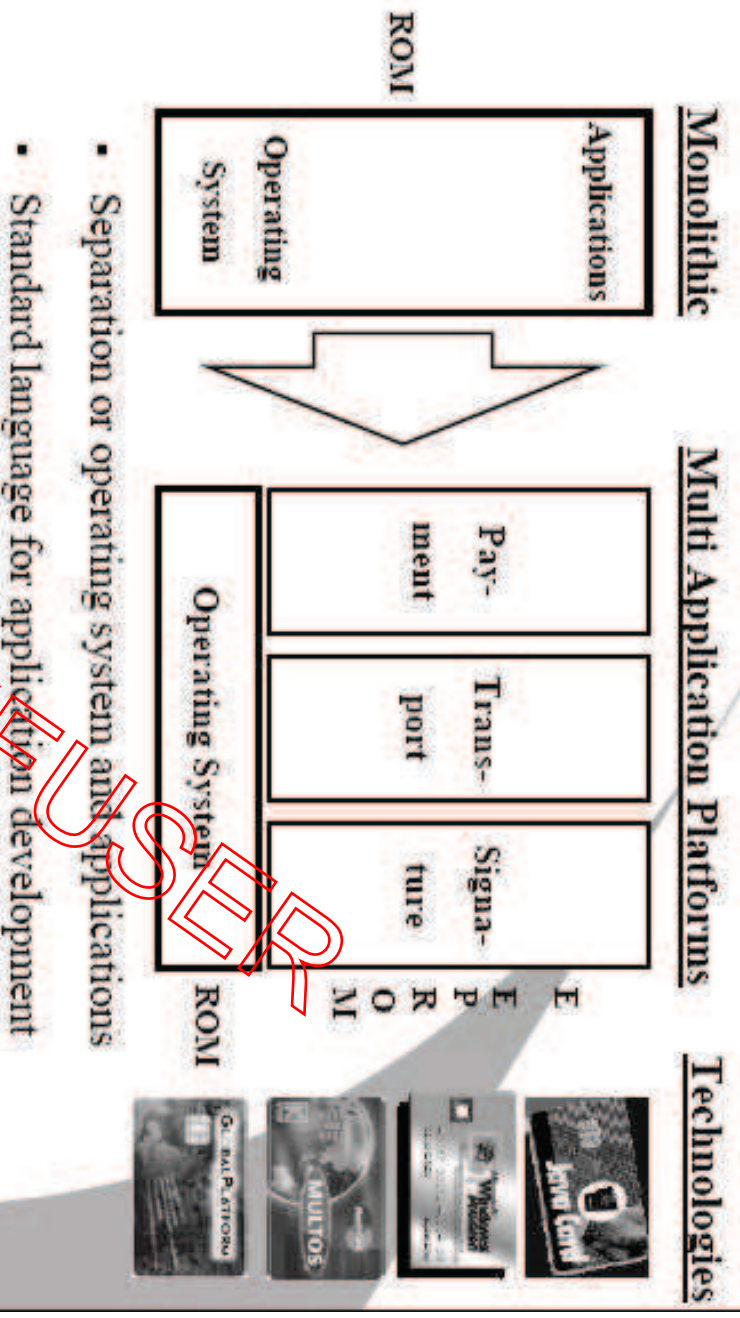
Cashless – Technologie Visa "wave and pay" pour des petits achats (inférieurs à £10) sans PIN.
Les transactions apparaissent sur le relevé de compte.



Credit – Application Visa classique avec PIN pour les paiements supérieurs à £10.



186

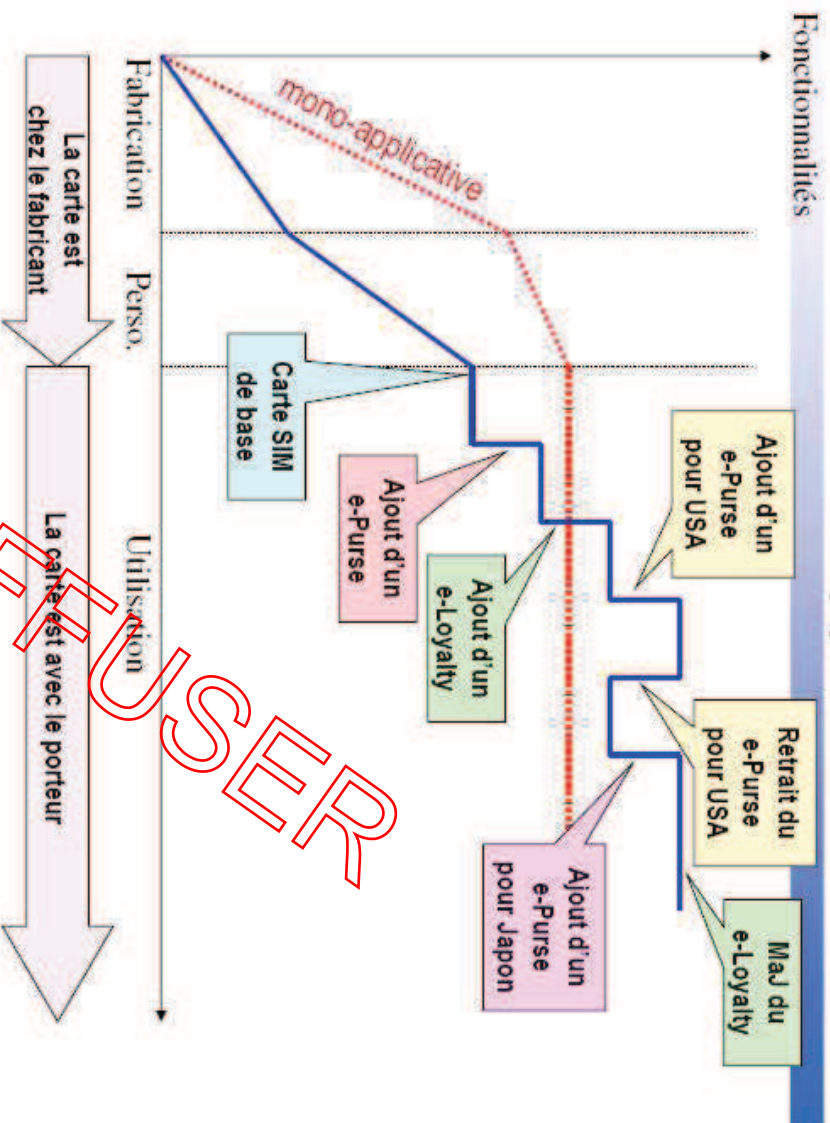


187

Une nouvelle génération : Les cartes multi-services

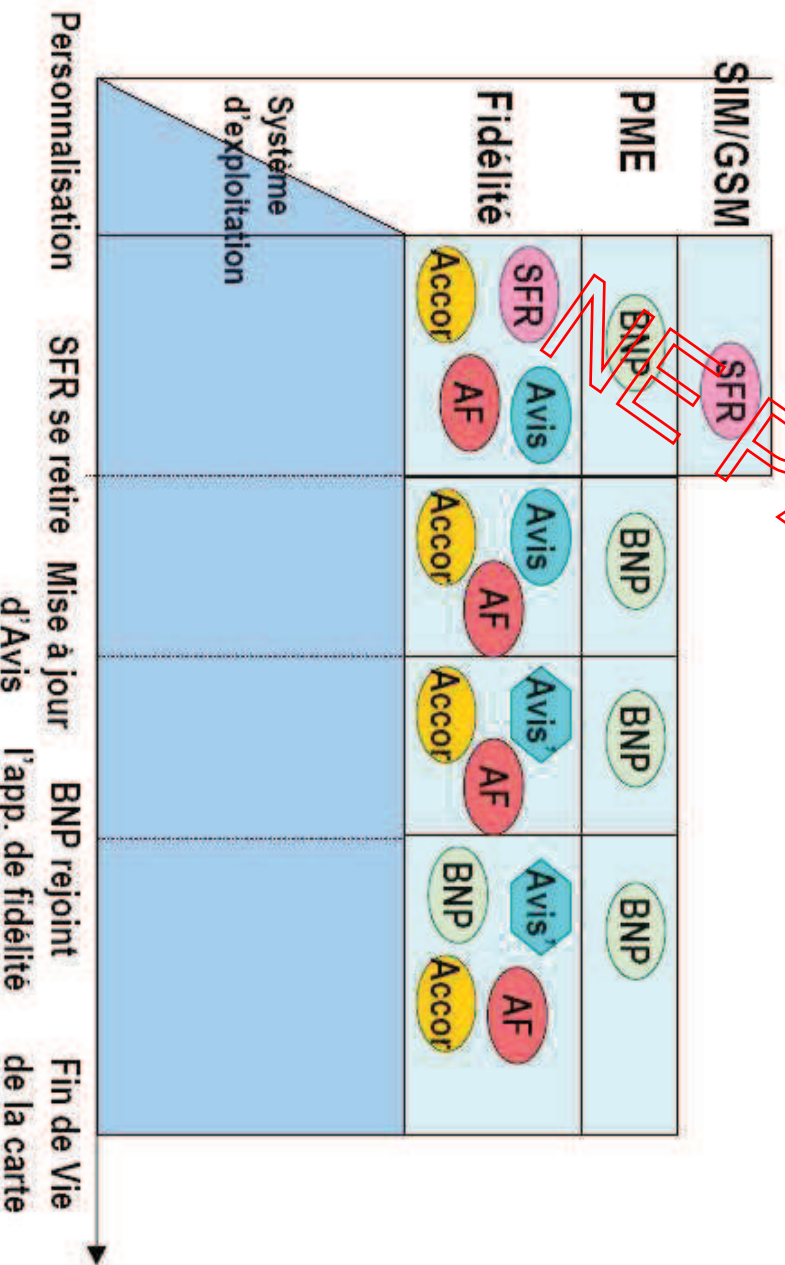
- **But :**
 - Permettre à plusieurs applications de coexister
 - Partager des données entre plusieurs applications (non redondance d'information)
 - Possibilité de charger/décharger des applications en cours de vie de la carte
- **Avantages**
 - une seule carte pour l'utilisateur
 - Possibilité d'évolution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

Le cycle de vie des cartes multi applicative



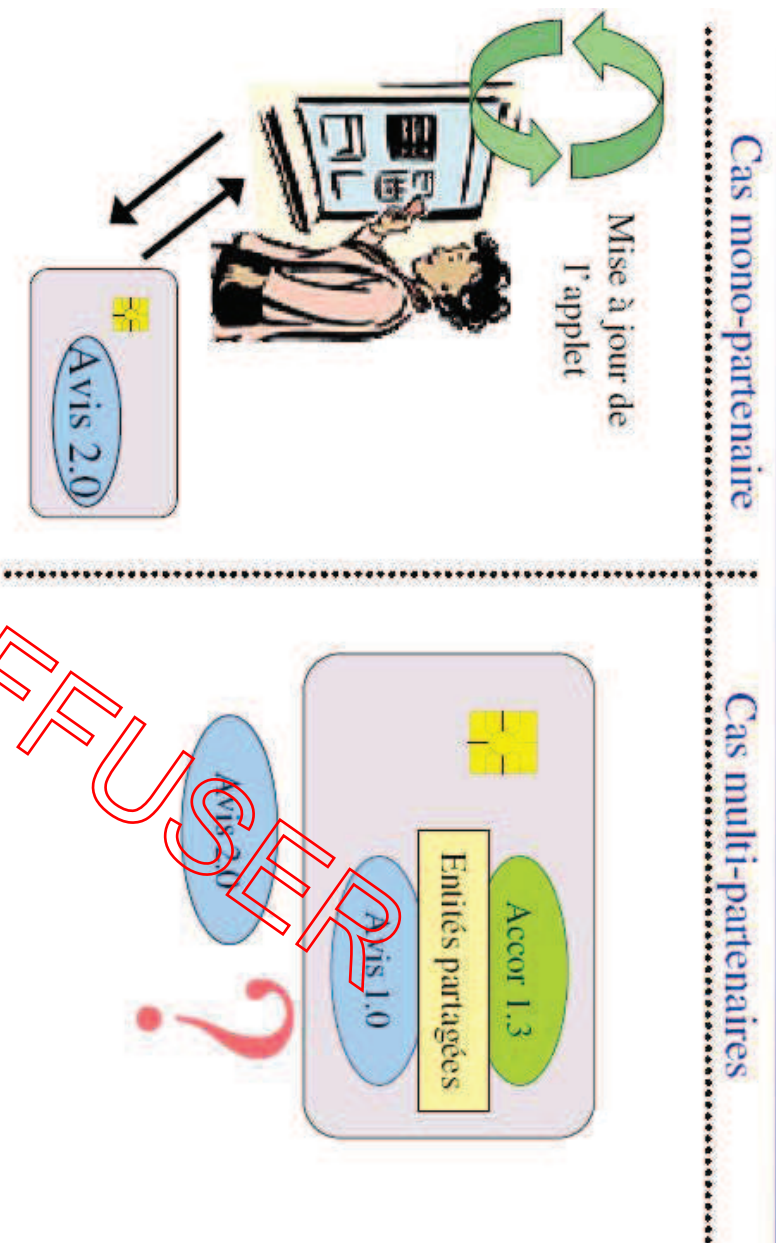
189

Cycle de vie d'une carte multi-partenaires



Évolution d'applications

Cartes multi-applications



191

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

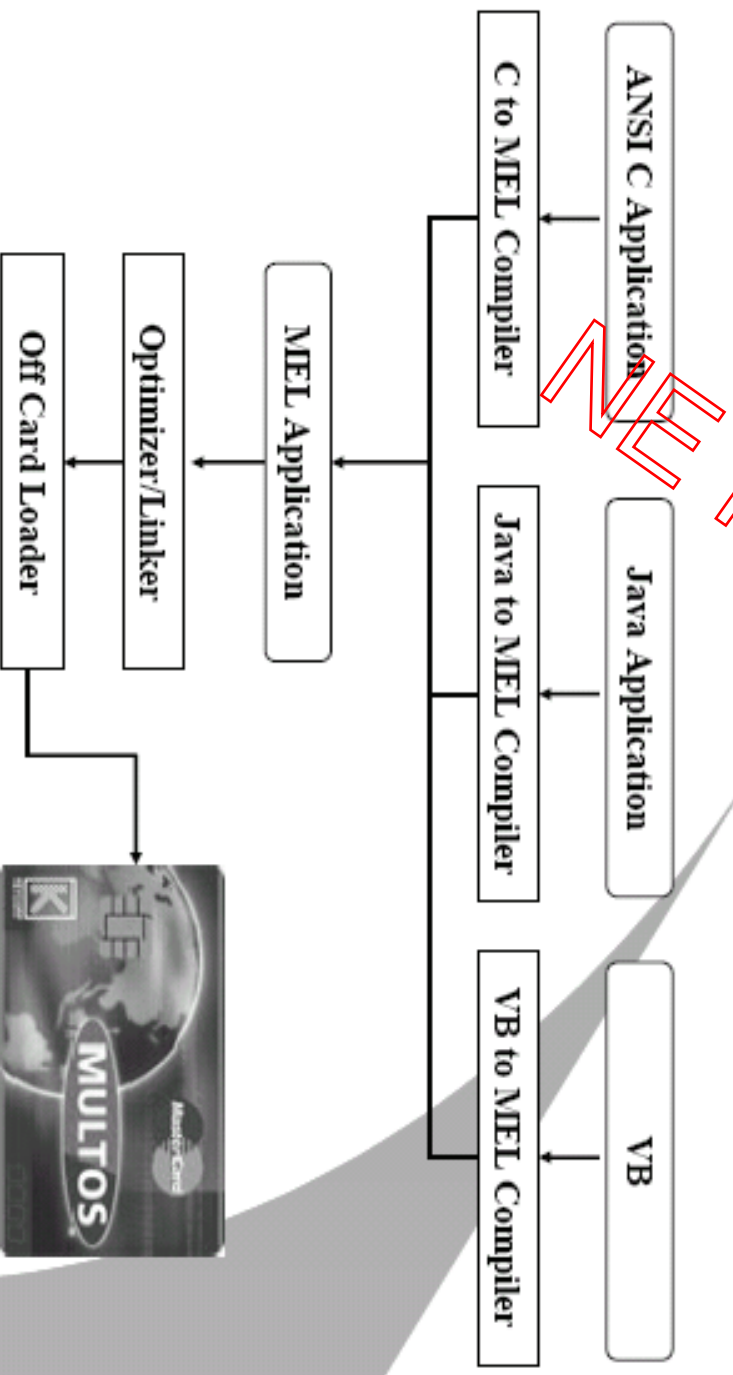
- Se simplifier la vie :
 - utiliser la même carte pour toutes les applications
 - Plusieurs applications sur une même carte
 - Pouvoir changer de prestataire sans avoir à recommander une carte
- Chargement / déchargement d'application

192

Multos



Multos Application Development



Multos

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



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

5

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 SmartCard !!
- Caractéristiques
 - 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

<http://www.hiveminded.com/>

- Implémentation de la CLI adapté à la carte
- Multi-applications
- Développement Multi-langage : C#, J#, VB, Jscript, Perl, ...
- Caractéristiques
 - 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

Technology Overview 1/2

Criteria	GP	Multos	WfSC	JavaCard
Concept	Platform	SCOS	SCOS	VM & API
Virtual Machine Technology	Interpreter	Interpreter	Interpreter	Interpreter
Byte Code	No predefined byte code	MEL	TBC	Java byte Code
Performance	N/A	2-3 times slower then native	TBC	2-3 times slower then native
VM & SCOS Extensions	Yes, subject to implementation	Yes, subject to ITSEC implementation	YES	Yes, subject to implementation
Security Level	EAL4+(France). EAL5+(Germany)	ITSEC 6 Achieved	Microsofts Approval	EAL4+, EAL5+
Based	Chip, SCOS, JVM, OP	Chip and SCOS	Chip, SCOS	Chip, SCOS, JVM
Crypto Engine	Yes (Optional)	YES	No	Yes (Optional)

Technology Overview 2/2

Criteria	GP	Multos	WfSC	JavaCard
Post Issuance Application Loading	Card Manager Security Domains, etc.	Application Load & Delete Certificates	Yes, protocol & security not defined	Yes, protocol & security not defined
Memory Requirements	~8K	~4K VM, ~7K Executive	TBC	Java Card VM: ~18K Java Card API: ~8K
Libraries	~8K for crypto	~15K for crypto	TBC	--
Programming Languages	No predefined language	MEL, C, even Java or VB	VB (Subset)	Java (Subset)
Extensible APIs	Yes (Third Party)	Yes, only after evaluation	Microsoft Verified code extensions	Yes, Third party
Processors	OS depended	Optimised for 8-bit processors	Designed for 8-bit processors	Optimised for 32-bit but available on 8-bit
Portability	Portable across any Java Card or WfSC	Fully portable across Multos implementations	Portable across WfSC implementations	Portable across 2 1 compliant Java Cards

Business Overview 1/3

Criteria	OP	Multos	WfSC	JavaCard
Specification	Open	"Open"	"Closed"	Open
Controlled/ Maintained	Global Platform	MAOSCO	Microsoft	SUN
Current Version	GP 2.1	Multos 6	WfSC 1.1	Java Card 2.2
Model	Issuer Centric & delegated management	Issuer Centric	Not Specified	Not Specified
Licence Required	No	Yes	YES	Yes
From	N/A	MAOSCO	Microsoft Approval	SUN
What for	N/A	Multos OS & VM Implementation	SCOS	VM Implementation
Who Pays	N/A	SCOS Implementer	SCOS Implementer	SCOS Implementer

Business Overview 2/3

Criteria	GP	Multos	WfSC	JavaCard
Cost Evaluation	Depends on the issuer, country, deadline, etc.	~\$600,000 (Varies)	Depends on the level, country, deadline, etc.	Will add ~40%-150% to the cost of the chip
Licence	N/A	€250,000+ €50,000 per annum	TBC	\$400,000+ \$70,000 Per annum
Card	~\$3 PK <\$2 non PK	~\$3-\$5 PK Card	~\$2-\$8	~\$2-\$7
Application Load/Delete Royalties (Issuer)	No	£0.025	Depends on the model	No
Application Loading Cost (Issuer)	~\$0.30-\$0.60, manufacturer Specific	~\$0.30-\$0.60, manufacturer Specific	~\$0.30-\$0.60, manufacturer Specific	~\$0.30-\$0.60, manufacturer Specific

Business Overview 3/3

Criteria	GP	Multos	WfSC	JavaCard
Card Management Systems	Several available	Several available	Several available	Several available
Enhancing Acceptance	Liaise with ETSI (not official member yet)	Member of ETSI	TBC	Member of ETSI
Personalisation and Back Office Systems	> 30 Vendors at special prices	~ 17 vendors	TBC	TBC
SIM Cards	>200 million cards	Multos SIMS since early 2001	N/A	>200 million Java Cards (GSM 03.48 [GP cards] and GSM 03.29[JC SIM card])
Multi Sourced	YES	"YES"	YES	YES
Development Tools	Same as standard Java	MDS, Hitachi, QuickSmart, etc.	VB/C++ Programming Environments	SUN, Symantec, Cyberflex, Gemplus, etc.

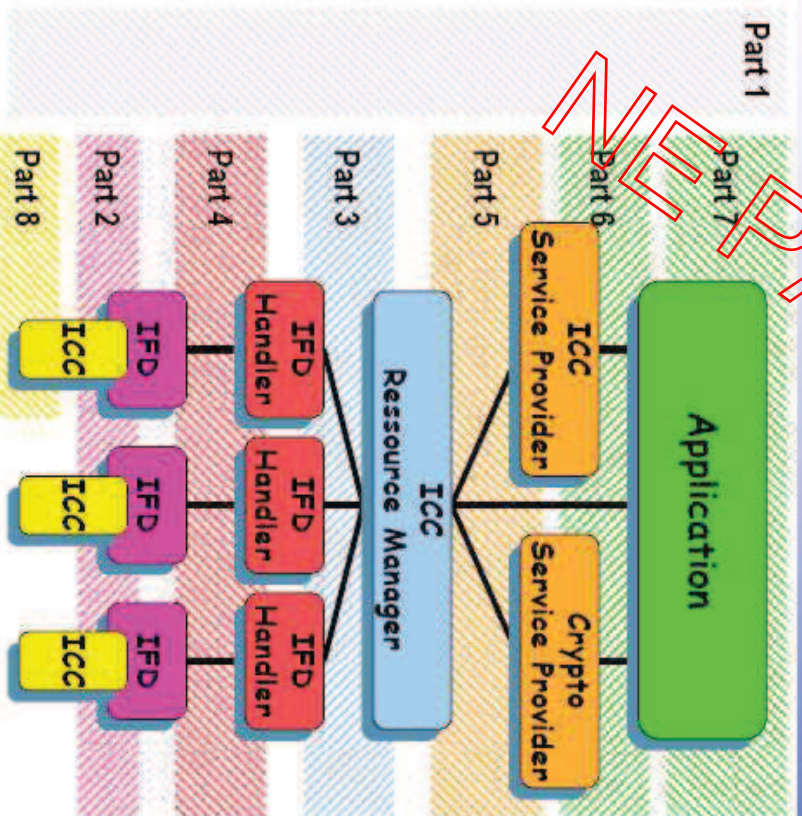


PC/SC

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

205

Architecture et spécifications PCSC



206

Bibliographie

Cours de Gemplus

Cours de Cartes à Microprocesseur de :

Didier Donsez (Univ. Joseph Fourier, Grenoble 1)
Gilles Grimaud (Univ. Lille 1)
Sébastien Jean (Univ Pierre Mendès France, Grenoble 2)
Sylvain Lecomte (Univ. Valenciennes)
Jean-Jacques Vandewalle (Gemalto R&D)

Cours du CNAM de Samia Bouzefrane

« Smart Card Handbook » de Rankl & Effing

Courses of the RHUL : Markantonakis et Mayes

- Javacard
 - <http://java.sun.com/products/javacard/specs.html>
- Multos
 - www.multos.com
- Windows for Smart cards
 - www.microsoft.com/smartcards
- GlobalPlatform
 - <http://www.globalplatform.org/>
- PC Client APIs
 - www.pcscworkgroup.com
 - <http://www.opencard.org/>
- Smart card & Security
 - www.gemplus.com/publications
 - www.iaik.tugraz.at

Webographie

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

207

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://www.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>

9

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: 3-540-63829-7,
 - <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.pcseworkgroup.com/>
 - MUSCLE pour Linux
 - <http://www.linuxnet.com/>

0

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)

...



Smart Cards, Tokens, Security and Applications
Mayes, Keith; Markantonakis, Konstantinos (Eds.)
2008, XXXVIII, 392 p. 128 illus., Hardcover
ISBN: 978-0-387-72197-2



Manifestations

Cartes (Paris en novembre) [www. cartes.com](http://www.cartes.com)

Conférence e-Smart (Nice, septembre)

Conférence Cardis (tous les deux ans)

Conférence CHES (tous les ans)

3GPP

...

Questions ?

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com



"My smart-card doesn't understand me."

**Si votre carte ne vous comprend pas,
la comprenez vous mieux ?**



NE PAS DIFFUSER

Java Card Grid Project

Présentation des grilles de calculs

Grille : ensemble de machines interconnectées.

Principe :

Partager de GROS calculs entre plusieurs machines.

Utilisateurs :

Organismes de la défense, CEA, laboratoires de recherche et universités, ...

Domaine d'utilisation :

Cryptographie, physique des particules, bio-informatique, observation de la terre, ...

Un des problèmes important : *La sécurité!*

217

Quelques projets utilisant la grille

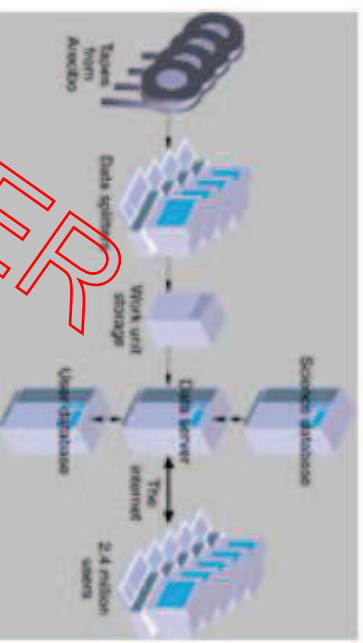


Décrypton

218

Seti@home

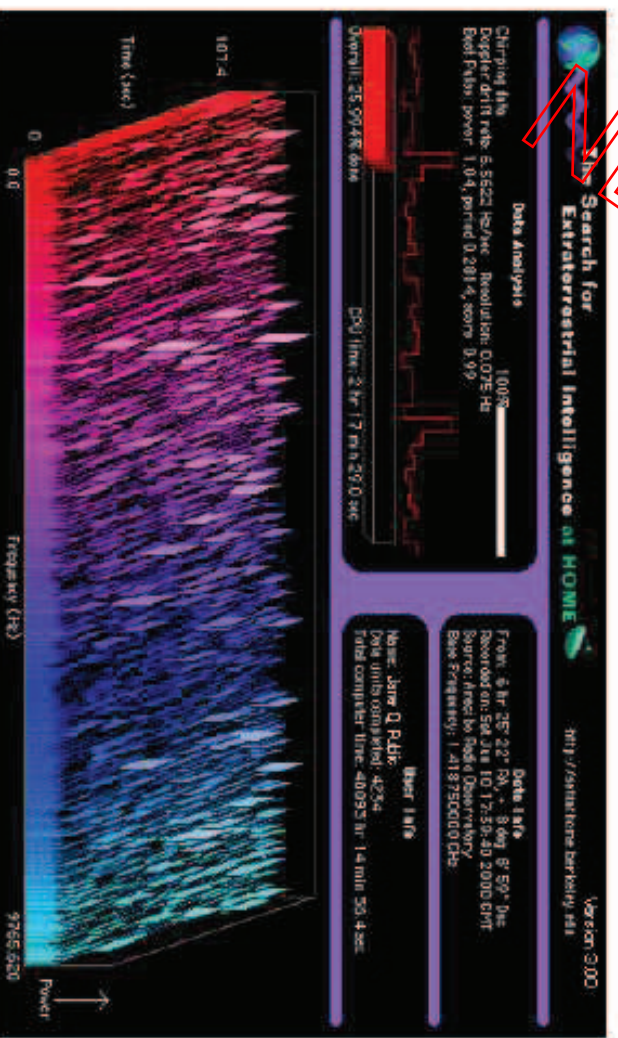
But : Recherche de signaux extra-terrestres.



219

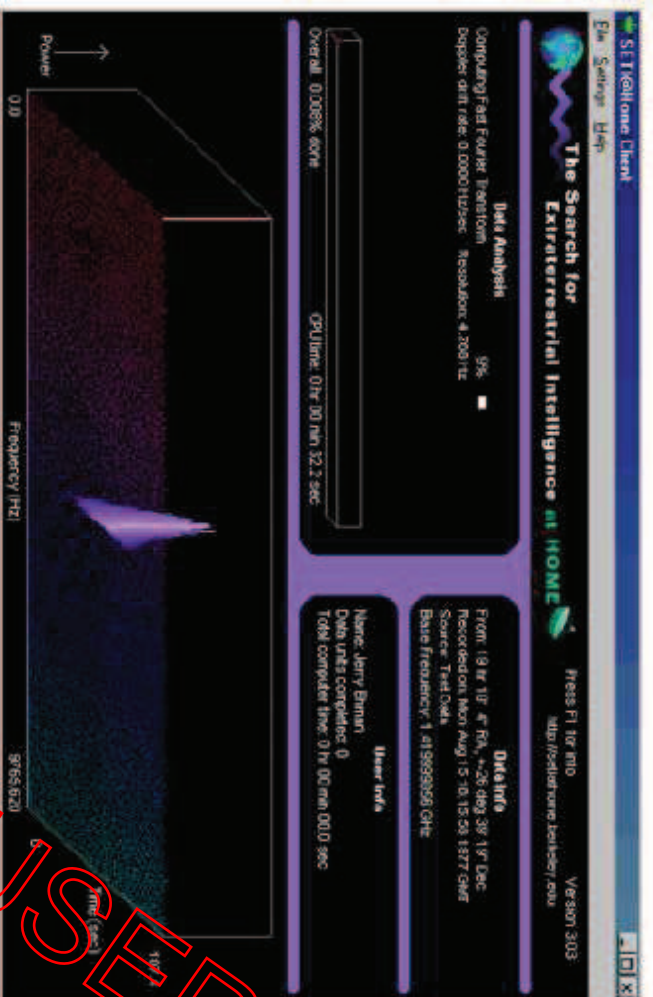
Les calculs

L'utilisateur télécharge un screensaver puis les données.



20

Les résultats



Nous ne
sommes PAS
SEULS dans
l'univers ?

SI ! $\Rightarrow$ Il s'agit de résultats truqués ! :-)

221

Les problèmes

Côté Seti@home :

- ☞ Les résultats positifs ou négatifs ne sont pas sûr.
 $\Rightarrow$ *solution* : Faire calculer les mêmes données plusieurs fois par différents utilisateurs

Côté utilisateur final :

- ☞ Code source non disponible.
 $\Rightarrow$ éviter les faux résultats.
- ☞ Que fait le code sur la machine de l'utilisateur ?

222

Le projet “Java Cards Grid”

Objectifs :

- ☞ Garantir la sécurité du code et des calculs sur la grille.
- ☞ Proposer un framework logiciel exploitant du matériel sécurisé pour assurer la confiance des utilisateurs.

Avantages pour :

- les utilisateurs du *distributed computing* : une plus grande confiance dans le fournisseur des ressources de calculs ;
- les fournisseurs des ressources de calculs : accéder à son marché avec des nouveaux clients comme le CEA, ...

223

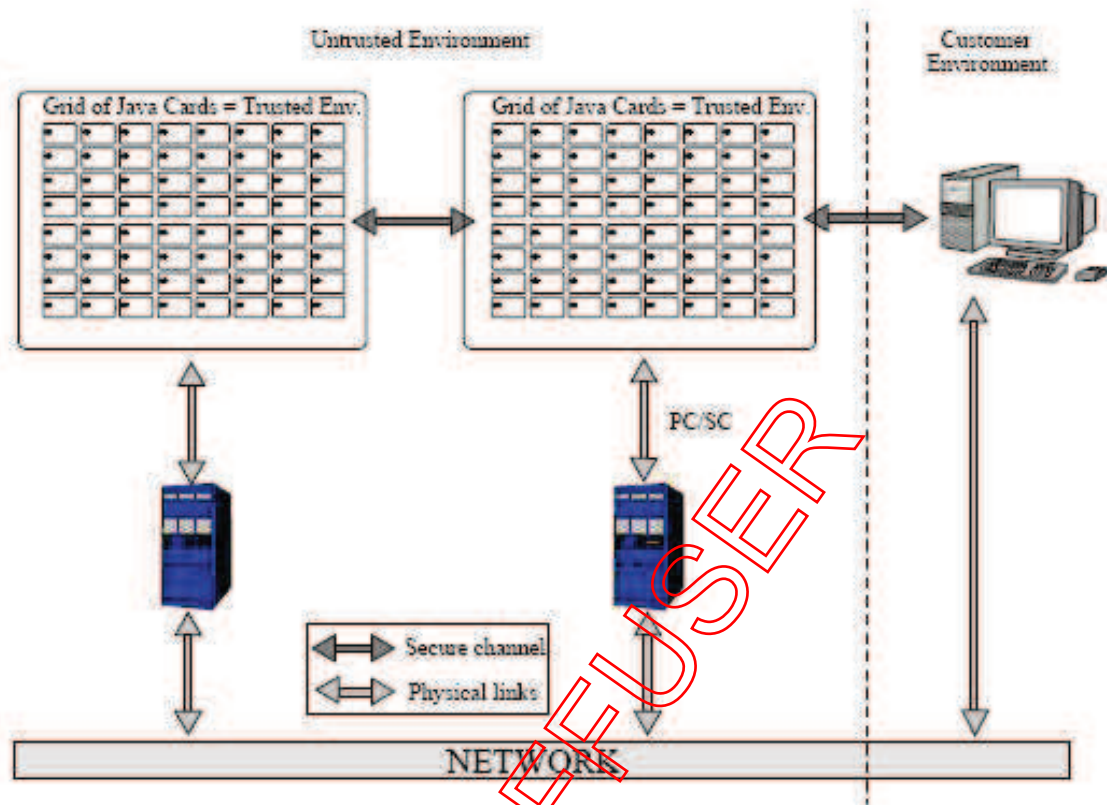
Buts de notre projet

- Premier but : Fournir un environnement sécurisé pour partager des ressources (matérielles, logicielles) et de la puissance de calcul

- Second but : Fournir une plate-forme pour expérimenter sur les réseaux ad hoc

224

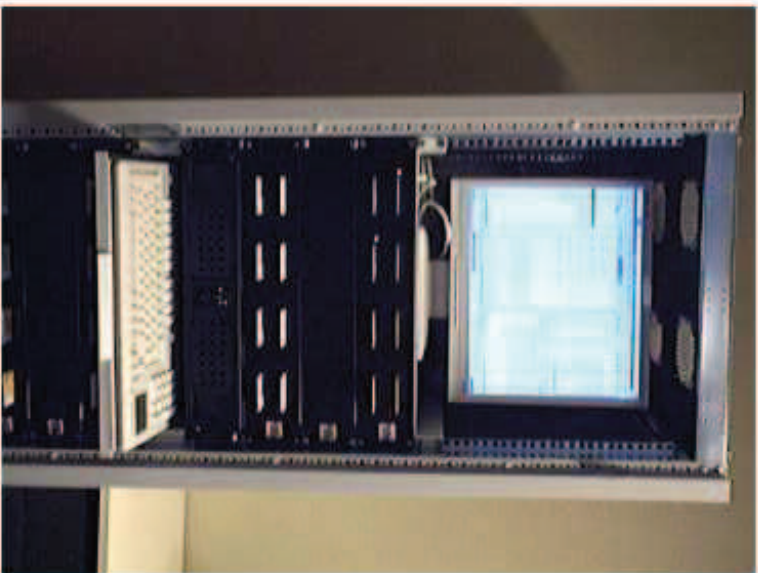
Notre proposition



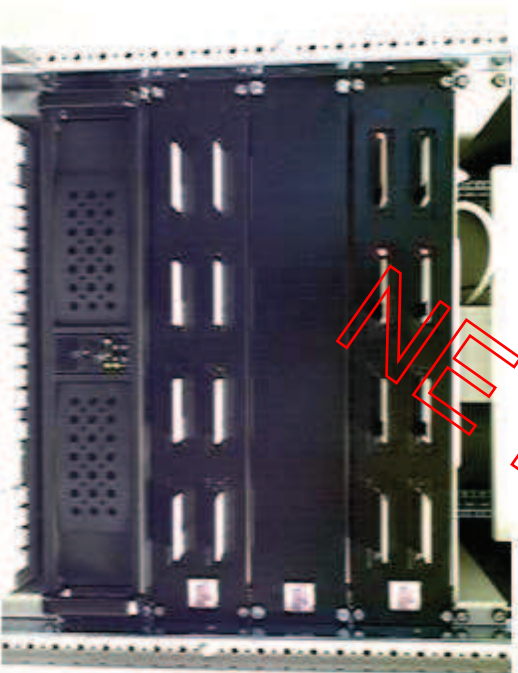
Mon bureau il y a en 2003/2004



La Plate-forme Actuelle

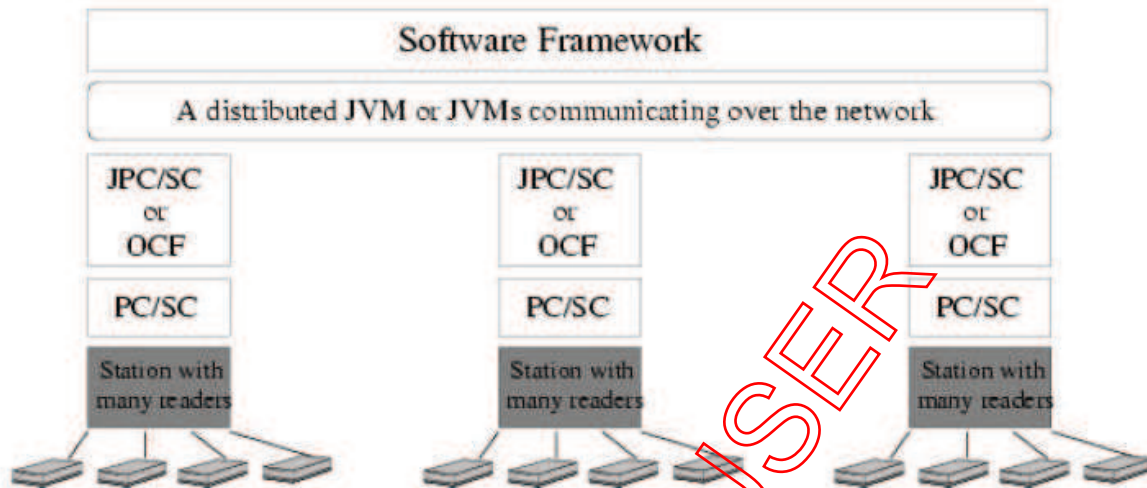


- 2 fois
 - 1 PC
 - 16 lecteurs de cartes
 - 1 point d'accès Wi-Fi
- Les deux machines sont connectées entre elles (réseau filaire)



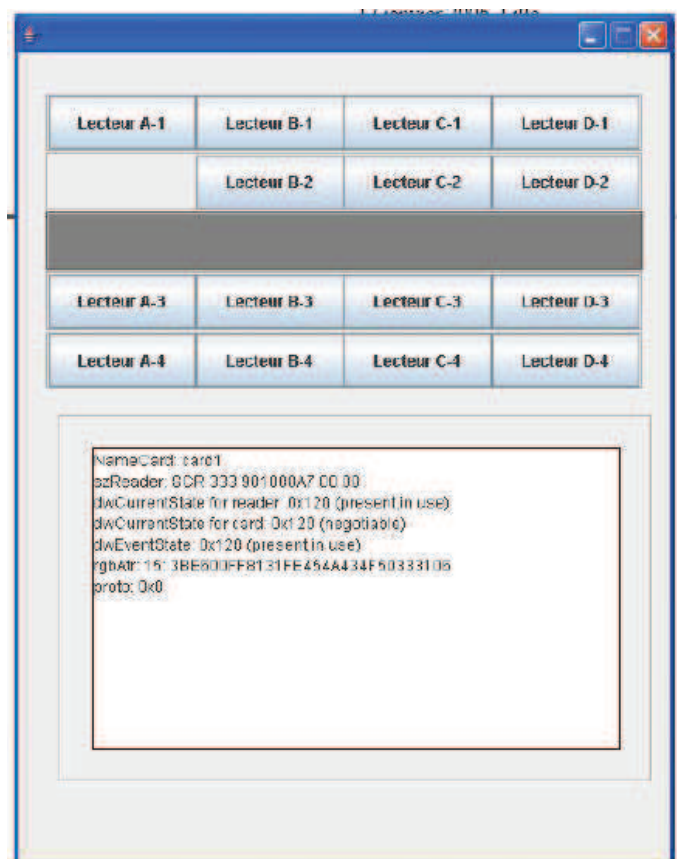
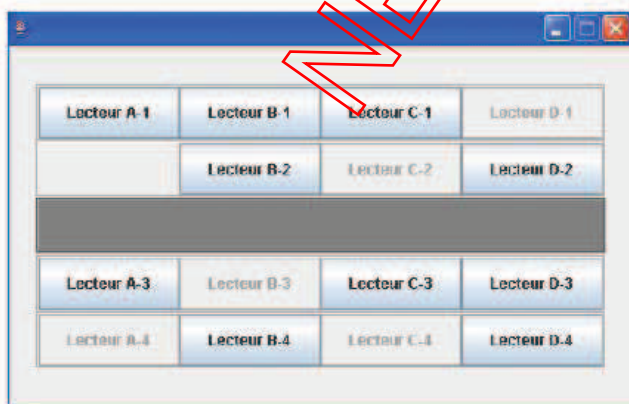


L'environnement logiciel



229

L'environnement d'administration



230

Première démonstration



Quelques benchmarks

9 Java Card (on) Fujitsu mb94r215b (FRAM)	122 min
9 GemXpresso Pro R3 E32PK	202 min
9 JCOP31bio	253 min
9 GemXpresso Pro R3 64PK	376 min
9 SmartC@fé Expert	389 min

Tab. 1 – Benchmarks sans secure channel

Scalabilité en cours d'expérimentation.

1 Java Card onto Fujitsu mb94r215b (FRAM) $\Rightarrow 18heures = 9 * 120min$

Application CBP/Air France

- On imagine (☺) que le *US Customs and Border Protection* (CBP) souhaite fouiller les fichiers passagers des compagnies aériennes comme Air France, pour les vols utilisant un aéroport US.

- Problème : la CEE interdit explicitement la diffusion d'informations confidentielles sur les passagers.

2003

Les Contraintes du Problèmes

- Code de fouille du CBP
 - Distribué sur les cartes
 - Doit demeurer confidentiel
- Fichier passagers d'Air France
 - Distribué sur les cartes
 - Doit demeurer confidentiel

2004

Etat Actuel et Travaux en Cours

- **État actuel**
 - La plate-forme est opérationnelle
 - Prix « Best innovative technology » à e-smart 2005
- **Travaux en cours**
 - Gestionnaire de swap sécurisé
- **Autres travaux liés :**
 - Aspects liés au ad hoc
 - une thèse en cours avec la DGA

Perspectives

- **Aspects logiciels**
 - Gestion des pannes
 - Assemblage de composants
- **Passage à l'échelle**
 - Avec plus de cartes:
 - 1000 lecteurs envisagés
 - Sera mené avec un industriel
 - (confidentiel pour l'instant)
 - Avec de vrais processeurs
 - Trusted Computing Group

Soutiens industriels

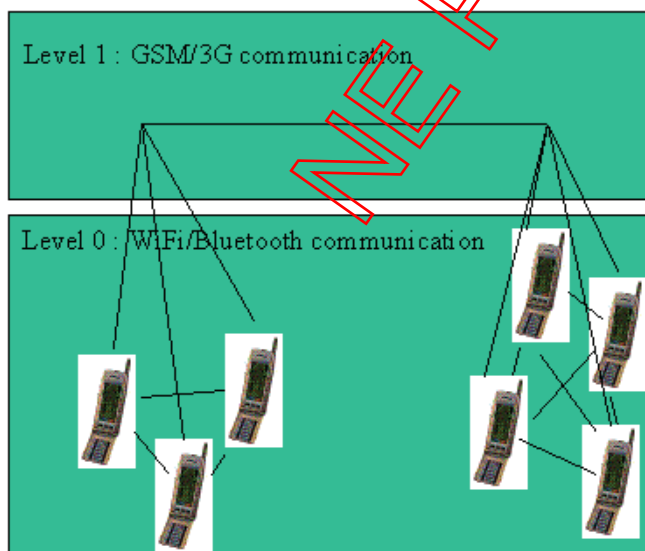
- Sun Microsystems
- IBM
- Oberthur
- Gemplus
- Schumberger
- Smartmount
- SCM
- Giesecke & Devrient GmbH

■ Fujitsu

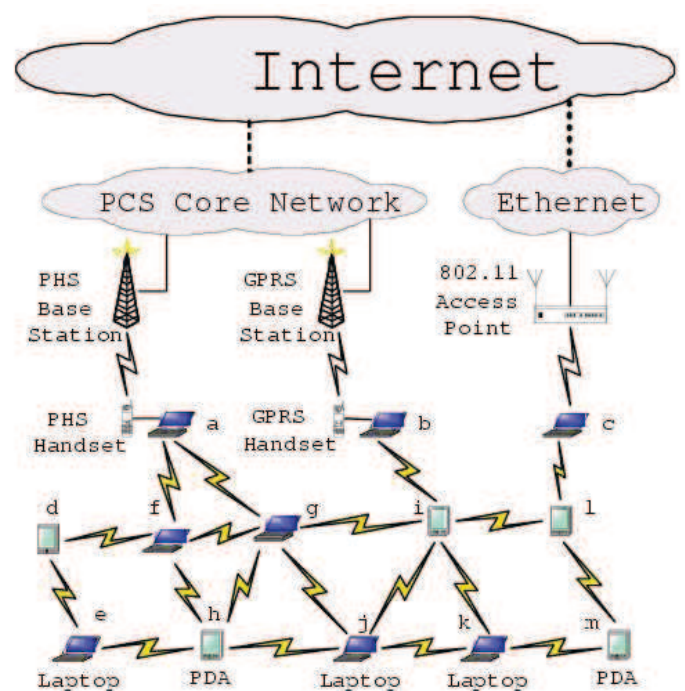


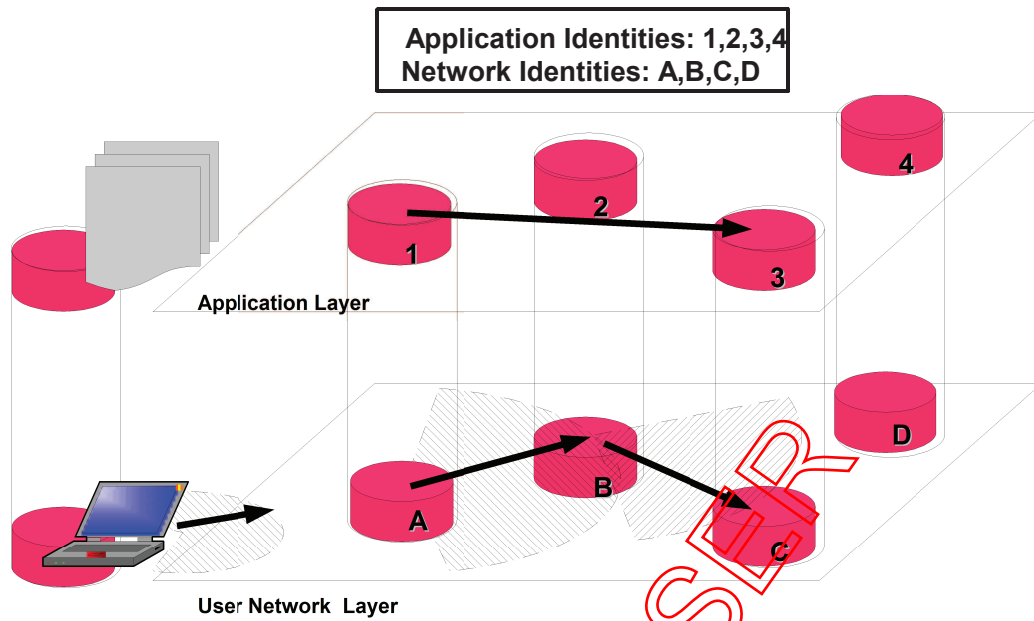
!37

La multilevel Java Card Grid (1/2)

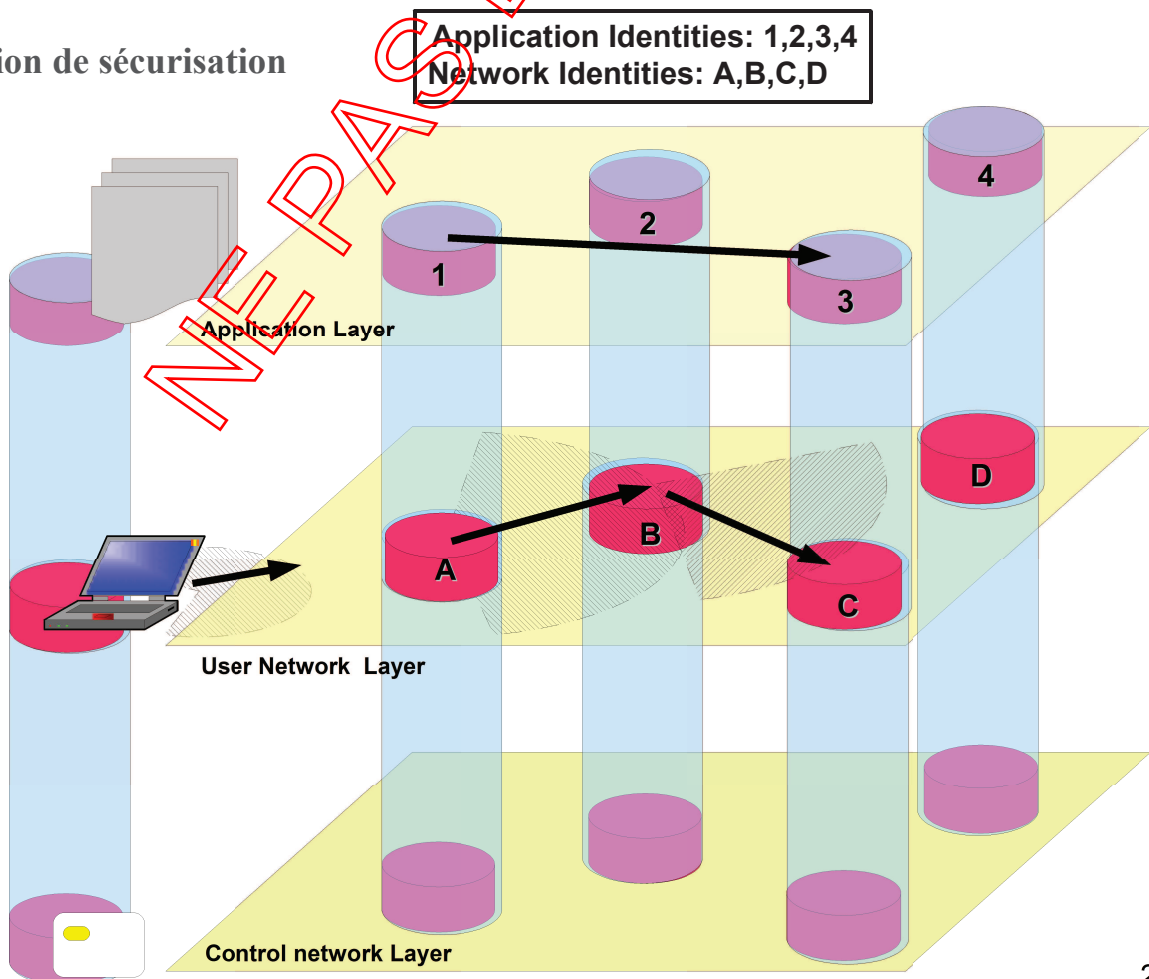


Multilevel Java Card Grid

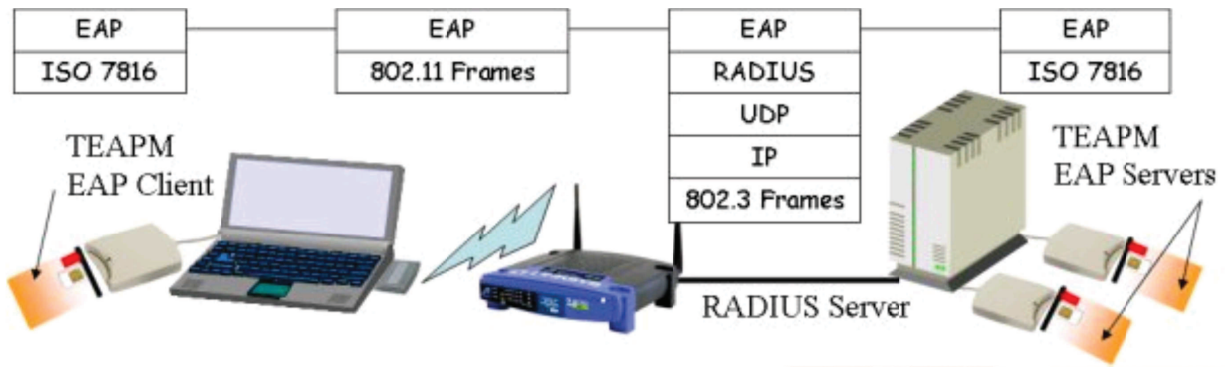




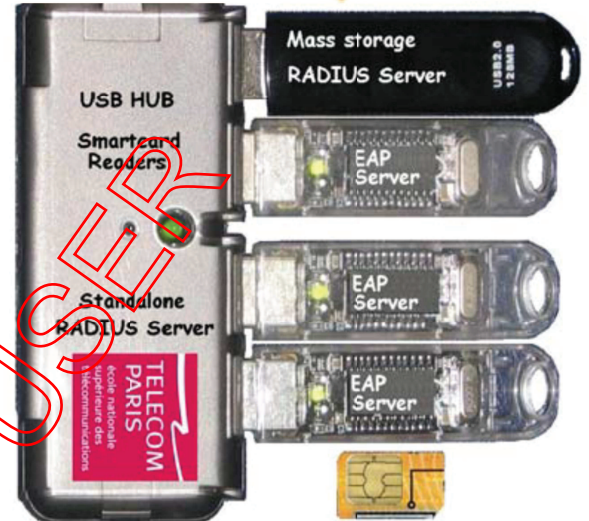
Une solution de sécurisation



Sécurisé le réseau WiFi avec EAP



EAP: Extensible Authentication Protocol



Réseaux domestiques

