Les cartes à puce pour tous

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

Conférence proposée par l'IREM, le CIJM, le TML et l'APMEP

30 janvier 2008

Plan

Mes activités

Qu'est-ce qu'une carte à puce ?

Historique

La carte à microprocesseur

Les technologies de communication

Quelques périphériques et terminaux cartes à puce

Quelques chiffres

Les applications
- La télécarte
- La carte bancaire
- Le porte-monnaie électronique
- La carte SIM

Les cartes du futur
- La Oyster Card

Université de Limoges et XLIM

Université de Limoges

890 enseignants-chercheurs
484 personnels administratifs et techniques
14 041 étudiants

177 enseignants-chercheurs
94 personnels administratifs et techniques
3007 étudiants

Faculté des Sciences et Techniques

ENSEIGNEMENT

CNRS

Xlim institut de recherche

350 personnes
dont 170 doctorants et post-doc

UMR 6172

RECHERCHE

Damien Sauveron

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
Site Jide
83 rue d'Isle
87000 Limoges, FRANCE

Email: Damien.Sauveron@unilim.fr
Web: http://damien.sauveron.fr/
Phone: +33 (0) 5 55 43 69 83
Fax: +33 (0) 5 55 43 69 77

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)

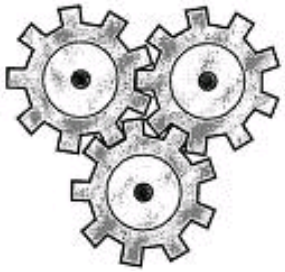
Organisateur de WISTP2007 (Héraklion) et WISTP2008 (Séville)
Vice président du groupe de travail de l'IFIP : ***Pervasive System Security***

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, ...) des informations

+



Smart = intelligente !
Pourquoi ?

La carte à puce, une innovation française ?

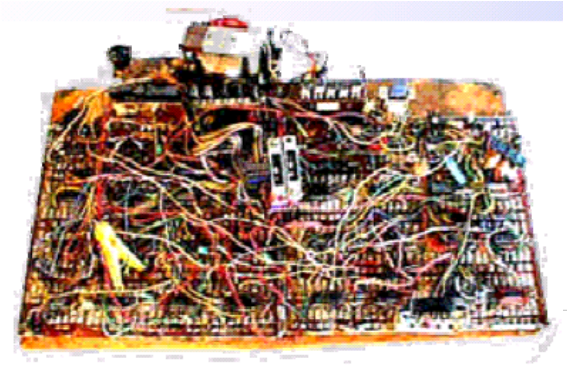
En France : OUI

Dans le reste du monde : NON

En 1968, deux Allemands **Jürgen Dethloff** et **Helmut Grötrupp** introduisent un circuit intégré dans une carte plastique

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

Entre 1974 et 1978, le français Roland Moreno, le père de la carte à puce dépose 47 brevets dans 11 pays.



Historique

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. »

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

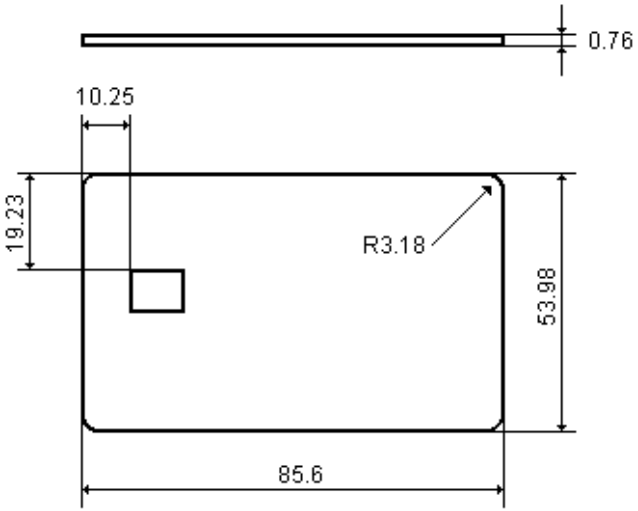
En 1983, apparition des premières cartes téléphoniques à mémoire

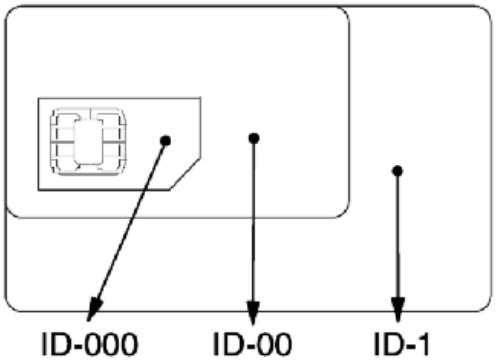
En 1984, adoption par le G.I.E carte bancaire de la « carte bleue »

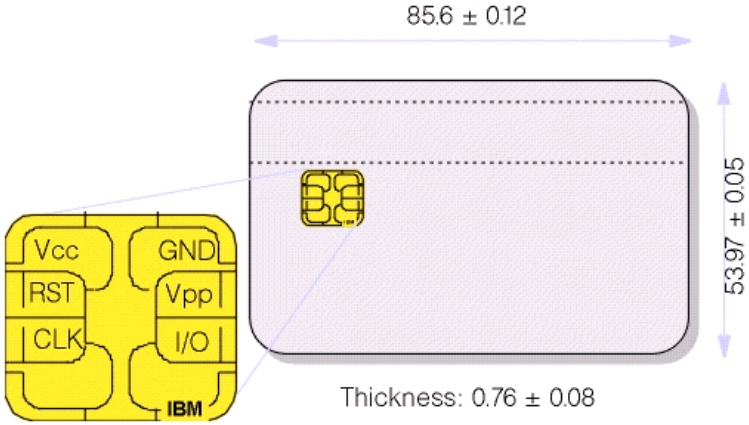
Historique

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

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

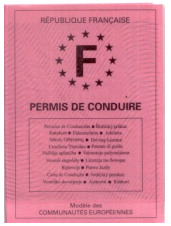






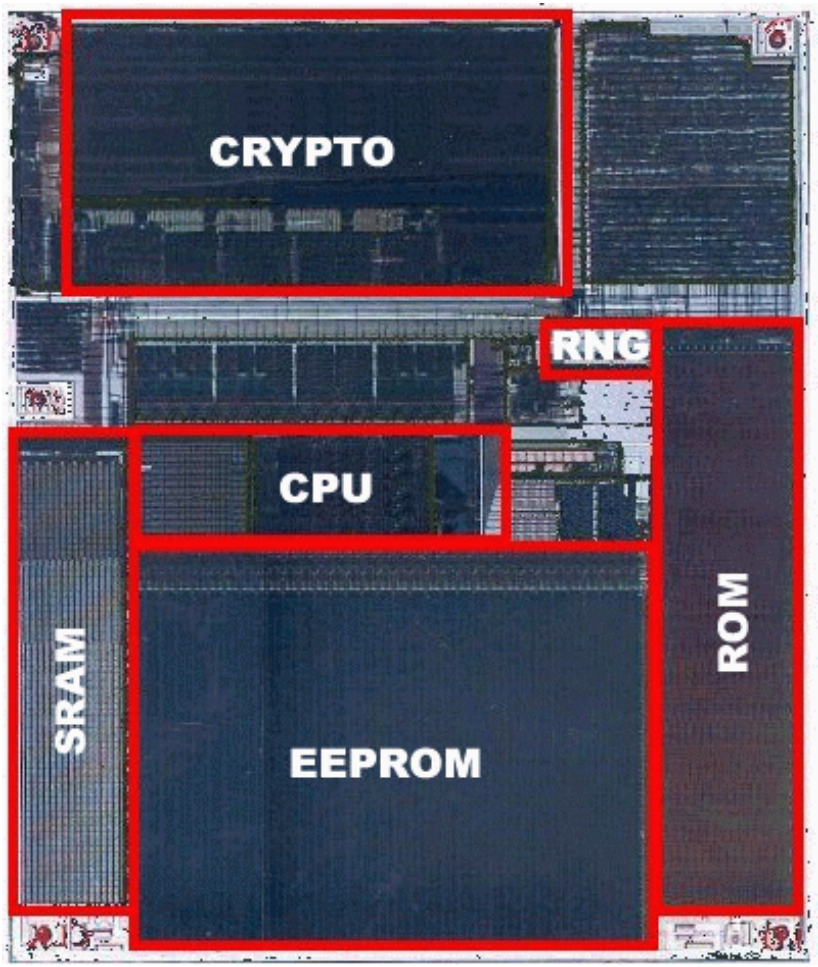
En 1997, apparition des premières Java Cards

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

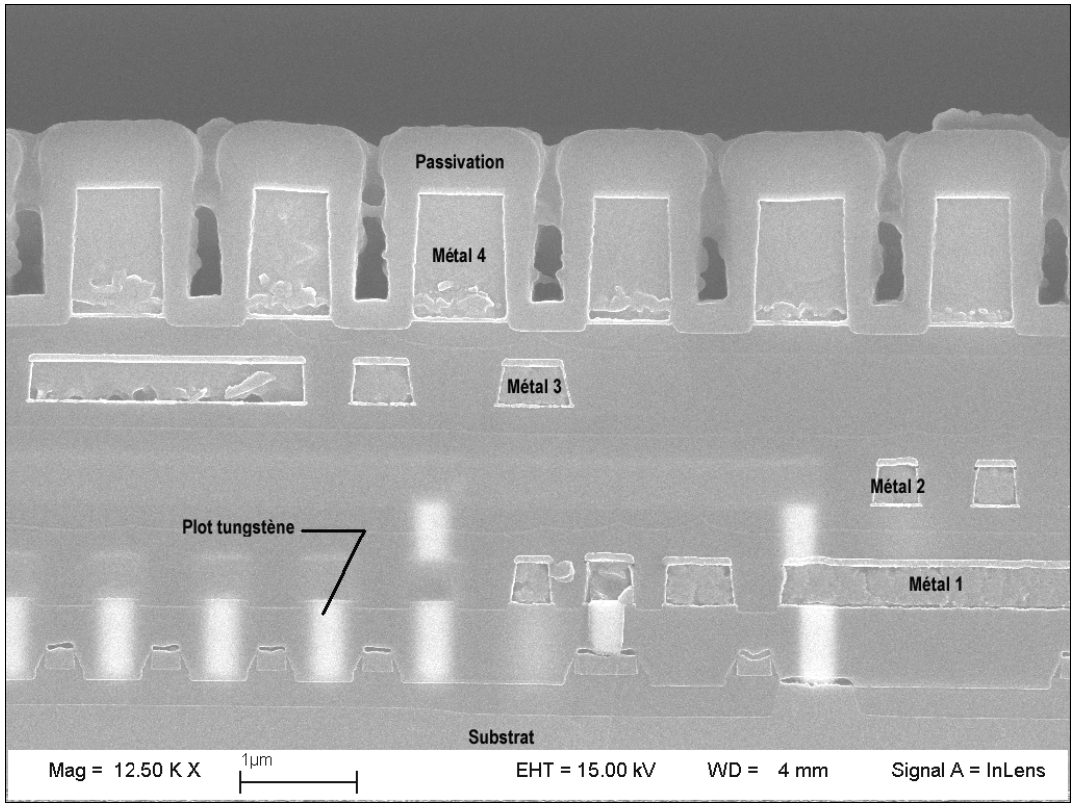


La carte à microprocesseur

Taille de la puce : 25mm² * 200µm (6µm)



Vue de dessus



Vue en coupe

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

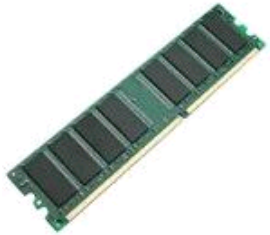
La carte à microprocesseur

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

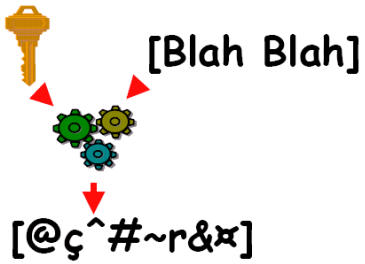
ROM : 32 à 256 Ko
Stocke le système d'exploitation et des données permanentes
Figée en usine

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



Coprocesseur cryptographique

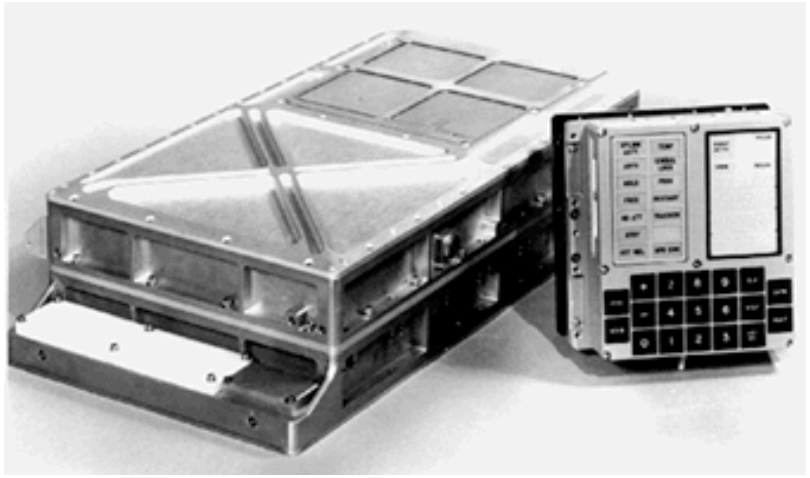


Générateur de nombres aléatoires (RNG)

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

les cartes à contact

versus

les cartes sans contact

versus

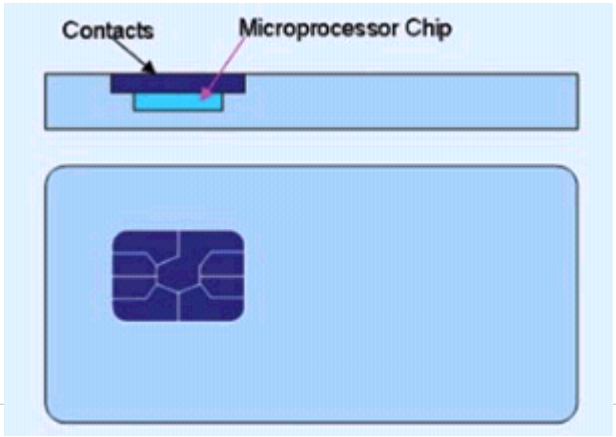
les cartes dual-interface

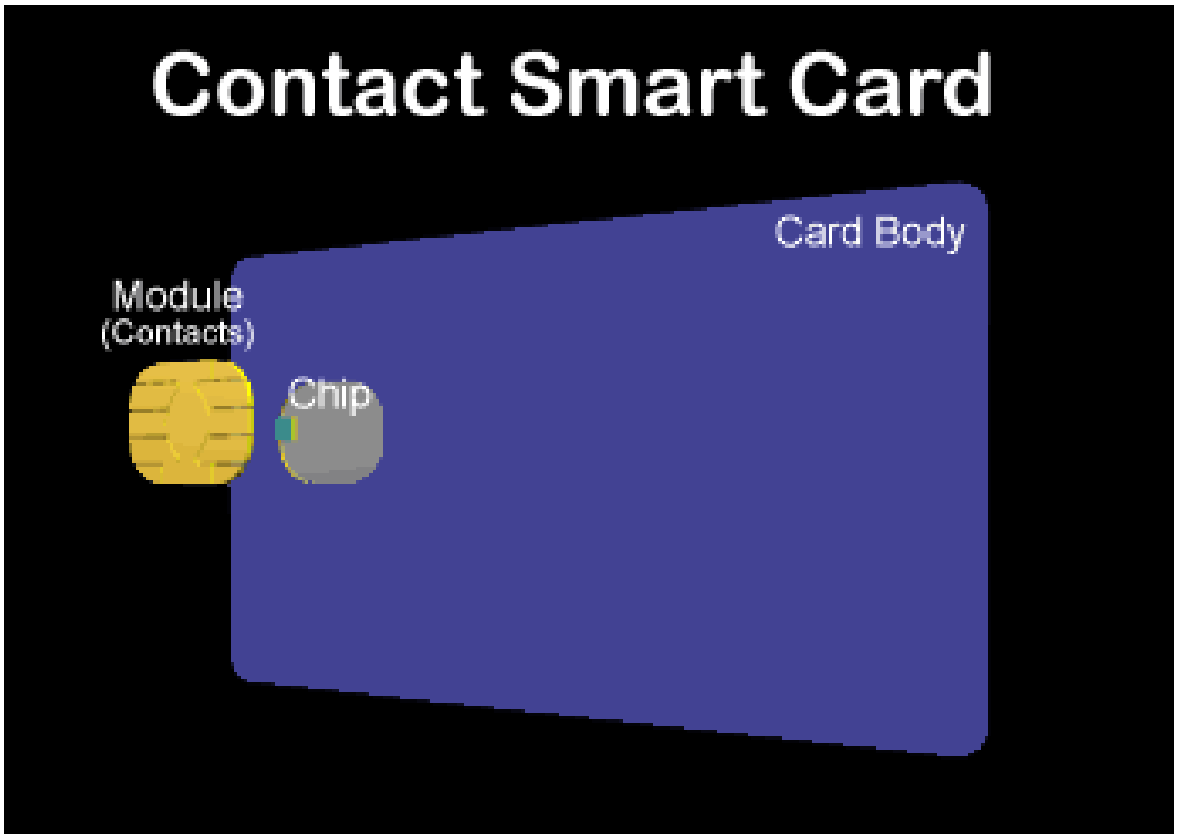
La carte à contact

Communication série via huit contacts
Energie fournie par le lecteur de carte
Suit le standard ISO 7816

Problèmes :

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



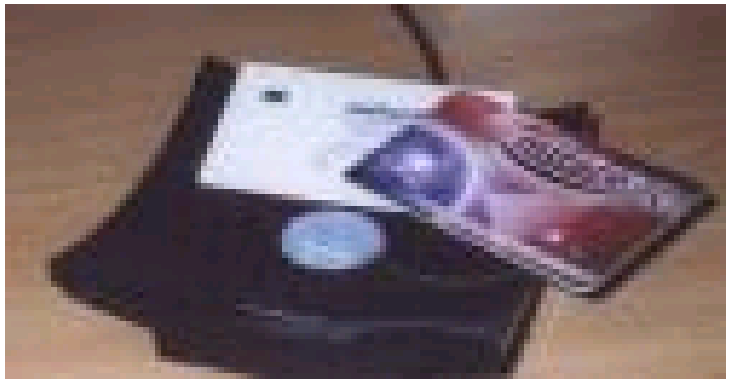


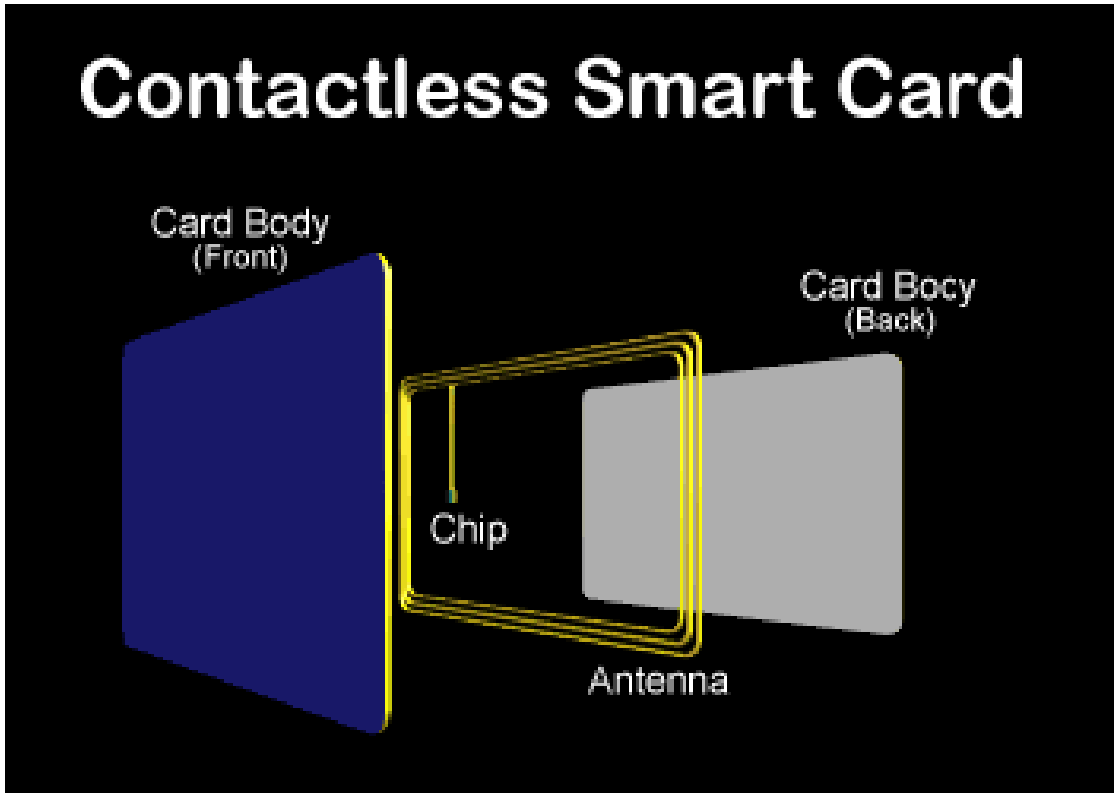
La carte sans contact

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 :

- la distance de communication limitée (environ 10 cm)
- le coût élevé



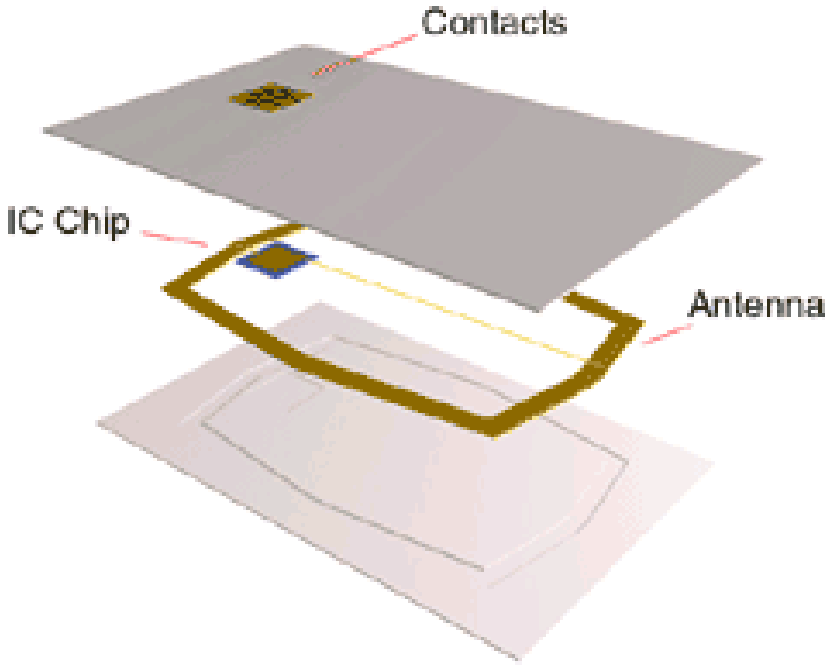


La carte combi

C'est une combinaison entre :

- la carte à contact
- et la carte sans contact

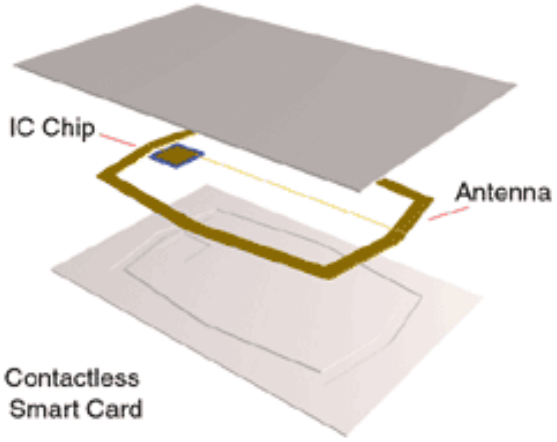
Ces deux possibilités de communication en font une carte « idéale ».



Quelques périphériques pouvant intégrer une puce sécurisée

Anneau Java

IButton



Dongles : Série, parallèle, USB

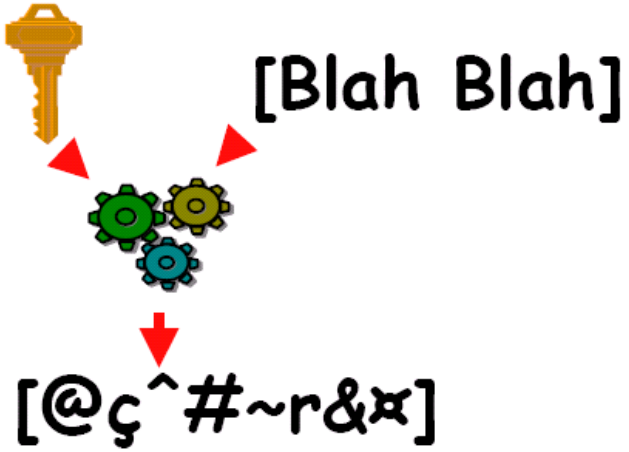
Les terminaux cartes

Contact / sans contact
Simple / complexe (clavier, LCD, multi-emplacement, biométrie, …)

Pourquoi utiliser la carte à puce ?

La sécurité du stockage

La sécurité du calcul



La portabilité

La personnalisation

La facilité d'utilisation

Le coût

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.

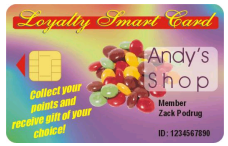
Le contrôle d'accés physique de personnes à des locaux, ...

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

Les "e-services"

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

Les applications de fidélité



Quelques chiffres

Livraison de cartes en 2007

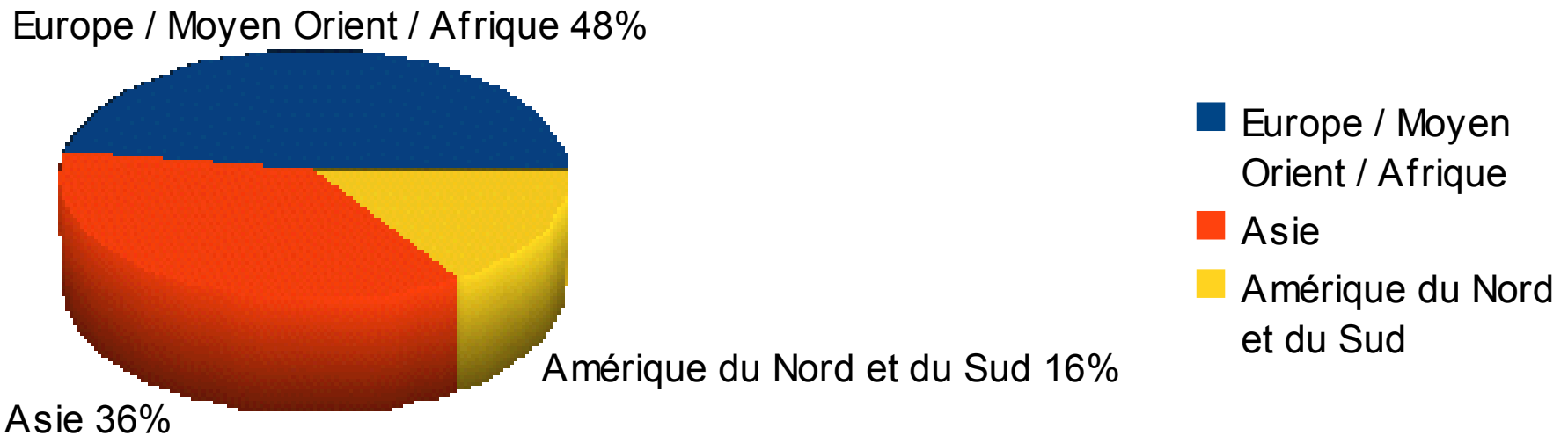
Cartes (Millions d'unités – Mu)		
Secteur	à Memoire	à Microprocesseur
Télécommunications	440	2600
Services financiers / Fidélité	30	500 (45)
Gouvernement / Santé	300	105 (45)
Transport	160	15 (15)
TV payante	-	70
Securité des Entreprises	20	20
Autres	10	15
Sous-Total	960	3325
Total 2007	4285	

( ) volume en sans contact

Répartition géographique du marché

Chiffres de 2005

Cartes %	
Zones Geographiques	à Microprocesseur
Europe / Moyen Orient / Afrique	48,00%
Asie	36,00%
Amérique du Nord et du Sud	16,00%
Total 2005	100,00%



Analyse du succès de la télécarte

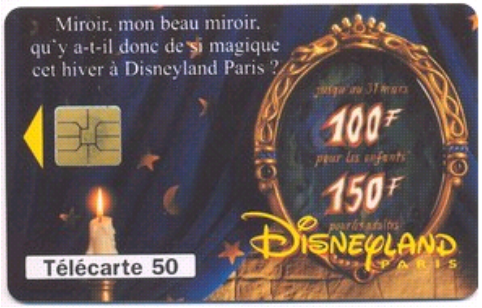
C'est une carte prépayée.
Elle contient des jetons (et non de l'argent)

Les raisons de sa réussite :

- Fin du vandalisme des cabines téléphoniques

- Temps de communication +50%

- Support publicitaire

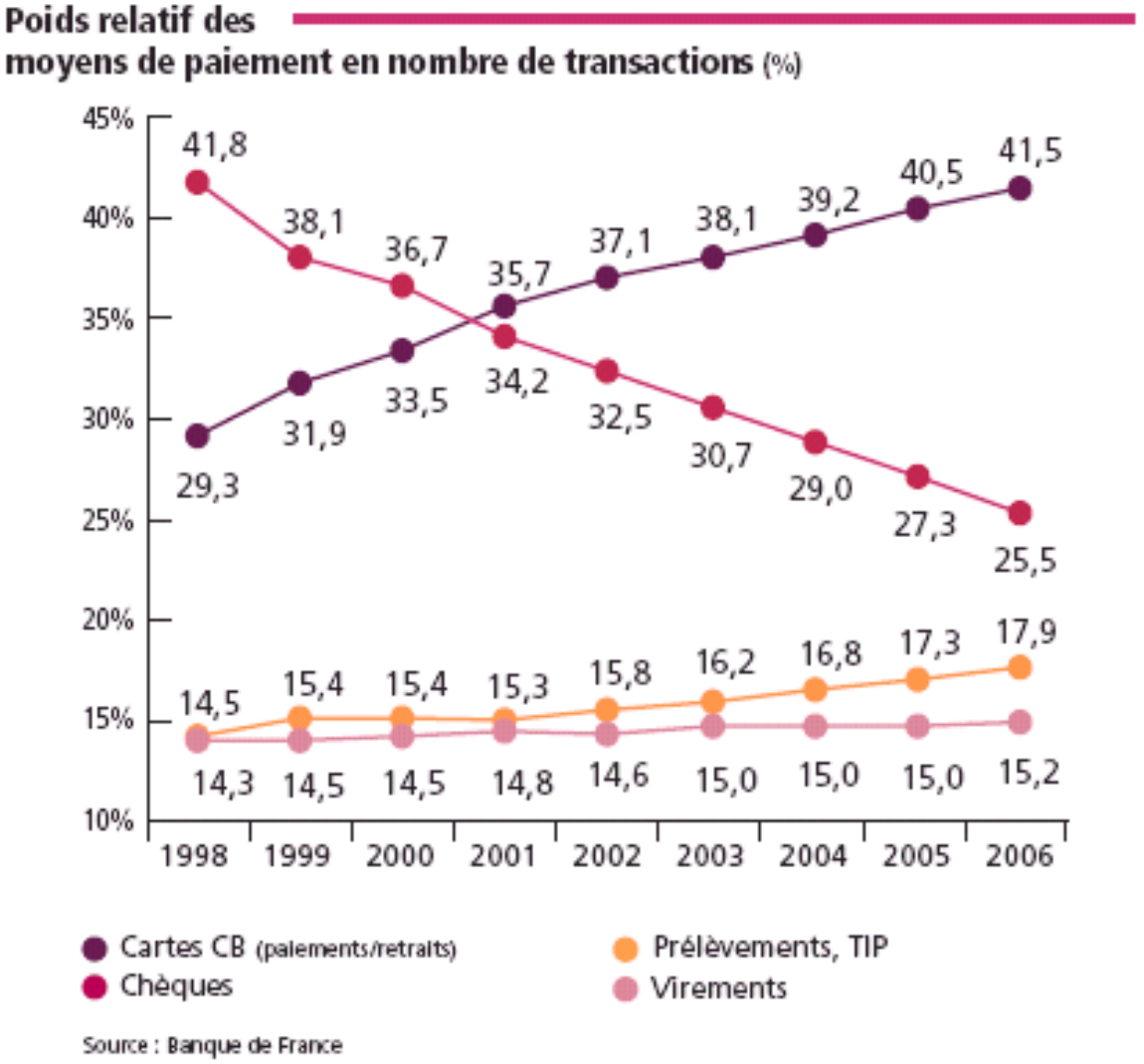


- Avance de trésorerie

Applications de paiement

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

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



Applications de paiement : Techniques

Authentification mutuelle carte et terminal commerçant

QUI ES-TU ?

QUI ES-TU ?

Signature Électronique

Contrôle du PIN

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

Applications de paiement (Exemple : GIE Cartes Bancaires)

53,6 millions de cartes

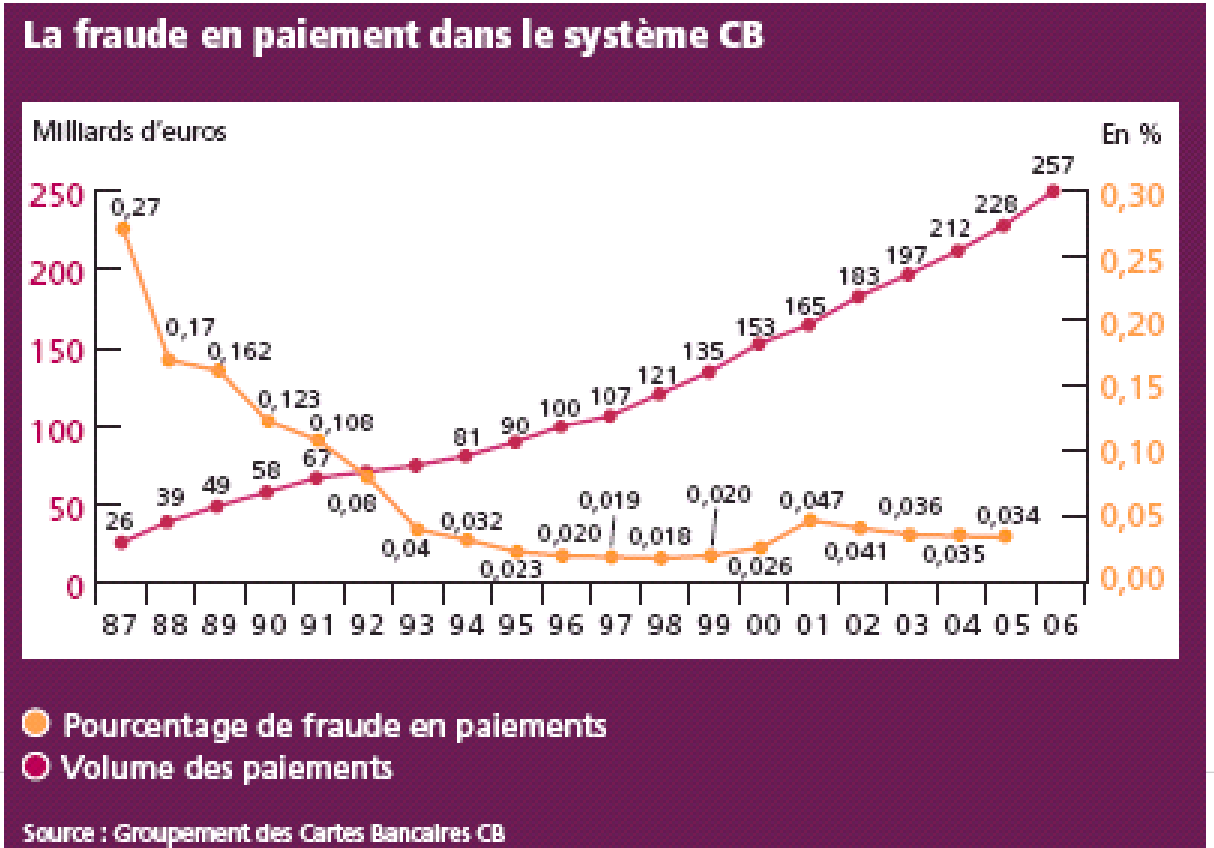
1,2 million de points d'acceptation :

- 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

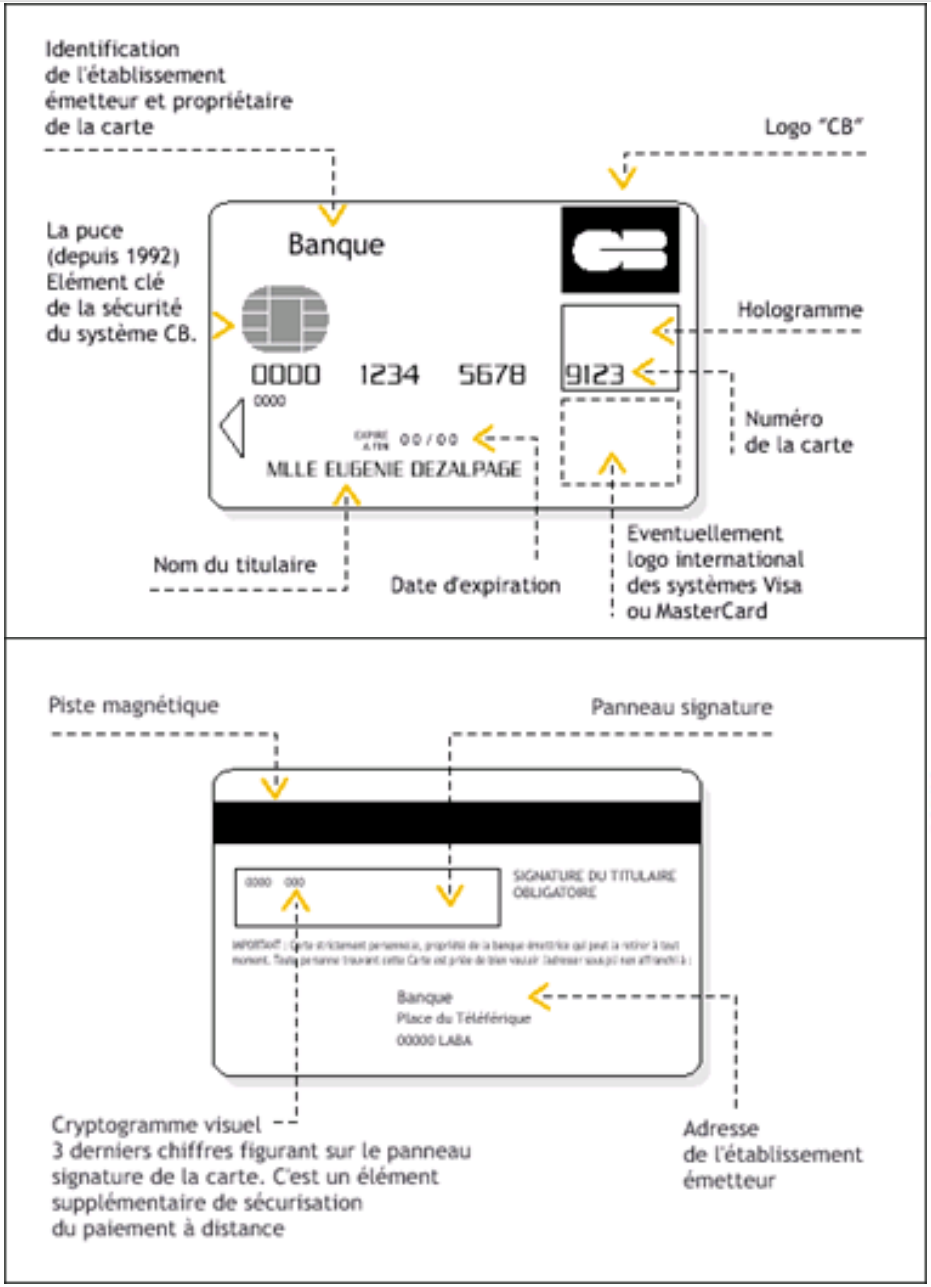
1 Distributeur Automatique de Billets pour 1200 habitant en France

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

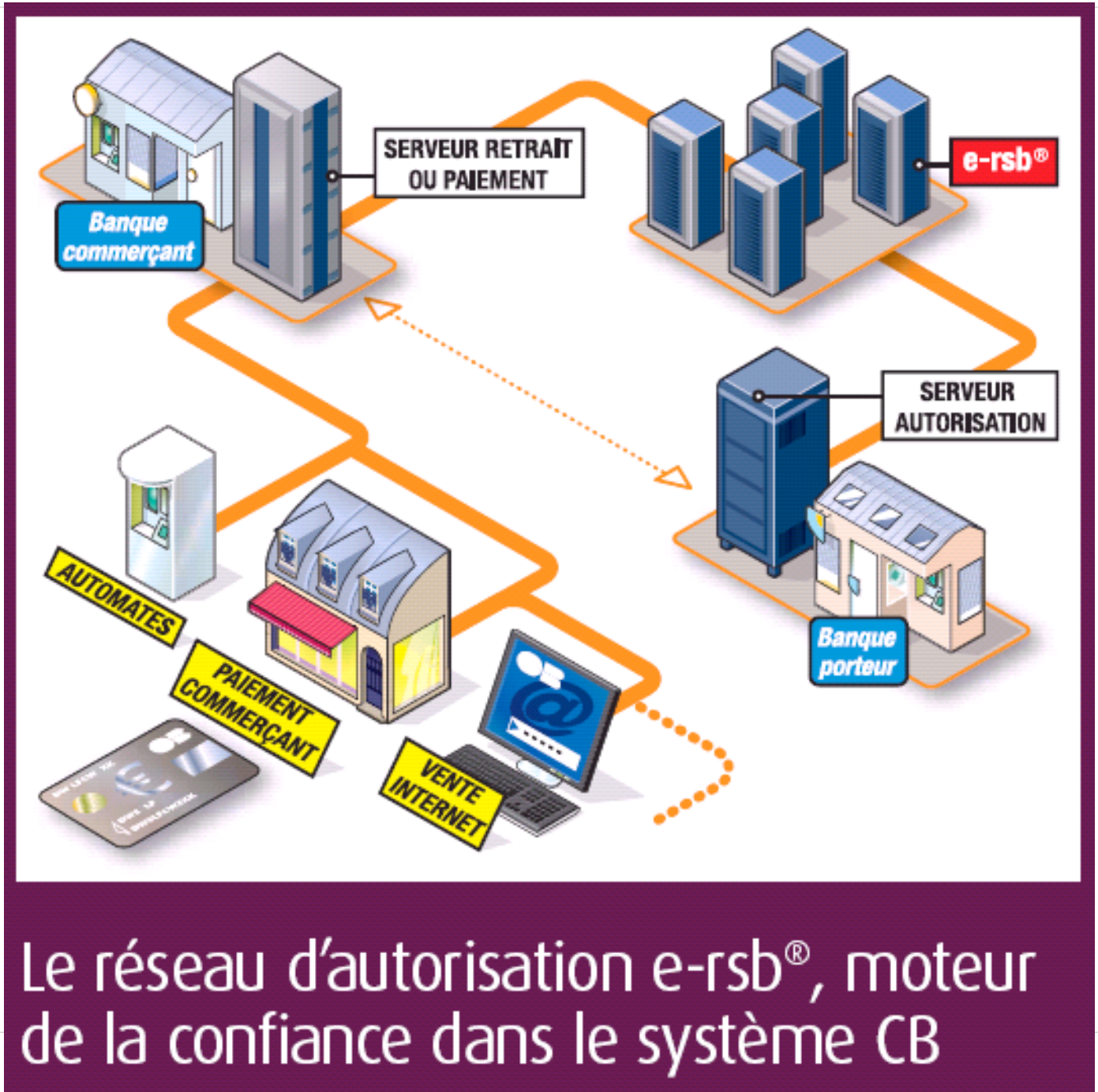
260 M€ de fraudes du à la piste magnétique contrefaite et utilisée depuis l'étranger (en 2003)



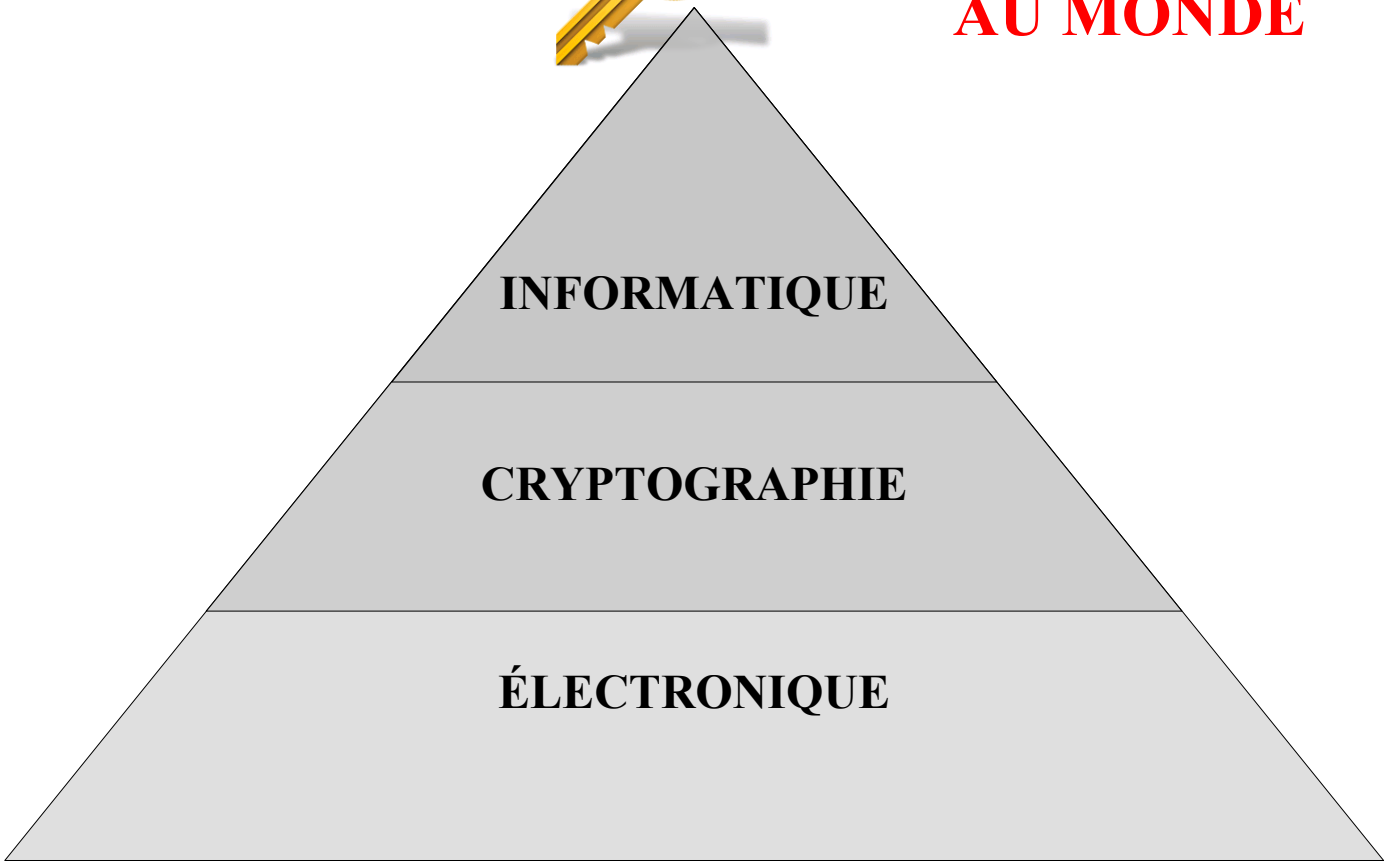
La carte bancaire



Utilisation de la carte bancaire

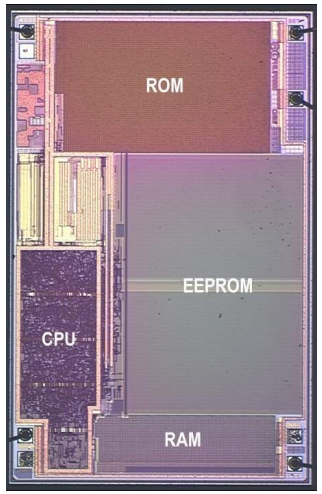


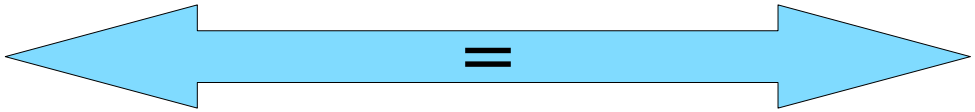
LE PÉRIPHÉRIQUE LE PLUS SÉCURISÉ AU MONDE



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

La carte à puce et sa sécurité





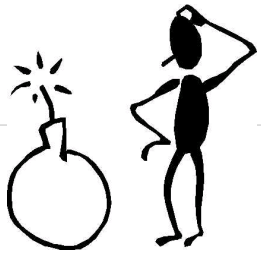
La Yescard : une carte « pirate » qui dit OUI à toutes les transactions !
Une remise en cause la sécurité de la carte à puce ?

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.

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**

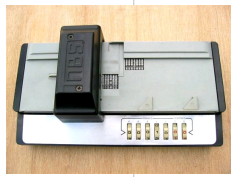
- Dans le cas de l'utilisation d'une carte bancaire, **la preuve est électronique et fournie par le PIN** !

- Dans certains pays qui n'utilisent pas le PIN

la puce est interrogée
OU
la piste magnétique de la carte est lue
OU
une empreinte physique de la carte est faîtes

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 prétent 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 !

Le porte-monnaie électronique (e-Purse)

Remplace les pièces et les petites coupures de billets

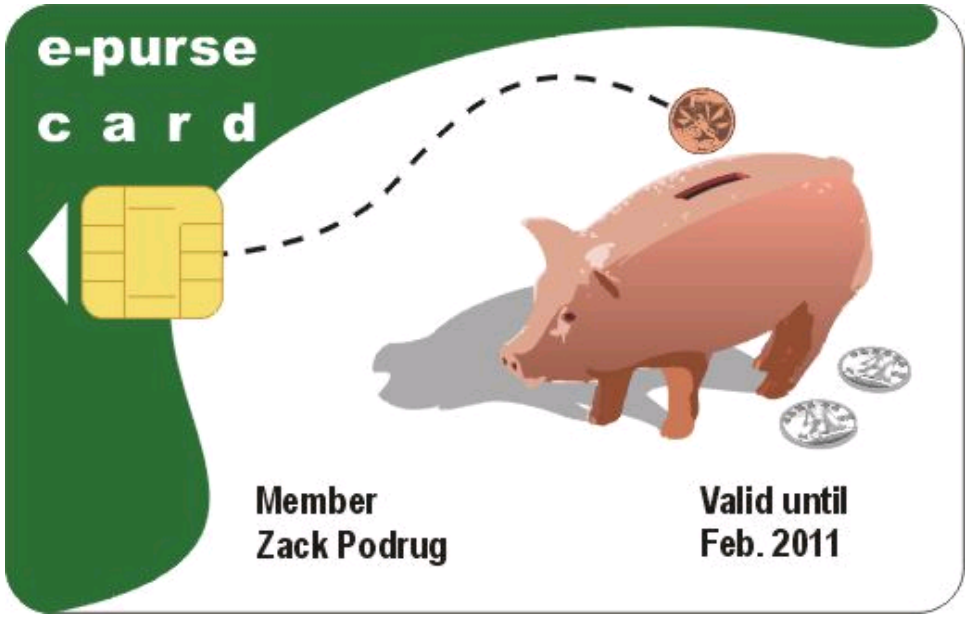
Carte rechargeable dans des guichets (ou chez le commerçant)

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

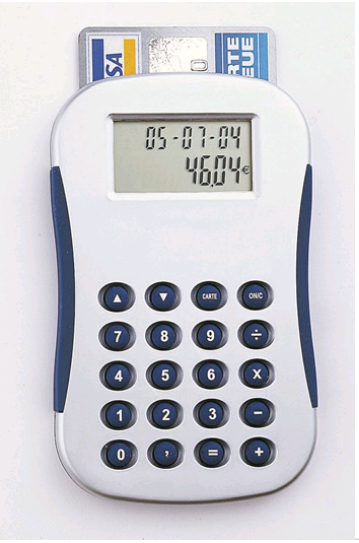


Le porte-monnaie électronique (e-Purse) : Avantages

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



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

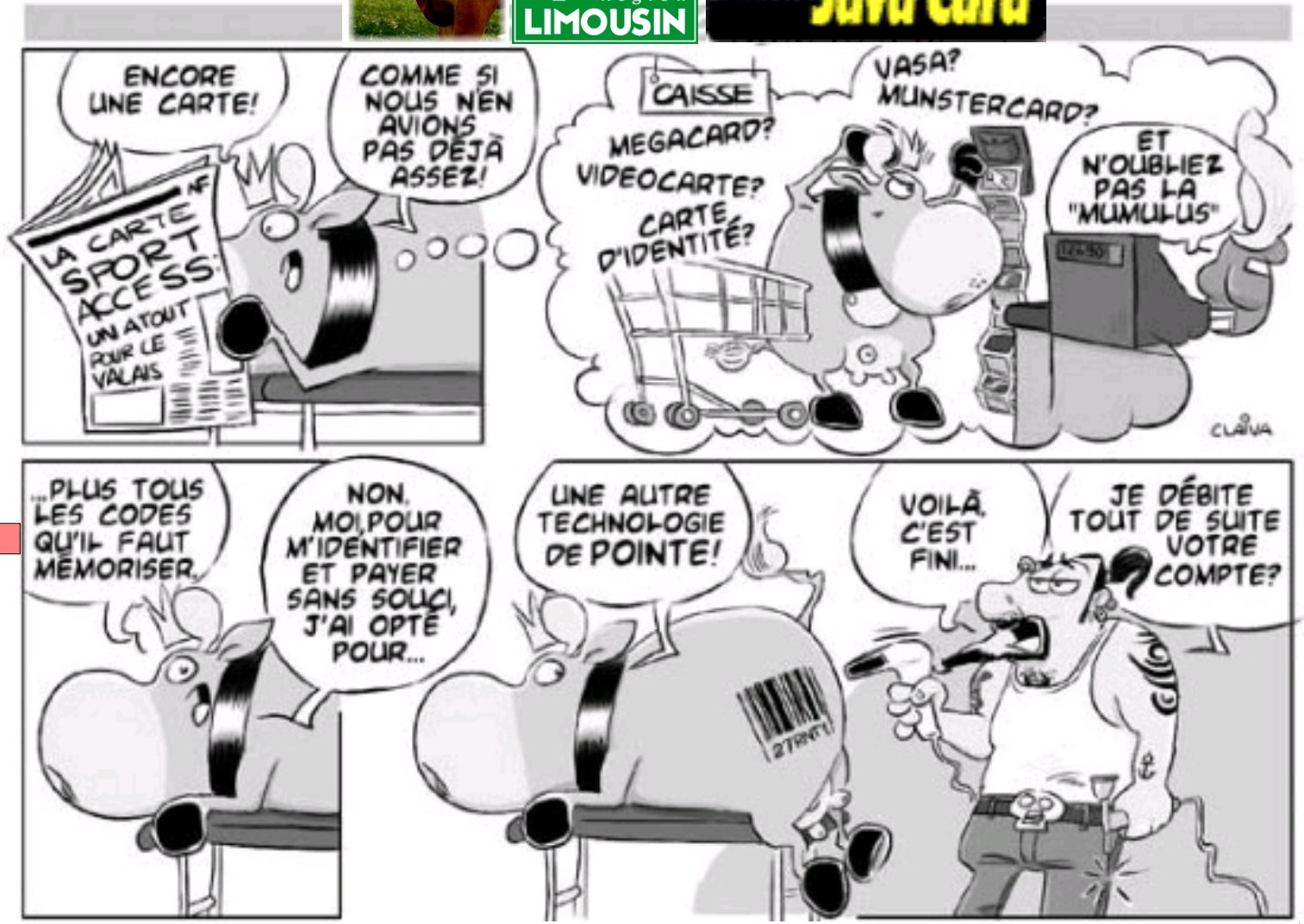
Bientôt, le paiement ?

Le futur de la carte à puce

Les cartes à puce du futur

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

Région LIMOUSIN



Comment résoudre ce problème ?

La carte multi-applicative

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 séparé 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.

Le difficile équilibre

Sécurité Fonctionnalités

LOI DE MOORE

Navette Spatiale
+2000

2010

x 250,000
TPD

Les Pyramides de Gizeh
-2000

1997

x 4000

Java Card
Programmes

Milieu du
Paléolithique
-200,000

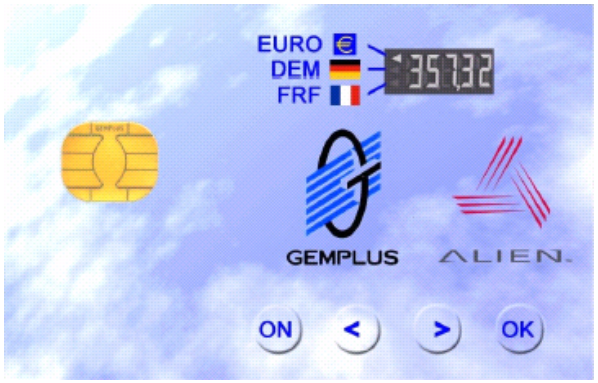
1979

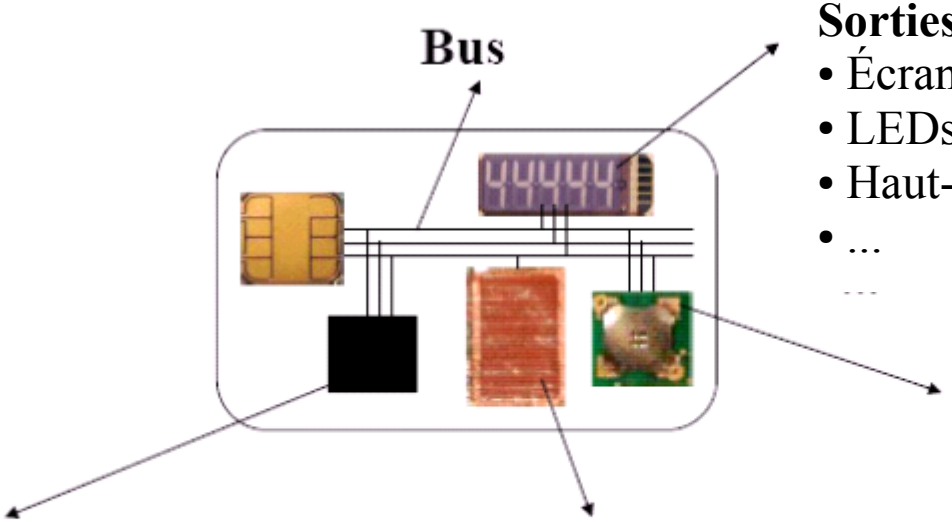
Smart card
ISO 7816

- Différents facteurs de forme
- Différentes interfaces (USB, ...)
- Connectivité IP
- Différentes Machines Virtuelles
- Système d'exploitation multi-tâches
- Support de la Biométrie
- Support de la Web

Les cartes du futur

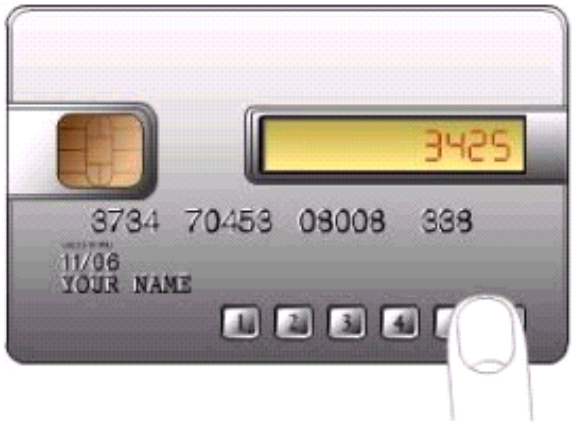
Quelques évolutions matérielles :





Sorties
- Écran
- LEDs
- Haut-parleur
- ...

Entrées
- Clavier
- Capteurs
- Micro
- ...



Amélioration des performances
- Microprocesseur
- Mémoire
- ...

Alimentation
- Batterie
- Capteur solaire
- ...

Questions ?

Crédits

Je remercie toutes les personnes à qui j'ai pu emprunter des images pour illustrer cet exposé. Ces personnes restent bien évidemment les seuls détenteurs des droits sur ces images.

Bonus

http://www.clipcardparking.com/