

Université de Boumerdès

Faculté de Technologie



Département Ingénierie des Systèmes Électriques

Spécialité: Electronique des systèmes embarqués

Module: Cartes à puces

Chapitre 1: Généralités sur les cartes à puce

Mme Belkacem Samia

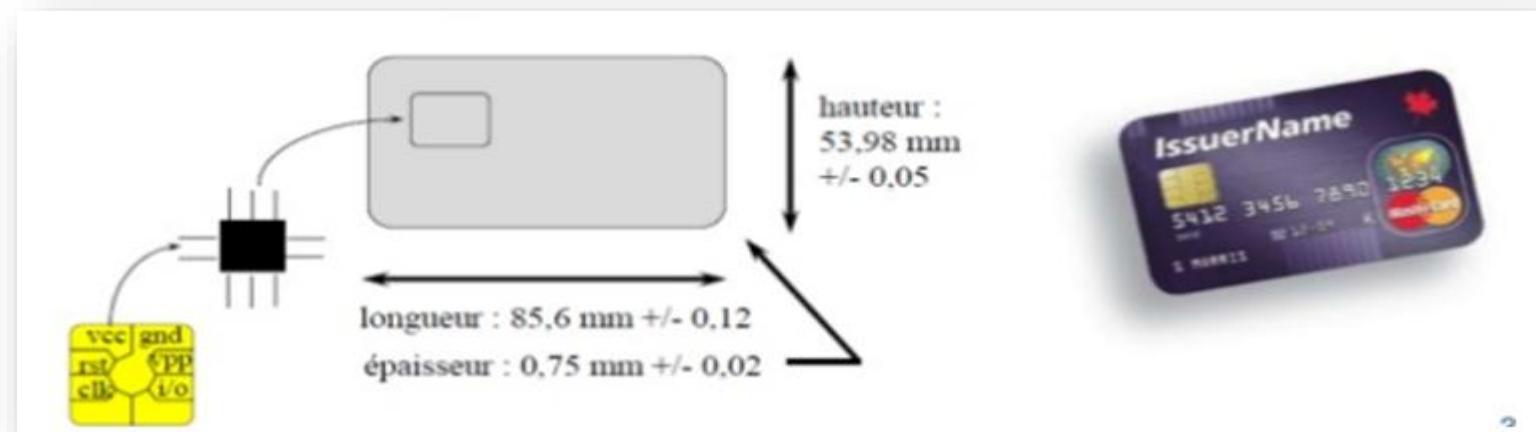
2021/2022

1) Qu'est ce qu'une carte à puce?

- Une carte à puce est constituée de **3 éléments**:
 1. une carte en matière plastique avec ou sans bande magnétique
 2. un module électronique supportant les contacts électroniques
 3. un circuit intégré en silicium

1) Qu'est ce qu'une carte à puce?

- Un morceau de plastique, papier ou carton de la taille d'une carte de crédit
- Un circuit électronique capable de manipuler (stocker, calculer) des informations
- Dimensions: quelques centimètres de coté et moins d'un millimètre d'épaisseur
- d'une surface de l'ordre du cm² et d'une épaisseur d'une fraction de mm



Exemple:

En Algérie, la carte nationale biométrique est constituée de deux puces : la première comporte des informations administratives et des informations sur son titulaire et la seconde comporte une application d'authentification du titulaire.

2) Historique

1950

Les premières cartes ont été développées en plastique avec une bande magnétique dans les années 50. La bande magnétique représente le support de stockage des informations.



1968

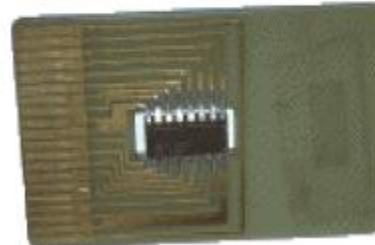
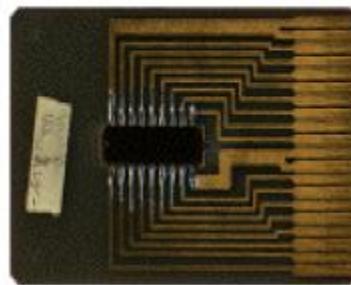
Deux allemands Jürgen DETHLOFF et Helmut GRÖTRUPP introduisent un circuit intégré dans une carte plastique

2) Historique

1974

- Le brevet du français **Roland Moreno** (le père de la carte à puce), déposé en 1974 et complété en 1975
- Le principal brevet sur les cartes à mémoire, avec composants électroniques mais sans microprocesseur.

Premières cartes en verre époxy à circuit intégré :



2) Historique

1977

- Le français Michel Ugon, dépose les deux principaux brevets sur les cartes à microprocesseur.
- En 1979 la première carte à microprocesseur avec deux composants(CP8).
 - Possède un up 8 bits
 - Avec une EPROM



3) Historique

1984

- Apparition des premières cartes téléphonique à mémoire



1987

- La norme des réseaux mobiles de 2^egénération (GSM) introduit la notion de module de sécurité (une carte à puce SIM –Subscriber Identity Module).
- En raison du succès de la téléphonie mobile, les télécommunications deviennent le premier marché de la carte à puce.

3) Historique

1988

Les standards de base des cartes à puces (ISO 7816) sont introduits

- Format carte de crédit
- Définition des contraintes physiques supportables (chaleur, humidité...)



3) Historique

1997

■Apparition des premières Java Cards

- Java Card est une carte asynchrone de type Smart Card. Donc elle possède une mémoire EEPROM. Les cartes standard ont une EEPROM de taille variant de 1 Ko à 128 Ko. Tandis que la carte Java Card est distinguée d'une EEPROM de taille égale à 256 Ko due à la présence de la machine virtuelle.
- Elle est souvent utilisée comme carte de fidélité



3) Historique

La carte à puce aujourd'hui

- Aujourd'hui : plus de 5 milliards de cartes
- **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)
- **Enseignement** (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 doté
d'un cryptopuce pour la génération des clés et le stockage de la clé privée).

3) Historique

- Aujourd’hui : plus de 5 milliards de cartes
 - Monétique: Carte bancaire: Groupement Cartes Bancaires, nouvelles cartes EMV, etc.
 - Identification: (Cartes d'identité nationales (**eIDen Belgique**), **E-passeports(août 2006 en France)**, Passeport biométrique (depuis la fin Juin 2009))
 - **Enseignement(carte d'étudiant et/ou de restauration)**
 - **éléphoniemobile(carte SIM)**
 - **Secteur médical(carte Vitaleen France, carte SISen Belgique).**
 - **Titre de transport(PasseNavigo à Paris, Oyster à Londres**
 - **Sécurité informatique(authentification forte et signature électronique): carte doté d'un cryptoprocesseur pour la génération des clés et le stockage de la clé privée).**

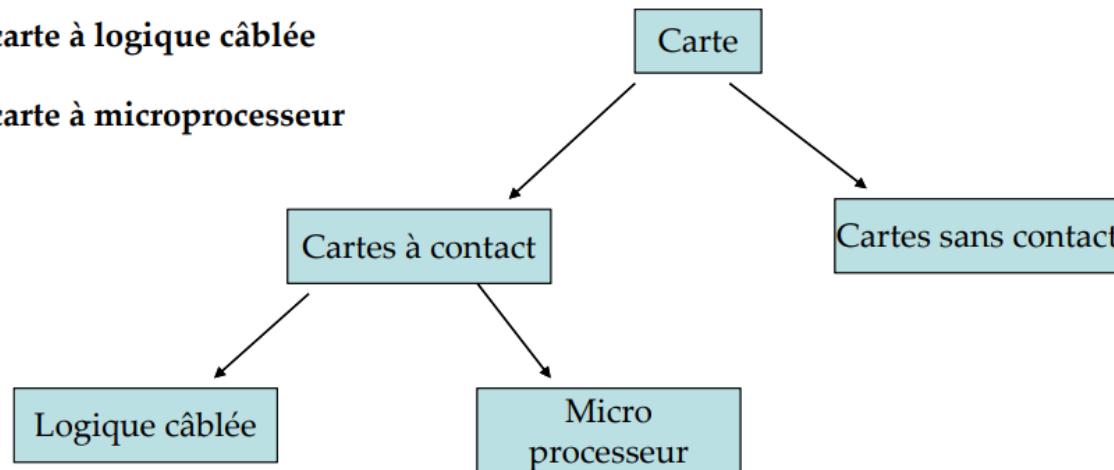
3) Historique

- ***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).

4) Types de cartes

Famille de produits/1

- carte à logique câblée
- carte à microprocesseur



4) Types de cartes

- Il existe différentes familles de cartes à puce:
 - Les cartes à mémoire simple servent de simple support de stockage ;
 - Les cartes à mémoire avec logique câblée possèdent un support de stockage et sont capables d'effectuer des opérations de logique simple ;
 - Les cartes à microprocesseur sont des cartes possédant une mémoire programmable ainsi que des fonctionnalités permettant des opérations logiques avancées (possédant un microprocesseur et son environnement (mémoires, entrées/sorties).)

4) Types de cartes

3. 1) Les cartes à bande magnétiques (magnetic strip card)

- 1950 enregistrements magnétiques des données numériques
- Les premières cartes apparues
- Ne sont pas sécurisées, plusieurs équipements peuvent lire le contenu d'une carte magnétique
- On peut trouver le code bar imprimé sur la carte badge

4) Types de cartes

3.2) Carte à mémoire

- mémoire simple (sans processeur) accessible en lecture sans protection, mais l'écriture peut être rendue impossible
- carte de consultation

- ☞ Premier modèle de cartes à puce
- ☞ Majorité des cartes vendues dans le monde en 1999

Elle possède :

- ☞ *une puce mémoire* de 1 à 4 Ko
- ☞ *une logique cablée non programmable*

Avantages :

- sa technologie simple
- son faible coût (1\$)

Inconvénients :

- sa dépendance vis-à-vis du lecteur de carte
- “assez” facile à dupliquer

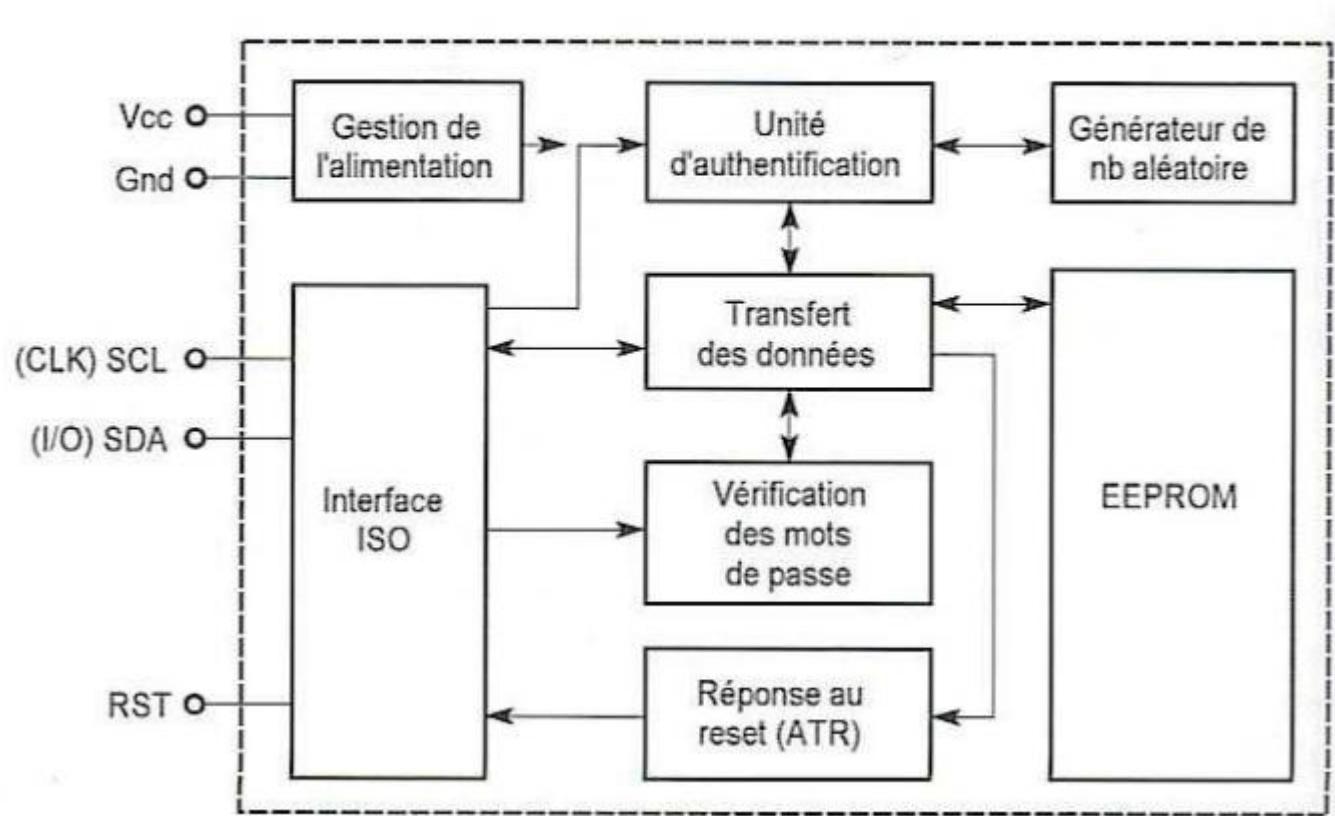
4) Types de cartes

3. 2) carte à logique câblée

- Fonctions simples fixées par les circuits électroniques entre la mémoire NVM (Non Volatile) et l'interface extérieure,
- Exemple: carte de parking, de cinéma

4) Types de cartes

Exemple d'une carte à logique câblée sécurisée



4) Types de cartes

3.3) Carte à logique programmée

Les cartes à microprocesseur dites aussi cartes “intelligentes”. Cette “intelligence” vient du fait que contrairement aux cartes à mémoire les cartes à microcontrôleur peuvent être programmées pour effectuer des décisions logiques complexes.

La carte est programmée par un logiciel enregistré dans la ROM (c'est le système d'exploitation et les applications)

The diagram illustrates the characteristics of programmed logic cards. It features a vertical list of bullet points on the left, with a large curly brace on the right grouping several items together. The grouped items are aligned under the heading "dans le même circuit".

- Cartes à puce intelligentes
- Comportent un microcontrôleur :
 - UC
 - PROM
 - RAM
 - EEPROM
 - interface d'E/S
 - crypto processeur
- Processeur : 16 ou 32 bits
- EEPROM : de 1Ko à 128 Ko (256 Ko pour une Java Card ou une Basic Card)
- Interface série: UART simplifié

Cartes à microcontrôleur

dans le même circuit

4) Types de cartes

3.3) Avantage de la logique programmée

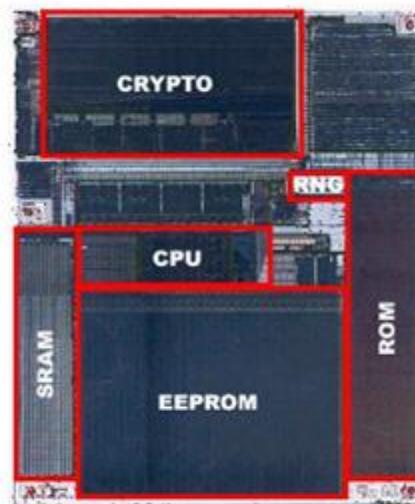
- + A base de microprocesseur
- + Utilisation de composants ayant une grande densité d'intégration → carte électronique de faible encombrement.
- + Les composants utilisés sont programmables : l'application peut être mise au point ou totalement modifiée.

4) Types de cartes

Carte à microprocesseur

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

- ☞ *Microprocesseur* (CPU) : 8, 16 ou 32 bits (à architecture RISC ou pas)
- ☞ *ROM* : 16 à 64 Ko
- ☞ *EEPROM/Flash/FeRAM* : 16 à 64 Ko
- ☞ *RAM* : 1 à 2 Ko
- ☞ Coprocesseur cryptographique
- ☞ Générateur de nombres aléatoires (RNG)



Avantage : le coût acceptable pour tant de sécurité (entre 1\$ et 20\$).

Microcontrôleur encarté (processeur+mémoires)

Processeurs 8-32 bits

Sécurisée

Peut traiter les données

Taille de la mémoire élevée

4) Types de cartes

Microcontrôleur pour carte

- Fondé sur la technologie **M.A.M.** (Microprocesseur Auto-programmable Monolithique)
 - microprocesseur + bus + mémoires réunis sur un même substrat de silicium (technologie de 0,7 à 0,35 microns)
 - peut être «re-programmé» par l'écriture de programmes en mémoire non-volatile
- Éléments de sécurité
 - composant inaccessible
 - détecteurs de conditions anormales
- Types de microprocesseur
 - 8-16-32 bits (+ coprocesseur cryptographique)
 - SGS-Thomson, Siemens, Motorola, Hitachi, NEC, etc.
- Types des mémoires
 - ROM jusqu'à 64 Ko, RAM jusqu'à 2 Ko
 - EEPROM jusqu'à 32 Ko

4) Types de cartes : Modes de communication

Deux classements possibles

les cartes à mémoire



versus

les cartes à microprocesseur

les cartes à contact

versus



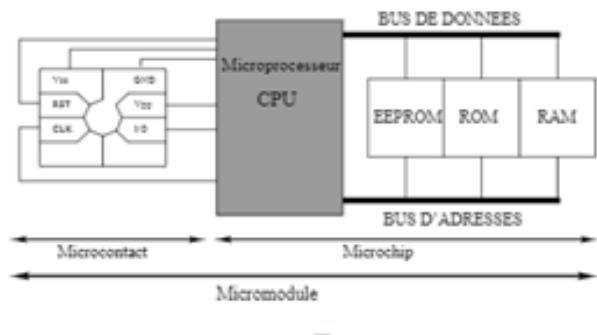
les cartes sans contact

versus

les cartes hybride

5) Carte à contact

- S'adapte au standard **ISO 7816**
- *Communication série via huit contacts* \Rightarrow insertion dans un lecteur de carte



Problèmes :

- insertion et le retrait de la carte dans le lecteur cause des frottements
- orientation de la carte dans le lecteur

5)Carte à contact

Signification des contacts

C1 Vcc
C2 RST Reset
C3 CLK
C4 RFU (*Reserved for future use*)
C5 GND
C6 Vpp (anciennes générations d'EEPROM)
C7 I/O (bi-directionnel, en mode *half-duplex*)
C8 RFU (*Reserved for future use*)



Caractéristiques électriques

Symbol	Minimum	Maximum	Unité
Vcc	4,75	5,25	V
Icc		200	mA

5) Carte à contact

Normes principales des cartes à puces à contact

ISO, International Organisation for Standardisation). C'est le plus important standard définissant les caractéristiques des cartes à puce qui fonctionnent avec un contact électrique. Sachant que 15 normes sont proposées pour les cartes à contact, nous décrivons brièvement ici uniquement les 7 premières normes.

- La norme ISO 7816-1 précise les caractéristiques physiques de la carte
- La norme ISO 7816-2 définit la position et le brochage des contacts de la carte
- La norme ISO 7816-3 définit les niveaux électriques utilisés pour le dialogue avec la carte
- La norme ISO 7816-4 définit les commandes de base des cartes à puce

5)Carte à contact

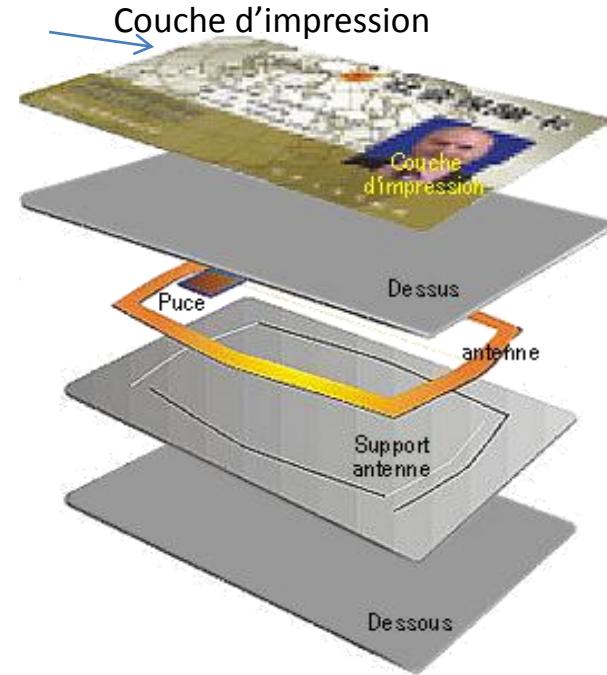
Lecteur de carte à puce à contact

- Une carte à puce est connectée à l'ordinateur via un **lecteur de carte** qui obtient des informations de la carte à puce et transmet en conséquence les informations à l'ordinateur.



6)Carte sans contact

- Apparue en **1948** pour distinguer les avions amis de ceux ennemis, l'identification par fréquence radio RFID (Radio frequency Identification)
- Fonctionnant avec une **puce** et une **antenne**
- Permet la reconnaissance du porteur sans qu'il soit nécessaire d'introduire la carte dans un lecteur.
- La lecture se faisant à distance (**quelques centimètres au plus**).
- Energie fournie par le champ magnétique émis par le lecteur



6)Carte sans contact

Famille des cartes à puce sans contact

- Cartes à puce à couplage très proche (quelques mm) (Close Coupling) : couvertes par les normes ISO 10536
- Cartes à puce à couplage de proximité (proximity coupling) (quelques cm) couvertes par les normes ISO 14 443.
- Cartes à puce à couplage éloigné ou de voisinage (vicinity coupling) (quelques dizaines de cm) couvertes par les normes ISO 15 693

6)Les cartes sans contact

Lecteur de carte à puce sans contact

- Lorsque la carte arrive dans la zone d'influence d'une antenne de lecteur et qu'elle se trouve donc suffisamment et correctement alimentée, elle effectue une reset interne et attend une commande de ce dernier.
- Le lecteur commence par l'envoie une commande appelée Request à laquelle la ou les cartes situées dans sa zone d'influence répondent par Answer To Request (ATR).
- La carte sélectionnée envoie au lecteur une réponse de type ATS (Answer To Select) qui l'informe du type de carte avec laquelle il doit s'attendre de dialoguer.

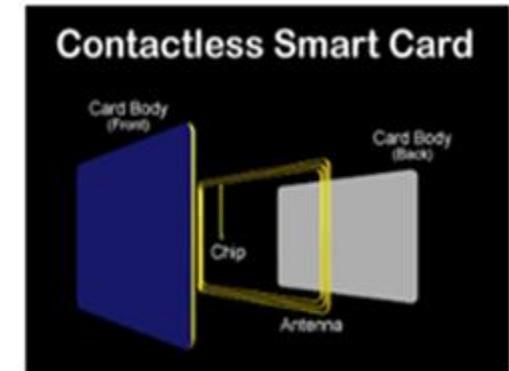
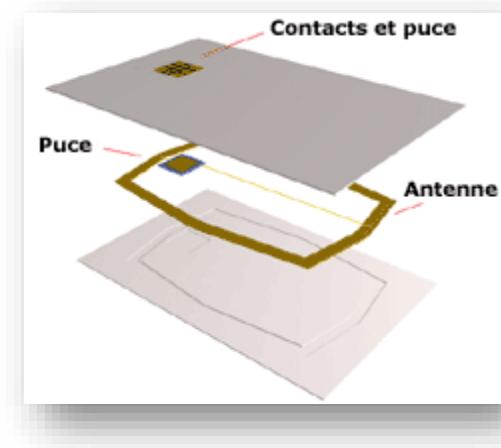
6)Les cartes sans contact

Normes principales des cartes à puces sans contact

- La norme ISO 14443-1 précise les caractéristiques physiques de la carte
- La norme ISO 14443-2 indique comment télé-alimenter la carte et décrit les signaux électriques pour établir le dialogue avec la carte
- La norme ISO 14443-3 définit les phases d'initialisation des échanges et de gestion de collision
- La norme ISO 14443-4 définit le protocole de transmission

7)Les cartes hybrides

- Embarquent 2 puces, la première reliée aux contacts, la deuxième à l'antenne.
- On fusionne donc deux cartes en une.
- Ces cartes sont le meilleur compromis car elles offrent les avantages des deux types de carte à puce.
- Cependant elles héritent de leurs inconvénients en plus d'un prix beaucoup plus élevé.
- Communication via une antenne dans la carte
- Récupère son énergie d'un couplage capacitif ou d'un couplage inductif
- Suit le standard ISO 14443



7)Les cartes hybrides

Avantages/Inconvénients des cartes à puce sans contact

C'est une combinaison entre :

- ☞ la carte à contact
- ☞ et la carte sans contact

Ces deux possibilités de communication en font une carte “idéale”.

- Les principaux avantages des cartes sans contact sont :
 - Absence de contacts susceptibles d'être salis ou endommagés
 - Elles ne doivent pas être insérées dans un lecteur
- Mais ce système a aussi des inconvénients :
 - Transfert assez lent
 - Distance de communication est limitée
 - Temps de transaction est de l'ordre de 200ms ➔ limite des données à échanger
 - Le cout élevé
 - Coût de fabrication plus élevé
 - Les cartes peuvent être endommagées quand elles sont pliées (contiennent plusieurs composants répartis dans la carte)

8) Applications

- Les cartes à puce sont principalement utilisées comme:
 - Moyens d'identification personnelle (carte d'identité, badge d'accès aux bâtiments, carte d'assurance maladie, carte SIM)
 - Moyens de paiement (carte bancaire, porte-monnaie électronique)
 - Preuve d'abonnement à des services prépayés (carte de téléphone, titre de transport)

8) Applications

- En 2020, l'Inde mettra en œuvre des cartes à puce qui seront à la fois des cartes nationales d'identité et des porte-monnaies électroniques.
- En Malaisie, depuis 2001, la carte à puce est à la fois un permis de conduite, une carte nationale d'identité, et une carte d'accès aux services de santé et des services bancaires. L'identification des citoyens est assurée au moyen d'une photographie renforcée par le codage des empreintes digitales.
- Le **contrôle d'identité** peut aujourd'hui s'appuyer sur de multiples preuves biologiques fournies par la numérisation des empreintes digitales, de l'image de l'iris et la reconnaissance vocale, chacune de ces techniques étant convertie en un format numérique pour **l'authentification** de la personne.

9) Acteurs du marché

Entreprises dans le domaine de la carte à puce



9) Acteurs du marché

L'industrie de la carte à puce implique différents acteurs :

- Les *fondeurs* fabriquent le hardware (les puces de silicium)
- les *encarteurs* fabriquent la carte proprement dite en intégrant la puce de silicium dans une carte plastique
- Les *développeurs* de système d'exploitation ou d'applets conçoivent les logiciels qui s'exécutent dans la carte à puce elle-même.
- Enfin, les *fabricants de lecteurs* fournissent aux intégrateurs et développeurs d'applications le matériel nécessaire pour s'interfacer avec la carte à puce.

Le Français **Gemalto**, acteur majeur du secteur.

9) Acteurs du marché

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

9) Acteurs du marché

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

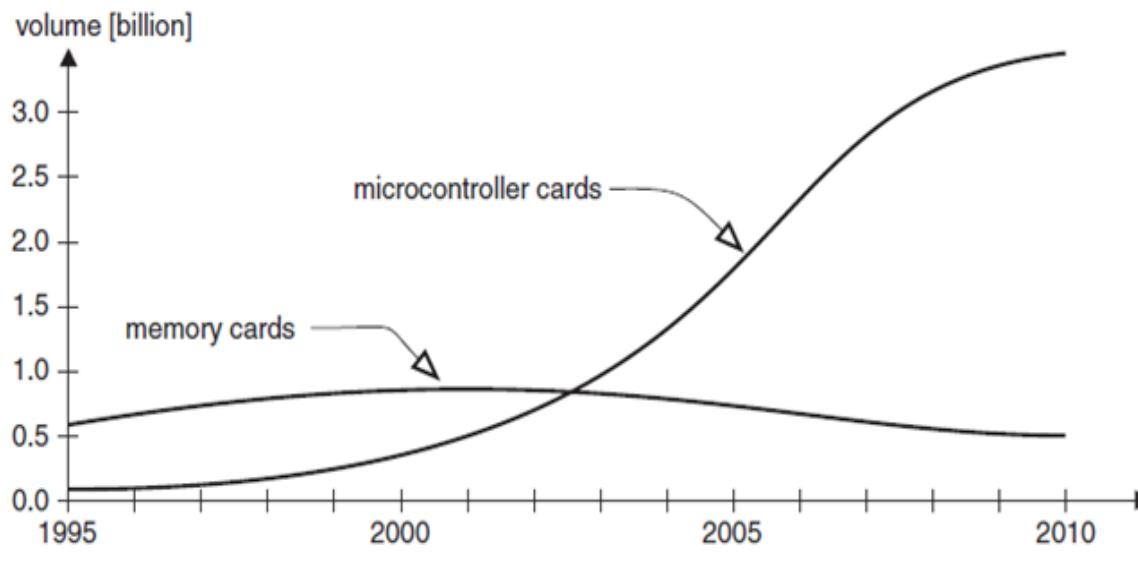
Chiffres du marché

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

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

9) Acteurs du marché

- C'est en 2000 que le nombre de cartes émis dans le monde est devenu supérieur à celui émis en France.
- A partir de 2003 la production des cartes à microcontrôleur dépasse la production en carte à mémoire



9) Acteurs du marché

- **Nombre de cartes dans le monde**
 - 2 milliards de cartes à puce en 2003
 - 52% de cartes à mémoire, dont 90% pour la téléphonie et 5% pour les transports
 - 48% de cartes à microprocesseur, dont 67% pour la téléphonie, 20% pour la banque, 6% pour la santé, 4% pour la télévision

9) Acteurs du marché

Marché et compétition en 2003

