KarKam Dvpt.

Les cartes à puce

INTRODUCTION

Une carte à puce est une carte en matière plastique de quelques centimètres de cotés et moins d'un millimètre d'épaisseur portant au moins un circuit intégré capable de porté des informations. Le circuit intégré (la puce) peut contenir un microprocesseur capable de traiter cette information ou être limité à des circuits de mémoire non volatile et éventuellement un composant de sécurité.

Les cartes à puce sont principalement utilisés comme moyen d'identification personnelle(carte vitale, badge d'accès aux bâtiments,carte SIM…)

La lecture peut se faire avec ou sans contact avec la puce.

Histoire

Dès 1947, on trouve des traces des idées du fonctionnement d'une carte à puce.

En 1974-1975, Ronald Moreno, un français, dépose le brevet de ce qui deviendra la carte à puce. Une mémoire portative protégé par des inhibiteurs à la lecture et/ou à l'écriture. Ce qui donne l'intérêt à la carte à puce.

Le premier brevet de Moreno est couplé à un lecteur à radiofréquence qui donnera les « carte sans contact ».

En 1975, il met en place :

- Comparaison interne du code confidentiel
- Compteur d'erreur qui provoque l'autodestruction de la puce en cas de soumission répétée d'un code faux.
- Lecture irréversiblement impossible de zones prédéterminés, notamment de code confidentiel, clés…etc.
- Ecriture, modification, Effacement irréversiblement impossible de zones prédéterminés de la mémoire.

Moreno crée la société InnoVatron pour exploiter ses brevets.

En 1977, l'allemand Detlhoff dépose un brevet pour une carte à mémoire portative dont les moyens inhibiteurs seraient constitués par un micro-processeur.Ce perfectionnement autorise un changement de fonction de la carte par une simple reprogrammation.

Quelques mois plus tard, le Français Ugon dépose un brevet sur une technique comparable, nommée CP8, pour *Circuit Portatif des années 80*, qui ne donnera lieu à une activité industrielle qu'à partir des années 1990.

En 1979, le géant des services pétroliers Schlumberger entre au capital d'Innovatron, pour 34 % : cette position l'aidera à devenir plus tard le numéro 1 mondial de la carte à puce (cartes, lecteurs, cabines téléphoniques, systèmes), absorbant notamment tous ses concurrents : Sligos, Bull, puis enfin Gemplus.

En 1981, le GIE "Carte à Mémoire" lance trois expérimentations de la carte à puce, respectivement à Blois avec Bull, Caen avec Philips, et Lyon avec Schlumberger. À la fin des années 1980, le GIE *Carte Bancaire*, qui a succédé au GIE "Carte à Mémoire", commande 16 millions de cartes CP8, lançant la généralisation de la carte à puce en France en 1992.

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

COMPOSITION

Les dimensions habituelles sont 0,85 725 × 0,53 975 mm (soit 3,375 × 2,125 pouce (unité)s) sur une épaisseur typique de 0,76 mm (minimum: 0,69 mm, maximum: 0,84 mm)

La puce d'une carte typique (la carte bancaire B0') est constituée d'un microprocesseur 8 bits tournant à une vitesse de 4 MHz, elle dispose de 6 à 32 Ko de mémoire morte, de 256 à 2048 octets de mémoire vive et de 1 à 32 kiloctets d'EEPROM. La puce dispose en outre d'une seule ligne d'entrée-sortie.

Les composants des cartes à puce suivent l'évolution générale de l'électronique: puissance des microprocesseurs (2005: 32 bits à plus de 10 MHz) et capacité de mémoire (plus de 256 ko d'EEPROM, 512 ko de mémoire morte), diversité des types de mémoire (mémoire Flash de plusieurs Mo dès 2005).

La puce composant peut être accessible :

- par contact avec des électrodes de cuivre ;
- sans contact: par radiofréquence à courte ou moyenne portée, via une antenne interne dont les spires sont moulées dans l'épaisseur de la carte;
- par une combinaison des deux précédentes : on parle alors de cartes *Avec et Sans Contact* (ASC) ou de carte "mixte".

Les cartes à puce

Les cartes à puce succèdent :

- Aux cartes à code-barre
- Aux cartes à bande magnétique.

Il existe trois types de carte :

- Les cartes à mémoire (télécarte France-Télécom)
- Les cartes à logique cablées (carte pour chaîne payante)
- Les cartes à microprocesseur

Parmi les cartes à microporcesseur :

- Les cartes mono-applicative : carte bancaire ou carte cryptographique pour la sécurité informatique (technologique PKI)
- Les cartes multi-applicative : carte bancaire (VISA) de téléphone (SIM).

Les normes

Pour définir une carte à puce, il faut au moins normaliser trois types de paramètres différents :
- des paramètres physiques qui indiquent la taille de la carte et la position de la puce et de ses contacts ;
- des paramètres électriques qui précisent les tensions d'alimentation et niveaux électriques mis en œuvre ainsi que le brochage de la puce sur la carte ;
- des paramètres logiciels qui définissent le mode de dialogue avec la carte, les commandes qu'elle peut interpréter et son comportement face à ces dernières.

Cela s'est traduit par un certain nombre de normes internationales dont le tableau ci-dessous
donne une liste aussi complète que possible dans le cas des cartes en général.

ISO 14443-A,B,C et 15693 : Norme pour les cartes sans-contact.

- PC/SC : API d'intégration de carte à puce en environnement Windows

http://www.pcscworkgroup.com/index.php?o

- OCF : Environnement Java et API pour application smartCard
- JavaCard pour programmation des cartes
- PKCS : Programmation des clefs cryptographique (PKI)

International Organization for Standardization

http://www.iso.org/iso/fr/

Norme ISO	Explication
ISO 7810	Identification Cards – Physical Characteristics Cartes d'identification – Caractéristiques physiques
ISO 7811-1	Identification Cards – Recording Technique Embossing Cartes d'identification – Techniques d'embossage
ISO 7811-2	Identification Cards – Recording Technique Magnetic Stripe Cartes d'identification – Techniques d'enregistrement magnétique
ISO 7811-3	Identification Cards – Recording Technique Location of Embossed Characters on ID 1 Cards Cartes d'identification – Emplacement des caractères embossés sur les cartes de type ID 1
ISO 7811-4	Identification Cards – Recording Technique Location of Read-Only Magnetic Tracks – Tracks 1 and 2 Cartes d'identification – Position des pistes magnétiques à lecture seule – Pistes 1 et 2
ISO 7811-5	Identification Cards – Recording Technique Location of Read-Xrite Magnetic Tracks – Track 3 Cartes d'identification – Position des pistes magnétiques à lecture/écriture – Piste 3
ISO 7812-1	Identification Cards – Identification of Issuers Part 1 : Numbering System Cartes d'identification – Identification de l'émetteur, partie 1 : système de numérotation
ISO 7813	Identification Cards – Financial Transaction Cards Cartes d'identification – Cartes pour transactions financières
ISO 7186-1	Identification Cards – Integrated Circuits Cards with Contacts – Physical Characteristics Cartes d'identification – Cartes à circuits intégrés avec contacts – Caractéristiques physiques
ISO 7816-2	Identification Cards – Integrated Circuits Cards with Contacts – Dimension and Location of the Contacts Cartes d'identification – Cartes à circuits intégrés avec contacts – Dimension et position des contacts
ISO 7816-3	Identification Cards – Integrated Circuits Cards with Contacts – Electronic Signals and Transmission Protocols Cartes d'identification – Cartes à circuits intégrés avec contacts – Signaux électroniques et protocoles de transmission
ISO 7816-3 Amendment 1	Protocol type T = 1, Asynchronous Half Duplex Block Transmission Protocol Protocole T = 1, protocoles asynchrone semi-duplex à transmission par blocs
ISO 7816-3 Amendment 2	Revision of Protocol Type Selection Révision du mode de sélection de protocole
ISO 7816-4	Identification Cards – Integrated Circuits Cards with Contacts – Interindustry Commands for Interchange Cartes d'identification – Cartes à circuits intégrés avec contacts – Commandes inter-industries
ISO 7816-5	Identification Cards – Integrated Circuits Cards with Contacts – Number System and Registration Procedure for Application Identifier Cartes d'identification – Cartes à circuits intégrés avec contacts – Système de numération et procédure d'enregistrement pour l'identification des applications
ISO 1177	Information Processing – Character Structure fort Start/Stop and Synchronous Character Oriented Transmission Traitement de l'information – Structure des caractères pour les échanges synchrones orientés caractères

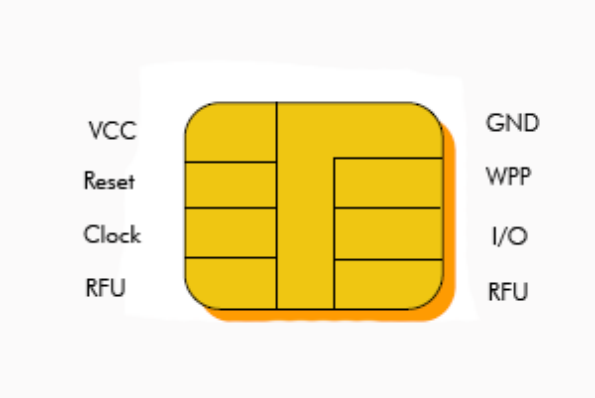
La carte

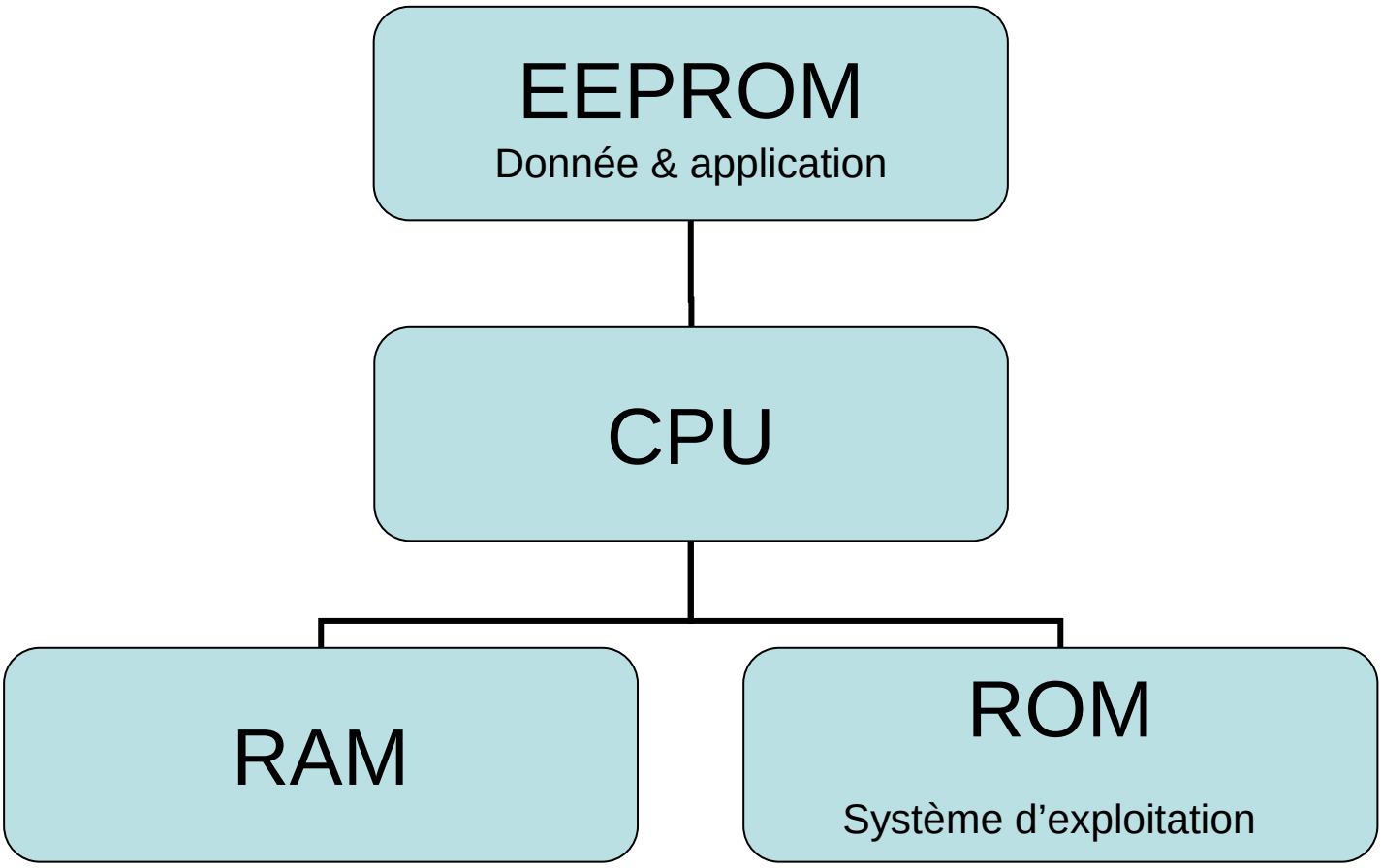
Largeur : 54mm
Longueur : 85 mm
Épaisseur : 0,76mm

La puce

ISO(7816-2)

Surface : 25mm²
Épaisseur : <= 0,3mm
Broche : 8 contacts
Alimentation : 3v
I/O : Half-duplex





OS de Base

Le masque « Hard-Mask » est le système d'exploitation de la carte.

Il est écrit en C ou en langage d'assemblage.Il est stocké en ROM et ne peut être modifié.

Rôle du masque :

- Gère les communications avec le monde extérieur,
- Exécute les commandes reçues via l'interface I/O,
- Supervise l'exécution des programmes stockés dans la carte
- Gère le SGF et assure un accès sécurisé à l'ensemble des fichiers
- Assure les fonctions de cryptographie(DES,RSA,SHA,ECC,…)
- Les plus modernes intègre une JVM(Java Virtual Machine) pour exécuter une applet

La fonction principale de l'OS est une boucle qui attend l'arrivé des commandes externes. A l'arrivée d'une commande, elle est exécutée puis une réponse est émise vers l'extérieure, puis la boucle recommence.

« Soft-Mask »

Le soft-Mask est une extension du masque.

Il peut être chargé dans le EEPROM tant que la carte n'est pas bloquée.

On a besoin d'un soft-Mask :

- Lorsque l'on doit ajouter de nouvelles fonctionnalités pour des applications spécifiques,
- Pour les besoins de « bug-fixing » au niveau du masque,

CPU :

Central **P**rocessing **U**nit

Le processeur interprète et traite les données d'un programme.

RAM :

Random Access **M**emory

Type de mémoire vive.Mémoire volatile dans laquelle sont placés les données pendant leur traitement.

Avantage : rapidité d'accès

Inconvénient : s'éfface si elle n'est plus alimenté en énergie.

ROM :

Read **O**nly **M**emory

Type de mémoire morte. Mémoire non volatile qui ne s'éfface pas quand il n'est plus alimenté en énergie.(!=RAM)

Mémoire programmé à la fabrication.

EEPROM :

Electrically **E**rasable **P**rogrammable **R**ead **O**nly **M**emory

Mémoire éffaçable et programmable