

"Stop acting so small. You are the universe in ecstatic motion".

« Arrête d'agir si petitement. Vous êtes l'univers en mouvement extatique »

Djalal Eddine Er-Rumi

2

Comment la Carte à Puce A-t-elle Evolve ? (How Did the Smart Card Evolve?)



2.1 Les Débuts

La carte a grandement évolué tout au long des dernières décennies. A l'instar des tous les produits électroniques destinés au grand public, son évolution a été fulgurante de sorte qu'au regard des CP actuelles, les anciennes catégories font figure de dinosaures.

THE FIRST CREDIT CARD



Fig. 2.1 Un Spécimen de la Première Carte de Crédit de Diners' Club

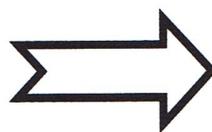


Fig. 2.2 Un Spécimen de la Première Carte de Crédit de Diners' Club



Fig. 2.4 Un Spécimen d'une Carte à Puce RFID Sans Contact

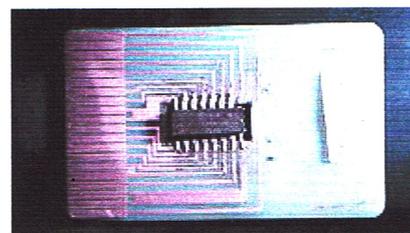
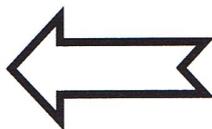


Fig. 2.3 Une des Premières Cartes de Roland Moreno

Cette évolution s'est opérée selon trois axes directeurs : La **puce**, le **support** et le **système d'exploitation**. Les figures 2.1 à 2.4 en donnent une bonne illustration.

2.2 La Puce

Il est clair que pour être utile, une carte à puce doit offrir la capacité de stocker des informations. Il faut donc un support de mémoire.

+ Carte à Bande Magnétique

L'information est stockée sur une sorte de ruban magnétique collé sur une face de la carte. Les données sont inscrites puis lues à la manière d'un magnétophone à cassette magnétique. Ces cartes souffrent d'un bas niveau de sécurité et sont exposées à une usure relativement rapide. En effet, il faut soit insérer la carte dans le lecteur, soit la faire glisser au dessus. Ces mouvements mécaniques contribuent à son usure.



Fig. 2.5 La première Carte de Crédit à Bande Magnétique.

+ Carte à Mémoire à Semi-conducteur

Tout comme la carte magnétique, la carte à mémoire n'est pas, à proprement dit, « smart » ou intelligente car elle ne dispose pas encore de processeur. Les informations sont simplement stockées dans une mémoire puis lues lors de son utilisation. Cette carte n'offre donc pas de possibilité de traitement cryptographique par exemple.

+ Carte à Support ASIC

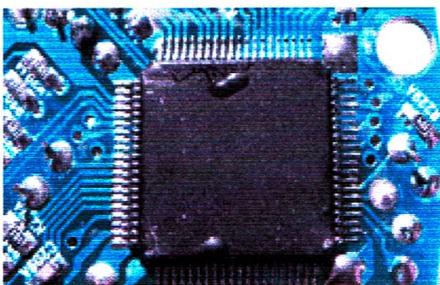


Fig. 2.6 ASIC. Wikipedia

L'acronyme anglais ASIC, Application-Specific Integrated Circuit, signifiant Circuit Intégré à Application Spécifique, désigne un circuit intégré VLSI (Very Large Scale Integration) qu'on peut adapter, via une programmation appropriée, à une application spécifique personnalisée.

Une puce ASIC offre des capacités de traitement substantielles faisant de la carte un objet relativement smart ou intelligent. Cependant, ce type de carte souffre d'un déficit de flexibilité car une fois programmé pour une application spécifique, les fonctionnalités de l'ASIC demeurent figées.

+ Carte à Microprocesseur

C'est l'intégration d'un microprocesseur dans la puce qui a permis de rendre la carte vraiment « smart ». Le tandem microprocesseur/système d'exploitation performant ouvre d'immenses possibilités en termes d'applications de toutes sortes. La CP qui incorpore un microprocesseur acquiert plus de rapidité, de sécurité et de facilité d'utilisation.

On peut notamment implanter des algorithmes complexes et performants pour crypter les informations confidentielles que contient la carte pour entraver, dissuader ou détecter toute tentative de fraude ou de falsification ou d'accès non autorisé.

2.3 Le Support

La CP est constituée d'un support rigide qui permet d'accueillir la puce et sur lequel on grave des objets tels que des photos ou des logos ainsi que des informations telles que les nom et prénoms du détenteur, son numéro de compte, la date de validité etc.

Le support des premières cartes de crédit étaient en papier. Du papier renforcé certainement mais du papier quand même. Puis elles ont été rapidement remplacées par des cartes en plastique, généralement PVC (PolyVinyl Chloride), mais parfois ABS (Acrylonitrile Butadiene Styrene) ou même polycarbonate. Ce type de support obéit à des normes strictes en termes de dimensions physiques, de rigidité, de résistance notamment aux rayons UV et X.

2.4 Système d'Exploitation de la Carte

Bien que ne disposant que d'un espace de mémoire relativement limité par rapport à un laptop ou un ordinateur de bureau, la CP, n'en déplaise à ses détracteurs, dispose néanmoins d'un système

d'exploitation. Le terme COS (Card Operating System), Système d'Exploitation de Cartes (SEC), est aujourd'hui accepté et adopté de part le monde. D'ailleurs un des premiers systèmes d'exploitation des cartes à puce STARCOS fut développé dans les années 1990.

Quelles sont les fonctionnalités d'un COS ? Vous l'aurez certainement compris, comme tout système d'exploitation, il doit permettre notamment de réaliser un certain nombre d'opérations de gestion, de transfert et d'exécution parmi lesquelles on peut citer :

- ✚ ***Le transfert des données de et vers la carte,***
- ✚ ***Le contrôle l'exécution des commandes,***
- ✚ ***La gestion les fichiers,***
- ✚ ***La gestion et l'exécution des algorithmes de cryptage,***
- ✚ ***La gestion et l'exécution des programmes code.***

Il faut noter qu'aujourd'hui, le système d'exploitation **JAVA Card** offre un environnement d'applications logicielles spécifiquement destinées aux cartes à puce. Ces applications représentent un sous-ensemble du langage **Java**. Ce système d'exploitation est transportable et permet aux applications développées sous ce langage d'être correctement exécutées quasi-universellement sur l'ensemble des cartes. Nous aurons certainement à revenir là-dessus plus loin dans ce document.

2.5 Carte à Contact vs Carte sans Contact

On l'a déjà dit, une CP dispose de contacts qui lui permettent de se connecter et de communiquer avec un lecteur tel un distributeur automatique ATM (Automatic Teller Machine) ou un TPE (Terminal de Payment Electronique) qu'on retrouve couramment au niveau des banques, des postes ou même chez tout marchand disposant d'un lecteur.



TPE pour CP avec Contact



Fig. 2.7 Lecteurs de CP Ou TPE
(Terminal de Payment
Electronique)

Tout au début, les CP n'étaient munies que de contacts à travers lesquelles le lecteur fournit l'énergie électrique nécessaire au fonctionnement des circuits et ce, à travers les broches Vcc/GND et communique via les broches d'entrées/sorties I/O et de mise à zéro RST.

Dès 2004, les fabricant avaient commencé à progressivement remplacer ces contacts par une antenne RF (Radio Fréquence) et de ce fait, on n'avait plus besoin de contact physique de la carte avec le lecteur. La carte qu'on appelle alors « sans contact » (Contactless Card) est née. On peut aisément distinguer la carte sans contact de la carte classique. Il y a un ou plusieurs pictogrammes parmi lesquels l'indicateur « sans contact » suivant :



Bien évidemment, cette innovation offre beaucoup d'avantages et de commodités d'usage par rapport à la carte avec contact. La technologie dite « sans contact » rend les opérations de paiement de retrait et autres encore plus faciles, plus pratiques et plus rapides.

2.6 Carte Hybride

A ce jour, la carte sans contact n'a pas complètement délogé la carte classique du piédestal de gadget indispensable aux diverses transactions de finances, d'identification et d'authentification. La carte classique est encore bien présente. Il existe même des cartes hybrides qui incorporent les contacts traditionnels de la carte classique ainsi qu'une antenne RF.