CETTE PARTIE INTERVIENT EN COMPLEMENT Du COURS FOURNI DANS LA SECTION UNE.

2-1- Historique de la carte à puces.

Les premières cartes ont été développées en plastique avec une bande à piste magnétique dans les années 50 (Figure 1.1). Celles-ci n'incluaient pas l'utilisation du papier ou du carton ; mais le prix, la résistance de la matière et le développementde l'industrie du matériel PVC a encouragé le développement de celle en plastique. La bande magnétique représente le support de stockage des informations, elle est limitée en taille mais restait suffisante jusqu'à une certaine époque. Les cartes Diners Club sont les premières à utiliser cette technologie. Elles ont été pensées par Frank McNamara afin de les utiliser comme carte de paiement en remplacement de l'argent liquide. Elles sont maintenant utilisées comme carte acceptées par plusieurs restaurants et magasins. Les géants du paiement électronique actuels qui sont MasterCard et Visa ont commencé leur développement à partir de ces années là en proposant leurs services aux États Unis puis en Europe et dans le reste du monde dans les années qui suivent. Ils utilisaient ces mêmes cartes à piste magnétique pour le paiement.

Figure 1.1

Plusieurs dates marquent l’avènement puis l’adoption et enfin la démocratisation de la carte à puce dans le monde. Depuis un quart de siècle, la carte a conquis de nombreux secteurs : la finance, la téléphonie mobile, les documents de voyages et de santé, la télévision à péage, les transports, les jeux, l’énergie et l’automobile. Elle est également à l’origine de nombreuses innovations comme le M2M, l’accès aux réseaux et l’internet des objets. Une histoire dont le salon CARTES est le témoin et l’un des acteurs majeurs depuis sa création en 1986. Huit dates s’inscrivent dans le livre d’or de l’histoire de la carte mais aussi quelques illustres inventeurs ayant marqué cette industrie de leur empreinte : K. Arimura, J. Ellingboe, J. Halpen, Roland Moreno, Jürgen Dethloff, et Michel Ugon.

**1979. La carte à microcontrôleur**

C’était à l’origine une carte à microprocesseur (CPU 3870 de Fairchild), associée à un circuit mémoire EPROM d’Intel (2716) programmable électriquement et effaçable par rayonnement UV. Elle deviendra pour des raisons de sécurité une carte à microcontrôleur (un seul circuit intégré regroupant la CPU et des mémoires ROM, RAM et EPROM) sous le nom de SPOM pour Self-Programmable On-chip Micro-computer. La production industrielle débute en 1981 chez Motorola. Le circuit dispose alors d’une mémoire RAM de 36 octets, d’une ROM et d’une EPROM de 1 Ko chacun, soit une capacité 1000 fois moins importante qu’aujourd’hui.

**1991. La carte SIM**

C’est au début des années 1980 que l’idée d’utiliser une carte à microcontrôleur pour authentifier l’abonné à un réseau mobile commence à faire son chemin, en France et en Allemagne notamment. 5 années sont nécessaires pour que la spécification de ce type de carte sous l’égide de l’ETSI aboutisse en 1991 au lancement des premiers réseaux et services GSM (roaming, SMS, etc.), et des premières cartes SIM (Subscriber Identity Module). Les cartes des années 1995-96 embarquent une mémoire ROM de 6 à 16 Ko, une RAM de 128 à 256 octets, et une EPROM de 2 à 8 Ko. Chaque carte contient les détails de l’abonnement et des codes (IMSI, PIN, des clés utilisées avec des algorithmes spécifiques) pour authentifier l’abonné et chiffrer les communications, et le PUK (Personal Unlock Code). Un succès jamais démenti, 3,6 milliards de cartes SIM seront livrées en 2010.

**1994. La carte sans contact**

L’idée de remplacer les contacts de la carte par une antenne, et d’utiliser la technologie du couplage inductif sur la bande de fréquence des 13,56 MHz pour non seulement transmettre des données à la carte, mais également lui fournir l’énergie qui lui permet de gérer ces données nait avec le lancement par la société Mikron de la première carte Mifare (1Ko de mémoire). Celle-ci est acquise par Philips Semiconductors 4 ans plus tard, et deviend NXP Semiconductors en 2006.

**1995. La carte EMV**

La téléphonie a son standard avec la carte SIM, le paiement a désormais le sien avec la carte EMV2[**1**] (Europay, Visa MasterCard). Cette carte à microcontrôleur équipée de quelques Ko de mémoire porte la sécurité des paiements par carte à un niveau jamais atteint et remplace progressivement la carte à piste magnétique. Elle va également proposer pour la première fois une carte offrant des capacités multi-applicatives mais encore mono-opérateur. Débit, crédit, porte-monnaie électronique, carte prépayée, mémoire réservée pour des données personnelles du porteur, plus d’un milliard de cartes EMV sont actuellement en circulation dans le monde.

**1996. La carte Java**

C’est l’une des grandes évolutions de l’histoire de la carte à puce. Le mariage réussi entre l’informatique, la micro-électronique et la cryptographie. Cette carte conclut également un débat sur le choix de l’environnement ouvert[**2**] que l’industrie allait adopter pour anticiper l’avènement des cartes multi-applicatives, et multi-opérateurs, grâce à l’utilisation d’une machine virtuelle. Cette technologie Sun Microsystems est ensuite adaptée par l’industrie de la carte réunie au sein du Java Card Forum. La toute première carte Java a été conçue par les équipes de Bertrand du Castel, alors Responsable de la R&D de Schlumberger Smart Card & Terminal.

**Cette partie est consacrée surtout aux cartes RFID qui ont fait l’objet du module RFID au premier semestre**

**2002. Le NFC et les « smart objects »**

Autre évolution majeure avec l’annonce en septembre 2002 du développement par Philips et Sony de la technologie NFC, et l’avènement d’un nouveau paradigme d’interactivité pour l’utilisateur le « Touch & Go, & Pay, & Connect », etc. Les perfectionnements apportés à la technologie sans contact développée notamment avec Mifare par Philips, et la technologie similaire développée par Sony (Felica) permettent de transformer une carte en lecteur et inversement, et de réaliser des échanges P2P. Ces possibilités avaient déjà été explorées par Inside Contactless qui avait en 1999, réalisé des transactions sans contact de type « lecteur à lecteur ».

Cette technologie qui se démarque par sa facilité d’utilisation se libère des facteurs de forme de la carte classique (celle de la carte bancaire à contact). Elle peut ainsi équiper des téléphones mobiles, et toute une famille de « smart objects » (des clés USB en particulier) capables de marier le sans contact de proximité et le sans fil longue distance ou des accès Internet.

**2004. Le e-passeport ICAO**

Après la téléphonie mobile, le paiement, les documents d’identité et les passeports en particulier trouvent leur standard et adoptent la puce grâce au sans contact. C’est la spécification de l’ICAO (International Civil Aviation Organization) dont la première version paraît en 2004, avec le déploiement des premiers e-passports. Cette fois encore, l’industrie de la carte élargit un peu ses frontières et combine son expertise à celles des technologies biométriques, en mettant au point le « match-on-card », c’est-à-dire la capacité pour la carte de comparer de façon sécurisée une empreinte stockée et une empreinte acquise sur un capteur extérieur, et ce dans des temps parfaitement opérationnels.

**2007. La carte SIM-USB-SWP-SCWS**

L’explosion de la téléphonie mobile et le volume de cartes SIM (devenue UICC USIM avec la 3G), combinés au potentiel de la technologie NFC, ont créé des synergies sans précédent pour le déploiement de cartes SIM multi-applicatives et multi-opérateurs. L’invention du SWP (Single Wire Protocol) par Gemalto a été un levier pour faire évoluer la SIM vers une véritable plate-forme de services. Il permet à la SIM de communiquer sur un seul fil avec un circuit NFC dans un téléphone mobile ou dans n’importe quel « smart object ». L’exploit technique est aussi stratégique, car en n’utilisant qu’un seul contact de la carte SIM, le SWP permet d’utiliser les deux contacts restants libres pour connecter un lien de type USB avec le processeur central du téléphone et ainsi communiquer en mode IP. La carte SIM se transforme alors en serveur web. Le SCWS (Smart Card Web server) n’est pas encore une technologie très répandue, mais elle devrait révéler tout son potentiel avec les futurs déploiements NFC.

###  **Utilisation des cartes à puce**

La carte à puce représente un moyen sécurisé dépassant de loin les cartes à piste magnétique. Depuis sa création, la carte à puce s'est fait un grand chemin dans les domaines suivants : le bancaire, les télécommunications, le multi-applicatif (carte d'université, carte d'accès, carte de fidélisation) et autres. Dans les années 2000, le premier client de ces cartes est l'industrie des télécommunications grâce aux cartes SIM et USIM. Selon l'étude de l'association Eurosmart, 5200 millions de pièces ont été distribuées l'an 2012 avec une part de marché représentant 68%. Une augmentation de ce chiffre est intervenue en 2013 dû à l'implantation de la nouvelle norme 4G dans les pays émergents. Les télécommunications sont talonnées par le secteur bancaire et le commerce avec 1260 millions cartes bancaires distribuées au monde avec toujours une forte augmentation chaque année qui atteint les 17%. La Table 1.1 présente la répartition du marché de la carte à puce sur les différents secteurs avec une estimation sur l'évolution au cours de l'année 2013.

Les cartes à puces sont de nos jours très largement utilisées dans des domaines très divers.

Les tableaux suivants donnent une idée du volume de cartes utilisées de nos jours par différents acteurs, parmi les plus gros utilisateurs



**Figure 2 Nombres en millions d'unités**

e



**Figure3 Production en million d'unités**



**Figure 4 Nombres en millions d'unités**

**Légende**

**Télécom** : Cartes SIM cards (éléments sécurisés avec une application SIM).

**Paiement et banque** : cartes émises par les banques et les enseignes pour des services de paiement (débit, crédit, prépaiement...). Cartes émises par d'autres fournisseurs de service ou enseignes pour la fidélité. Cartes à usage social avec application de paiement.

**Gouvernment et santé** : cartes émises par des organisations gouvernementales pour l'identification des citoyens (documents de voyage, d'identité, de santé) et les services en ligne opérés par des compagnies d'assurances privées dans le domaine de la santé.

**Fabricants d'équipements** : Téléphones mobiles, tablettes, outils de navigation et autres objets connectés comportant un élément sécurisé sans application SIM.

**Autres** : Cartes émises par des opérateurs pour le transport, le stationnement (i.e. transport). Cartes émises par les opérateurs de télévision à péage (i.e. pay-tv). Cartes d'accès physique ou logique.

VOUS TROUVEREZ DANS LE COURS FOURNI DANS LA SECTION UNE UN HISTORIQUE DES DIFFERENTES GENERATIONS DE CARTES.

VOUS ETES PRIES DE VOUS Y REFERER.