PAR CHRISTIAN GOIRE
Java Card Forum President
Head of Advanced Technologies Strategy and Promotion
Technology and Innovation. Gemalto

ET LAURENT CASTILLO (96)
Head of Advanced Technologies Strategy and Promotion
Technology and Innovation. Gemalto

Sécurité et liberté dans le monde numérique

Concrétisation du « bijou électronique » imaginé par René Barjavel, la carte à puce a tout d'abord répondu à des besoins de sécurité en paiement (télécarte et carte bancaire). Mais le développement du téléphone mobile et de l'Internet tout comme les évolutions technologiques (microprocesseurs de plus en plus puissants, clés USB, communications sans contact…) donnent naissance à toute une famille d'objets de la vie quotidienne : passeport électronique, dossier médical « portable ».
Ils changent aussi l'usage des objets familiers et permettent par exemple d'utiliser son téléphone mobile pour régler des paiements ou prendre le train.

Genèse d'une innovation

L'histoire de la carte à microprocesseur, communément appelée « carte à puce », est représentative des étapes de l'innovation technologique.
Dans un premier temps, des chercheurs d'origines diverses imaginent un concept, et essaient de formaliser sous forme de brevets une idée qui pourrait venir de Jules Verne ou de Léonard de Vinci. Des industriels ou des clients potentiels s'y intéressent et s'organisent pour mettre en œuvre l'idée suivant leurs conceptions et intérêts propres. C'est en général une période trouble où plusieurs variantes de l'innovation s'affrontent sur le marché, jusqu'au moment où un consensus se dégage dans les comités de normalisation favorisant une version plutôt qu'une autre.

Le Jules Verne de la carte à puce est l'écrivain français, René Barjavel, qui, dans *La Nuit des temps*, décrivait un bijou électronique offrant de nombreux services à son porteur.

> ***Protéger les données de la carte contre toute modification frauduleuse***

Dans les années soixante de multiples brevets vont aborder cette problématique ; on peut citer ceux de J. Ellingboe, J. Dethloff, de K. Arimura, de P. Castrucci, de J. Halpern, de K. Ehrat. Puis arrive l'ère des brevets fondateurs que la postérité a retenue.
Le Français Roland Moreno dépose six brevets fondamentaux, en 1974 et 1975, décrivant l'architecture d'une carte à puce et notamment les moyens de protéger les données de la carte contre toute modification frauduleuse. Les premières télécartes vont naître de ces brevets.
L'acte fondateur est la décision de Mme Victoire Chaumont de la Datar (Délégation à l'aménagement du territoire et des régions), en 1976, de réunir les banquiers, la banque de France et la DGT (Direction générale des télécommunications). Ils vont demander à CII-Honeywell Bull de démontrer la faisabilité d'une telle carte et en 1979 les banquiers et la DGT lancent le premier appel d'offres de la carte bancaire à puce.
Chez CII-Honeywell Bull, Michel Ugon, dès 1977, veut faire de cette

carte un vrai moyen sécurisé (paiement, authentification, protection du contenu). Pour cela il lui faudra changer de technologie.

Le début d'un schisme

Ce fut le début d'un schisme. Il y eut les partisans de la logique câblée en technologie bipolaire et ceux qui, derrière Michel Ugon, assuraient qu'il fallait un microprocesseur en technologie MOS. Après en avoir démontré les avantages et la faisabilité, Michel Ugon dépose, en mai 1977, le brevet 2141 dit « SPOM ». C'est le début de la carte à microprocesseur telle que nous la connaissons aujourd'hui. En 1980 Motorola recevra les spécifications en vue de fabriquer le premier composant.

> ***Toutes les applications avaient été imaginées***

Il est à noter que, dans les documents des origines, presque toutes les applications avaient été imaginées ; seule l'évolution des composants électroniques en termes de fonctions, de prix et aussi d'acceptation de facteurs de formes différents pour l'objet personnel sécurisé a été un frein à un développement plus rapide des applications.

Des objets de la vie quotidienne

La carte est devenue un objet de la vie quotidienne. Pourtant, un phénomène bien particulier s'est produit avec les cartes bancaires à puce, touchant la relation entre la carte et son porteur : la carte bancaire n'est pas la propriété de l'individu mais celle de la banque.
Mais voilà que progressivement avec la notion d'objet personnel de confiance (TPD, Trusted Personal Device) cette relation change. L'objet n'est plus seulement un moyen d'acheter ou de communiquer, il devient le garant de l'identité de l'individu. Non seulement il lui permet de se faire reconnaître, de communiquer, de faire valoir ses droits mais il lui permet aussi d'échanger avec autrui ; de faire connaître son « espace de vie » en délimitant les frontières et de préserver sa vie privée à sa guise.
C'est un exemple où les individus se sont réapproprié les concepts d'une technologie.
Aujourd'hui nous parlons de la sécurité digitale et de la place fondamentale que la carte (ou tout autre facteur de formes) y joue et de l'importance de plus en plus grande qu'elle prend tant pour les entreprises, les collectivités que pour les individus.
La révolution digitale transforme notre vie quotidienne. Elle nous permet de communiquer, d'acheter, de voyager, où et quand nous le voulons.
Les grandes compagnies et le secteur public s'orientent vers ces technologies.
L'individu et le citoyen en sont de plus en plus demandeurs.
Fin 2006, il y avait un milliard d'utilisateurs Internet, trois milliards d'abonnés pour le téléphone mobile.
L'un des nouveaux écueils de ces nouvelles technologies est la complexité des nouveaux appareils et outils, la multiplication des interfaces, des mots de passe et des coûts tant pour les organismes que pour l'utilisateur final. De plus, deux nouvelles craintes sont apparues.
La première concerne la fraude, l'intrusion dans les systèmes, le vol d'identité de l'utilisateur ou du service. La conséquence en est un frein dans l'utilisation des services « en ligne ».
La seconde crainte concerne le respect de la vie privée. Il nous faut garantir le respect de la vie privée de l'utilisateur final. Celui-ci veut communiquer, partager des informations, demander des services. Il est prêt à partager « un espace de vie » mais il veut en délimiter les frontières. Il souhaite aussi garantir la protection de son identité, de ses données et de ses transactions.
C'est la dualité qui est attendue des TPD (Trusted Personal Device), que l'on pourrait traduire par objets personnels de confiance.

Un marché en très forte croissance

L'enjeu industriel est considérable. En 2007 le marché traditionnel de la carte était estimé à cinq milliards de dollars, nous estimons celui de la sécurité digitale à 25 milliards de dollars.
Pour être leader sur ce marché il faut avoir compris cette dualité, être capable d'apporter des services offrant la sécurité, l'ergonomie et la facilité d'utilisation, la portabilité des applications indépendamment des environnements, des appareils.

> ***Chaque objet est personnalisé avec les données de l'utilisateur***

C'est un marché unique dans le sens où chaque objet est personnalisé avec les données de l'utilisateur. Cela a des conséquences importantes sur la conception de l'outil de production.
Le nombre de cartes vendues en 2007 fut de 4 285 millions d'unités contre 3 580 en 2006. On estime le marché des seules cartes à microprocesseur pour 2008 à 4 milliards d'unités (3 325 millions en 2007).

Des champs d'application de plus en plus nombreux et variés

De nouvelles évolutions technologiques ont fait sauter les goulots d'étranglement qui limitaient le développement de nouvelles applications.

SECTEURS	CARTE À MÉMOIRE	CARTE À MICROPROCESSEUR
Télécommunications	440 000 000	2 600 000 000
Services financiers, etc.	30 000 000	500 000 000
Gouvernement-santé	300 000 000	105 000 000
Transport	160 000 000	15 000 000
Pay TV	-	70 000 000
Sécurité entreprise	20 000 000	20 000 000
Autres	10 000 000	15 000 000
TOTAL	960 000 000	3 325 000 000

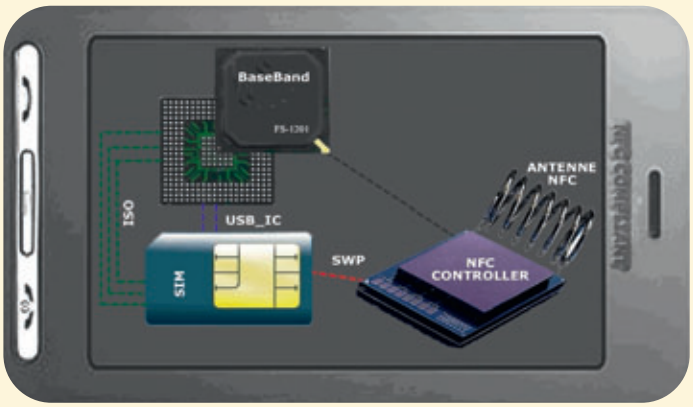
Ce tableau montre que les trois marchés « historiques » et de masse sont les télécommunications, les services financiers, les services liés au secteur public. Ces services évoluent très vite et de nouveaux services apparaissent liés à de nouvelles demandes et à l'évolution technologique.

La carte s'est ouverte sur le monde de l'Internet avec une connectique et des connections de type USB, puis l'ajout des protocoles réseaux TCP/IP. L'évolution des composants en taille mémoire, sécurité et performance a permis le développement de nouveaux environnements de développement tels que « .NET » ou « Java Card » rendant le développement des applications « Web » plus aisé et permettant la portabilité des applications. Les cartes peuvent être de véritables « Web Servers » (Smart Card Web Server). Elles deviennent ainsi proactives et non passives, offrant une nouvelle manière de présenter les données, plus intuitive pour l'utilisateur final.

> ***Une carte contenant le dossier médical d'un patient***

L'introduction des communications sans contact dans la carte SIM (qui équipe les téléphones mobiles) est un autre bon exemple de cet accroissement de l'interconnexion des cartes. Aujourd'hui, cette SIM NFC est l'une des plus sophistiquées actuellement sur le marché. Grâce au Single Wire Protocol (SWP) la connexion d'une carte est désormais possible avec une puce NFC. Le téléphone mobile s'ouvre vers de nouvelles applications telles que le paiement des moyens de transport ou le porte-monnaie électronique sans contact.
Avec le Bluetooth, le Wifi et les NFC, la carte SIM s'ouvre vers le monde de la radiofréquence.
Les évolutions ne se limitent pas

Near Field Communications : la carte sans contact



La technologie SIM NFC permet de relier simultanément la carte SIM au processeur du téléphone mobile et à un circuit NFC, chargé de la communication radiofréquence (RF). Les communications RF sont caractérisées par leur basse fréquence (13,56 MHz), leur courte portée (quelques centimètres) et leur capacité à fonctionner sans alimentation de la carte ou du mobile. La SIM NFC se comporte comme une carte sans contact standard, tout en bénéficiant du téléphone comme interface usager.

Une application majeure pour les mobiles équipés de la carte SIM NFC est le paiement et le ticket électronique. En utilisant la technologie NFC les voyageurs passent simplement leur portable devant un lecteur pour payer ou débiter un ticket enregistré pour le voyage. Cela est commode et rapide pour l'utilisateur, et plus efficace pour la société de transports. Pour cela, les banques, les opérateurs de télécommunications et les transporteurs doivent harmoniser leurs outils et en confier la gestion à un tiers de confiance, tel que Gemalto.

aux capacités de communications, ni à leur secteur. De plus en plus souvent, la carte s'insère dans de nouveaux facteurs de formes, tels que la clé USB ou encore les cartes micro-SD. Elle y est apte à établir de nouveaux ponts entre des mondes qui s'ignoraient jusqu'à présent. Dans le secteur public, les grandes capacités de mémoire des nouvelles cartes peuvent être exploitées de façon significative par de véritables systèmes de bases de données embarqués. Ceux-ci cumulent la souplesse de leurs grands frères, avec la sécurité traditionnelle des cartes pour créer des applications à la fois conviviales et sûres. Une application intéressante en est le Dossier médical sécurisé partagé (DMSP), où l'on verra une carte contenant le dossier médical d'un patient, accessible par les différents professionnels de santé selon leurs droits propres.

La quantité d'évolutions que connaît la carte rend notre définition traditionnelle de la « carte à puce » de plus en plus caduque. Peut-être ne faut-il en retenir finalement que la quintessence, celle d'un *objet personnel portable de confiance.*

Vers l'agrégation de services

Dans ce marché de la sécurité digitale, la carte n'est que la partie immergée de l'iceberg.

La multiplicité des opérateurs et des fournisseurs, les centaines de millions d'abonnés conduisent à des modèles économiques différents, à des infrastructures et des déploiements différents.

La sécurité est au cœur du système car nous allons vers des systèmes qui s'interconnectent (les mobiles, mobile-TV, paiement mobile, authentification, etc.). L'intermédiation est le facteur clé de la réussite de ces associations.

Il est fondamental de fournir aux clients des services opérés (gérés par un fournisseur pour compte des prestataires directs). Les services opérés comprennent, par exemple, la personnalisation et l'émission des cartes, ainsi que la gestion des serveurs OTA (« Over the Air ») pour administrer les cartes SIM à distance et donc déployer rapidement de nouveaux services. La carte semble être la plateforme par excellence pour l'agrégation de services. Elle est connectée aux serveurs, elle est un serveur, elle peut se connecter sur de multiples appareils sans contraintes particulières, elle est sûre, personnalisée, élément de confiance pour les organismes et pour l'individu. ■

Cet article n'engage que l'opinion de ses auteurs et ne peut être tenu comme la position officielle de Gemalto.