«L'odyssée de la carte à puce»

par Michel Ugon, Unité Recherche & Développements de Bull CP8

Il arrive rarement que les réalisations technologiques soient le résultat d'un coup de chance. James Watt a inventé le moteur à vapeur à l'apogée de la révolution industrielle, à un moment ou l'on avait besoin de machines toujours plus puissantes.

De la même façon la carte à puce porte l'empreinte de son temps, la connaissance technologique ainsi que les circonstances sociales et économiques qui entourent sa naissance.

En 1976, la Direction Générale des Télécommunications (l'actuelle France Télécom) en France recherchait une nouvelle forme de communication ainsi que les nouveaux produits émergents. Vidéotex, Minitel, Télétext, courrier électronique, TV à péage, la banque à domicile, semblaient être le résultat possible du mariage de la communication et de l'informatique. Très ambitieux, ces projets ont d'emblée déclenché plusieurs problèmes techniques. Afin de créer des réseaux parfaitement adaptés pour des fonctions aussi diverses que l'automatisation des petits commerçants, des guichets bancaires automatiques dans les rues, des terminaux d'ordinateur personnels à domicile... il fallait mettre au point des systèmes différents de ceux utilisés dans les procèdures classiques en mode en ligne. Par conséquent, à cause de cette difficulté, les systèmes de sécurité ont du être repensés. La question étant: comment identifier un utilisateur pour pouvoir exécuter en toute sécurité un transfert électronique de fonds?

L'histoire de la carte à puce est largement comparable à celle des premiers avions. Au début, de nombreuses personnes imaginaient aussi pouvoir voler dans des machines inhabituelles mais personne n'y parvenait. C'était la période des premiers brevets déposés par un certain nombre d'inventeurs. On citera:

- Aux Etats-Unis, Pomeroy (1967) et en particulier Ellingboe (1970) qui décrit concrètement un moyen de paiement électronique sur une carte de crédit à contacts; Halpern (1972) avec son stylo électronique sécurisé de paiement.
- Au Japon, Arimura (1970) propose une méthode d'authentification dynamique réalisé à l'aide d'un dispositif d'identification.
- En Allemagne, Dethloff (1977).

- Et en France, Moreno (1974), Ugon (1977) et Guillou (1979) ainsi que de nombreux autres.

En remontant encore un peu le temps on lit dans l'ouvrage du romancier français René Barjavel intitulé «La Nuit des Temps» l'histoire d'un peuple mythique, les Gondas une civilisation vieille de milliers d'années mais très avancée qui utilise un anneau magique ayant des moyens de mémorisation et de communication.

Du rêve à la réalité

«Chaque fois qu'un Gonda désirait quelque chose de nouveau, des vêtements, un voyage, des objets, il payait avec sa clé. Il pliait le majeur, enfonçait sa clé dans un emplacement prévu à cet effet et son compte, à l'ordinateur central, était aussitôt diminué de la valeur de la marchandise ou du service demandés».

Mais l'industrie devait passer du domaine du rêve à celui de la réalité, du simple projet sur papier à des réalisations concrètes. Dans le cadre de la société CII-Honeywell Bull, j'ai rassemblé une équipe technique et pluri-disciplinaire afin de donner une forme concrète à ces concepts. A cette époque, la carte à puce était au croisement de trois techniques différentes : la micro-électronique, le traitement de données et et la cryptographie. Rien de comparable n'existait et la faisabilité d'un tel produit n'était pas prouvée. Dans une telle situation, par où devait-on commencer ?

Une des premières questions concernait le choix de la technologie des semi-conducteurs en particulier pour la mémoire non volatile. Un long débat eut lieu entre les tenants de la technologie bipolaire qui était testée et plus facile à assembler dans un package plat et ceux qui mettaient en avant la technologie émergente MOS avec une consommation d'énergie réduite et une interface beaucoup plus flexible. Après de nombreux essais le choix s'est porté sur la technologie MOS en particulier à cause des coûts plus bas et le niveau sécuritaire bien plus élevé, la mémoire bipolaire non volatile étant visible par des procédés optiques. Dès l'origine, nous avions constamment en vue le besoin fondamental de sécurité et nous le considérions comme une priorité. Nous savions que personne n'était prêt à accepter un système de paiement à faible niveau de sécurité. En fait, la sécurité est la pierre angulaire de tout système de transaction et c'est la raison pour laquelle nous avons favorisé dans nos choix et dans nos développements, la sécurité.

Une autre préoccupation de base était la définition des fonctions et donc l'architecture de la carte. Devait-on baser la carte à puce sur une simple mémoire ou bien sur un circuit plus sophistiqué?

Après une enquête importante, il apparaissait qu'il était trop tôt pour définir avec précision les fonctions de la carte non seulement dans le domaine bancaire mais encore dans de nombreux autres marchés potentiels tels que la télévision à péage, les dossiers portables ou les cartes santé, mais il n'y avait aucun doute concernant le besoin de sécurité. Cet impératif impliquait le besoin de traitement d'informations à l'intérieur de la carte et le calcul des algorithmes cryptographiques.

Ces considérations plaidaient en faveur d'un produit flexible et sûr, fiable et économique, capable d'évoluer et d'être normalisé, en d'autres termes une carte à base de microprocesseur. En 1978, j'ai breveté le «SPOM», une nouvelle architecture pour un microprocesseur autoprogrammable monolithique capable de traiter de façon sûre des applications multiples grâce aux opérations d'auto-programmation à l'intérieur d'une mémoire non volatile.

Ma société était le leader dans le domaine du TAB (Tape Automated Bonding), nous avons ainsi développé quelques prototypes à l'aide de cette technologie très avancée. Mais, rapidement, nous avons migré vers la technique traditionnelle du «wire bonding» pour des raisons économiques ainsi que pour sa compatibilité avec les processus courants de fabrication de semi-conducteurs. Pour arriver au succès, il nous a fallu plus de deux ans d'efforts. En même temps nous avons défini la répartition et l'emplacement des contacts électriques qui ont été adoptés afin de simplifier les problèmes de packaging et d'améliorer la fiabilité. Il nous apparaissait comme évident que nous devions réduire au minimum le nombre de contacts et adopter une interface série pour une communication en semi-duplex. Des considérations similaires ont contribué à la décision concernant la position du module électronique sur la surface et non pas sur le bord de la carte.

Lorsque je suis venu aux Etats-Unis pour convaincre les fabricants de semi-conducteurs de coopérer à ce projet ambitieux, j'ai été reçu avec intérêt mais aussi avec scepticisme concernant la faisabilité du produit Il n'était pas évident de maîtriser la technologie consistant à combiner un microprocesseur de technologie MOS avec une mémoire EPROM. Quelques semaines plus tard le magazine Electronics mentionnait qu'un Français voyait «un microprocesseur dans chaque portefeuille» et expliquait qu'une carte avec un microprocesseur pouvait mémoriser le solde bancaire de son détenteur avec une protection plus efficace contre une utilisation frauduleuse.

Le 21 mars 1979, la première carte à puce était opérationnelle. C'était le fruit d'une solide coopération entre CII-Honeywell Bull et Motorola, où j'avais rencontré des personnes aux pensées futuristes qui étaient motivées par la

même conviction. Cette carte à puce comprenait deux puces: une mémoire 2716 EPROM et un microprocesseur 8 bits 3870. Ce préalable d'une carte à deux puces était essentielle afin de prouver la faisabilité du produit et de fournir un outil expérimental flexible et pratique. Par ailleurs, il s'agissait surtout de convaincre les décideurs d'utiliser cette technologie émergente. Cette carte à deux puces a également joué un rôle prépondérant dans l'initialisation des applications et dans le développement des différents éléments des systèmes utilisant ces cartes.

En parallèle, nous avons conçu la solution de la puce monolithique avec Motorola et, en octobre 1981, le premier micro-ordinateur équipé d'une puce auto-programmable, dont l'abréviation courante est «SPOM», fonctionnait du premier coup. Ainsi, les cartes à puce avaient été créées et le jeu pouvait commencer.

La carte CP8 fut choisie par la DGT (Direction Générale des Télécommunications) pour la toute première expérimentation en matière de télépaiement dans le monde à Vélizy, près de Paris, en utilisant la chaîne de télévision Antiope, pour transmettre des informations aux détenteurs de cartes et le réseau téléphonique pour le paiement électronique.

Entre 1982 et 1984, les banques françaises conduisirent trois expérimentations dans trois différentes villes: Blois, Lyon et Caen, afin de tester la fiabilité technique et économique de la carte dans des conditions réelles d'exploitation et afin de déterminer des spécifications définitives.

Baptisée «IPSO», cette expérience mettait en œuvre 125000 cartes et 650 terminaux. Une carte logique câblée était distribuée à Lyon par Schlumberger, Caen revint évidemment à Philips qui avait une usine implantée dans la ville, tandis que CII-Honeywell Bull équipait Blois avec une carte à microprocesseur CP8 à une puce.

1984 fut le jour de la reconnaissance: seule l'expérience menée à Blois s'est avérée convaincante et les banques choisirent le micro-ordinateur Bull plutôt que la carte logique câblée, et sa généralisation sur l'ensemble du territoire français fut lancée en 1986. Pendant ce temps, la «télécarte», une carte à mémoire prépayée pour le téléphone fit son apparition en 1983 sous l'impulsion de la DGT. Elle fut d'abord fabriquée par Schlumberger. Depuis cette époque, d'importants progrès ont été réalisés. Plus d'un milliard de cartes sont en service dans différents domaines de l'activité humaine. Des progrès énormes réalisés dans la technologie des semi-conducteurs ont eu des répercussions sur les cartes à puce avec l'avancée rapide vers la technologie CMOS et avec la densité qui a été multipliée par deux tous les quatre ans. Cela a amélioré la taille des mémoires, la

performance, la consommation de puissance, la sécurité et les coûts. D'ici l'an 2000 il sera possible d'avoir la puissance d'exploitation d'un PC dans une carte à puce ainsi que des coprocesseurs cryptographiques performants. Les organisations de standardisation nationales et internationales ont produit des normes acceptées sur le plan universel et, plus récemment, Europay, MasterCard et Visa se sont mis d'accord sur une plate-forme pour des applications à l'échelle mondiale. Je me rappelle un trait d'esprit d'un ancien ingénieur en chef de mon entreprise qui disait : «Vous l'avez fait parce que vous ne saviez pas que c'était impossible»