ARTICLE PARU DANS LA REVUE INTERNE
« L'ECHO DES ALPAGES »
DE SUPELEC RENNES,

P. CHOUR

3 décembre 1986

CARTE A PUCE

1 STRUCTURE D'UNE CARTE A PUCE

1.1 Architecture matérielle

Une carte à puce se présente comme une carte de crédit munie d'un micro-circuit qui est en fait un micro-ordinateur.

Comme tout micro-ordinateur, il se compose d'un processeur, d'une mémoire, d'une logique de commande et d'organes d'entrée-sortie. La mémoire de ce micro-ordinateur est composée d'une ROM dans laquelle se trouve un programme, d'une RAM de travail (actuellement 36 octets) et d'une mémoire programmable électriquement (actuellement, une E2PROM de 1 à 2 kilo-octets). C'est dans cette dernière que vont être stockées les informations que l'on aura à mémoriser durant ce que l'on appelle la "vie de la carte". Cette mémoire est organisée en zones ayant des niveaux de protection différents. En premier lieu, on distingue la zone secrète. Elle contient les différentes clés et codes secrets liés à la sécurité de la carte. Cette zone n'est pas accessible de l'extérieur de la carte. La zone suivante permet de mémoriser les accès à la carte, on l'appelle "zone de contrôle d'accès". Seul le processeur de la carte peut y écrire des informations.

Suite page suivante...

Sa lecture est liée à la présentation d'un code secret. La zone suivante va servir à mémoriser des informations liées au(x) domaine(s) d'application(s) de la carte. Son accès peut être différemment protégé. La dernière zone est en lecture libre.

La carte communique avec l'extérieur par une ligne série.

1.2 Phases de la vie d'une carte

Durant sa vie, la carte passe par plusieurs phases. La phase courante de la vie d'une carte est mémorisée par la présence d'un verrou se trouvant dans la zone de lecture libre. On distingue:
- la phase de fabrication,
- la phase de personnalisation,
- la phase d'utilisation,
- la phase d'invalidation (la carte n'est plus utilisable).

Lors de la phase de fabrication, le fabricant inscrit dans la mémoire de la carte des octets de test permettant de savoir si le système fonctionne correctement, un numéro de série et une clé dite "clé de fabrication". Il positionne ensuite le verrou indiquant que la phase de fabrication est achevée. La phase de personnalisation peut alors commencer.

La phase de personnalisation consiste à:
- définir des pointeurs indiquant où se trouvent les différentes zones mémoire (ces pointeurs se trouvent dans la zone de lecture libre),
- definir le niveau de protection de chacune de ces zones,
- inscrire dans la zone secrète les différentes clés et codes secrets qui serviront à l'application qui utilisera la carte (exemple : application bancaire)...

Toutes ces informations sont inscrites sous le contrôle de la clé de fabrication, clé qui est recalculée pour chaque carte par une autre carte particulière que l'on appelle "carte lot". On positionne ensuite le verrou indiquant que la phase de personnalisation est terminée. La zone secrète n'est plus accessible que par le processeur.

La carte est maintenant utilisable par l'application pour laquelle elle a été personnalisée. Au fur et à mesure que l'on y stocke des informations, la mémoire va se remplir. Lorsque celle-ci sera pleine, la carte sera dite "saturée" et ne sera plus utilisable. Elle devra alors être remplacée. En effet, on n'utilise pas actuellement la possibilité consistant à effacer des informations dans la mémoire. La carte est dite CONSOMMABLE.

2 SECURITE

2.1 Sécurité matérielle

Un premier niveau de sécurité de la carte à puce est défini par son architecture matérielle. Le micro-ordinateur est entièrement contenu sur un seul micro-circuit ce qui interdit d'aller espionner à l'aide de pointes de touches, les informations qui circulent entre le processeur et la mémoire contenant les informations secrètes. La technologie utilisée pour cette mémoire est celle d'une E2PROM ce qui interdit de lire quels sont les bits à 1 et à 0 à l'aide d'une loupe binoculaire. Enfin, tous les accès extérieurs à cette mémoire sont contrôlés par le processeur qui peut donc interdire la lecture et/ou l'écriture de certaines zones.

2.2 Sécurité logicielle

A la différence des cartes magnétiques, la carte à puce gère elle même sa propre sécurité à l'aide de codes secrets et de clés secrètes.

- Identification du porteur d'une carte :

La carte contrôle l'identité de son porteur à l'aide d'un code secret. Chaque présentation d'un code secret à la carte, qu'il soit bon ou faux, est mémorisée dans la zone de contrôle d'accès. Après 3 présentations consécutives de codes

secrets faux, la carte se bloque. Il est possible de la débloquer en lui présentant, d'une part, le bon code secret, d'autre part, une clé particulière qui est celle de l'émetteur principal de la carte (une clé de banque s'il s'agit d'une carte bancaire par exemple). Cette clé est recalculée pour chaque carte par celle qui a permis de générer la clé secrète lors de la personnalisation (carte mère). En cas de succès, la carte se débloque et peut de nouveau être utilisée. Afin d'éviter qu'un fraudeur tente de débloquer la carte par ses propres moyens en essayant des clés secrètes, la carte continue de mémoriser les tentatives d'accès à l'aide de cette clé dans la zone de contrôle d'accès. Au bout d'un nombre d'essais dépendant de la taille de cette zone, la mémoire sera saturée et la carte restera muette à toutes autres tentatives de déblocage. Ultime précaution, pour toute tentative d'utilisation d'une clé secrète fausse, la carte "saute" des bits dans la zone de contrôle d'accès afin de consommer celle-ci plus rapidement.

- Authentification

L'opération d'authentification permet de s'assurer qu'une carte est bien ce qu'elle prétend être. Pour ce faire, le système qui a besoin d'authentifier une carte lui envoie un nombre aléatoire et lui demande de lui renvoyer le résultat d'un chiffrement effectué à l'aide d'une clé secrète contenue dans dans sa mémoire. Le système émetteur fait le même calcul de son coté. Si le résultat renvoyé par la carte correspond à celui obtenu par le système émetteur, celui-ci saura qu'il a bien à faire à la carte attendue.

- Télé-écriture

La généralisation du système précédent permet l'écriture à distance dans la mémoire de la carte. Un émetteur envoie un message chiffré à inscrire dans la mémoire de la carte. Si cette dernière peut le déchiffrer, elle saura que l'opération a été émise par un organisme autorisé et la mémorisera.

3 LA CARTE A PUCE BANCAIRE

3.1 Généralités

La carte à puce bancaire est une des applications de la carte à puce. Elle utilise donc une carte standard qui sera personnalisée pour les applications bancaires. Elle autorise les mêmes fonctions que la carte magnétique classique mais avec une plus grande sécurité. Elle permet également de faire des opérations à distance. En attendant sa diffusion nationale, elle est actuellement évaluée dans l'agglomération Rennaise où environ 50000 cartes ont été émises.

3.2 Description de la mémoire

On distingue 4 zones mémoire :

- La zone secrète

Elle contient les clés secrètes, en particulier, la clé de la banque émettrice qui seule aura le droit d'effectuer certaines opérations sur les cartes qu'elle émet, et le code secret de 4 chiffres du porteur de la carte. Ce code peut être "modifié" une fois.

- La zone de contrôle d'accès

Elle permet au maximum 512 accès sous contrôle du code secret. La taille de cette zone étant définissable lors de la personnalisation, elle pourra être modifiée dans l'avenir.

- La zone de transaction

Cette zone mémoire est protégée en lecture et en écriture par le code du porteur. Elle sert à mémoriser les transactions faites à l'aide de la carte (montant, date, type de transaction (achats à crédit,au comptant, virements, retraits)). Les transactions sont inscrites par les terminaux de paiement (chez les commerçants, dans les distributeurs ou lors d'une opération de télé-paiement).

On y trouve également les plafonds de paiement pour chaque type de transaction ainsi que leur périodicité (sans périodicité, 1 à 10 jours glissants, un mois). Ces plafonds peuvent être changés par la banque émettrice. Pour cela, il suffit d'écrire un nouveau plafond dans la zone de transaction, les anciens plafonds inscrits pour le type de transaction choisi devenant alors invalides. Pour changer un plafond, il est nécessaire de disposer de la clé de la banque émettrice de la carte. La présentation de cette clé permettra de "signer" l'opération

effectuée et la rendra valide.

C'est également dans la zone de transaction que l'on va trouver un espace mémoire appelé "zone des certificats" qui est utilisé lors des paiements manuels chez les commerçants qui ne sont pas munis de terminaux capables d'inscrire des transactions dans la carte. Ils disposent alors d'un appareil appelé "certificateur" dont le rôle est de vérifier que la carte présentée appartient bien à son porteur (vérification du code secret) et que la carte est bien une carte bancaire par émission d'un certificat calculé par la carte. Ce certificat est alors reporté sur une facturette et servira de garantie de paiement pour le commerçant vis-a-vis de la banque (du moins jusqu'à un certain plafond de paiement). Le certificateur va progressivement remplacer le "fer à repasser" utilisé actuellement pour les paiements manuels (le "fer à repasser" est le nom donné à l'appareil permettant de reproduire l'embossage de la carte sur une facturette).

- La zone libre

Dans cette zone, on trouve pêle-mêle, des informations concernant les phases de la vie de la carte, les adresses des autres zones mémoire, l'identité du porteur, le numéro de série de la carte, son numéro bancaire, la devise dans laquelle sont exprimés les montants, le pays émetteur de la carte, le type de la carte (nationale, internationale...), etc...

4.3 Evolutions

La carte à puce bancaire actuelle peut encore se comparer à la carte magnétique bancaire. Elle offre les mêmes services mais avec plus de souplesse (plusieurs plafonds, possibilité de les modifier) et plus de sécurité.Ce dernier point autorise les opérations à distance ce qui est un plus par rapport à l'ancienne carte. A terme, d'autres possibilités pourront être introduites :

- Carte multi-service

Avec la prochaine génération de cartes à puce, il sera possible d'avoir plusieurs prestataires de service sur la même carte (banque, téléphone, parking...). Cette possibilité pose toutefois un problème de partage de la mémoire de transaction entre ces différents prestataires. Techniquement, ce n'est pas un problème et la carte existe déjà, économiquement, il reste à définir qui, de tous ces prestataires, paiera la carte...

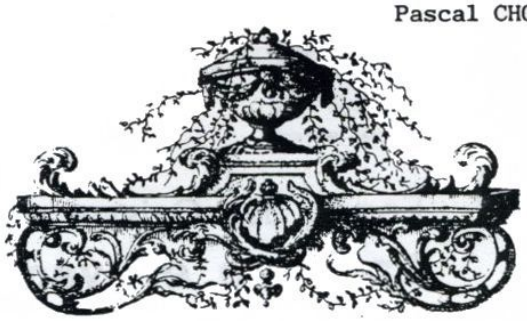
- Les montants préchargés

Actuellement, la carte à puce bancaire ne contient pas d'argent. Elle ne fait que mémoriser des transactions. Si la carte multi-services voit le jour, il sera possible d'acheter des droits d'accès à ces services sous la forme de montants préchargés (taxes téléphoniques, jetons de parking).

- L'effacement de la mémoire

Actuellement, la carte à puce n'est plus utilisable lorsque une des zones mémoire est saturée. Si l'on considère la carte multi-service dans laquelle seraient contenus des montants préchargés sous la forme de taxes de base (téléphone, parking...), il serait intéressant de pouvoir recharger ces zones lorsqu'elles sont saturées. Etant donné la mémoire utilisée (E2PROM), cette opération est techniquement possible. Il s'agira probablement d'une des nombreuses évolutions de la carte à puce.

Pascal CHOUR



"There are three ways to ruin yourself: gambling, women and technology. Gambling is the fastest. Women are the most pleasurable. Technology is the most certain".