Traitement de données

Les cartes à puce

Mise en situation.

La carte à puce succède :

- aux cartes à codes barres
- aux cartes à pistes magnétiques.

La carte à puce est une carte plastifiée aux dimensions de 85,6×54 millimètres comportant un circuit intégré (la puce). Ce composant est accessible électriquement par des contacts de cuivre. Les cartes SIM utilisées dans les téléphones portables sont une version faible encombrement de ces cartes.

Quelques exemples

La carte à puce a été inventée par le français Roland Moreno qui en déposa le brevet en 1974, après plusieurs travaux réalisés dans ce sens par des techniciens japonais et allemands.

Les premières cartes à puce étaient passives : l'équivalent d'un ensemble de fusibles (cartes téléphoniques, cartes de stationnement) formant la mémoire de travail, sous la protection d'une circuiterie logique interdisant l'écriture frauduleuse.

Les différents types de carte à puce.

Il existe trois catégories principales de cartes à puces:

- Cartes à mémoire
- Cartes à Microprocesseur
- Cartes sans contact

Seules ces deux dernières catégories peuvent embarquer des fonctionnalités cryptographiques. Il existe aussi des cartes hybrides afin d'exploiter les champs d'application des cartes à microprocesseur et des cartes sans contact. Selon la terminologie, les cartes hybrides comportent deux puces: une puce avec contact et une puce sans contact. Les cartes duales comportent une seule puce accessible par les deux procédés.

Les cartes à mémoire.

Simple support de stockage. La première utilisation de masse a été la télécarte : stock de points décrémenté à chaque appel.

Elle peut être en lecture seule. Grâce à l'augmentation de la mémoire des puces, on peut l'utiliser pour stocker des données plus importantes (cartes d'identité dans certains pays, dossier médical...). Mais les fonctionnalités sont limitées. La protection des données n'est pas assurée.

La plupart des cartes à mémoire simple sont réalisées en technologie EEPROM, et sont donc recyclables. Leur capacité est de l'ordre de quelques kilobits. Ces cartes sont destinées à des applications n'ayant pas à être sécurisées

Pour mériter l'appellation de « carte à mémoire personnalisée », une carte à puce doit contenir l'un des trois systèmes de protection suivant, réalisé en logique câblée sans le secours d'aucun microprocesseur :

- zone protégée en écriture après destruction d'un fusible

- zone protégée en lecture et écriture par un « code porteur (PIN)», le porteur étant défini comme l'utilisateur final de la carte
- blocage de la carte au bout de 4 présentations d'un PIN erroné
- protection par un « code émetteur » (l'émetteur étant l'organisme qui délivre les cartes et décide de leur contenu)

Les cartes à microprocesseur.

Le premier champ d'applications a été la carte bancaire française. Des fonctionnalités cryptographiques sont ajoutées dans ces cartes, qui disposent néanmoins de mémoire. Depuis l'augmentation de la puissance de leur processeur et de la taille de la mémoire, le nombre d'applications qui peut y être embarqué est (quasiment) sans limite.

Les premières fonctionnalités qui ont été demandées à ces processeurs furent cryptographiques, afin de s'assurer que le possesseur d'une carte en est bien son propriétaire.

Elles sont actuellement utilisées dans les téléphones mobiles, les cartes bancaires... Cartes multifonctionnelles avec possibilité d'utilisation de :

- identification
- signature électronique
- stockage sécurisé de données
- autres applications avancées seules ou en ajout des fonctionnalités précédentes

L'énergie nécessaire au fonctionnement de la carte ainsi que les données sont transmises entre le lecteur et le terminal par contact électrique. Ces cartes possèdent les caractéristiques suivantes :

- zone protégée en écriture ou en écriture et lecture par un code secret émetteur.
- zone protégée en lecture et en écriture par un code secret porteur.
- blocage de la carte après présentation de codes secrets erronés, mais avec possibilité de réhabilitation par l'organisme émetteur.
- mise en oeuvre d'algorithmes cryptographiques pour assurer la sécurité des transferts.

Certaines cartes à microprocesseur sont supportées par un puissant système d'exploitation appelé « COS » (Chip Operating System) par analogie avec le DOS.

La puce d'une carte typique (la carte bancaire B0') est constitué d'un microprocesseur 8 bits tournant à une vitesse de 4 MHz, elle dispose de 6 à 32 Ko de ROM, de 256 à 2048 octets de RAM et de 1 à 32 Ko d'EEPROM. La puce dispose en outre d'une seule ligne d'entrée-sortie.

Les cartes à puce de haut de gamme récentes contiennent des microprocesseurs plus puissants (32 bits à plus de 10 MHz) et des quantités de mémoire plus importantes (dépassant les 256 Ko d'EEPROM, 512 Ko de ROM). Les types de mémoire rencontrées dans les cartes à puce se diversifient également, notamment avec l'introduction de Mémoire Flash de plusieurs Mo à partir de 2005.

Gestion de la sécurité.

Un programme de codage (décodage) et/ou un code (mot de passe) dans la puce, inaccessibles de l'extérieur, sont le garant d'une bonne sécurité (au sens bancaire).

Avant d'être remises à la personne qui l'utilisera, une carte à puce est normalement 'personnalisée' électriquement (par l'organisme émetteur) via un lecteur de cartes et un programme informatique (outil de personnalisation), afin d'inscrire dans la puce les informations nécessaires à son utilisation. Par exemple, on inscrira dans une carte bancaire les références bancaires de l'utilisateur, ou dans la carte d'un contrôle d'accès, les autorisations accordées au porteur de la carte.

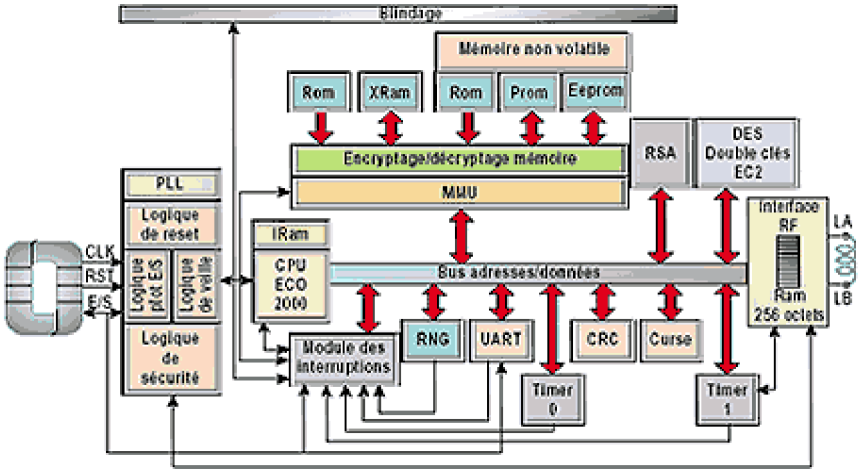
On peut considérer jusqu'à un certain point que les clefs USB, récemment apparues, font partie de la famille des « cartes à mémoire », mais il faut noter que leur mémoire n'intègre aucune protection limitant son accès, contrairement aux cartes à puce proprement dites, dont l'une des caractéristiques majeures est de protéger les données qu'elles contiennent de toute intrusion.

Les cartes sans contact.

Dans ces cartes, l'énergie et les données sont transmises sans aucun contact électrique entre la carte et le terminal.
Ces cartes sont typiquement utilisées pour de l'authentification (transports en commun, bagages, bâtiments...). Elles peuvent être utilisées jusqu'à environ un mètre du terminal. On voit bien le danger dans le cadre d'opérations de paiement. Une authentification du porteur est normalement requise dans ce cas (par le geste d'introduire la carte dans le terminal et de valider la somme par exemple).

Pour les problèmes d'authentification et de paiement sur une seule et même carte, on utilisera des cartes combinant les deux technologies.

Exemple : la carte à base du circuit SLE66CLX320P d'Infineon réunit sur sa puce toutes les caractéristiques d'un microcontrôleur pour carte à puce : double interface avec contact et sans contacts types A, B, et Felica (premier produit compatible avec les trois types). CPU 16 bits, diverses mémoires, cryptoprocesseur et toutes les logiques de sécurité.



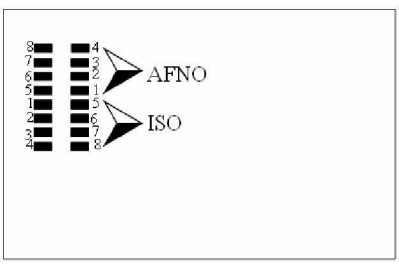
Les standards.

Les principaux standards en matière de carte à puce sont le fruit des travaux de l'ISO. La norme internationale ISO-7816 est découpée en 6 parties:

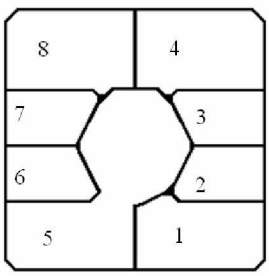
- ISO-7816-1 : caractéristique physique de la carte
- ISO-7816-2 : emplacement des contacts électriques
- ISO-7816-3 : nature des signaux électrique et protocole de transmission entre le terminal et la carte.
- ISO-7816-4 : organisation des données et sécurisation
- ISO-7816-5 : procédure d'inscription des applications
- ISO-7816-6 : données communes et règles de codage.

Les cartes normalisées épousent les dimensions des cartes à pistes magnétiques, c'est à dire 85x54 mm pour une épaisseur de 0,76 mm.

La carte à puce étant une invention française, les développements les plus anciens ont appliqué la norme « AFNOR », dite à contacts excentrés. Puis sont apparues les normes ISO 7816, définissant un positionnement « centré » des contacts du micromodule, avec de surcroît une rotation de 180°.



1 : Vcc
2 : RST
3 : CLK
4 : RFU
5 : GND
6 : Vpp
7 : I/O



Mise en œuvre des cartes à puces.

La mise en œuvre des cartes à puces nécessite l'usage d'un lecteur qui, en plus de l'aspect connectique, embarque une interface logicielle que l'on sollicite grâce à un protocole. La connexion physique du lecteur est en générale série, USB, Ethernet…

Les échanges entre le lecteur et la carte à puce nécessite (en plus de la connexion physique normalisée) un protocole définit par le fabricant de la carte à puce. Certaines cartes et lecteurs permettent de modifier la vitesse de l'échange entre la carte et le lecteur en utilisant le protocole PPS (au reset la carte indique les possibilités en vitesse, le lecteur utilise une vitesse compatible).

On parle d'échange de type APDU (Application Protocol Data Unit ou Paquet échangé entre deux applications sur un réseau. C'est le plus haut niveau du modèle en couches OSI).

Le cas de la carte Bull CP8.

La sécurité de CP8 comporte trois volets : sécurité du composant, sécurité des accès, résistance à la **fraude.**

Sécurité du composant.

- Les mémoires ROM (programmes) et EPROM (données) sont indélébiles et donc non modifiables.
- La technologie de ces mémoires les rend inaccessibles par voie physique directe, donc frauduleuse.
- Des protections spécifiques sont prévues contre les effacements par rayons UV et X.
- Dès sa fabrication le composant est protégé par une clé de fabrication après que ses points de tests aient été détruits. D'autre part, des témoins d'effacement sont dispersés dans le silicium et sont testés en permanence lorsque la carte fonctionne.

Sécurité des accès

- La sécurité des accès en lecture tient à la présence du microprocesseur qui contrôle totalement la nature des adresses impliquées secrètes, publiques, etc... et agit en conséquence.
- L'écriture en EPROM ou EEPROM est aussi totalement sous le contrôle du microprocesseur. Cette caractéristique d'autoprogrammabilité spécifique à CP8 permet des automodifications ou autodestructions en fonction de circonstances prédéfinies dans le masque.

A noter, de plus, que chaque mot écrit est accompagné d'un bit de validation qui garantit son écriture correcte. D'autre part certains mots comportent des codes correcteurs d'erreurs permettant de tester la non altération des données et éventuellement de les corriger.

Résistance à la fraude

Le composant CP8 n'est pas violable et il n'est pas duplicable.

Les accès sous clés sont comptabilisés par le composant lui-même, qu'ils soient bons ou mauvais. Par exemple trois essais incorrects consécutifs sur la clé porteur entraînent le blocage de la carte. Le déblocage est possible sous contrôle de l'émetteur de la carte.

Il y a symétrie de fonctionnement du composant sur clé correcte ou non. L'écriture, systématique en zone d'accès, du résultat d'un contrôle de clé ne permet pas de déceler par voie physique une différence de comportement de la carte.

L'écriture du résultat du contrôle de clé est nécessaire pour assurer un fonctionnement correct de la carte. En conséquence, la coupure de tension d'écriture ne peut être exploitée par un fraudeur.

Le circuit ne fonctionne plus sur horloge à fréquence réduite : pas d'investigations possibles "au ralenti".

Le circuit adopte le mutisme sur les ordres litigieux.

Le circuit autocontrôle sa vie depuis sa fabrication, puis lors de la personnalisation de la carte, et pendant son utilisation courante, avec possibilité d'autoblocage sur manoeuvres illicites.

L'invalidation d'une carte ou d'une partie de la mémoire se traduit par le positionnement d'un bit qui empêche définitivement les modifications et éventuellement les accès.

A noter qu'il est possible à l'usager de changer lui-même de clé porteur. Il peut ainsi avoir un code unique, connu de lui seul, pour les différentes cartes qu'il possède.

L'ensemble de ces caractéristiques fait que l'on peut mettre en service des équipements dans le public ne comportant aucune partie sensible fraudable car le lecteur ne fait aucun traitement, il ne fait que dialoguer avec la carte. Tout ce qui concerne la sécurité (calculs, traitements…) est porté par la carte, dans la carte,

Zones mémoires et droit d'accès :

L'espace mémoire de la carte comporte 6 zones qui sont détaillées dans le tableau ci-dessous.

	Effacement	Lecture	Ecriture
Zone Secrète	interdit	interdit	interdit
Zone d'Accès	interdit	Code porteur 2A	interdit
Zone Confidentielle	interdit	Code porteur 2A	interdit
Zone de Travail	Code porteur 2A	libre	libre
Zone de Lecture	interdit	libre	interdit
Zone de Fabrication	interdit	libre	Interdit (sauf verrous)

Zone secrète : Cette zone contient les clés et le code porteur de la carte. Elle n'est accessible que par le système d'exploitation qui utilise son contenu lors des vérifications de clé ou code.

Zone d'accès : Cette zone est utilisée pour mémoriser les présentations (bonnes et mauvaises) de clé et de code porteur. Elle est donc gérée par le système d'exploitation. Celui-ci peut bloquer la zone (et la carte) après 3 présentations successives de code porteur faux ou après une présentation de clé émetteur fausse. La zone peut être lue afin de connaître l'historique des présentations de clés.

Zone confidentielle : Les informations inscrites dans cette zone en cours de personnalisation sont ensuite protégées en lecture et ne sont plus modifiables.

Zone de travail : Cette zone contient les informations qui évoluent au cours de la vie de la carte.

Zone de lecture : Les informations inscrites dans cette zone en cours de personnalisation sont ensuite en lecture libre et ne sont plus modifiables.

Zone de fabrication : Cette zone en lecture libre contient des informations de personnalisation relatives à la structure de la carte (pointeurs de zone), à la protection de la (des) zone(s) de travail et à l'application (code d'application). Elle contient de plus des informations de fabrication comme le numéro de série de la carte.

Identification et authentification.

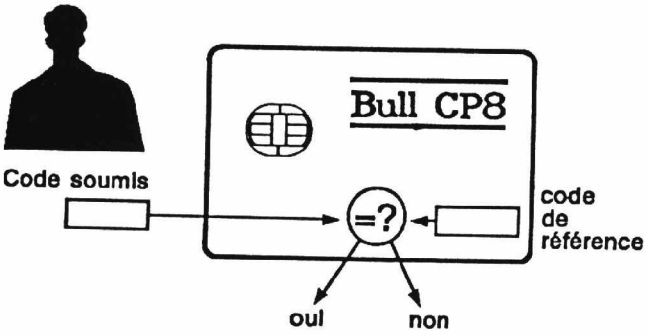
La sécurité, d'une manière générale, met en oeuvre plusieurs notions.

La première d'entre elles est l'identification.

Identifier une personne est un problème très difficile. On se contente généralement de l'identifier par le biais d'un badge qui lui a été remis, avec un code associé à ce badge, code qu'elle aura à fournir, pour prouver son identité à chaque usage de ce dernier.

On demande donc au porteur de présenter son code. La comparaison entre le code donné par le porteur et la référence contenue dans la carte CP8, est faite par la carte elle-même ou plutôt par le composant qu'elle contient.

Ceci est un "plus" très important, car dans les systèmes classiques, on se contente de lire la référence dans la carte (en clair, ou mieux, en chiffré) et de faire la comparaison à l'extérieur après un éventuel déchiffrement du code lu dans la carte. Ceci est donc très vulnérable, d'abord parce que l'on peut prélever la référence quand elle est lue, ou la lire simplement par ailleurs, ou bien s'approprier l'algorithme de déchiffrement et en faire un usage frauduleux, sur des cartes volées par exemple.



Identification par code

Avec CP8, tout se passe donc dans la carte, ce qui veut dire que l'appareil dans lequel on introduit la carte est parfaitement neutre sur le plan de la sécurité : il ne contient aucun élément secret à protéger.

L'information d'identification est généralement un code à 4 chiffres, (plus rarement à 5, 6 chiffres) mais compte tenu de la mémoire dont dispose la carte, on peut utiliser un critère très personnel comme un profil de reconnaissance biométrique empreinte digitale, forme de main, fond de l'oeil, caractéristiques dynamiques de signature, voix, etc. De telles informations peuvent nécessiter plusieurs centaines de bits.

La deuxième notion est celle d'authentification

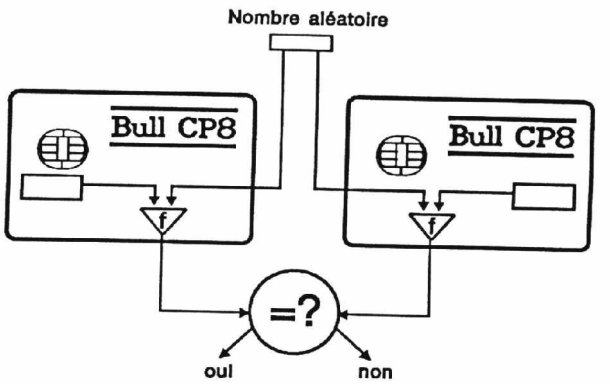
C'est le complément, à distance, de l'identification qui, elle, s'est déroulée localement entre le porteur et sa carte.

Il s'agit donc de savoir si c'est bien la personne habilitée (via sa propre carte) qui désire accéder à des informations, des services, des locaux, etc.

Il faut faire intervenir ici la notion de famille de carte, avec une carte mère ou carte de référence, et des cartes filles, qui sont les cartes des usagers du système.

Faire partie de la même famille, c'est partager le même algorithme, le même secret et être capable de le re-calculer, s'il s'agit d'un secret diversifié c'est à dire différent pour toutes les cartes de la famille.

Cela veut dire que le système central chargé de la sécurité possède une carte mère ou module de sécurité capable d'authentifier seulement les cartes filles faisant partie de sa famille.



L'AUTHENTIFICATION ENTRE CARTES

Authentification entre carte

Cette authentification se fait en demandant à la carte mère, toujours présente au niveau central, et à la carte fille qui a été introduite dans un terminal, d'exécuter chacune pour leur compte l'algorithme de cryptage qu'elles contiennent (TELEPASS dans notre cas).

L'algorithme travaille avec les données qu'il trouve dans chaque carte en particulier le secret, mais aussi avec un nombre aléatoire d'origine externe ou interne à la carte suivant son type.

L'immense avantage de ce procédé d'authentification est qu'il n'est pas répétitif en ce qui concerne les informations échangées. Si l'on exécute des authentifications successives avec des cartes différentes, ou des ré authentifications avec la même carte, les nombres aléatoires échangés à l'aller et au retour seront différents et ce, avec une très grande probabilité.

Ceci prémunit donc contre la fraude par restitution d'un dialogue de connexion préalablement enregistré à l'insu de l'usager.

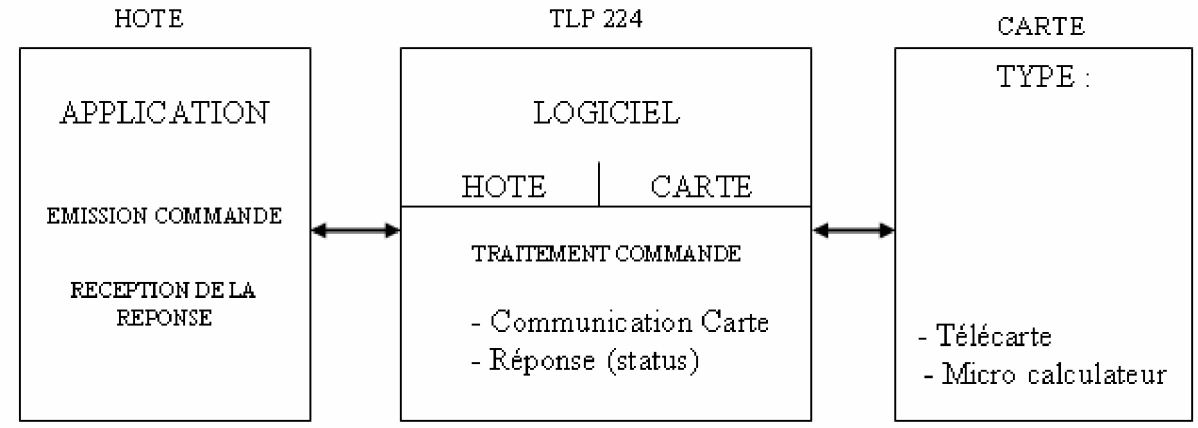
Le lecteur de carte TLP 224.

Le TLP224 est un lecteur/encodeur de cartes à microcircuit, à insertion manuelle. Il est raccordé à une Station de Travail par une liaison asynchrone RS 232 en utilisant un protocole spécifique d'échange avec la station de travail.

Il est capable de traiter :

- Les télécartes conformes au standard du Centre National d'Etudes et des Télécommunications (CNET) ; document, ST/PAA/TPA/PRI/1069 - Edition 3.
- Les cartes équipées de composant TS1200 de STM, ou compatibles.
- L'octet d'adresse OA doit contenir la valeur suivante 10001, xxxx. Le quartet de poids fort définit une tension de programmation de 21v.
- Les cartes à microcalculateur conformes à la norme ISO 7816, avec les restrictions suivantes :
  - fréquence initiale de la carte : Fo = 3,579545 MHz,
  - fréquence de travail de la carte : F = 1 (fs = fo),
  - traitement du dialogue asynchrone uniquement,
  - reset actif bas uniquement,
  - cadence du dialogue à 9600 bits/s uniquement,
  - limitation Icc (carte) à 110 mA,
  - limitation Ipp (carte) à 50 mA.

Le TLP224 permet un couplage transparent des Cartes c'est-à-dire qu'il exécute les ordres, élabore les réponses, mais ne fait aucun traitement sur les informations. Ces ordres sont au nombre de six, dont deux sont dédiés aux télécartes.



Chaque échange s'opère en 3 phases :

1. Emission d'une commande de l'Hôte vers le TLP224.
2. Traitement de la commande par le TLP224.
3. Réception par l'Hôte de la réponse du TLP224 relative à l'exécution de la commande.

Les échanges sont rythmés de la manière suivante :

1. Le TLP224 se met en mode réception,
   - § à sa mise sous tension,
   - § après l'émission d'une réponse.
1. Le TLP224 se met en mode émission,
   - § après l'émission d'une réponse.
   - § quand il est prêt à émettre sa réponse à l'Hôte (signal RTS).

La cadence du dialogue est de 9600 bits/s. avec 8 bits de données, pas de parité et 1 bit stop.

Les protocoles de communication.

Les protocoles de communication utilisés sont au nombre de 2 :

- Le protocole TLP224 qui définit la nature des échanges entre la poste de travail (PC) et le lecteur.
- Le protocole d'échange entre le lecteur et la carte ISO7816.

Les trames destinées à la carte seront encapsulées dans la trame TLP224 en tant que données.

Les trames.
La constitution d'une trame : è Caractère de début : STX ici $60
è Longueur de la trame (LNG) comprise entre LNG (exclu) et LRC (exclu).
è Puis trame CP8
è Puis checksum appelé LRC, qui est un OU exclusif de tous les octets compris entre STX (inclu) et LRC (inclus).
è Puis caractère de fin de trame, ici ETX ($03)

Exemple d'une trame reçue par le PC : 60 07 00 FF FF FF FF 90 00 F7 $^{E}_{X}$
Cette trame vient en réponse à un ordre de lecture de 4 octets.