**CE CHAPITRE DOIT ETRE PRECEDE PAR LA LECTURE DU COURS COMPLET SECTION UNE POUR SE RAPPELER LES PROTOCOLES D’ECHANGES CARTE-LECTEUR.**

**Rappel :**

Principe de l’authentification mutuelle

Lorsque la carte est insérée dans le lecteur, le lecteur envoie une commanded’authentification- La carte envoie au lecteur un numéro unique contenu dans un des registres
- Le lecteur traite ce nombre avec un algorithme cryptographique et
retourne le résultat obtenu à la carte
 En même temps, la carte fait le même calcul
- La carte compare son résultat avec celui du lecteur, s’il y a égalité =>
le lecteur est identifié par la carte
- La carte utilise ce résultat pour calculer une nouvelle valeur à l’aide d’un algo
cryptographique
- La carte envoie le nouveau résultat
 Le lecteur procède de la même manière, si égalité => il a identifié la carte

**LECTEURS DE CARTES**

Les CAM communiquent avec l'environnement par l'intermédiaire de lecteurs ou, pour être plus précis, de lecteurs-encodeurs. En effet, à l'inverse de ce que l'on trouve dans le monde des cartes à pistes magnétiques pour lesquelles il existe des systèmes permettant la lecture de la piste (lecteur) et des systèmes permettant à la fois de lire et d'écrire (lecteurs-encodeurs), il est rare que l'on puisse utiliser une CAM sans que le lecteur sache également écrire, ou au moins, offrir à la carte la possibilité de modifier sa mémoire. Dans la suite de ce chapitre, on considérera que tous les lecteurs sont des lecteurs-encodeurs.

.

**ANATOMIE D'UN LECTEUR DE CAM**

Schématiquement, un lecteur de CAM se compose de trois sous-ensembles :

* le connecteur,
* le coupleur,
* l'unité de traitement.

**Le connecteur**

Le connecteur est un élément mécanique assurant la liaison électrique entre les contacts de la carte et le coupleur devant offrir les caractéristiques suivantes :

* assurer le guidage de la carte de façon à assurer un positionnement correct de ses contacts,
* assurer la liaison électrique entre les contacts et le coupleur,
* autoriser ou non l'activation des contacts de la carte, celle-ci ne devant avoir lieu que lorsque les contacts du connecteurs sont correctement positionnées par rapport à ceux de la carte,
* il ne doit pas risque d'entraîner une détérioration du support plastique, que ce soit par torsion ou par frottement excessif.

Plusieurs méthodes sont utilisées de la plus simple à la plus sophistiquée.

**Connecteur à balais**

Le connecteur se présente sous la forme d'un boîtier parallélépipédique de dimension légèrement supérieure à celle de la carte. Une fente permet l'introduction de la carte qui est naturellement guidée par les cotés du boîtier. Des contacts à balais viennent frotter sur la carte. Lorsque celle-ci arrive en butée, les balais sont exactement positionnés sur les contacts de la carte (à condition que celle-ci ait été introduite dans le bon sens !). L'autorisation d'activation des contacts peut être faite par un micro-interrupteur à faible course ou par un dispositif opto-électronique.

Ce type de connecteur présente l'avantage d'avoir un encombrement réduit, d'être simple à fabriquer et d'offrir une bonne robustesse étant donné l'absence de pièces en mouvement. Le fait que les balais frottent sur la carte permet d'arracher la couche d'oxyde qui aurait pu se former sur les contacts de la carte. Par contre, ce frottement tend à rayer le support plastique et peut à la longue encrasser les balais et par contre coup, encrasser les contacts de la carte.

**Connecteurs à mâchoires**

Ce type de connecteur comporte un certain nombre d'éléments mobiles décrits ci-dessous :

* un boîtier plastique forme le corps du connecteur. Il présente une fente en sa face avant pour l'introduction de la carte,
* à l'intérieur de ce boîtier se trouve un chariot mobile guidé par des rails. Au repos, ce chariot est positionné à l'extrémité du boîtier où se trouve la fente. Ce chariot comporte également un aimant dont nous verrons l'usage par la suite.
* Une mâchoire comportant des contacts est placé sur le chariot. Au repos, cette mâchoires est maintenue ouverte grâce à un ressort de rappel. Lorsque le chariot se déplace vers l'arrière du boîtier, la mâchoire se referme.

la carte est insérée dans la fente du boîtier et poussée dans le connecteur. Elle se place sur le chariot et tend à l'entraîner vers l'arrière du boîtier. La mâchoire se referme et vient positionner ses contacts sur ceux de la carte. Le jeu mécanique du système introduit un léger frottement permettant d'arracher la couche d'oxyde qui aurait pu se former. Si l'on continue de pousser la carte, l'ensemble chariot, mâchoire et carte se déplacent vers le fond du boîtier jusqu'à arriver en butée. L'activation des contacts est autorisée par un relais magnétique qui réagi au champ de l'aimant placé sur le chariot. Lorsque celui-ci arrive à une certaine distance du relais, celui se ferme et les contacts de la carte peuvent être activés. La précision n'a pas besoin d'être parfaite car la carte est correctement placée quasiment dès son introduction.

Ce type de connecteur a été fabriqué par la société Bull-CP8. Il présentait l'avantage de ne pas détériorer le support de la carte avec pour corollaire le fait de ne pas encrasser les contacts du connecteur puisque ceux-ci ne frottaient pas sur le support plastique. Il était par contre très volumineux ce qui empêchait son utilisation dans des équipements miniaturisés et relativement complexe à fabriquer étant donné le nombre de pièces entrant dans sa composition.

Les connecteurs venant d'être décrits ne concernent que des systèmes à insertion manuelle de la carte. D'autres procédés existent pour des équipements motorisés.

**Les coupleurs**

Le coupleur est le dispositif électronique destiné à gérer l'interface carte. Réalisé en élément discret à l'époque héroïque de la CAM, on trouve désormais des dispositifs intégrés relativement miniaturisé. Généralement, le coupleur offre les fonctions suivantes :

* génération de l'horloge. Elle et généralement fixe et vaut la valeur de base fixée par la norme,
* génération des tensions et courant de programmation,
* gestion de la ligne d'entrée-sortie.

L'avènement des cartes comportant leur propre générateur de tension a permis la réalisation de coupleurs simplifiés ne gérant pas la tension de programmation (Vpp n'est plus utilisé).

**L'unité de traitement**

L'unité de traitement gère le coupleur et le programme en fonction des octets systèmes que celle-ci fournie lors de la remise à zéro. Elle gère également le dialogue avec le système auquel est raccordé le lecteur de carte. De cette façon, ce dernier n'a pas à se préoccuper des caractéristiques physiques de la carte.

**Les lecteurs de table**

Sous cette appellation, on trouve des lecteurs raccordables à des systèmes informatiques via une ligne asynchrone ou une prise USB. Ils disposent de leur propre alimentation pour les plus anciens ou sont directement alimentés par l'USB pour les lecteurs actuels.

Certains d'entre-eux sont programmables.

**Les lecteurs portables**

Ces lecteurs sont généralement munis d'un clavier et d'un afficheur LCD. Ils disposent de batteries rechargeables ou parfois une simple pile leur donnant une certaine autonomie et sont raccordables à un système informatique via une ligne asynchrone ou une prise USB. Les premiers lecteurs étaient tous programmables. Dans les années 1990, la plupart étaient programmables ce qui leur permettaient d'adresser plusieurs types de marchés.

Depuis le milieu des années 2000, avec la baisse de coût de production des appareils électroniques et la généralisation des cartes, on trouve de plus en plus de lecteurs dédiés (par exemple, pour lire le contenu de sa carte, pour générer des mot de passe à usage unique, etc.).

**Les lecteurs à intégrer**

Il s'agit le plus souvent de lecteurs OEM destinés à être intégrés dans d'autres équipements. Ils ne disposent pas d'alimentation en propre et ne sont généralement pas programmables. Certains d'entre eux sont motorisés et peuvent également lire les cartes à piste magnétiques. Dans cette catégorie, on se souvient que dans les années 1990 existait également une offre de lecteurs intégrables dans des micro-ordinateurs qui pour certains se branchait directement sur le bus. Souvent, la partie visible avait l'apparence et les dimensions d'un lecteur de disquette et pouvait donc être installés en face avant de l'ordinateur.

Philips-TRT proposait même un ensemble complet de contrôle d'accès qui empêchait le PC de démarrer le système d'exploitation tant que l'utilisateur ne s'était pas correctement authentifié (la carte additionnelle gérant le lecteur prenait la main sur le bus du PC).

En 1997, Microsoft avait annoncé que le prochain périphérique standard des compatibles PC serait le lecteur de carte. Pour cette raison, Microsoft avait décidé d'intégrer dans son système d'exploitation Windows les primitives permettant à un programme de dialoguer de façon transparente avec des cartes. Pour être d'un coût abordable, le lecteur cible annoncé se résumait quasiment à un simple connecteur. La partie coupleur et unité de traitement était directement gérée par le système d'exploitation, une UART du PC fournissant les signaux nécessaire au dialogue avec la carte.

Au final, cette intégration a donné le PC/SC et en pratique, les lecteurs ont directement été intégrés dans des périphériques USB.

**Dialogue lecteur-carte**

Lorsqu'il est dit « transparent », le lecteur n'est qu'un intermédiaire entre une unité centrale (UC) et la carte. La procédure de liaison de données permettant à l'UC de communiquer avec le lecteur est en général très simple et permet :

* de mettre la carte sous ou hors tension. Ces ordres sont directement interprétés par le lecteur et sont les seuls pour lesquels il n'est pas transparent,
* d'émettre des ordres élémentaires à la carte et d'en recevoir les réponses.

Ces lecteurs sont bien adaptés à des applications pour lesquelles toute l'intelligence peut être ramenée au niveau de l'UC.

Les lecteurs doivent normalement être conforme à la norme ISO concernant les CAM. Ce n'est malheureusement pas toujours le cas. Les principaux problèmes rencontrés sont les suivants :

* Certaines cartes (anciennes) nécessitent une tension de programmation sur le contact Vpp. La norme prévoit que la valeur de cette tension se situe dans un intervalle [Vmin, Vmax] avec un pas de 0,1 volt. Beaucoup des premiers lecteurs disposaient d'un générateur de tension fonctionnant par pas de 1 volt. Les cartes demandant un Vpp de 12,5 volts (par exemple) n'étaient donc pas acceptées.
* Certains lecteurs ne supportent que les cartes travaillant dans une certaine convention (inverse ou directe, cf chapitre sur la normalisation).
* Certains connecteurs n'acceptent pas les puces en position basse (ou en position haute).
* Beaucoup de lecteurs ne savent travailler qu'avec des cartes asynchrones (qui sont devenues les plus courantes, heureusement).
* Certains lecteurs « mangent » une partie des octets émis par la carte lors de la mise sous tension ce qui complique leur reconnaissance.

Heureusement, la généralisation des applications bancaires à travers l'adoption de la norme [EMV](https://www.pascalchour.fr/ressources/pccam/cours/cartes.htm#emv) et la simplification que cela a occasionné ([EMV](https://www.pascalchour.fr/ressources/pccam/cours/cartes.htm#emv) utilise un sous-ensemble de la norme) fait que finalement, la conformité à [EMV](https://www.pascalchour.fr/ressources/pccam/cours/cartes.htm#emv) a été recherché par la plupart des acteurs ce qui garanti, au moins pour les cartes avec contacts, une certaines garantie d'interopérabilité

On notera que pour des raisons de sécurité, certains lecteurs dits transparents ne le sont pas tout à fait. il s'agit en particulier des lecteurs disposant d'un écran-clavier

Pendant une vingtaine d'années, les tenants de la sécurité prônaient que la saisie du code porteur devait être faite localement sans que le PIN circule sur l'ordinateur auquel il était raccordé.

Cela impliquait généralement de disposer de lecteurs programmables afin de pouvoir leurs faire exécuter la séquence d'ordres nécessaires à la saisie et la présentation du PIN à la carte

Cette volonté partait certes d'un bon sentiment (et accessoirement, d'une bonne vision de la sécurité) mais oubliait complètement l'aspect économique des choses : les lecteurs programmables coûtaient chers.

Au final, beaucoup de projets ont capoté a cause de cette obstination et beaucoup d'énergie a été dépensée pour définir le « futur » standard de lecteur programmable (j'en a connu pas mal  le [TLP124](https://www.pascalchour.fr/divers/lecteurs_cartes/lecteurs/tlp124.htm), le [LECAM](https://www.pascalchour.fr/divers/lecteurs_cartes/lecteurs/lecam.htm) et ses concurrents, Cybercom, Finread...).

Evidemment, les tenants de cette solution avaient raison... mais beaucoup trop tôt. Il aura fallu attendre la fin des années 2000 pour voir apparaître des lecteurs très bon marché et des standards suffisamment stables pour que ce type de lecteur soit économiquement viable

Ces lecteurs ne sont donc plus complètement transparents puisqu'ils exercent leur intelligence lors des saisie et présentation de code. Bien sûr, cela ne marche que si les applications sont conçues pour. Si elles demandent elles-mêmes le code porteur dans une fenêtre de saisie sur le PC de l'utilisateur, cela annule l'intérêt de disposer d'un tel lecteur. Et il suffit qu'il soit saisie une fois sur le PC pour que le code soit potentiellement compromis (du moins, selon la politique de sécurité qui interdit cette saisie).

Malheureusement, dans un environnement grand public, il est très difficile de maitriser les multiples applications qui pourraient accéder à la carte et il est encore plus difficile de maîtriser un éventuel *malware* qui se faisant passer pour une application légitime, demandera à l'utilisateur de saisir son code porteur dans une fenêtre idoine, ce que l'utilisateur ne manquera pas de faire, à moins d'avoir été particulièrement bien éduqué ou d'être un paranoïaque accompli