DOSSIER 2

LA CARTE A MICROCIRCUIT, PREMIER MÉDIA A ACCÈS LOGIQUE

par **Roland Moreno**, Président directeur général de la Société INNOVATRON

Ce qu'il faut avant tout retenir concernant la Carte à microcircuit, c'est le caractère original du média que représente ce nouveau dispositif.
Contrairement à la désignation française habituelle (« Carte ***à mémoire*** »), qui n'exprime à l'évidence qu'une moitié du principe mis en œuvre, la formule américaine « smart card » représente de façon parfaitement imagée la caractéristique de la Carte à microcircuit : celle-ci, rendue maligne, ou encore ***futée*** par les microcircuits qui protègent l'accès logique à sa mémoire, ne se laisse pas « rouler » par les tentatives malveillantes d'un humain ou surtout d'une ***machine***.
Or, c'est bel et bien la carte magnétique (que précisément la Carte à microcircuit espère détrôner) qui constitue la carte à mémoire la plus typique : un badge plastique au format normalisé, dont les pistes brunes supportent ces oxydes métalliques utilisés comme mémoires depuis l'aube même de l'informatique. Offrant un espace d'enregistrement unidimensionnel, la carte magnétique accueille et conserve l'information qui lui est confiée exactement dans les mêmes conditions d'accessibilité et de pérennité qu'une feuille de papier.
Les rapports d'influence qui peuvent être établis entre le monde extérieur, le média, et l'information sont donc strictement équivalents, et l'on peut ainsi, sans aucune entrave, condition ou restriction :
– adresser un point quelconque de l'espace,
– lire l'information enregistrée à cet endroit,
– effacer l'information,
– altérer l'information,
– écrire une information.
Au contraire, la Carte à microcircuit oblige l'opérateur extérieur à se placer, non pas face à un espace mais plutôt face à une sorte de ***guichet :*** l'opérateur dépose dans la gouttière de communication sa ***requête*** (adresser l'espace-mémoire, lire, écrire, etc) et reçoit peu après l'indication du ***sort*** subi par sa requête : agréée ou non, et, éventuellement, résultat.

La Carte à microcircuit

Quinze ans après que son inventeur Roland Moreno en a déposé le brevet, la « Carte à microcircuit » ne cesse aujourd'hui de se développer.
Technologie de pointe, elle trouve de nombreuses applications, plus particulièrement dans le domaine de la sécurité. De par son principe même, elle est un outil des plus sûrs.
Elle permet d'assurer des contrôles divers : contrôle d'accès physique des personnels, contrôle d'accès logique à des applications informatiques (par identification et authentification des opérateurs).
Le Service de sécurité de FRANCE TELECOM étudie ses possibilités d'emploi dans ces différents domaines.

DOSSIER 2

SUITE

Cette caractéristique est fondamentale : la fonction MÉMOIRE est en arrière-plan de la fonction TRAITEMENT vis-à-vis du monde extérieur (ce qui justifie totalement une appellation telle que « carte active » (Philips), ou « smart card » (Intelmatique).
Tous les média antérieurs (et d'une façon plus générale, tous les médias « passifs ») partagent, avec la feuille de papier et la carte à pistes magnétiques les caractéristiques liées au « ciel ouvert » qui surplombe l'espace d'enregistrement. Carte perforée, carte holographique, disque ou bande magnétique, tableau noir, badge plastique à embossage, photographie, microfilm : tous ces média supportent l'information, aucun ne la contient. Malveillant ou bienveillant, l'opérateur extérieur arrive dans le volume des données par les mêmes moyens d'accès, puisque aucune discontinuité ne peut être observée entre le monde extérieur et l'espace de stockage.
Le support réagit de la même façon aux sollicitations du monde extérieur : accessibilité permanente quelle que soit l'identité ou la volonté de l'éventuel opérateur.
Un coffre-fort, au contraire, contient les objets (ou les données) qui lui ont été donnés à garder et marque une discontinuité entre extérieur et intérieur : le passage d'un milieu à un autre est marqué par la double nécessité d'avoir à manœuvrer une lourde porte (ce qui prémunit le système contre les transitions accidentelles), et de s'identifier par la conjugaison d'une clef complexe et d'un mot de passe (ce qui limite l'accès aux seuls utilisateurs qui détiennent la clef et qui connaissent le code).
Encore, dans un coffre-fort, les papiers conservés ont-ils tous le même statut vis-à-vis de l'utilisateur : une fois la porte ouverte, ils peuvent être indistinctement consultés, écrits, corrigés, déchirés.
L'espace d'enregistrement offert par la Carte à microcircuit ne présente pas cette caractéristique d'isotropisme : d'une adresse à l'autre, les données n'ont pas le même degré d'accessibilité : lecture impossible, écriture impossible, lecture/écriture autorisées, etc. Si la Carte à microcircuit contient bien les informations – plutôt que de se contenter de les supporter – les traitements qu'elle effectue préalablement à tout accès aux données la distinguent fondamentalement de tout autre système de stockage.
En ce sens, la Carte à microcircuit est un dispositif original, dont les caractéristiques de défense sont généralement mal connues, et globalement enveloppées la plupart du temps sous l'appellation un peu magique de carte à circuit intégré ou encore de carte à microprocesseur. Le caractère parfaitement magique et omnipotent du « microprocesseur» (tout autant d'ailleurs que celui du « circuit intégré ») suffisent alors à résumer tout un ensemble de fonctionnalités présumées sous le chapeau simpliste « inviolable ».
Quels sont donc les tenants et les aboutissants de cette « inviolabilité » ?
Premier dispositif, la notion de NIVEAU DE SÉCURITÉ attachée à chaque enregistrement, combinée à des moyens (matériels et/ou logiciels) d'inhibition de lecture et d'écriture.
La mémoire est divisée en MOTS (par exemple de 32 bits) chacun d'entre eux repéré par une ADRESSE A et organisé en N bits d'information (par exemple : 30) et P bits de STATUT (ici : 2). Le niveau de sécurité attaché au mot est représenté par le sous-mot PØP1, où PØ signifie lecture interdite, et P1 écriture interdite.
Dès l'adresse A sollicitée, et indépendamment de toutes instructions complémentaires, le bit PØ (s'il est fixé) interdit toute éventuelle lecture, et de même le bit P1 interdit, s'il est fixé, une éventuelle écriture.
Ce cas correspond ici à un enregistrement définitif (écriture interdite) destiné à être traité à l'intérieur même de la Carte à microcircuit (lecture interdite) : le code confidentiel attaché à la carte par exemple.
Dans un autre cas de figure (PØ = Ø, P1 = 1), la lecture est autorisée et l'écriture interdite : cas de la date de validité de la carte par exemple (celle-ci doit être consultée par chaque lecteur de Carte à microcircuit, afin de vérifier si la carte présentée n'est pas périmée).
De nombreux niveaux de sécurité, plus fins, sont donc concevables (notamment avec P > 2 et compte-tenu éventuellement de sommes de contrôle ou codes autocorrecteurs d'erreurs), par exemple : lecture autorisée si carte invalide ET code émetteur correct. Ou encore : écriture interdite si code prestataire N° 2 correct, etc.
Dès ce stade, et sans même être dotée des autres moyens de sécurité ou d'identification qui la rendent si familière au plus grand nombre (code secret, compteur d'erreurs, etc.), la Carte à microcircuit constitue bel et bien une ***source de référence.***
Ce nouveau type de support d'informations fonctionne un peu comme un bureau d'enregistrement (où les documents stockés et les écritures passées reproduisent exactement l'histoire des événements qui ont été enregistrés), recevant successivement des informations, puis les nouvelles données amendant par addition les informations antérieures sans jamais procéder par substitution.
Une donnée enregistrée dans la Carte à microcircuit est donc nécessairement stable, et présente la même valeur informationnelle, dix minutes ou dix années après son enregistrement quel que soit le nombre et la nature des opérations logiques ayant été effectuées sur la carte pendant l'intervalle. La donnée n'a pas pu être modifiée si celle-ci était déclarée comme protégée en écriture, et n'a pas pu être consultée si son statut était une protection en lecture.
Par contre, elle a pu passer entre temps de mains en mains, et chacun de ses détenteurs a pu consulter les informations qui y étaient lisibles aussi bien qu'écrire aux adresses qui étaient inscriptibles, ce qui amène à introduire le second des systèmes de sécurité qui caractérisent la Carte à microcircuit : la comparaison interne du code personnel du porteur.
Le contexte d'utilisation visé est ici plus grave, puisqu'il permet en l'occurence de parvenir à la définition d'un support individuel d'information, caractérisé :
– par une confidentialité totale de l'essentiel des données contenues, celles-ci n'étant accessibles qu'au seul détenteur habilité de la carte,
– par une protection complète de la mémoire contre toute tentative d'écriture – même sur les mots vierges – ne provenant pas du détenteur habilité de la carte,
– par une dissimulation totale des informations secrètes éventuellement enregistrées dans la mémoire, y compris vis-à-vis de son propre porteur.
Exemple d'application : transmission de dépêches chiffrées entre ambassades, états-majors, etc. (exemple ambitieux, et même romanesque à dessein, afin que soit bien perçu le niveau de sécurité – presque ultime – qu'on se propose d'atteindre ici : d'une part, en raison de l'importance démesurée que présentent

La société INNOVATRON

La carte « à microcircuit » a été inventée en 1974 par un Français, Roland Moreno, qui a repris le support plastique de la carte classique pour y monter un micro-circuit.
La même année, Roland Moreno a créé la société INNOVATRON afin de déposer les brevets couvrant son invention et proposer sa carte aux utilisateurs éventuels : banques, DGT...
INNOVATRON n'a aucune unité de fabrication. Elle est, en revanche, détentrice de brevets et, à ce jour, a accordé 35 licences dans le monde, ce qui constitue un véritable « décollage » de la carte à microcircuit. Parmi les licenciés d'INNOVATRON figurent BULL en France, SIEMENS en Allemagne, PHILIPS aux Pays-Bas, SCHLUMBERGER aux États-Unis et le géant MITSUBISHI au Japon.

DOSSIER 2

SUITE

les informations manipulées ; d'autre part, en raison des moyens intellectuels, techniques et financiers qui ne manqueraient pas d'être mis en œuvre par l'adversaire éventuel en vue de violer la dépêche électronique).

Le principe retenu pour cette fonction de reconnaissance est celui de l'identification par corrélation entre deux données d'habilitation identiques (« code confidentiel ») :

— l'une, associée à la personne proprement dite du détenteur, et que celui-ci conservera en tête, par exemple un mot (T) de 4 à 12 caractères ;

— l'autre, enregistrée à l'intérieur de la mémoire de la carte, et qui constitue la référence (R).

De façon à éviter que la donnée R doive être envoyée à l'extérieur pour y être traite, c'est la Carte à microcircuit elle-même qui est chargée du travail de comparaison entre R et T. Ceci suppose que T soit introduite temporairement à l'intérieur de la carte, en provenance par exemple d'un petit clavier numérique sur lequel le porteur tabule son code confidentiel.

(On reconnaît au passage l'intérêt qu'il y avait à envisager, dans le cas du dispositif précédent, un statut d'interdiction de lecture : à quoi donc pourrait servir une donnée enregistrée dans la carte et spécifiée comme définitivement inacessible en lecture, si ce n'était pour exploiter cette donnée ***à l'intérieur même de la carte à microcircuit ?***).

En cas de comparaison positive, la suite du processus s'enclenche, tandis qu'en cas de comparaison négative, les circuits internes de la Carte à microcircuit se bloquent, ce qui contraint à déconnecter la carte avant de tenter un nouveau mot de passe.

Un tel système constitue une solution à la fois simple et parfaitement sûre dès lors que le format utilisé pour le code confidentiel est suffisamment long : le mur combinatoire fait très rapidement sentir ses effets dans ce type de spéculation et ainsi, dans l'hypothèse d'un mot de passe à 12 chiffres, environ un demi-millénaire serait nécessaire à une sorte d'« automate-casseur », générant en séquence toutes les combinaisons possibles de 12 chiffres et communicant avec la carte, sous forme sérielle, à la vitesse de 1 000 caractères par seconde.

A ce seul titre, et même sur la base du cahier des charges diplomatico-militaire envisagé plus haut, la Carte à microcircuit peut légitimement être considérée comme un support d'information ***indéfiniment inviolable.***

Il n'en est malheureusement plus de même si dans un contexte plus « civil » on s'efforce de n'utiliser qu'un classique code confidentiel à quatre chiffres : quarante secondes seulement seront nécessaires à l'automate-casseur, dans les mêmes conditions que précédemment, pour proposer à la Carte à microcircuit la combinaison adéquate.

Autant dire, on le voit, que dans le cas d'une donnée d'habilitation ***courte,*** la comparaison interne du code confidentiel n'apporte en définitive aucune sécurité réelle.

Et incidemment, il apparaît comme particulièrement choquant qu'un dispositif désormais aussi intelligent, finalement, que ce circuit intégré, ne s'aperçoive pas que 10 000 rafales successives de 4 chiffres représentent un événement aberrant, constitutif d'une présomption sérieuse d'agression : le troisième bouclier dont est équipée la Carte à microcircuit se situe donc en aval de son dispositif de comparaison du code confidentiel, et consiste en un système de ***mémorisation des erreurs de code.*** Sur la base d'un plafond pré-fixé par construction (20 erreurs par exemple), les circuits logiques du compteur d'erreurs sanctionnent la rafale par un blocage irréversible du fonctionnement de la Carte à microcircuit, de façon telle que toute exploitation ***utile*** de la mémoire de celle-ci devient impossible.

Ce mode de réaction peut très légitimement être assimilé à une forme d'autodestruction, et c'est indiscutablement ce mécanisme qui, par anthropomorphisme, est le mieux compris du public et des non-spécialistes qui assimilent volontiers la « carte à mémoire » à ce système de code confidentiel et d'héroïsme microélectronique.

En réalité, la sécurité apportée par ce dispositif particulier ne pourra que rester marginale dans le futur sur le plan des risques qu'elle permet d'éliminer : aucune systématisation ne peut être envisagée, par une organisation criminelle, du travail de vol de Carte à microcircuit dans la poche des utilisateurs puis de tentative d'appropriation des données contenues par essai systématique de combinaisons numériques.

Au contraire, le système de blocage des enregistrements par bits spécifiques de statut garantit une résistance des réseaux basés sur la Carte à microcircuit à une forme d'agression infiniment plus dangereuse : l'altération des données.

Supposons que soient convoitées les données échangées à l'intérieur d'un système d'information, lui-même basé sur la circulation d'un important parc de Cartes à microcircuit (par exemple les 20 millions de cartes d'un réseau de paiement interbancaire) : si le numéro identifiant la carte pouvait être ***modifié*** par les criminels de façon telle que la carte soit vue par le réseau comme ***une autre carte,*** il suffirait alors aux escrocs de détourner ou de dérober en sortie d'usine, sans nécessité particulière de discrétion, le plus grand nombre possible de cartes fraîches (par exemple 10 000, 100 000), et de les réinitialiser convenablement pour pouvoir exploiter aussitôt chacune des cartes frauduleuses dans d'excellentes conditions de tranquilité (c'est-à-dire sans que jamais le risque ne se présente d'une interpellation, la main dans le sac, par un quelconque policier, banquier ou caissier).

Un tel scénario-catastrophe n'aurait qu'une issue : la mise en sommeil du réseau dans sa totalité, le rappel des cartes en circulation et la destruction de toutes les cartes inventoriées, le changement de standard industriel, puis le redémarrage.

On devine que les promoteurs de tels systèmes d'information évaluent avec beaucoup de prudence les solutions techniques qui s'offrent à eux, et qu'ils sont évidemment beaucoup plus soucieux de parer ce type de fraude industrielle que la manipulation artisanale de cartes trouvées ou dérobées dans la poche de leur propriétaire.

Enfin, la Carte à microcircuit tire désormais parti de la présence sur son propre carré de silicium de puissantes ressources logiques pour traiter énergiquement (en entrée comme en sortie) les données dont elle a à connaître, notamment sous la forme de calculs et ***de chiffrement.***

Cette dernière fonction s'avère en effet indispensable pour toutes les applications de la Carte à microcircuit où un doute pourrait exister sur l'authenticité de la source de données se ***faisant passer*** pour une Carte à microcircuit : environnement « distant » (messagerie électronique, banque à domicile, vidéotex, etc.) ou « technicien » (protection de logiciel).

Ce domaine extrêmement fécond mériterait à lui seul un examen aussi détaillé que celui de la Carte à microcircuit proprement dite, car l'importance dans le futur de ces applications dépend en grande partie de la sécurité dont elles pourront bénéficier : pas de messagerie, pas de transferts de fonds, pas de logiciel pour microordinateurs sans une protection intégrée au système lui-même. Les indiscrétions (courrier), les abus (banque), la copie (logiciel) diviseront par cent les marchés possibles, et par conséquent provoqueront avant terme une désaffection des ***fournisseurs*** de telles applications.

La Carte à microcircuit contribuera donc à favoriser l'insertion de ces nouvelles activités dans la vie économique, par la sécurité, la confidentialité, la pérennité, qu'elle permet de garantir aux informations : nombreux sont désormais ceux qui pensent — en France où elle est apparue, mais aussi maintenant ailleurs dans le monde, USA et Japon compris — que la Carte à microcircuit a un rôle essentiel à jouer dans l'échange et dans la circulation des Biens du futur.