La sécurité «CB» un an après…

Des investissements considérables sont mis en œuvre pour renforcer la sécurité de la carte. Des dispositions juridiques vont compléter les améliorations apportées par les banques.

«La carte bancaire reste le moyen de paiement le plus sûr au monde».
Laurent Fabius, ministre de l'économie, des finances et de l'industrie, conférence de presse du 22 février 2001.

YVES RANDOUX
Administrateur
Groupement des Cartes Bancaires

A cette profession de foi envers le système «CB», répond une enquête Sofres effectuée récemment à la demande du Groupement des Cartes Bancaires. Il en ressort une perception extraordinairement positive des clients à l'égard du système «CB» : plus de 98 % des porteurs s'estiment satisfaits de leur carte. En d'autres termes, les turbulences médiatiques de l'an 2000 n'ont pas atteint la confiance dont nous honorent nos clients porteurs et commerçants. Cette confiance est-elle méritée ? et quels risques potentiels demeurent ?

La fiabilité du système sécuritaire du paiement par carte repose sur un microprocesseur. Celui-ci n'a jamais été attaqué en France et la seule tentative effectuée par l'américain Kocher, il y a quelques années, a été rendue inopérante par le progrès technologique. En revanche, lorsqu'une carte rencontre un lecteur – par exemple un automate de paiement – la reconnaissance mutuelle se réalise par un jeu d'algorithmes, dont l'un opérant dans le terminal a été effectivement cassé. Mais aucune fraude n'a été décelée sur la base de ce délit [1]. L'impact médiatique de cette affaire a conduit néanmoins le Groupement à anticiper certaines dispositions du plan de migration sécuritaire envisagé pendant la période 1998-2004. Les principales dispositions mises en œuvre sont les suivantes :

«Les serveurs bancaires seront l'objet de programmes de mise à jour considérables, notamment pour prendre en compte les modifications sécuritaires.»

■ Cartes

Généralisation d'une clé plus longue pour protéger la zone d'échange entre la carte et le terminal. Actuellement, pratiquement toutes les cartes «CB» en circulation sont dotées de ces nouvelles clés.

Mise en place sur les cartes «CB» d'une puce de nouvelle génération à partir de la rentrée 2001. Cette amélioration incorpore une protection renforcée du code secret et intègre les dernières évolutions de la technologie en matière de sécurité.

■ Terminaux

Le Groupement a signé un protocole avec les Fédérations de commerçants aux termes duquel les évolutions techniques sont pilotées en commun. Il en résulte les dispositions suivantes :

- tous les terminaux sont dotés du logiciel CB5.1 au 31 décembre 2001. Ceci signifie que tous les terminaux du commerce ont à la fois une solution logicielle pour traiter l'euro et de nouvelles normes sécuritaires. Celles-ci intègrent le calcul des clés longues ainsi que la télétransmission d'informations enrichies vers les serveurs bancaires ;
- le commerce basculera l'ensemble de ses terminaux aux normes EMV le 30 avril 2003.

■ DAB

Tous les retraits espèces se feront dorénavant en France, par lecture de la puce, la piste restant sur les cartes pour effectuer des seules opérations de paiement et de retrait à l'étranger.

■ Serveurs et back-offices bancaires

Les serveurs bancaires sont en première ligne de toutes ces évolutions. Ils seront l'objet de programmes de mise à jour considérables, notamment pour prendre en compte les modifications sécuritaires qui ont une implication dans la totalité de la chaîne de traitement. Celles-ci auront un impact sur les protocoles

[1] Il s'agit de l'affaire Humpich. Cet informaticien a trouvé la clé RSA 312 bits qui protége la valeur d'authentification, c'est-à-dire les données de reconnaissance mutuelle de la carte et du terminal.

d'échanges, les transmissions et la cryptographie ; en d'autres termes, c'est la totalité du dispositif technique bancaire d'émission et d'acceptation des cartes qui est remise à neuf à l'occasion du passage à EMV.

Des investissements de plusieurs milliards de francs

Banques et commerces investissent donc massivement pour le progrès technique et le renforcement sécuritaire des produits monétiques utilisés par leurs clients.

Au-delà de ces efforts qui représentent pour les deux communautés plusieurs milliards de francs, quels risques potentiels demeurent sur la filière de paiement par carte ?

Le risque zéro n'existe pas dans la monétique, ni dans aucun domaine. L'ampleur des investissements techniques et sécuritaires, complétés par la refonte du réseau d'autorisation, démontre la volonté de tous les acteurs de disposer d'un outil totalement modernisé et sûr. Cartes et serveurs monétiques seront donc à la hauteur de l'enjeu, et la mise en œuvre de l'authentification dynamique réduira définitivement les derniers risques sur les cartes. En effet, sur ce point particulier, l'objectif de l'authentification dynamique de chaque transaction est parfaitement identifié mais la technologie est encore trop récente pour être industrialisée et affronter dans l'immédiat l'épreuve du terrain.

Enfin, une réponse juridique a également été apportée à l'appui de tout cet arsenal technique. Largement étudiée dans les groupes de travail Lebranchu, tout au long de l'année 2000, une Charte est venue «boucler» ce dossier en définissant de nouvelles pistes d'améliorations ergonomiques ou sécuritaires, sans oublier la voie législative qui devrait renforcer la protection du système de paiement «CB». ●