PAR JEAN-MARC BORNET

Ancien élève de l'École supérieure de commerce de Paris, administrateur du Groupement des Cartes Bancaires « CB »

Cartes Bancaires « CB » : plus de sécurité pour plus de services

Le système « CB » créé en 1984 par la communauté des banques opérant en France pour promouvoir l'usage des cartes de paiement et de retrait a rapidement dû faire face à des problèmes de fraude, dont les conséquences étaient aussi bien économiques – les pertes induites – que commerciales – la confiance dans le produit. En retenant la technologie de la carte à puce pour répondre à ce défi, les Banques « CB » ont fait un choix porteur d'avenir : les cartes à puce – par leur caractère évolutif – permettent de répondre de façon durable aux besoins de sécurité technique et juridique ; elles se généralisent au plan mondial ; enfin elles ouvrent la porte à un enrichissement sans précédent de l'offre commerciale autour de ce qui n'était au départ qu'un moyen de paiement.

La carte de paiement à puce : un facteur de sécurité technique, juridique et donc économique

Émettrices de cartes de débit à piste magnétique au lancement du système Cartes Bancaires « CB », les Banques « CB » ont dû faire face à la fin des années quatre-vingt à une forte augmentation du nombre de cartes à piste contrefaites. Avec un taux de fraude de l'ordre de 0,3 % en constante progression, les Banques « CB », face à la menace sur l'équilibre économique du système, décidaient d'inverser durablement la tendance en faisant le choix de la technologie des cartes à microcircuit, le programme « carte à puce » était lancé. Quelques années plus tard, au début des années quatre-vingt-dix, les résultats étaient à la hauteur des enjeux : le taux de fraude constaté sur le système « CB » était divisé par 10, il est aujourd'hui stabilisé aux environs de 0,03 %.

Hors de France, divers facteurs ont retardé la prise en compte des enjeux de la fraude. Mais désormais les réseaux Visa et MasterCard ont fixé dans de nombreuses régions des règles qui conduisent de nombreuses banques en Europe, Asie du Sud-Est et Amérique latine à faire migrer leurs cartes au standard « puce » EMV.

L'évolutivité, atout majeur de la carte à puce

Le dimensionnement des algorithmes cryptographiques dans les cartes bancaires répond à un double besoin : les clés doivent être assez longues pour rester à l'abri des attaques basées sur les données produites, et assez courtes pour tenir compte des limitations des puces en mémoire et en vitesse de calcul. À ce jour, les clés RSA embarquées ont une longueur

Système « CB » en chiffres

Avec plus de 55 millions de cartes en circulation, 1 million de commerces et 51 000 distributeurs automatiques de billets, le nombre d'opérations réalisées annuellement par le système Cartes Bancaires « CB » excède les 7 milliards.

Les paiements par carte – plus de 280 milliards d'euros par an – représentent ainsi un quart de la dépense des ménages français.

Le système « CB » est le plus important d'Europe avec un volume de transactions de l'ordre de 25 % du total européen des paiements par carte, ou de 35 % dans la zone euro.

Le standard international EMV

EMV (Europay MasterCard Visa) désigne le nouveau standard international de sécurité des cartes de paiement (cartes à puce) qui tire son nom des organismes fondateurs :
– Europay International,
– MasterCard International,
– Visa International,
rejoints, depuis, par le japonais JCB International, au sein d'EMVCo. EMVCo LLC, créée en 1999, gère, maintient et développe les spécifications de cartes à circuit intégré EMV™ dont la première version est parue en 1996. Le premier rôle de cette organisation est d'assurer la maintenance de normes qui assurent l'interopérabilité et l'acceptation des cartes à circuit intégré utilisées sur les systèmes de paiement, à une échelle mondiale. Fin 2007, on comptabilise au niveau mondial plus de 700 millions de cartes EMV dont plus de 50 % émises dans les pays de l'Union européenne.

de 960 à 1 152 bits, ce qui est faible devant la longueur typique sur un PC (2 048 bits), mais encore bien supérieur aux records actuels de factorisation des entiers (de l'ordre de 700 bits ; la factorisation d'une clé publique RSA permettrait la divulgation de la clé privée).
Les algorithmes doivent également être renforcés pour résister aux combinaisons d'attaques logiques et physiques auxquelles les puces sont soumises, telles que la recherche de corrélations entre les secrets contenus dans les puces (clés, codes confidentiels) et les paramètres physiques les plus variés, ou les perturbations et injections de fautes pendant les calculs cryptographiques. Seule l'évaluation sécuritaire d'une puce, qui teste toutes les attaques connues au niveau de résistance le plus élevé, permet d'acquérir la confiance nécessaire pour la diffuser auprès des porteurs.
Le Groupement des Cartes Bancaires « CB » a choisi d'avoir recours à une méthode d'évaluation basée sur un standard international de sécurité « Les critères communs ». Ce processus d'évaluation s'appuie sur des laboratoires indépendants, totalement extérieurs au Groupement, dûment accrédités par la Direction centrale de la sécurité des systèmes d'information (DCSSI), sous l'égide du Secrétariat général de la Défense nationale, dans le cadre du schéma français d'évaluation et de certification.

> ***La caractéristique essentielle du paiement par carte bancaire est la garantie de paiement***

Le Groupement des Cartes Bancaires « CB » a été un des tout premiers acteurs ayant activement contribué à l'émergence du schéma national d'évaluation et de certification au sein duquel se mettent maintenant en place de puissantes synergies avec d'autres types de cartes (carte nationale d'identité, carte santé…) dans le cadre d'une méthode internationalement reconnue ; c'est là un élément central de la confiance dans le moyen de paiement.

Droit et technique

Ils sont intimement liés depuis l'essor des Nouvelles technologies de l'information et de la communication (NTIC). Elles ont entraîné des réformes majeures dans le domaine juridique notamment dans celui du droit de la preuve.
Le droit de la preuve numérique est né en France avec la carte bancaire à puce. Dès 1986, la Cour de cassation a reconnu une valeur juridique à l'écrit électronique. Le code à quatre chiffres ou code PIN (*Personal Identification Number*) est assimilé à une signature, le porteur a validé l'ordre de paiement qu'il a donné dès qu'il a frappé son code confidentiel. Un acte juridique est ainsi créé.
La signature électronique de l'ordre de paiement est calculée dans le microcircuit de la carte grâce à un algorithme cryptographique et une clé unique propre à chaque carte. Cette opération ne peut être effectuée qu'avec la saisie du code confidentiel. En cas de contestation de l'ordre de paiement par

Plus de cinquante mille distributeurs de billets.

La cinématique d'une transaction EMV

Lorsqu'un client règle un achat avec sa carte bancaire, le commerçant n'échange pas son bien contre de l'argent, mais contre une promesse de paiement délivrée par la carte sous forme électronique, ce qui impose de sécuriser les termes de la transaction. En particulier :

• la carte doit être entre les mains de son porteur légitime ;

• il doit s'agir d'une carte authentique remise par la banque à son porteur ;

• les données de la transaction (date, montant, identifiant de la carte...) doivent être certifiées pour éviter toute manipulation ou contestation ultérieure.

Une transaction de paiement de proximité EMV se déroule de la manière suivante (cf diagramme page de droite) :

Phase 0 :
La carte transmet au terminal de paiement ses données publiques, c'est-à-dire en accès libre : numéro de carte, date de fin de validité, donnée statique d'authentification ou certificat de clé publique « carte ».

Phase 1 :
L'authentification de la carte est faite par le terminal du commerçant, qui vérifie que la carte détient des données d'identification signées par la banque du porteur. Ce mécanisme est basé sur une cryptographie de type « asymétrique » (biclé RSA), ayant pour particularité que la clé qui vérifie peut être rendue publique sans compromettre la sécurité de la clé qui signe. Encore faut-il que les données à vérifier soient différentes à chaque fois, sinon elles pourraient être réutilisées pour fabriquer des fausses cartes[1]. Dans ce but, les données signées par la banque incluent elles-mêmes une biclé RSA unique par carte. À chaque session d'authentification, le terminal génère un aléa que la carte signe avec sa clé privée, ce qu'il vérifie avec la clé publique correspondante : il a ainsi une preuve non réutilisable (car basée sur l'aléa) de l'authenticité de la carte.

Phase 2 :
Le terminal demande ensuite à la carte d'authentifier le porteur : il présente à la carte le code confidentiel que le porteur a frappé au clavier. La carte le compare avec son second secret, la vraie valeur du code confidentiel, et répond au terminal par oui ou non. La carte n'autorise que trois essais et mémorise les essais négatifs.

Phase 3 :
Le terminal demande à la carte de signer la transaction (identifiant du commerçant, date et heure de la transaction, montant de la transaction...) avec son troisième secret. Si la transaction donne lieu à une demande d'autorisation, en règle générale pour une transaction d'un montant supérieur ou égal à 100 euros, l'émetteur (le serveur de l'émetteur) vérifie cette signature en temps réel. La sécurité repose alors sur une cryptographie de type « symétrique » (clé Triple DES de 128 bits) où une même clé secrète sert à signer et à vérifier les messages échangés entre la carte et le serveur de la banque. La clé utilisée par la carte varie à chaque transaction ; le serveur est capable de reconstituer cette clé à partir de ses clés maîtresses et des données fournies par la carte.

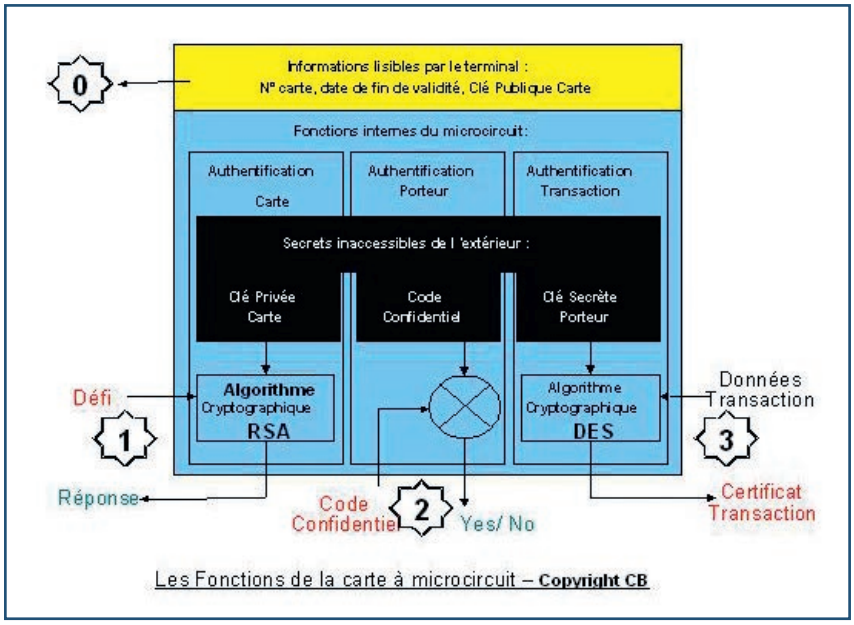
Enfin, lorsque les acteurs sont authentifiés et ont approuvé les termes de la transaction, la carte émet un certificat de transaction qui reprend ces termes et les protège par une signature numérique. Pour des raisons pratiques, cette signature est réalisée par une clé symétrique, selon le même principe que l'authentification en ligne. Le certificat de transaction est imprimé sur les tickets de caisse afin que tous les acteurs en aient une copie.

preuve que cette signature électronique émane bien de cette carte.
Le droit des nouvelles technologies a également généré des craintes de la société, ainsi un droit entièrement nouveau a été organisé : le droit de savoir et contrôler les données personnelles organisé et reconnu par la loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi du 3 août 2004.
Il est par ailleurs important de rappeler que, du point de vue du commerçant, la caractéristique essentielle du paiement par carte « CB » est la garantie de paiement.

Le futur : évolutions technologiques, innovations commerciales et ouverture internationale

Jusqu'à une période récente, les instruments de paiement n'étaient pas considérés comme des outils marketing par leurs utilisateurs ou émetteurs. L'attention était portée sur la reconnaissance, la sécurité, la permanence des échanges. Les évolutions n'avaient donc pour objectif que de répondre à des attentes purement fonctionnelles et économiques. Désormais, les banques ont bien compris l'intérêt d'innover et s'appuient sur la carte, et la richesse des innovations technologiques qui l'accompagnent, pour répondre aux attentes et besoins des utilisateurs.
Outre un instrument de paiement, la carte est, pour les acteurs de la distribution, un outil permettant d'affiner leur marketing par une meilleure connaissance des clients, de leur proposer des offres plus ciblées, et de gagner en productivité au niveau des encaissements. La technologie « sans contact », les cartes multiapplications et le cobranding (comarquage des cartes

avec une marque commerciale) contribuent à ces objectifs et permettent d'accroître la valeur ajoutée de la carte pour les enseignes et les consommateurs. Grâce à la superposition de technologies, la carte, matérialisée ou non, peut techniquement accueillir aujourd'hui d'autres fonctions, comme, par exemple, des programmes de fidélisation et répondre ainsi favorablement à l'évolution du comportement des consommateurs.



Les Fonctions de la carte à microcircuit – **Copyright CB**

> ***Un accès immédiat à des biens ou services grâce aux automates de vente ou location***

Ceux-ci sont de plus en plus sensibles à la personnalisation, que ce soit pour leurs sonneries de téléphone, leurs fonds d'écran, leurs profils utilisateurs sur le Web... La carte bancaire s'inscrit dans cette tendance et répond aujourd'hui à ce besoin par une plus grande diversité de visuels, se rapprochant ainsi des styles de vie des porteurs. Pour répondre à l'instantanéité de l'acte d'achat, les cartes bancaires pourront bientôt être délivrées en quelques minutes sur le point de vente.

Cumuler des points de fidélité

L'ouverture du cobranding, depuis octobre 2007, permet aux banques de faire figurer sur la carte CB leurs partenariats avec des commerçants ou associations. Le consommateur, en utilisant sa carte « CB », peut cumuler des points de fidélité, des réductions ou des avantages auprès d'enseignes ou d'associations (sportives, par exemple) partenaires de sa banque ; ou, si ses affinités sont plutôt d'ordre caritatif ou environnemental, reverser à une association par l'intermédiaire de sa carte une partie du montant de ses achats. Les cartes prépayées, dont l'exemple le plus connu est la carte cadeau lancée en 2006, sont un autre exemple de différenciation pour les banques.

Le support carte en tant que tel n'est pas non plus en reste en termes d'innovation. Les industriels disposent déjà d'effets de textures, couleurs ou matières qui permettent aux banques de mieux distinguer leurs gammes de cartes « CB ». Demain, les cartes à écran interactif créeront sans doute de nouvelles possibilités d'enrichissement du support carte et des usages.

La carte bancaire suscite également l'intérêt marketing d'acteurs non bancaires, grâce à ses possibilités de simplification de l'acte d'achat. La carte à puce est seule à pouvoir offrir un accès immédiat et spontané vingt-quatre heures sur vingt-quatre à des biens ou services grâce aux automates de vente ou location. Le « phénomène » Velib' à Paris en est un exemple récent.

La carte permet aux banques d'exercer leur créativité et de segmenter leurs offres pour mieux cibler les besoins et attentes de leurs clients. La carte bancaire allie ainsi les fonctions de moyen de paiement sécurisé à fort potentiel de séduction, et de support de différenciation dans le contexte de la concurrence entre établissements de crédit et instruments de paiement.

Un espace unique pour la zone euro

Le système « CB » a vocation à créer le cadre permettant ces évolutions. Structurellement ouvert à l'international, il doit s'organiser pour gérer les risques inhérents à l'acceptation des cartes dans des environnements significativement différents et contrastés, notamment dans le monde du commerce électronique et dans les nombreux pays n'ayant pas encore migré vers la technologie de la puce.

C'est en particulier le cas au niveau européen où le système « CB » participe activement à la création et la mise en place du SEPA (Single Euro Payment Area : futur espace unique de paiement pour la zone euro). ■

1. C'est ce qui s'est produit sur le système « CB » au début des années 2000 avec l'apparition des « Yescards » : les fraudeurs récupéraient les données d'authentification statiques de cartes volées et les dupliquaient sur de fausses cartes bancaires émulées. Ce type de fraude est aujourd'hui totalement impossible grâce à la nouvelle génération des cartes « CB » qui met en œuvre un mécanisme d'authentification dynamique.