LA SÉCURISATION DU PAIEMENT SUR LES RÉSEAUX OUVERTS

YVES RANDOUX

Les nouvelles technologies de traitement de l'information deviennent chaque jour de plus en plus banalisées. La médiatisation naturelle qui accompagne leur évolution leur donne un retentissement considérable, au point qu'elle sous-entend que tout est possible, facile, disponible et… opérationnel. Mais la réalité du terrain atténue quelque peu les espoirs et les attentes légitimes que les différents acteurs mettent, à plus ou moins bon escient, dans ces technologies.

Il en va ainsi du commerce électronique. La lecture de la presse nationale et internationale illustre le foisonnement d'idées et de réalisations au quotidien, sans que des solutions pertinentes puissent voir durablement le jour.

Les banques du Groupement des Cartes Bancaires « CB » proposent de franchir un pas décisif dans le domaine de la sécurisation du paiement sur les réseaux ouverts. En expliquant de façon détaillée les voies et moyens empruntés pour mettre en œuvre cet ambitieux projet, cet article se veut donc résolument pédagogique. Il expose dans un premier temps la problématique actuelle du paiement sur Internet, présente ensuite les différents éléments de la solution proposée, évalue dans une troisième partie les enjeux sous-jacents et éclaire dans une dernière partie les attentes des divers acteurs économiques face à ce formidable défi que constitue désormais la nécessaire sécurisation des transactions de paiement sur les réseaux ouverts.

Avant d'entrer dans le vif du sujet, il paraît judicieux de rappeler quelques notions de base, de nature à expliciter ensuite le modèle mis en place.

Au quotidien, la plupart des achats se font en face à face : un acheteur est devant un fournisseur et l'opération de paiement est réputée

1 Administrateur du Groupement des Cartes Bancaires « CB «

« parfaite » parce que le bien ou le service existe, vendeur et acheteur se rencontrent ; le prix est connu voire discuté et l'instrument de paiement vient clore physiquement la transaction : nous sommes dans un monde réel, où confiance et sécurité sont réciproques et tangibles.

En revanche, dans le monde de l'achat dit électronique, c'est-à-dire à travers un réseau et via un support informatique - traditionnellement mais non exclusivement un PC - un client réputé réel, achète un bien potentiellement délivrable (mais existe-t-il réellement ?) à un marchand virtuel, et d'autant plus virtuel qu'il se situe quelque part dans le monde et seul un accès sur le réseau le rend « réel ». Confiance et sécurité sont perçues alors comme aléatoires et l'incertitude voire l'insatisfaction résident dans le cœur même de l'acte d'achat. C'est donc pour instaurer la confiance et la sécurité dans de telles opérations à distance que le paiement sur réseau ouvert constitue un réel enjeu pour tous les acteurs.

LES TENTATIVES DE SÉCURISATION DU COMMERCE ÉLECTRONIQUE SUR RÉSEAUX OUVERTS

La France s'est dotée depuis près de vingt ans, grâce au minitel, d'une infrastructure technique et juridique du paiement à distance. Dans cet univers, l'expérimentation du paiement dématérialisé et délocalisé est un acquis durable, grâce à l'utilisation récurrente de la carte bancaire mais aussi du chèque. S'agissant du paiement par carte, sécurité et confiance ont été renforcées depuis une dizaine d'années par l'utilisation de la carte à puce et la composition au clavier du code confidentiel par le client effectuant l'achat. C'est ainsi que le minitel Magis est venu récemment élever le niveau de sécurisation du commerce électronique grâce au lecteur de carte à puce dont il est désormais doté.

Le contexte bancaire français est donc riche d'une expérience éprouvée, mais il n'est pas le seul puisque, par exemple, les cartes privatives représentent à elles seules 23 % des paiements par carte dans le monde du paiement à distance contre 16 % effectués par carte bancaire « CB ». Enfin, d'autres approches ont vu le jour spécifiquement sur Internet parce que ce dernier est un réseau ouvert et qu'il présente des caractéristiques d'acheminement des informations dans le domaine du commerce électronique qui conviennent aux commerçants.

Brève typologie des instruments de sécurisation de paiement sur Internet

Au risque d'être simplificateur, on peut considérer deux grandes familles de paiement à l'heure actuelle : les paiements de petits montants et les paiements d'opérations commerciales courantes.

La sécurisation actuelle des paiements de petits montants

On recense, aujourd'hui, toutes solutions confondues, plus de trois cents modes de paiement sur Internet. Il serait fastidieux de les lister de façon exhaustive ici, d'autant plus que la plupart n'ont eu qu'une existence éphémère, ou se déroulent dans un environnement tellement restreint, qu'ils ne peuvent prétendre au titre d'instrument de paiement, au regard du seul critère de l'universalité que celui-ci doit revêtir, parmi d'autres, pour être reconnu comme tel.

A titre d'exemple pour illustrer le propos, on citera aux USA, les solutions telles que Cybercash, First Virtual, Digicash, voire Netscape ou E-cash. Certains ont d'ores et déjà disparus de cette brève nomenclature !

En France, on peut citer la solution Klebox de KLELine, mais aussi Payline développé par Experian, Globe ID développé par CG-TECH, SIPS commercialisé par Atos. L'Europe s'est elle-même lancée dans une expérience identique dans le cadre du projet ESPRIT en proposant un projet européen de monnaie électronique : CAFE (Conditionnal Access For Europe).

La protection des opérations commerciales courantes

De nombreux « dispositifs » sont actuellement en vigueur pour sécuriser les transactions autres que celles de petits montants. Deux protocoles dominent néanmoins le marché ; on s'y limitera.

• SSL (Secure Socket Layer)

SSL est un protocole de sécurisation des échanges de données conçu par Netscape, et intégré dans son *browser*, ainsi que dans celui de Microsoft. Il permet de régler en partie les problèmes d'authentification des acteurs et de confidentialité des échanges, mais ne traite pas la chaîne de confiance qui s'établit entre les divers moments de l'acte d'achat. Sans entrer dans le détail de ce protocole, on peut le résumer de la façon suivante, en distinguant 2 phases :

- phase initiale de connexion : le client se connecte sur le serveur d'un marchand pour y effectuer ses achats.

Le serveur du marchand envoie dans cette phase initiale, sa clé publique de chiffrement. Le logiciel du PC du client, à la réception de cette clé publique, génère une variable aléatoire et secrète, dite clé de session, et l'envoie chiffrée par la clé publique au serveur du commerçant. Le dialogue sécurisé peut alors s'établir entre le PC et le serveur du commerçant.

- phase d'achat : le client choisit ensuite le produit désiré et envoie sa commande avec ses coordonnées bancaires - par exemple le numéro de sa carte bancaire - le tout chiffré par la clé de session du commerçant.

A l'arrivée du message, le serveur déchiffre le message avec la clé secrète du commerçant, appelle la banque du client pour obtenir l'autorisation de débiter le client - s'il y a lieu - ou obtenir une garantie bancaire de la bonne fin du paiement. En cas de réponse positive, il délivre le bien au client et fait recouvrer sa créance par les voies traditionnelles de la compensation.

Cette solution est simple, rapide et efficace ; mais on verra qu'elle comporte quelques failles importantes.

• SET (Secure Electronic Transaction)

Ce protocole présente une structure de fonctionnement plus spécialisée - car il est dédié aux cartes des réseaux Visa et Mastercard - et plus complexe car il organise clairement la séparation entre les données liées à l'achat et celles liées au paiement à l'aide de clés séparées.

La phase initiale de mise en relation client/commerçant n'existe pas réellement : l'opération débute par la connexion du client au serveur du marchand et le choix d'un bien qu'il désire acquérir. Dès que ce choix est effectué, le client indique également le mode de paiement retenu et en l'espèce le paiement par carte, en sélectionnant le réseau utilisé : Visa ou Mastercard. Pendant cette phase, le serveur du commerçant, comme dans SSL, envoie au PC du porteur la clé publique du commerçant et celle de sa banque.

Le logiciel du client fabrique alors un enregistrement comprenant :

- l'identification du client ;
- les données relatives au bien acheté par le client ;
- les références bancaires du client (n° de carte bancaire par exemple) ;
- un numéro unique de transaction transmis par le serveur du commerçant.

L'ensemble ainsi constitué, est concaténé puis signé et chiffré par les clés publiques de la banque et du commerçant et enfin envoyé au serveur du commerçant.

Celui-ci reçoit en fait deux types de données :

- celles destinées à l'achat proprement dit : elles sont directement exploitables par le marchand ;
- celles destinées au banquier : elles ne sont jamais accessibles par le commerçant, mais routées vers le serveur bancaire, qui vérifie les données ainsi reçues, effectue le traitement approprié et renvoie un acquittement au serveur commerçant.

En fin d'opération, c'est-à-dire quelques secondes plus tard, le client reçoit un accusé de réception de bonne fin de l'opération d'achat qu'il vient d'effectuer.

Les différentes étapes brièvement décrites ci-dessus sont protégées par des clés de chiffrement de type symétrique et asymétrique.

Performance de ces solutions du point de vue bancaire

La diversité avérée des solutions appliquées aux petits montants démontre une créativité assez extraordinaire des équipes dans ce domaine. S'agissant pour la plupart d'entreprises non bancaires, elles préconisent l'émergence de la monnaie électronique, ou plus exactement d'une monnaie dite électronique et privative. Ce qui n'est pas sans poser de nombreuses questions.

En effet, le concept de monnaie électronique a toutes les apparences d'une notion opérationnelle, assimilable à celle des instruments de paiement, mais n'en revêt pas les principales caractéristiques, à savoir : universalité, fiabilité, sécurité. Leur faible degré de diffusion dans le grand public, même pour des produits récents, illustre la difficulté pour les utilisateurs de se mouvoir avec confiance dans cet univers et la réticence des vendeurs d'ouvrir largement leurs produits dans ces nouveaux mécanismes ou supports de paiement.

En ce qui concerne SSL, son développement est beaucoup plus important, au point que certains pensent qu'il est devenu désormais le protocole standard de sécurisation des transactions électroniques. Deux critiques majeures sont adressées à SSL.

• D'une part, la faiblesse de la cryptographie (clés à 40 bits) constitue pour l'instant un véritable handicap, d'autant plus que les gouvernements ne lèvent pas rapidement l'interdiction de chiffrer les messages avec des clés supérieures à 40 bits[1].

• D'autre part - et ce point est plus critique - l'encapsulage de données bancaires du porteur insérées dans le message destiné au commerçant peut faire l'objet d'usages frauduleux : duplication des données, constitution de fichiers de numéros de cartes, recensement des habitudes d'achat, etc.

C'est vraisemblablement là que réside le facteur de risque le plus élevé de ce protocole.

C'est pour éviter de tels inconvénients que le protocole SET a été conçu. Développé par Mastercard et Visa, experts s'il en est du paiement par carte, SET sépare bien les données commerciales des données bancaires. Mais le travail en commun s'est traduit par un « empilage » de procédures pour répondre aux exigences d'un paiement bancairement sécurisé, à savoir :

• le chiffrement pour sécuriser les échanges ;

• la mise en place d'une véritable chaîne de confiance grâce aux nombreux certificats dont est entouré SET (trop nombreux disent certains) ;

• la validation formelle du paiement effectuée par le client soit par une signature logicielle ou, comme nous allons le voir, par une signature « puce » provenant directement de la carte bancaire à microcircuit.

Cette complexité est nécessaire en regard de l'objectif poursuivi : la confiance de l'internaute, s'est provisoirement traduite par une complexité du paiement par SET affectant la performance du dispositif dans sa première version.

En effet le niveau de sécurité atteint est très élevé. Complexité qui n'a pas empêché la communauté bancaire française de s'emparer du protocole SET pour l'implémenter en l'améliorant de façon notoire grâce à l'utilisation de la carte à mémoire. Après avoir tâtonné sur la meilleure approche possible, à travers le projet E-Comm et le protocole de haut niveau C-SET, la convergence entre les deux solutions a donné naissance à une solution internationalement reconnue.

LA SOLUTION PROPOSÉE PAR LA COMMUNAUTÉ BANCAIRE « CB »

Contexte général

Il est coutumier en France de s'autoflageller. Le monde bancaire n'échappe pas à ce travers. La France est, dit-on, en retard dans le commerce électronique. On ne sait pas qui est en avance et en fonction de quels critères, mais il est nécessaire parfois de recourir aux formules alarmistes pour prendre conscience collectivement des véritables obstacles à la modernisation, taire les dissensions, réduire les atermoiements et mobiliser en définitive toutes les forces vers un objectif commun jugé essentiel.

C'est ce qui a été fait en termes du processus de convergence. Auparavant, 3 pilotes avaient été initiés par les banques sur la base unique du logiciel SET :

• le projet VSEC (Visa Secure Electronic Commerce) : initié par Visa dans plusieurs pays dans le monde et notamment en Europe. Il est concrétisé en France par le projet SEC (Secure Electronic Commerce) placé sous la responsabilité du Groupement Carte Bleue.

Il consiste à sécuriser dans un PC le numéro de carte Visa de l'internaute et de le faire circuler de façon cryptée dans le réseau.

• le projet E-Comm : a été initié par, la BNP, la Société Générale et le Crédit Lyonnais auxquels ont été associés Visa International, France Télécom et Gemplus. Ce projet, dont le déploiement est effectif depuis septembre 98 met en œuvre autour du logiciel SET, un dispositif sécuritaire combinant le certificat SET et le contrôle de code sur la puce.

• le protocole C-SET (Chip-Secure Electronic Transaction) conçu par le Groupement des Cartes Bancaires, fait reposer la sécurité essentiellement sur la carte à puce, associée à un lecteur de carte, séparé du

PC. Il a été mis en œuvre depuis octobre 97 par Europay France dans le projet appelé Cybercard, entité regroupant le Crédit Agricole, le Crédit Mutuel, les Banques Populaires, La Poste, le CIC et les Caisses d'Epargne.

La même philosophie de conception entre ces deux derniers projets a permis d'organiser en début 98 une convergence, point de départ d'une solution originale des banques « CB » dans la voie de la sécurisation des transactions de commerce électronique.

L'architecture technique de Cyber-COMM, solution de convergence sous l'égide du Groupement des Cartes Bancaires « CB »

Trois types d'acteurs sont partie prenante au commerce électronique :
- l'internaute
- le marchand
- la banque, sous une double relation, celle existant avec son client, l'internaute et celle existant avec son client, le marchand.

C'est donc en progressant pas à pas que nous allons découvrir les composants techniques et fonctionnels de la solution.

Les outils de l'internaute

Derrière son PC, le client navigue sur le Web. Il choisit un bien ou un service et désire l'acquérir. Dans la solution de convergence, dont le protocole est désormais connu sous le nom de Cyber-COMM, le client dispose :

- d'une carte bancaire « CB » à puce ; cette carte va « signer » la transaction ;
- d'un lecteur de cartes à puce, téléchargeable, équipé d'une zone d'affichage d'au moins 16 caractères (voire davantage) pour présenter au client le montant et la devise de son achat, et permet de composer le code confidentiel du porteur ;
- un *wallet* (ou portefeuille électronique) : c'est en fait un programme informatique spécial, installé dans le PC de l'internaute, conçu par l'équipe Cyber-COMM qui sert d'interface entre le navigateur Web, le lecteur de carte et le PC. En effet lorsque le porteur a composé son code confidentiel sur le clavier du lecteur de cartes à puce, celle-ci « émet » sa signature dans l'enregistrement d'achat, le crypte et le transmet au *wallet* qui le prend en charge, le formate et finalement l'envoie au commerçant par le réseau de télécommunication. C'est donc la cheville ouvrière du dispositif de paiement électronique.

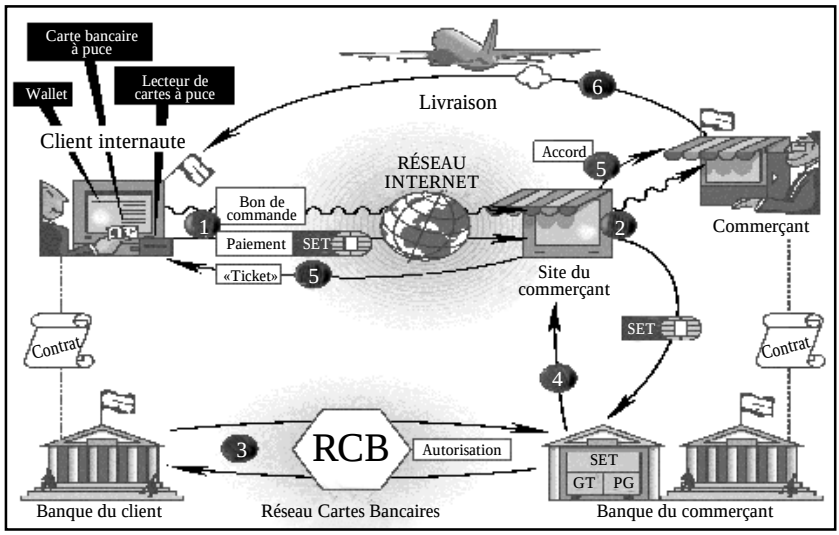
Les outils du commerçant

• S'agissant d'un commerçant français, pour les transactions nationales :

- il dispose essentiellement du logiciel SET standard augmenté du module de traitement de la signature réalisée par la carte à puce et d'un contrat commerçant CB. L'opération se déroule selon le schéma suivant :

Schéma n° 1

Les outils de l'internaute, du commerçant et de la banque, lorsque l'opération se déroule en France



1. Le client envoie par Internet vers le site du commerçant un message comportant une partie du « bon de commande » et une partie ordre de paiement.

2. Sur le site commerçant le message est séparé en deux : une partie de l'enregistrement (commande) lui est destinée tandis que l'autre est acheminée vers sa banque ; elle comprend le message « SET+ signature puce ».

3. Les étapes 3 et 4 sont facultatives car elles correspondent à une demande d'autorisation qui, selon la typologie des commerçants ou le montant des achats peut ne pas exister.

La banque du commerçant peut demander une autorisation auprès de la banque du client, émettrice de la carte. Une telle demande est transportée par le réseau cartes bancaires (RCB).

4. La banque donne l'autorisation et l'envoie au site du commerçant.

5. Le site du commerçant reçoit cette information et transmet à l'internaute l'acceptation de la transaction par la banque, sous forme d'un ticket électronique analogue au reçu papier lors d'une transaction de proximité. L'internaute peut archiver ce ticket sur son PC.

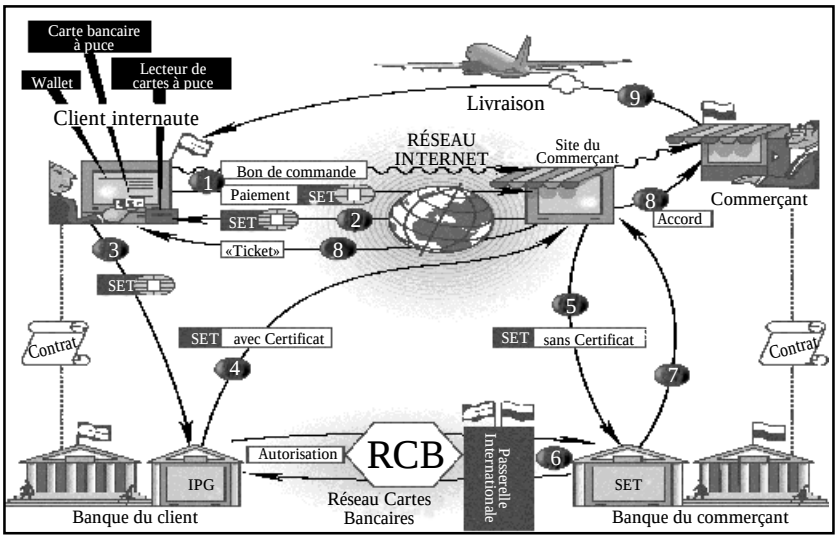
6. Le commerçant procède ensuite à l'envoi de la marchandise.

• S'agissant d'un commerçant étranger, seule l'obligation de disposer du logiciel SET est requise. Comme nous l'avons décrit précédemment, si un porteur français effectue un achat auprès du commerçant étranger, l'Issuer Payment Gateway effectue le rôle de « transformation », c'est- à-dire remplace dans cette transaction française réalisée par le couple SET

+ carte à puce, la signature puce par un certificat SET gérable dès lors par le commerçant étranger comme une transaction SET « pure ». Le schéma suivant décrit les différentes phases d'une opération avec un commerçant étranger.

Schéma n° 2

Les outils de l'internaute, du commerçant et de la banque, lorsque le commerçant se trouve à l'étranger



1. Le client envoie par Internet vers le site du commerçant un message comportant une partie du « bon de commande » et une partie ordre de paiement.

2. Sur le site commerçant le message est séparé en deux : une partie de l'enregistrement (commande) lui est destinée tandis que l'autre est acheminée vers sa banque ; elle comprend le message « SET+ signature puce ».

3. Le message « SET + signature puce » est automatiquement envoyé par le client à l'IPG de sa banque.

4. L'IPG de la banque « transforme » la signature puce par un certificat SET pour le serveur du commerçant.

5. Celui-ci l'envoie automatiquement à la banque du commerçant.

6. Cette dernière demande s'il y a lieu une autorisation auprès de la banque émettrice de la carte. La demande transite par une passerelle internationale (CIBLE pour les cartes Visa et EPSNet pour les cartes Eurocard/Mastercard).

7. La banque du commerçant reçoit l'autorisation qu'elle achemine au serveur du commerçant.

8. Le commerçant informe le client que le paiement est accepté.

9. Le commerçant procède ensuite à l'envoi du bien commandé par le client.

Les outils de la banque

On distingue volontiers en France, les dispositifs installés chez l'acquéreur de ceux installés chez l'émetteur, même si, dans la plupart des cas, la même banque assure les 2 fonctions. La banque dispose dans tous

les cas, du logiciel SET et du complément nécessaire au traitement de la signature puce. On retiendra donc cette double fonction pour présenter les divers composants bancaires de la solution Cyber-COMM :

La Banque « acquéreur »

La banque acquéreur dispose de deux outils lui permettant de vérifier et d'acheminer les transactions reçues du serveur du marchand.

• Un Payment Gateway (PG) : c'est une passerelle (c'est-à-dire un programme informatique), qui va permettre à la banque du commerçant (dite « banque acquéreur »), de vérifier les données du client acheteur d'un produit chez son commerçant et d'obtenir le feu vert pour effectuer l'opération. En outre, grâce à un certificat spécialisé, l' internaute est assuré de traiter avec une « vraie » banque, reconnue par l'un des deux grands réseaux internationaux.

• Un Gestionnaire de Télépaiement (GT), qui est une fonction classique dans l'univers de Cartes Bancaires de contrôle des signatures émises par des cartes bancaires « CB » et de routage des transactions vers les serveurs bancaires pour en obtenir les autorisations et en fin de journée en effectuer la synthèse, le crédit en compte et l'acheminement des transactions vers la compensation.

Ce gestionnaire peut être collectif ou développé en propre par chaque banque.

La Banque « émetteur »

Elle joue un double rôle : d'une part elle dispose d'un outil lui permettant de recevoir des transactions signées par une puce afin de les convertir en certificat SET et les acheminer à l'étranger. D'autre part elle utilise l'outil de délivrance des certificats pour le besoin prédéfini. On le voit bien, à partir du moment où les banques à l'étranger sauront traiter la signature puce ce double dispositif disparaîtra.

Les avantages de cette solution : le paiement de qualité

La sécurisation technique et juridique des différents acteurs

Dans une opération d'achat/vente en face à face, commerçant et acheteur déroulent, sans s'en rendre compte, plusieurs « moments » juridiquement importants, au cœur de l'acte d'achat, qu'il faut s'efforcer de reconstituer grâce à l'arsenal technologique décrit précédemment. La facilité évidente du commerce en face à face se transforme en complexité avérée dans le commerce à distance.

En quelques mots, la sécurisation par carte à puce résout définitivement les problèmes laissant planer un doute sur la qualité ou l'existence des différents acteurs, lors d'un paiement sur Internet. Il faut en effet recréer les conditions optimales de confiance et de preuve.

Pour réduire ce risque, les banques « CB » créent la notion de *paiement de qualité*, reposant sur la signature électronique de la carte à puce. Ce paiement de qualité est :

• *techniquement sécurisé* par 3 dispositifs insérés dans la chaîne de traitement :

1. l'authentification du porteur, réalisée par la frappe du code confidentiel, dans l'environnement hautement sécuritaire du lecteur de cartes à puce ;

2. les données transmises sont protégées par une série de clés et dans la conception initiale de SET, données bancaires et données commerciales sont séparées et ne peuvent être accessibles que par le destinataire autorisé ;

3. enfin, les données circulent de façon confidentielle grâce à la fonction de chiffrement.

• *juridiquement protégé*, grâce au dispositif contractuel français, déjà connu pour les cartes bancaires « CB ». En effet, dans le contexte du commerce électronique sécurisé par le protocole Cyber-COMM, le paiement électronique se rapproche du paiement fiduciaire. Il est particulièrement adapté aux besoins des commerçants car :

1. il est irrévocable : la signature par la carte à puce authentifie le porteur et rend le paiement irrévocable, comme c'est le cas actuellement lors d'un paiement de proximité ;

2. il est garanti pour le commerçant. Comme dans le système « CB » du paiement de contact, le commerçant est garanti contre l'insolvabilité du client, en allant chercher l'autorisation, grâce au Gestionnaire de Télépaiement, auprès de la banque du porteur ;

3. il est incontestable dans son fondement même par la technologie mise en place, dans la mesure où le dispositif complexe de clés en cascade constitue un système de preuve particulièrement efficace.

• *internationalement accepté* par le soutien effectif de Visa et de Mastercard/Eurocard qui, à travers la solution Cyber-COMM, offrent au commerçant une organisation sécuritaire internationale quelque soit l'origine du porteur. La possession du logiciel SET est la garantie quasi absolue de ne plus se préoccuper du paiement. C'est un atout évident que la communauté bancaire « CB » peut fournir en raison de son avance avérée dans le domaine de la monétique.

Cet « avantage » commerçant, dont les composantes se comparent en fait à celles d'un paiement en face à face, se complète d'une sécurité juridique analogue, perceptible par le client. Le certificat final, transmis par le serveur du commerçant, atteste de façon irréfragable, que le client est bien l'auteur de la commande et qu'il sera débité pour le montant signé par la frappe de son code confidentiel.

En même temps, le Mécanisme d'Accréditation du Commerçant

(MCA) certifie au client que le commerçant existe bien et qu'il opère sur le Web avec l'accréditation d'une banque. Cette « autorisation » doit donner au client une garantie de sérieux du commerçant et l'assurance que le produit commandé sera effectivement livré.

En définitive, s'agissant de commerce électronique, c'est l'ETAT qui est l'acteur invisible, garant du dispositif contractuel ainsi mis en place. Sans s'immiscer dans la construction technique, ni dans les relations entre les différents acteurs, il assure notamment par les règles de la cryptologie, que les solutions mises en œuvre le sont de façon sécuritaire et pérenne.

L'extension de la solution Cyber-COMM en Europe : un défi majeur

La volonté de promouvoir les solutions reposant sur l'usage de la carte à puce dans le domaine du paiement, n'est pas un projet nouveau pour le Groupement « CB ».

Déjà avec la Société Belge Banksys, un programme approuvé par la Commission européenne avait été subventionné et s'était concrétisé par la délivrance des spécifications d'une pré-norme de sécurisation des échanges dans le commerce électronique, appelé IC-SET (pour Interoperable Chip Secure Electronic Transaction). La solution Cyber-COMM va s'intégrer dans le droit fil de cette pré-norme, pour devenir, grâce à l'intégration dans la prochaine *release* de SET-2-0, la solution de sécurisation du commerce électronique pour les banques utilisant des cartes à puce.

Préalablement, un pas devra néanmoins être franchi avec la mise à disposition de lecteur permettant aux cartes à puce d'être traitées par les PC. En effet, le Groupement « CB » a entrepris, avec l'aide de la Commission européenne, de participer à un projet se déroulant dans le cadre du programme communautaire Isis (Information Society Initiative for Standards).

Connu sous le nom de Finread, ce projet vise à faire émerger en Europe, sinon au plan international, les spécifications d'un lecteur sécurisé de carte à puce. Ces spécifications constituent une pièce essentielle dans la construction du puzzle de la sécurisation du commerce électronique. Plusieurs initiatives ont été prises récemment par les constructeurs de PC au sein de l'organisation PC/SC, groupe de travail destiné à « normaliser » les divers composants des PC construits par les différents équipementiers à travers le monde. On voit l'intérêt immense que peut susciter ce type d'initiative : intégrer dès aujourd'hui dans les PC, un lecteur de cartes à puces. D'ores et déjà, plusieurs constructeurs se dirigent résolument dans cette voie et on ne peut que les encourager. Restera néanmoins l'importance du parc actuel de PC ne disposant pas de lecteur sécurisé. Pour pallier cette absence, le projet Finread doit

fournir aux constructeurs les spécifications aptes à leur permettre de fabriquer des lecteurs séparés du PC, connectables sur un port du PC, faciles à transporter, pour banaliser dès demain la présence d'un lecteur à côté du PC.

Le Groupement « CB » est donc très fortement impliqué dans ce projet dont il a pris l'initiative et qui regroupe plusieurs pays européens (Belgique, Italie, Espagne, Allemagne) mais aussi Visa International et Europay International. Offrir à l'internaute un outil adéquat, pour 10 à 20 euros, constitue donc un enjeu majeur pour faciliter l'appropriation des procédures d'achat sur le Web grâce à un lecteur sécurisé.

Au-delà du développement des spécifications Finread, dont l'échéance est prévue avant la fin de 1999, la Commission européenne devrait également être sensibilisée à la nécessité de se livrer à une expérimentation très large de la solution Cyber-COMM.

L'Europe connaît en effet une large utilisation de la carte à puce ; situation qui ne se trouve dans aucun autre continent. Vouloir développer un tel projet est une ambition à l'échelle communautaire. Cyber-COMM va devenir le protocole international de la sécurisation du commerce électronique pour les clients possesseurs d'une carte à puce.

On le voit dans les pages précédentes, un véritable projet industriel international est en germe dans cette solution. C'est la raison pour laquelle nous inviterons les responsables européens à prendre conscience de la formidable opportunité qui s'offre à eux d'assurer massivement le succès de cette opération en accompagnant, à travers le cadre institutionnel existant, le protocole proposé par Cyber-COMM. C'est en effet un enjeu à la mesure de l'Europe, créateur de richesse, d'emploi, permettant au Vieux Continent, de conserver l'avance qu'il a acquise dans les technologies de la carte à puce pour sécuriser le commerce électronique.

La consécration internationale de la solution Cyber-COMM

Fondé sur l'expérience de près de 10 ans de travail sur la carte à mémoire, Cyber-COMM est le fruit de la convergence des pilotes initiés par les banques françaises relayés par les deux organisations internationales Visa et Mastercard.

De même que ces organisations ont adopté le principe de basculer leurs cartes à pistes en cartes à puce dans la prochaine décennie, elles viennent de confirmer que l'option carte à puce dans le protocole SET fait partie intégrante de ce protocole, sous forme d'extension générique, dans la version SET 1.0 maintenant stabilisée.

En d'autres termes, la solution que les banques « CB » développent va devenir le standard international du commerce électronique avec une carte à puce, pour les banques utilisant SET. L'engagement des deux

réseaux internationaux démontre la pertinence de la réponse fondée sur la carte à puce et la mise en œuvre de l'extension générique au plus tard en 2001 en Europe constitue l'amorce d'une solution unique pour le continent européen, en attendant que les Etats-Unis basculent également sur la carte à puce.

Gagner la confiance des internautes

La dernière phase du projet sera réussie si le *wallet* Cyber-COMM est incorporé comme une solution standard dans les *wallets* des grands éditeurs de logiciel. En effet, tout ce qui peut être fait pour faciliter l'extension de la solution de paiement sécurisé par cartes à puce, doit être entrepris à tous les niveaux de la chaîne industrielle. On le sait, nombre d'internautes abandonnent leur transaction en phase d'achat parce qu'il manque le maillon du paiement sécurisé. C'est donc ce dernier qu'il faut s'efforcer d'introduire dans le PC, en faisant appel à ces fabricants de *wallets* et obtenir une place dans leur dispositif actuel. C'est un objectif ambitieux mais à la hauteur de la promotion du paiement de qualité tel qu'il a été défini précédemment. C'est au prix de cette simplicité d'utilisation et d'universalité de présence dans les solutions de base des éditeurs de logiciel que la confiance des internautes sera gagnée.

LES ENJEUX DU COMMERCE ÉLECTRONIQUE EN FRANCE

Avant d'aborder cette troisième partie, il est utile de faire un peu de sémantique car, de cette réflexion, peuvent surgir bien d'autres enjeux que ceux, nécessairement réducteurs, traités dans ce texte.

« Commerce » vient du latin *commercium*, la racine « merx » signifiant marchandise. Etymologiquement, le mot représente donc l'idée d'échange de biens ou de services. Ce mot s'en enrichi ultérieurement de deux termes plus spécialisés « négoce » et « trafic » pour s'appliquer à des formes particulières d'échanges. Très rapidement, le sens opérationnel a fait place au concept relationnel : tout échange avec une autre personne est une forme de commerce. Or, cette vision très large de la notion de commerce, qui, à travers le commerce électronique, est réduite à un échange utilitaire de biens et services dont la technologie n'a que pour objet de sécuriser l'acte de paiement, est totalement perdue de vue. Le « commerce » sur Internet revêt donc une signification beaucoup plus large que l'achat de biens et services adossés à un paiement sécurisé.

Mais dans l'immédiat, il faut s'en tenir à la notion opérationnelle en analysant les principaux enjeux. Sécuriser le commerce électronique répond à un triple enjeu : commercial, financier et technique.

Le marché domestique du commerce électronique

Globalisation, mondialisation, massification : le commerce électronique n'échappe pas à la logorrhée médiatique. Organismes d'analyse des marchés, consultants, prévisionnistes et autres gourous annoncent l'explosion de ce marché pour l'an 2000 et il est vrai que l'on constate un frémissement dans ce domaine. La France, pour sa part, dispose d'une expérience ancienne dans la vente à distance. Néanmoins, l'examen des chiffres tempère quelque peu « l'explosion » attendue du commerce électronique dans les prochaines années.

Les échanges entreprise/consommateur (Business to consumer)

• Les paiements réguliers

En 1997, le marché de la vente à distance représentait quelque 50 milliards de francs d'achats, dont 16 % ont été réglés par carte bancaire, soit 8 milliards de francs pour un peu plus de vingt millions d'opérations (22,3 exactement). Les cartes privatives représentaient un volume d'affaires d'environ 12 milliards de francs. Enfin, particularité française, le minitel, à travers le kiosque de France Télécom, annonçait 8 milliards de francs de recettes, essentiellement sur des opérations de petit montant. Dans le marché du paiement à distance, le paiement par carte bancaire est donc loin d'être majoritaire, le chèque y joue encore un rôle prépondérant. Et c'est bien pour réduire tant les paiements par chèque que pour faciliter le règlement des petits montants que la communauté bancaire se lance dans un projet aussi important pour sécuriser le paiement sur Internet.

Telle est la réalité française actuelle. Quelles en sont les perspectives d'évolution dans les prochaines années ?

L'utilisation d'Internet ne se compare pas à celle du minitel. En revanche, de nouveaux outils peuvent accélérer le processus de recourir aux achats sur Internet : Webphone, téléphones à carte, GMS, TVBox et autres outils à la convivialité renforcée, devraient faciliter l'évolution des modes d'achat du consommateur. L'explosion attendue n'est pas aussi évidente que cela : avec un marché de 50 milliards de francs, s'accroissant de 10 % par an, ne portera la taille qu'à 65 milliards en 2002, à condition que les outils de sécurisation, les applications, et surtout les consommateurs soient au rendez-vous.

Là encore, les chiffres actuels doivent nous rendre pragmatiques : en 1998, la France compte environ 3 millions d'internautes[2] mais peu nombreux sont ceux qui osent effectuer des opérations de paiement. A l'horizon 2002, on pense que 5 millions de foyers seront raccordés à Internet, représentant un potentiel d'utilisateurs d'une dizaine de millions de personnes. Ce qui ne signifie pas qu'il y aura 10 millions

d'acheteurs. Néanmoins, un marché potentiel existe, il peut faire rêver et c'est la raison pour laquelle la plus grande prudence s'impose dans les calculs prévisionnels. S'ajoutera à cela la conversion progressive des paiements à l'euro, ce qui est de nature à faire étendre le champ actuel du paiement en francs à la dimension du nouveau marché européen. C'est un impact essentiel, difficile de mesurer à l'heure actuelle mais qui peut faire varier fortement les données précitées.

En définitive, pour les cartes bancaires « CB », le *business case* de ce segment de marché peut se résumer ainsi : à l'aube du troisième millénaire, le commerce électronique des porteurs de cartes bancaires françaises pourrait représenter quelques dizaines de millions d'opérations pour un chiffre d'affaires de 5 à 8 milliards de francs. Sans être négligeables, ces chiffres n'annoncent pas une envolée significative du commerce électronique dans un environnement sécuritaire ; ils n'en constituent pas moins les prémisses. Reste le secteur qui représente une véritable inconnue dans ce domaine : les paiements de petits montants. Toujours annoncé, jamais avéré ; frémissant sans être franchement présent ; potentiel mais difficile à évaluer, le commerce électronique demeure insaisissable, relevant encore de nos jours plus de la chronique d'une technologie naissante que de celle d'un nouveau canal de distribution à exploiter. C'est là que réside la formidable ambiguïté actuelle d'Internet.

• Les paiements de petits montants

Avec les achats par minitel, nous disposons de données récurrentes sur de tels achats. Déjà depuis quelques années, existent des solutions évoquées au début de cet article ; on rappellera, pour la France, les solutions développées par KLELine avec la Klebox ou la solution Payline mise en œuvre par Experian. Ces solutions existent, mais restent à ce jour limitées dans leur utilisation.

C'est la raison pour laquelle les Banques « CB » offrent, à côté et en même temps que la solution de sécurisation du commerce électronique, un mécanisme de règlement des petits montants.

Cette solution, développée initialement par l'ex-société E-Comm, se présente de la façon suivante : l'internaute se connecte à sa banque et par sa carte bancaire s'ouvre une ligne de dépenses d'un montant (vraisemblablement compris entre 100 et 200 F) qu'il place dans un porte-monnaie virtuel[3]. Il effectue ensuite des achats (articles de journaux, informations diverses, biens de faible montant, etc., et sa situation comptable du point de vue du porte-monnaie virtuel se trouve décrémentée à chaque achat. En fin de mois, les opérations sont remises en compensation pour les montants des dépenses effectuées et les différents commerçants sont crédités. Ce projet, en cours de développement, est complexe en raison de la multitude des acteurs en jeu : plusieurs millions

d'internautes, face à plusieurs centaines de milliers de commerçants en France, mais aussi à l'étranger.

La base de données est donc conceptuellement gigantesque, pour traiter de nombreuses opérations, de très petits montants.

On le voit, ce seul projet constitue à lui seul un défi. Mais il est essentiel dans la solution globale qui est proposée de sécuriser le commerce électronique : chaque paiement se fait avec la présence de la carte bancaire. Cette option a été retenue d'une part pour en favoriser l'usage, mais aussi pour sécuriser le paiement en créant, par la carte, un lien entre le PMV et le porteur.

La frappe du code confidentiel n'a pas été retenue pour accélérer le processus d'achat et simplifier l'ergonomie de paiement de l'opération de petit montant. En revanche, l'insertion de la carte du porteur dans le lecteur accroît la sécurité tant pour ce dernier que pour le commerçant.

Ce marché enfin est difficile à appréhender. Actuellement, on estime qu'un paiement de petit montant représente en moyenne 7 F. Nos prévisions évaluent entre 50 et 70 millions d'opérations réalisées par ce canal vers 2002, pour un chiffre d'affaires d'environ 500 MF. De nouveau, le pragmatisme et la prudence sont de mise devant les incertitudes de développement de cet outil.

Les échanges entre entreprises (business to business)

Si la perplexité prédomine dans l'évaluation des paiements de petits montants, on l'aura deviné, une perplexité et une incertitude plus grandes encore pèsent dans l'évaluation des règlements entre les entreprises. Si la vente *business to consumer* représente 50 milliards de francs actuellement, les paiements courants entre entreprises peuvent être évalués à 500 milliards de francs ; une dernière catégorie, les paiements de gros montants ne constituent pas un segment pertinent à ce jour pour le commerce électronique, car des instruments spécifiques fonctionnent dans ce domaine à la satisfaction des usagers.

La solution Cyber-COMM s'applique sans aucune modification à ce segment de marché. Le seul problème est celui de l'évaluation de l'impact du paiement électronique : actuellement, quatre banques mettent en œuvre la Purchasing-Card de Visa. La BNP, les Banques Populaires le Crédit Commercial de France et la Société Générale se sont lancés dans cette formule pionnière de règlement des dépenses courantes dans les entreprises, depuis 3 ans. La nécessité de constituer au préalable un réseau d'entreprises acceptant cette nouvelle formule représente un frein non négligeable au développement. Avec la solution de règlement sécurisé, il est vraisemblable que ce projet peut être amené à de nouveaux développements par une prise de conscience des opportunités réelles qu'offre désormais cette solution.

L'ambition des banques « CB » est bien de s'attacher à mieux connaître dans les années qui viennent ce secteur, car il est plus facile à cerner que le secteur grand public, il est vraisemblablement plus ouvert au nouveau type de paiement pourvu que la sécurité offerte soit bien expliquée et il est naturellement plus porteur de revenus.

Pour ces diverses raisons, et en dépit du halo d'incertitude qui l'entoure dans l'immédiat, ce segment de marché porte véritablement en lui les espoirs du développement du commerce électronique.

Les autres échanges

Dans le préambule de cette partie, le recours à la sémantique laissait entrevoir que d'autres aspects des échanges sécurisés peuvent voir le jour sur Internet. Ce ne sont pas nécessairement des échanges marchands.

On retiendra quelques exemples qui peuvent induire l'usage de la carte bancaire comme vecteur d'accès à ce type d'échange.

• La banque électronique paraît une zone d'impact naturelle de la sécurisation de l'accès par carte bancaire. Actuellement, de nombreuses banques offrent un accès au compte de leurs clients soit à travers une liaison sécurisée par SSL ou par un logiciel maison. Avec la solution de convergence, elles disposent désormais d'un mécanisme de contrôle d'accès rapide, sûr et fiable, ainsi que d'un mécanisme de signature électronique d'ordres de banque fiable, sans oublier une ergonomie éprouvée pour le client qui se retrouve dans des modes de fonctionnement qui lui sont familiers.

• La sécurisation de la messagerie personnelle pourra demain, dans des conditions à définir, recourir également à un tel protocole.

• Les relations avec les administrations locales ou régionales (fiche d'état civil par exemple, mais aussi déclaration des impôts voire paiement de ceux-ci) pourront se trouver sécurisées par ce type de protocole pour peu que l'accès à ces organisations puissent se faire avec la signature d'une carte bancaire ayant une application d'identification spécifique. Il est évident que l'administration est en train d'effectuer un gigantesque effort de modernisation, notamment dans le domaine de l'Internet. Plus de 200 formulaires sont d'ores et déjà disponible sur le Web et de très nombreuses expériences locales sont en train de constituer un faisceau d'expériences qui progressivement vont changer la relation entre l'administration et le citoyen.

• La banque par téléphone va connaître des progrès sensibles grâce à l'utilisation de l'écran du GSM et avec l'apparition prochaine de téléphones portables dotés de lecteurs de cartes bancaires, on devine aisément qu'il sera possible un jour proche d'effectuer des paiements avec un GSM ! Le Groupement « CB » est très impliqué dans ces activités de Recherche et Développement du paiement à distance, car elles consti-

tuent le socle technique incontournable de nouvelles activités commerciales bancaires.

Ces quelques exemples pratiques illustrent que les domaines couverts par le protocole de sécurisation des banques « CB » sont multiples, qu'ils recèlent de réelles potentialités, mais aussi qu'il faut donner du temps au temps pour que « les fruits dépassent la promesse des fleurs ».

Les enjeux financiers du commerce électronique

La mise en œuvre du projet de sécurisation du commerce électronique représente pour la communauté bancaire française un investissement de plusieurs dizaines de millions de francs sur 5 ans, dont la moitié a déjà été consommée par les expériences pilotes de Cybercard, d'E-Comm fusionnées en Cyber-COMM, voire de KLEline. Pour importants que soient ces montants, ils représentent une dépense modeste dans l'ensemble des budgets informatiques des banques.

Vouloir constituer un outil de paiement représente un enjeu d'une rare complexité et le plus souvent l'alliance et la coopération sont nécessaires.

On le voit actuellement plusieurs centaines d'initiatives existent pour tenter de sécuriser le commerce électronique : aucune n'est adoptée de façon déterminante par le marché. La voie que les banques « CB » ont choisi, après des expériences séparées, est celle de la coopération et de l'union.

C'est à cette seule condition que l'on peut, actuellement, voir décoller une solution originale, tirant profit des investissements importants consentis par le passé par ces mêmes banques mais aussi par les commerçants.

Retrouver dans un nouvel outil de paiement adapté au commerce électronique toutes les pièces du puzzle du paiement de proximité est en effet un atout irremplaçable pour le commerçant qui dispose déjà des briques de base du paiement sécurisé par carte à puce, quitte à les adapter au paiement sur réseaux ouverts.

Il ne s'agit donc pas de créer un outil *ex nihilo* mais d'optimiser l'existant, en l'adaptant.

LES ATTENTES DES DIFFÉRENTS ACTEURS DU COMMERCE ÉLECTRONIQUE A L'AUBE DU TROISIÈME MILLÉNAIRE

Le commerce électronique suscite un immense intérêt ; les chiffres les plus fantaisistes et les plus attractifs circulent dans les revues « spécialisées » ; beaucoup appellent de leurs vœux ce qui n'existe pas encore mais ne manquera pas de se produire : l'explosion des échanges sur les réseaux ouverts. Même si l'on constate çà et là un frémissement dans ce

domaine, on s'aperçoit que les attentes des différents acteurs économiques ne sont pas encore à la hauteur de leurs espérances : le commerce électronique revêt aujourd'hui en effet trop souvent l'aspect « babel » avant d'être le nouvel esperanto du *business* de demain.

Les attentes des internautes

Même si l'ergonomie des logiciels subit régulièrement une cure de rajeunissement, il faut avoir été confronté à une ou deux installations de PC pour constater que c'est très simple à condition… de connaître quelques notions du BIOS et de la carte mère, de comprendre les rudiments des télécommunications et des modems, de savoir dominer les incompatibilités entre les logiciels de Microsoft… Bref c'est une expérience qui laisse des traces, sans oublier une *hot line* souvent accorte et bienveillante… mais rétive parfois à fournir la bonne explication sur la difficulté rencontrée ou sur la pertinence de la solution proposée. A cette complexité technique s'ajoute la difficulté de maîtriser l'immensité des centres d'intérêt ouverts sur le Web. Et en définitive pour les rares internautes qui voudraient passer du simple butinage de l'information à l'achat d'un bien ou d'un service un frein supplémentaire se glisse dans leur démarche par le risque potentiel de voir leurs données personnelles capturées. Bien plus s'ils n'étaient pas vigilants sur cette question la dernière version d'Explorer[4] leur rappelle, à temps et à contretemps, le risque systématiquement pris, de transmettre des données sur Internet.

Surfer sur le Net est donc dangereux ; payer constitue un acte hautement risqué. Pourtant les internautes attendent des logiciels de paiement qu'ils soient simples, fiables et universels ; en d'autres termes leur besoin est pratiquement conforme aux critères de confiance que l'on exige d'un instrument de paiement.

Simplicité : si mettre en marche un PC constitue une aventure, c'est également une aventure de payer aujourd'hui sur Internet. Avec SSL, nous l'avons vu l'internaute est captif de son PC par les certificats mis en œuvre à chaque transaction. Avec Cyber-COMM et la carte bancaire, ce lien esclave est supprimé : le lecteur de carte s'adapte à tous les PC (demain il sera incorporé en standard dans les PC) et la signature puce supprime tout recours préalable au certificat et à l'enregistrement. Pour payer sur le Net avec Cyber-COMM il suffit de disposer d'une carte bancaire, nationale ou internationale. Il est donc aussi simple de payer avec Cyber-COMM à domicile que chez le commerçant, immédiatement et à tout moment, dans une ergonomie parfaitement maîtrisée par tout porteur d'une carte bancaire.

Fiabilité : l'internaute souhaite disposer d'un outil sécurisé, pour s'assurer à la fois de l'existence du commerçant et d'éviter de voir son numéro de carte capturé lors de son passage dans les réseaux de télétrans-

mission. Cyber-COMM réduit ce double risque : d'une part les échanges sont fiabilisés par la garantie bancaire de l'existence du commerçant en raison du certificat délivré par Visa ou Mastercard et d'autre part les données circulant sont signées par la carte puis chiffrées avant d'être pris en charge par le protocole SET. Il y a donc un haut degré de fiabilité inséré dans le couple SET + signature par la carte à puce.

Universalité : commerçants et internautes sont déboussolés devant la multiplicité de l'offre de logiciels de paiement et spontanément ils font confiance à leur banque pour traiter cette question. Les banques doivent donc répondre à cette attente en proposant avec la carte bancaire un outil de paiement universel, véritable support du commerce électronique. L'un des freins au développement du commerce électronique c'est effectivement le caractère « propriétaire » et donc réduit des offres privatives d'instruments de paiement. Avec Cyber-COMM, développé et soutenu par Visa et Eurocard/Mastercard, une véritable solution internationale et inter opérable est en train de voir le jour. Ceci constitue une authentique réponse aux besoins des internautes assortie en outre d'une solution de traitement des micro-paiements.

Le commerce électronique s'accommode mal de l'extrême diversité des solutions offertes actuellement. Le marché, dans son pragmatisme habituel tranchera entre les meilleurs outils. Néanmoins avec la solution combinant la carte bancaire et la signature sécuritaire de la puce, nous avons la conviction de fournir une réponse à la hauteur des attentes et des exigences de la clientèle des internautes.

Les attentes des commerçants

On pourrait se contenter de résumer les attentes des commerçants en trois points : réaliser du chiffre d'affaires, être sûr d'être payé, mais d'abord et avant tout que le système soit simple.

• *Pour accroître son chiffre d'affaires*, le commerçant a besoin que les clients soient nombreux à pouvoir utiliser le système et à avoir envie de l'utiliser.

Un système qui apporte immédiatement, sans enregistrement préalable de leur part, 30 millions de cartes CB et plusieurs centaines de millions de cartes Visa ou Eurocard-Mastercard, offre d'emblée un potentiel maximum d'acheteurs. Et cela avec une spontanéité essentielle dans l'acte d'achat à distance où le moindre obstacle technique fait avorter l'intention d'achat.

• *Pour être certain d'être payé*, le commerçant doit disposer d'un système sûr. Il en est ici comme pour les assurances, plus la sécurité est forte, plus la garantie est importante. Si le système de paiement comprend un dispositif d'authentification réciproque, d'intégrité et de confidentialité, comme nous l'avons expliqué précédemment, les pos-

sibilités de répudiation de la part du client sont étroites et les banques peuvent aisément garantir le paiement.

Ces dispositions ne sont pas accessoires, puisque de la bonne authentification du client dépend aussi sa situation en termes *marketing* et géographique. En commerce à distance, il est en effet fondamental de disposer d'informations fiables sur le client.

Au-delà de ces deux préoccupations le commerçant formule également d'autres exigences : pour lui le système de paiement doit être standard, à défaut d'être unique afin de limiter les coûts d'investissements et les coûts d'exploitation.

Il doit également être simple à intégrer, c'est-à-dire connu et recommandé par les hébergeurs, les intégrateurs de solutions et les éditeurs de logiciels, et pouvoir ainsi évoluer d'autant plus facilement.

Cyber-COMM répond à ces attentes en s'appuyant sur le protocole SET, désormais intégré dans les solutions de commerce électronique du marché (*front-office* et *back-office*) et sur la carte à microprocesseur, également maîtrisée par de nombreux industriels.

Enfin, pour répondre aux besoins spécifiques suscités par le développement de la vente de services ou d'informations en ligne (édition électronique aujourd'hui textuelle, demain vidéo ou vidéographique), Cyber-COMM intègre le traitement des paiements de petits montants.

Les attentes des banques : renforcer la confiance

La Communauté Bancaire depuis plus d'une décennie, au sein du Groupement des Cartes Bancaires « CB », a su construire les infrastructures du paiement par carte pour en faire un instrument sûr, peu coûteux et plébiscité par les utilisateurs consommateurs et commerçants, en sachant adapter les modalités techniques et réglementaires aux exigences des besoins de la distribution commerciale moderne.

Il n'est plus en effet de secteur d'activité privé ou public (la santé et l'administration y viennent progressivement) qui n'accepte les cartes sous les formes les plus adaptées : intégration aux systèmes d'encaissement complexes de la Grande distribution, automates de distribution de carburant ou de titre de transport, publiphones, vente par correspondance ou par téléphone, par minitel équipés de lecteurs de cartes à puce, et même un million de décodeurs TV… Autant de dispositifs facilitant un paiement par carte répandu, bon marché et très sûr.

Il est naturel que les établissements bancaires « CB », forts de cette expérience et de ce savoir-faire, soient nantis de la confiance de leurs clients dans le système de paiement par carte à microcircuit.

Dès lors, les attentes des banques sont centrées sur la capacité des industriels à les aider dans le développement des produits demandés par les acteurs du commerce électronique. Elles sont attentives à la volonté

des pouvoirs publics de les aider à exercer ce rôle d'intermédiaire de confiance pour lequel elles sont dûment contrôlées.

Loin d'une expression corporatiste, le positionnement des banques sur la gestion des moyens de paiement est la garantie de l'indépendance nécessaire à l'établissement de la confiance entre les acteurs.

Cyber-COMM présente à cet égard, une architecture au sein de laquelle les banques engagent leur responsabilité sur la sécurité du système :

- en distribuant les cartes et les codes confidentiels aux porteurs,
- en affiliant les commerçants par contrat spécifique pour le commerce électronique,
- en gérant les dialogues de paiement entre les parties,
- en organisant un système de paiement sécurisé apte à instaurer la confiance des porteurs et la garantie de paiement pour le commerçant dans le commerce électronique sur les réseaux ouverts.

Pour ce faire, elles accréditent les différents acteurs de la transaction et assurent les services de cryptographie nécessaires à cette gestion sécuritaire.

En un mot, les banques constituent le pivot de la confiance dans l'univers des transactions électroniques par des dispositifs appropriés communément appelés « tiers de confiance », dont le rôle dans le cadre du commerce électronique, se limite à certifier les différents acteurs ainsi que nous l'avons démontré à la seconde partie de ce document.

La position de l'administration

La mission Lorentz, le rapport de madame Falque Perrotin ou ceux de messieurs Yolin ou Abramatic montrent la dynamique de l'administration sur l'Internet en général et le Commerce électronique en particulier.

Les projets de l'administration rejoignent les attentes des citoyens et des entreprises sur plusieurs points.

D'un point de vue général, l'administration a pour rôle de structurer la confiance des acteurs entre eux et, au besoin, édicter des règles nouvelles.

Elle s'appuie pour cela sur un dispositif juridique et un dispositif sécuritaire. Les deux sont intimement liés. A titre d'exemple, la reconnaissance de la validité des signatures électroniques qui touche au droit de la preuve, implique une assise cryptographique solide qui devra être mise à disposition des acteurs du commerce électronique.

Pour créer l'élan économique qui doit faire émerger le commerce électronique, l'administration joue un rôle d'accompagnement significatif y compris dans le domaine du paiement : c'est ainsi que le ministère de l'Economie et des Finances vient de donner son accord à la digitalisation des factures payées dans le cadre du service *purchasing card*.

La mise en place de « tiers de confiance » doit s'effectuer à la fois dans un cadre légal clair et favoriser la création d'entités de recherche (calculs,

algorithmes...), de développement et d'exploitation. Elle ne peut que faciliter les desseins d'un système qui valorise les points forts de l'industrie ou des entreprises de service nationales. Plus encore, un système qui puisse s'exporter.

Utilisant des technologies avancées et répondant à des normes internationales, Cyber-COMM répond à ces exigences.

Si l'Etat se veut exemplaire, comme le préconise le rapport Lorentz, l'administration a besoin, pour ses services ou ceux qu'elle rend aux administrés, d'un système de paiement confidentiel (le paiement des impôts est un sujet sensible en France...), peu onéreux et incitatif.

Enfin l'administration française se doit de favoriser un système largement répandu. C'est la raison pour laquelle les Pouvoirs publics ont vivement encouragé la convergence des solutions bancaires à base de carte à puce.

Une monnaie est universelle, fut-elle électronique, et si l'euro remplit ce rôle de dénominateur commun monétaire, il doit être supporté sur l'ensemble du territoire communautaire par un système de paiement sur Internet, moderne et inter opérable.

La Commission européenne, tout comme l'administration française, ne manqueront pas d'exhorter les acteurs sur ce point.

En misant le développement du Commerce électronique sur le protocole de sécurisation des paiements SET, la Communauté Bancaire « CB » exerce un choix comportant plusieurs risques qui ont été clairement identifiés :

• risque de voir ce choix sécuritaire boudé, ou pire, méconnu par les commerçants à travers le monde ;

• risque de voir les internautes rester indifférents à une solution qui leur apporte confort d'utilisation, convivialité dans le dialogue et ergonomie dans le paiement en ligne ;

• risque de voir des solutions moins riches que SET s'étendre, voire de demeurer durablement dominantes ;

• risque enfin de voir les banques réticentes à se lancer dans une énième campagne d'information sur la sécurité du paiement sur le Net.

C'est la raison pour laquelle l'appui et le relais des deux organisations internationales Visa et Mastercard - très impliquées dans le projet - confèrent à Cyber-COMM un statut international activement recherché et de nature à réduire les risques ci-dessus énoncés. L'Europe reste néanmoins notre cœur de cible, car la carte à puce s'y développe rapidement, et la solution qui est proposée se présente comme un facteur déterminant pour faciliter le passage à l'euro du commerce électronique.

Cyber-COMM intègre dans SET tous les ingrédients décrits dans cet article pour devenir la structure de départ d'une vaste expertise euro-

péenne dans la sécurisation du commerce électronique. Les acteurs bancaires « CB » doivent donc conforter jour après jour cette convergence qu'ils ont appelées de leurs vœux pour donner à leurs clients une solution simple, fiable et universelle. Fort des enseignements issus des expériences respectives de Cybercard et d'E-COMM, disposant en outre d'un capital de confiance fondé sur l'expertise avérée du Groupement « CB », Cyber-COMM possède tous les atouts pour devenir, - comme le fut la puce en son temps - la référence internationale de la réussite des banques « CB » dans le domaine ultra compétitif de la sécurisation des paiements sur les réseaux ouverts.

BIBLIOGRAPHIE

ESPAGNON M. - *Computer and Telecoms Law Review - 1997/4*, « Le paiement électronique « en réseau ouvert » - Internet : Problématique juridique ».

Dictionnaire Permanent Droit des Affaires « Commerce électronique : la sécurisation des transactions par des procédés de cryptologie » .

« Cryptologie, mode d'emploi » *Service Central de la Sécurité des Systèmes d'Information (SCSSI) - Juin 1998.*

SALZMAN C. « La monnaie électronique » - *Décembre 1996 dans « L'informatique professionnelle » N° 149.*

« Le commerce électronique facteur de croissance des PME » - *Livre blanc - Mars 1997.*

GIRAULT M. et GUERIN D. - *CNET - Revue Télécom - N° 111 - 1997.* « La cryptographie et son utilisation dans le commerce électronique sur Internet ».

PICORY C. - ENST - « Electronic Commerce, industrial organization and financial issues ». *Contribution au groupe 22454 du projet ESPRIT - G7-10WG - Juin 97.*

THIVEAUD JEAN-MARIE - « Le phénomène financier et les marchés financiers en perspective historique : des sociétés antiques à la création de la Bourse de Paris, en 1724 » in *Revue d'Economie Financière* N° 48 juillet 1998.

MARTIN-LALANDE P. « L'Internet : un vrai défi pour la France ». *Rapport au Premier Ministre 1997.*

« Internet et les réseaux numériques », Conseil d'Etat, 2 Juillet 1998.

« AFTEL : INTERNET, les enjeux pour la France », L'Edition 1999.

Rapport LORENTZ 2 : « La nouvelle donne du commerce électronique. Réalisations 1998 et perspectives ». Ministère de l'Economie et des Finances, mars 1999.

NOTES

1. SSL n'est autorisé en France, à l'heure actuelle, qu'avec un cryptage utilisant des clés d'une longueur de 40 bits alors que des solutions de cryptage à 128 bits existent notamment aux USA. Mais le Premier Ministre, dans son discours du 19 Janvier 1999 vient d'élargir « à 128 bits le seuil de la cryptologie dont l'utilisation est libre ».

2. Sources : Association des Fournisseurs d'Accès (AFA) et Mediangles on-line.

3. Il s'agit d'un porte-monnaie lié aux achats sur Internet. Il est donc bien virtuel et ne saurait être confondu avec le Porte-Monnaie Electronique Interbancaire (PMEI) que le Groupement « CB » essaie de promouvoir par ailleurs en France.

4. Explorer est la version d'accès à Internet de Microsoft.