

Cyber-COMM sécurise le paiement sur l'Internet

*Au début de l'an 2000,
la solution Cyber-COMM
ouvrira l'accès au paiement
sécurisé sur Internet
grâce à la carte à puce.*

Impliquées à divers titres, les banques, et les banques françaises en particulier, ne peuvent pas rester en retrait du phénomène du développement du commerce électronique :

- elles ont des relations commerciales avec des entreprises qui souhaitent vendre leurs produits ou leurs services sur le web à une clientèle quelquefois située à des milliers de kilomètres. Les banques doivent donc accompagner leurs clients dans ce nouveau challenge ;

- elles gèrent les comptes de millions de particuliers et des professionnels qui sont autant d'acheteurs potentiels tant sur des sites français qu'au-delà des frontières ;

- elles assurent directement ou indirectement – via, par exemple les réseaux CB, MasterCard ou Visa – la gestion des flux financiers qui accompagnent nécessairement les transactions commerciales entre acheteurs et vendeurs ;

- avec ce qu'il suppose comme défi marketing, le web peut devenir un nouveau champ de recrutement de clients, notamment – mais pas uniquement – dans le domaine des services bancaires liés aux cartes ou à la banque en ligne.

Les établissements bancaires développent donc, chacun pour son propre compte ou sous des formes associatives, une offre commerciale destinée aux différents segments de marchés évoqués ci-dessus. Par ailleurs, ils continuent à œuvrer au sein d'instances internationales pour améliorer et fluidifier les paiements transfrontières.

OBJECTIF : CONFIANCE ET SÉCURITÉ

Toutes les études sur le phénomène web sont concordantes au moins sur un point : la sécurité et la confiance sont les principaux facteurs du développement du chiffre d'affaires du commerce sur l'Internet. L'acheteur doit non seulement pouvoir être certain que nul ne pourra intercepter les données qu'il envoie vers un site web, mais encore que, derrière ce site, il y a bien un commerçant «réel». Selon l'American National League, 6 millions d'Américains auraient été, en 1998 victimes d'escroqueries aux cartes de crédit sur Internet, soit une progression de 600 % sur un an pour ce type de fraude.

Confiance et sécurité sont d'autant plus indispensables lorsqu'il s'agit de saisir puis de véhiculer des données financières. Mener à bien des transactions monétaires requiert donc le plus haut niveau de sécurité.

L'industrie du *net* est en train d'inventer de nouveaux circuits, de nouveaux services. Il est par conséquent du devoir des banques de développer de nouveaux modes de paiement, voire de nouveaux moyens de paiement. Sinon, grand serait alors le risque de voir de nouveaux entrants cultiver un terrain que les systèmes bancaires ou financiers auraient laissé en jachère. Par ailleurs, l'intérêt des pouvoirs publics est également évident : pour la bonne marche du système, la maîtrise des flux doit rester dans le domaine d'établissements financiers dûment contrôlés.

D'ailleurs, la Commission européenne s'est emparée du problème et une Direc- ...



HERVÉ SITRUK
Directeur général



SERGE BLANC
*Directeur chargé
du déploiement et
des relations avec
les réseaux
bancaires*

Cyber-COMM*

*Cyber-COMM compte parmi ses actionnaires les neuf principaux établissements financiers et bancaires français, les systèmes cartes nationaux et internationaux, ainsi que des industriels et un opérateur téléphonique.

tive est en préparation. Quant à l'OCDE, elle envisage d'élaborer une charte du commerce électronique dont les grandes lignes devraient être rendues publiques à l'automne.

LA QUESTION DE LA PREUVE

Pour remédier à l'insécurité des paiements qui est l'un des principaux freins au développement du commerce électronique, il existe de nombreuses réponses qui assurent des degrés de sécurité divers.

Ainsi, il y a SSL (*Secure Socket Layer*) que certains jugent satisfaisant. Le protocole SSL crypte en effet les données qui voyagent sur l'Internet... mais pas ce qui se passe sur le micro-ordinateur.

Lorsque le numéro d'une carte bancaire est crypté, des failles existent avant et après le cryptage, même si, et c'est le cas avec SSL, il sera difficile de détourner le numéro de la carte en cours de route. En revanche, l'acheteur n'a aucune garantie de la réalité même du commerçant. De surcroît, le cryptage des données n'apporte aucune garantie quant à la fiabilité du montant affiché sur l'écran qui peut être modifié a posteriori par le commerçant, au titre de frais de port par exemple ou d'éventuelles taxes. Le marchand ne peut avoir,

des opérations de paiement car ne pouvant produire aucun mandat de débit dûment signé, elles devraient rembourser le client à première demande.

SET + CYBER-COMM :

LA RÉPONSE DES BANQUES FRANÇAISES

De leur côté, Visa et MasterCard, en association avec JCB et American Express et de nombreux établissements bancaires de par le monde ont mis au point le protocole SET (*Secure Electronic Transaction*). A la différence notable de SSL, ce protocole basé sur des échanges de certificats digitaux, permet le paiement par carte en garantissant l'inviolabilité des données transmises au travers de l'Internet et authentifie toutes les parties prenantes à un acte d'achat-paiement. En effet, outre le cryptage des données sur l'Internet, SET permet d'authentifier non seulement le porteur de la carte et le commerçant, mais aussi leurs banques réciproques qui sont ainsi entièrement intégrées au système. Avec SET, on évite les achats avec des cartes «non autorisées» (vraies-fausse cartes, par exemple) et la captation, par quiconque, y compris par le commerçant, de données bancaires confidentielles. Avec SET, les banques ne sont pas désintermédiées car la banque du porteur de la carte et la banque du commerçant sont appelées l'une et l'autre à certifier ces deux acteurs qui sont leurs clients.

Pour sa part, le client a la certitude qu'il contracte avec un vrai commerçant, et que c'est bien celui-ci qui encaissera le montant de la transaction. Quant au commerçant, il est assuré de l'existence du consommateur et de la validité de sa carte.

L'APPORT DE CYBER-COMM

On aurait pu en rester là. Et, d'ailleurs, de nombreux pays en resteront à ce stade pendant encore les quelques années nécessaires à la généralisation de la carte bancaire à microprocesseur en Europe et ailleurs dans le monde. En effet, le «plus» de la solution mise en œuvre par les banques françaises au travers de Cyber-COMM, c'est bien la carte à puce qui le permet. SET est une solution logicielle qui, dans sa version de base, avec l'établissement d'un certificat pour le porteur, nécessite le numéro de la carte, mais ne requiert pas le recours à un dispositif qui prouve la présence de la carte et authentifie le support physique.

La solution Cyber-COMM, en revanche,

500 000 acheteurs sur le web

A fin juin 1999, on dénombre en France 1 000 sites marchands sur le web (+ 30 % en 4 mois !) dont le tiers ne proposent pas le paiement en ligne. 500 000 internautes français ont fait un achat sur le web depuis le début de l'année. Face aux e-marchands il y a plus de 4 millions d'internautes

disposés, pour peu que certaines conditions soient réunies, à devenir, eux aussi, des e-consommateurs. On estime à 180 millions d'euros le chiffre d'affaires réalisé par l'ensemble des sites web marchands français sur le premier semestre, soit l'équivalent d'un gros hypermarché.

en ce qui le concerne, aucune certitude que la carte, en supposant qu'elle existe, appartient bien à l'acheteur. Enfin, comment s'assurer que le consommateur a, en l'absence de toute signature électronique, juridiquement approuvé le montant et les conditions de la transaction ? La répudiation du paiement peut, à tout moment, être mise en œuvre par le porteur, aucune preuve de son accord formel ne pouvant être apportée. Les banques ne peuvent accorder dans ces conditions une garantie à

nécessite un lecteur sécurisé de carte à puce. Il s'agit d'un appareil de la taille d'une petite calculette et semblable à un terminal de paiement électronique. Cet appareil est connecté au micro-ordinateur du consommateur qui, au moment de payer, doit introduire sa carte bancaire, puis doit en composer le code secret. Le mode opératoire est identique à celui du commerce de proximité. Le lecteur de carte comporte un écran à cristaux liquides sur lequel apparaissent le montant de la

«La sécurité et la confiance sont les principaux facteurs du développement du chiffre d'affaires du commerce sur l'Internet.»

transaction à valider, ainsi que la devise utilisée. Le code secret, directement vérifié par le lecteur, n'est pas acheminé vers l'unité centrale du micro-ordinateur et ne circule donc pas sur l'Internet ; les autres données de la transaction sont chiffrées.

DE MULTIPLES PERSPECTIVES

Le lecteur sécurisé labellisé par Cyber-COMM est universel et pourra être utilisé pour d'autres applications que le paiement. Certaines banques l'utiliseront comme moyen d'accès à leurs services de banque à distance ou, par exemple, pour signer électroniquement des ordres de bourse. De plus, la solution Cyber-COMM est susceptible d'être utilisée dans d'autres domaines que le web...

Les banques françaises promotrices de la solution Cyber-COMM et actionnaires de la société ont la maîtrise de plus de 95 % des flux liés aux cartes bancaires CB ; elles distribueront, au début de l'année prochaine, des lecteurs de carte à 20 000 de leurs clients. Il s'agira là d'un test à la fois technique et marketing auquel seront probablement associées quelques agences bancaires. Dans l'avenir, le lecteur de carte sera très certainement intégré au clavier de l'ordinateur, voire dans un GSM. Cyber-COMM travaille déjà dans ce sens avec des constructeurs et des industriels du secteur de la péri-informatique. ●