SYSTÈMES ET INSTRUMENTS DE PAIEMENT EN LIGNE : QUELLES PROBLÉMATIQUES ? QUELS TYPES DE SOLUTIONS ?

CLAUDE DRAGON *
JEAN-FRANÇOIS SUSBIELLE **

Au dernier recensement, la population mondiale des internautes a franchi la barre des 600 millions et le pourcentage de pénétration planétaire de l'Internet a atteint 9,68 %, l'équivalent mondial de l'automobile ! Qui pourrait nier qu' Internet représente un marché considérable pour l'e-commerce et constitue l'une des composantes de la mondialisation ?

Certes, l'e-commerce est encore un marché marginal, qu'il s'agisse des échanges commerciaux interentreprises (B to B pour *business to business*), ou qu'il s'agisse du commerce grand public (B to C pour *business to consumer*). Mais il est aujourd'hui évident qu'il a déjà « décollé » et que son rythme de développement laisse entrevoir un bel avenir.

Quelques chiffres « flash » pour donner un ordre de grandeur des enjeux :

- *B to B* : ce sont, selon une estimation de Gartner Group, 8 630 Md$ de flux financiers qui sont concernés au plan mondial à l'horizon 2006, dont 2300 pour l'Europe (contre, il est vrai, 77 Md$ seulement en 2001, soit moins de 1 % des échanges interentreprises). La mise en place de « places de marché » qui touchent les plus grands groupes industriels et commerciaux dans la plupart des secteurs économiques : aéronautique, automobile, grande distribution... devrait contribuer à l'essor de ce nouveau type de relations commerciales entre acheteurs et fournisseurs. À titre d'exemple, certaines places de marchés de la grande distribution pourraient concerner 70 000 fournisseurs (GNK) voire 100 000 (WWRE) ;
- *B to C* (et c'est à ce marché « grand public » que nous limiterons notre contribution) :

* Consultant libéral, ancien sous-directeur honoraire à la BNP.
** Consultant libéral.

- aux États-Unis, le chiffre d'affaires réalisé sur Internet a atteint 6 Md$ pour le seul mois de juillet dernier. C'est, à peu de choses près, le chiffre d'affaires réalisé sur l'ensemble de l'année 2001 par l'e-commerce au Royaume-Uni... ;
- en Corée du Sud, le nombre d'internautes ayant effectué des transactions bancaires via Internet est passé de 14,5 millions à fin mai 2002 à 17 millions au 30 septembre, soit une augmentation de 17 % en un trimestre !
- en Europe, une étude réalisée par l'institut GfK-Webgauge et portant sur six pays (Belgique, France, Allemagne, Pays-Bas, Espagne et Royaume-Uni), a montré que la proportion de consommateurs en ligne est passée de 27,7 % à 31,4 % entre l'automne 2001 et le printemps 2002. Toutefois, ce taux moyen recouvre des disparités importantes puisqu'il est de 26 % en Allemagne et seulement 19 % France (aux dernières nouvelles, ce dernier taux serait de 22 %).

Cela veut dire, concrètement, que près de 59 millions d'internautes sur 187 millions dénombrés ne se contentent pas de surfer, mais ont franchi le pas de l'achat en ligne.

Autre tendance mise en avant par cette étude, le montant déboursé en ligne par les consommateurs augmente. Pendant la même période considérée, les dépenses des « cyber-acheteurs » seraient ainsi passées de 4,20 à 11,50 Md€, dont 4,86 Md€ en Allemagne et seulement 1,45 Md€[1] en France (2,35 Md€ en prévision 2002) et un panier moyen de 163 € pour l'internaute français contre 437 € pour son homologue allemand : de quoi alimenter notre réputation de frilosité !

Les perspectives de croissance de l'e-commerce en France sont très fortes, puisque seulement 10 Français sur 100 achètent aujourd'hui en ligne, contre 14 Allemands et 22 Britanniques. Mais déjà, selon le bilan que vient de dresser l'Acsel (Association pour le commerce et les services en ligne) :
- 51 % des internautes se connectant quotidiennement achètent en ligne contre 15 % des personnes se connectant une à trois fois par mois ;
- 45 % des habitués d'Internet depuis plus de trois ans achètent en ligne, contre 15 % des personnes connectées depuis moins d'un an.

Du constat actuel, on peut retenir quelques éléments-clés :
- Internet ne constitue pas seulement un canal supplémentaire de vente à distance mais aussi ouvre la voie (déjà amorcée dans le cadre franco-français du Minitel) à de nouveaux produits et services « livrables en ligne » et donnant lieu à des transactions qui peuvent être d'un prix unitaire de quelques centimes à quelques euros : téléchargement d'articles de presse, de musique, de vidéos, de jeux..., marché qui devrait exploser avec la banalisation du haut débit qui concerne déjà, en France

2,3 millions d'internautes...) et nécessite d'urgence des solutions spécifiques de micro-paiement ;
- il existe un certain nombre d'obstacles au développement de l'e-commerce : le Gbde (Global business dialogue on electronic commerce), lors de son récent sommet de Bruxelles, en a inventorié les principaux et s'est fixé comme objectif de les abattre.

Parmi ces obstacles[2] retenons ici notamment :
- restaurer la confiance,
- développer le paiement électronique.

Ce sont ces thèmes qui vont constituer la toile de fond des réflexions que nous proposons au lecteur, en soulignant d'emblée que la notion de confiance doit englober bien évidemment aussi bien l'aspect commercial de la transaction que son épilogue financier.

Il est en effet (quelquefois...) de bon ton d'accuser l'insécurité des moyens de paiement en ligne d'être le frein majeur au développement de l'e-commerce.

Si, selon un sondage effectué aux États-Unis auprès de 1 500 internautes, 67 % des personnes interrogées citent effectivement la sécurité du paiement comme frein à l'achat en ligne, d'autres réticences liées, cette fois, à la transaction commerciale elle-même ne sont pas très loin : 50 % citent le surcoût de livraison, 47 % la réutilisation possible des données personnelles, 44 % les craintes sur le service après-vente, 25 % les délais de livraison, 23 % l'absence de relation commerciale « face à face ».

D'autres études mettent en outre en évidence le nombre très élevé (27 %, selon Forrester research) des tentatives de paiement en ligne qui avortent du fait d'une mauvaise ergonomie des processus de paiement proposés ou de défaillances techniques des serveurs dédiés.

Quant aux moyens de paiement, on pourrait faire remarquer que, les transactions commerciales induisant le plus souvent un règlement financier, les scores de l'e-commerce témoignent que des systèmes et instruments de paiement existent bel et bien et que les internautes les utilisent déjà de plus en plus...

En réalité, ce n'est pas l'absence de moyens qui pose problème, mais d'une part, leur foisonnement et, d'autre part, les risques de fraude liés au niveau plus ou moins sécuritaire des processus mis en œuvre :
- *leur foisonnement* : l'Epso (Observatoire des systèmes de paiement électronique) a dénombré, pour la seule Europe, pas moins de 150 « outils » de paiement opérationnels ou, le plus souvent, en tentative de déploiement sur le marché ;
- *leur sécurité* : dans un récent rapport, le CES (Conseil économique et social) déplore à juste titre, qu'il « n'existe pas de solutions communément admises pour sécuriser les paiements en ligne ».

Aujourd'hui, la carte bancaire couvre, à elle seule, près de 90 % des paiements en ligne, mais autant son utilisation en règlement de proximité peut-être jugée sécuritaire, au moins en France grâce à la « signature » que constitue le contrôle du code confidentiel, autant son utilisation en ligne, pour laquelle elle n'avait pas été conçue, ne répond pas aux critères sécuritaires même, nous le verrons, si le paiement est dit « sécurisé ».

En toile de fond - et les tâtonnements du secteur financier (banques et émetteurs de cartes en particulier) y ont sans doute contribué - d'autres acteurs (opérateurs télécoms, éditeurs de logiciels...) cherchent aujourd'hui à investir ce marché des moyens de paiement en ligne.

Souhaitant aider le lecteur à s'y retrouver dans le dédale des solutions opérationnelles ou largement annoncées (le faire savoir précédant bien souvent le savoir-faire...), nous nous proposons de répondre dans une première partie, à la double question : « Qu'attendent les acteurs d'un système de paiement et quelles sont les composantes à prendre en compte ? », ce qui constituera, nous l'espérons, une grille de lecture pour aborder, dans la seconde partie, le « Panorama » des principaux types de solutions.

LA PROBLÉMATIQUE DU PAIEMENT EN LIGNE

Qu'attendent les utilisateurs ?

La réponse est assez évidente : un système sûr et rassurant, simple et sinon universel, du moins largement diffusé.

Ce que cela implique est quand même un peu plus complexe que ce simple énoncé qui va de soi...

En premier lieu, un système sûr et donc rassurant

Les médias ont (quelquefois...) tendance à monter en épingle les fraudes enregistrées par le commerce en ligne, au risque, avéré..., de freiner les internautes à communiquer leur numéro de carte bancaire, ou même d'acheter sur Internet.

Il ne s'agit pas de nier qu'il y a de la fraude en ligne, tout comme il en existe dans le monde réel (fausse monnaie, chèques en bois...). Il s'agit plus de la cerner et de la prévenir.

Quelques chiffres : dans une récente étude, Fianet estime que la fraude en ligne a représenté, en 2001, 1,35 M€ et le GIE des cartes bancaires annonce pour sa part un taux de 0,037 % du chiffre d'affaires. L'Observatoire du commerce électronique, mis en place récemment, devrait contribuer à avoir une approche plus précise de son coût réel pour les différents acteurs concernés.

Aux États-Unis, la fraude est estimée à 704 M$ dont 87 % seraient liés aux enchères en ligne, c'est-à-dire à une activité bien ciblée.

Enfin, à notre connaissance, aucun piratage en ligne de numéro de carte n'a été effectivement constaté et la plupart des sites « sérieux » sont aujourd'hui sécurisés, notamment par le cryptage en ligne des éléments sensibles de la transaction : nous y reviendrons.

On ne peut pour autant se satisfaire d'une situation qui, même relativisée, conduirait à négliger la sécurisation du commerce en ligne.

Ceci recouvre plusieurs aspects :

- *la sécurité de l'ensemble de la transaction*, ce qui comprend deux aspects : l'authentification et l'identification. L'authentification, c'est-à-dire l'assurance que les télé-acteurs en « présence » sont bien ce qu'ils prétendent être. C'est notamment le rôle du « certificat », véritable carte d'identité numérique de son détenteur, qui contient notamment la « clé » délivrée par une autorité de certification et signée de la clé privée de celle-ci : il permettra au titulaire de prouver à son interlocuteur que ce certificat lui appartient bien[3]. L'identification : c'est la fonction de signature électronique, qui complète l'authentification, comme la signature d'un chèque. Cette signature électronique est constituée d'un élément réputé n'être connu que du signataire et du système qui le contrôle. Il s'agit généralement d'un mot de passe, d'un code confidentiel voire, pour les alternatives dont on parle régulièrement, d'un attribut dit « biométrique » de la personne (empreinte digitale, iris... et, pourquoi pas un jour, l'ADN ? !) ;
- *la sécurité du processus de paiement*, qui comporte elle-même deux aspects : l'intégrité et la confidentialité. L'intégrité du message, c'est-à-dire l'assurance que les données transmises n'ont pas été altérées entre leur envoi et leur réception : c'est la fonction du « scellement » de la transaction. La confidentialité, c'est la fonction de cryptage, destinée à protéger les informations sensibles contre des piratages en ligne, mais qui vise également à ne communiquer à chaque acteur que les informations qui lui sont nécessaires pour exécuter son engagement. C'est ainsi que le commerçant n'a pas à connaître le numéro de carte de son client, ce numéro étant par contre indispensable pour traiter les processus d'autorisation et de recouvrement de la transaction ; ceci suppose l'intervention d'un intermédiaire entre le marchand et son client, rôle joué le plus souvent actuellement par des Sociétés de services ;
- *l'assurance de bonne fin de la transaction.* Pour l'acheteur, c'est la certitude d'être correctement livré par le commerçant. N'oublions pas que cette crainte figure parmi les tout premiers freins au développement du commerce en ligne. À moins d'avoir eux-mêmes une notoriété et une

image très fortes, les commerçants se doivent de rassurer leurs clients et peuvent recourir à des « relais » ou « intermédiaires de confiance », reconnus des consommateurs : adhésion à la Fevad (Fédération des entreprises de vente à distance), obtention de labels, délivrés par de tels intermédiaires[4]... L'un d'entre eux, FiaNet, a été le premier à franchir une étape de plus dans cette voie, en s'engageant à rembourser tout internaute qui constaterait une fraude sur un site labellisé par lui. D'autres intervenants, principalement la SPB, Société de prévoyance bancaire, sont également sur ce « marché de la confiance »[5]. Pour le commerçant, c'est, bien sûr, la certitude d'être payé, ce qui n'est pas encore le cas même avec le paiement par carte bancaire « classique », puisque, tant qu'il n'a pas réellement « signé » la transaction, le porteur de la carte peut « répudier » la transaction, par simple lettre adressée à sa banque.

En conclusion de ces quelques considérations sur la sécurité, nous voudrions attirer l'attention du lecteur sur le fait que la sécurité a un coût, celui des dispositifs à mettre en œuvre pour prévenir la fraude. Ce coût ne saurait, économiquement parlant, être plus important que le coût de la fraude qu'ils sont censés prévenir et combattre.

Il s'agit donc de concilier la gestion du risque et l'optimisation des coûts, sachant également que le risque lui-même doit s'apprécier en fonction de certains critères, tels que la nature ou le montant de la transaction[6].

Une micro-transaction en ligne ne requiert pas nécessairement les mêmes dispositifs sécuritaires que le règlement d'une transaction en ligne portant sur un ordinateur ou un caméscope.

Un système simple dans sa mise en œuvre et son utilisation

Sur l'existant, les constats sont durs et ne concernent pas seulement les promoteurs de systèmes de paiement en ligne : une étude Retail forward, constate en effet que 35 % des internautes se déclarent frustrés face à des pages Internet trop complexes (trop d'images, trop de publicités, trop d'informations sur une seule page...). À telle enseigne que, selon une analyse de Bizrate.com, 75 % des internautes abandonneraient leur panier lorsqu'ils effectuent un achat *online* pour cause de processus de commande trop long (41 %), ou confus (27 %), (Vividence), ou encore mauvaise « usabilité » des processus de paiement des sites (43 %) (Creativegood).

Selon Forrester, 27 % de la totalité des transactions Internet échoueraient au niveau de la seule page de paiement.

Nous le verrons plus loin, la complexité de chargement de logiciels - les *wallets* - et la multiplication des « clics » pour parfaire une transaction ont été à l'origine de l'échec d'un certain nombre d'initiatives de

processus sécurisés pourtant promus par les plus grands acteurs (Visa, Master Card, Microsoft...).

Un système, sinon universel, du moins suffisamment diffusé

Pour que les acteurs soient incités à l'adopter :
- les commerçants pour attirer de nouveaux clients... ou éviter d'en perdre parce qu'ils ne l'acceptent pas ;
- les internautes, parce qu'ils auront une forte probabilité de pouvoir l'utiliser sur les sites marchands qu'ils fréquentent.

C'est la problématique de l'œuf et de la poule... une problématique qui exige le plus souvent temps et investissements considérables[7].

Cet élément, à lui seul, peut condamner le développement de systèmes techniquement, commercialement et financièrement très prometteurs tels que, nous le verrons plus loin, le paiement sécurisé par carte bancaire sur les téléphones mobiles.

De plus, Internet a introduit une dimension nouvelle, celle de la mondialisation des échanges en ligne auxquels peuvent participer directement les consommateurs, ce qui induit la prise en compte de la possibilité d'opérer des règlements transfrontières même si, en termes de volumes, les transactions domestiques devraient encore longtemps constituer l'essentiel des flux.

Sur ce thème, on pourrait engager un véritable débat philosophico-économique sur les mérites comparés de la création d'une monnaie électronique universelle (certains ont cru en cette sorte « d'esperanto » monétaire) et les tenants d'une organisation de passerelles suffisantes pour assurer l'interopérabilité des systèmes nationaux, schéma sur lequel fonctionnent - à la satisfaction générale - Visa ou Master Card.

En conclusion de cet aspect de l'« universalité » du système, nous voudrions souligner deux aspects :
- l'universalité dont il est question ici concerne essentiellement la diffusion et l'acceptation des systèmes. Elle ne concerne pas nécessairement son utilisation pour tout type de transaction, quel qu'en soit le montant. Il y a en effet une problématique spécifique aux micro-paiements, c'est-à-dire aux règlements dont le montant est disproportionné à leur coût de traitement. On comprendra aisément que le risque encourru - et le coût de sa gestion en termes de processus sécuritaires - soient différents pour une transaction de quelques euros et une transaction de plusieurs centaines d'euros. C'est vrai dans le monde « physique », où les moyens de paiement scripturaux - tels que le chèque ou la carte - sont inadaptés aux micro-paiements, c'est vrai également pour le commerce en ligne, à cette différence près que ce dernier ne supporte pas les règlements en pièces de monnaie ! Les enjeux sont considérables puisqu'ils concernent tout le marché du contenu délivré en ligne, (articles de presse, charge-

ment de musique ou, demain, de vidéo...). Un marché déjà non négligeable estimé à 252 M€ sur l'Europe (dont 30 % pour les jeux en ligne et les informations économiques et financières, et 70 %, nous dit-on, pour les sites de charme..., ce qui rappelle la place du « minitel rose » dans le succès commercial du Minitel !). Un marché qui offre des perspectives considérables avec le développement des services en ligne (tant sur ordinateur que sur les téléphones mobiles et autres PDA) et la généralisation progressive du haut débit. Des solutions spécifiques émergent, nous le verrons plus loin, mais le plus souvent en ordre dispersé et conduisant l'internaute à multiplier ses comptes chez les prestataires dont il utilise les services payants ;

- il serait aussi absurde de prôner « le » système unique que d'espérer que les porteurs accepteront de multiplier leurs façons de payer en ligne, en fonction des systèmes sélectionnés par les sites marchands : ne serait-ce qu'en raison de l'impossibilité de gérer au-delà d'un certain nombre, les identifiants et mots de passe le plus souvent requis pour y accéder...

Les composantes d'un système de paiement

Rappelons que, basiquement, tout paiement met en action quatre acteurs : le payeur (le débiteur), le bénéficiaire (le créancier), et leurs banques respectives, qui gèrent leurs comptes.

De même peut-on déterminer quatre composantes à tout système de paiement :

- *un support*, qui contient les éléments indispensables à la transmission des fonds du débiteur au créancier : ce support peut être physique tel que la carte ou virtuel, les informations étant alors enregistrées sur un support numérique ;
- *un terminal*, qui permettra de transmettre les informations : c'est le terminal de paiement électronique. Dans le monde virtuel, ce sera par exemple l'ordinateur, le téléphone mobile ou tout autre « outil communiquant » permettant d'initier le transfert de fonds ;
- *des infrastructures de traitement des transactions*, ce qu'on appelle généralement le *back office*... ;
- *des infrastructures et des procédures de recouvrement*, c'est-à-dire des circuits permettant de transférer les fonds de la banque du débiteur à la banque du créancier.

Le promoteur d'un système de paiement peut ambitionner de développer et de contrôler lui-même l'ensemble d'un tel dispositif, auquel cas les acteurs sont réduits au nombre de trois, l'émetteur de la carte et l'acquéreur des transactions étant alors confondus : c'est le cas par exemple d'American Express ou, au niveau national, de Cofinoga ou de la carte Aurore.

Par contre, d'autres promoteurs peuvent se regrouper pour offrir à leurs clients une meilleure universalité d'émission et d'acceptation : c'est la démarche qui a présidé en France à la création en 1967 du réseau carte bleue puis en 1984 du réseau des cartes bancaires. C'est cette même démarche qui, au niveau mondial cette fois, a permis la création des deux grands réseaux : Visa et Master Card.

Dans le cas de réseaux de ce type, il faut ajouter aux composantes évoquées ci-dessus des infrastructures communautaires, chargées, principalement, de la définition des normes et règles s'imposant à tous les membres, de la gestion des infrastructures communautaires, de la concertation sur le développement commercial de la marque et de la fonction de juge de paix en cas de conflits entre les membres du réseau.

PANORAMA DES SYSTÈMES DE PAIEMENT EN LIGNE

Que le lecteur se rassure : nous n'avons pas la prétention de lui imposer l'inventaire exhaustif des 150 outils de paiement recensés par l'Epso (l'Observatoire des systèmes de paiement électronique), d'autant que ceux-ci sont peut-être à ce jour 170 ou 180, tant l'actualité nous propose de façon quasi quotidienne de nouveaux projets, dont la plupart sont destinés au cimetière des innovations...

Nous nous limiterons à certaines étapes, en évoquant successivement :

- l'ère des pionniers ;
- l'utilisation des cartes ;
- les plates-formes d'intermédiation ;
- l'utilisation du téléphone mobile, très prometteur.

L'ère des pionniers

Personne ne conteste l'importance de l'événement qu'a constitué l'ère du Minitel dans l'émergence de l'e-commerce et le rôle très significatif qu'il y joue encore aujourd'hui.

Moins connues sont sans doute les tentatives de monnaie numérique : elles n'en méritent pas moins quelques lignes...

L'ère du Minitel

Deux moyens de paiement ont été essentiels dans le développement des services Minitel : le paiement par carte bancaire (CB) et le système kiosque.

Le paiement par carte bancaire CB

Conçue pour le paiement de proximité, la carte bancaire était déjà utilisée, en fait, comme moyen de paiement dans les transactions à

distance (vente par correspondance ou par téléphone) ; c'est donc naturellement qu'elle s'est imposée dans le paiement des transactions commerciales par Minitel.

Toutefois, faute de pouvoir produire une facturette dûment signée, le commerçant était sous la menace, comme dans les autres cas de vente à distance, d'une « répudiation » de la transaction par son client.

Même si le nombre d'incidents est resté relativement limité, on ne peut pas dire qu'un processus consistant à transmettre en clair son numéro de carte et sa date de validité, (éléments suffisants pour générer un paiement) corresponde aux critères d'un paiement sécurisé tels que nous avons tenté de les présenter !

C'est pourquoi l'Adtp (Association pour le développement du télépaiement) a défini des procédures basées sur la sécurité induite de lbhtecknologie de la puce qui se généralisait sur la carte bancaire et qui permet, grâce au contrôle à distance du code confidentiel, une véritable signature de la transaction, authentifiant du même coup l'utilisateur de la carte.

Seul inconvénient, la mise en œuvre de cette procédure supposait d'adjoindre au Minitel un lecteur de carte à puce assurant, en mode local comme sur un terminal de paiement, le contrôle du code. Après une malheureuse tentative de diffusion d'un lecteur à connecter (le Lecam), France Télécom l'a intégré, en 1995, dans le nouveau type de Minitel, le Magis.

Le Service kiosque

C'est à France Télécom que revient le mérite de l'innovation majeure que constitue le Service kiosque : il a largement contribué au développement commercial du réseau Télétel grâce à un modèle économique performant qui a permis la multiplication de l'offre de services télématiques.

Le principe en est à la fois très ingénieux et simple : dans le cadre de ses relations avec les fournisseurs de services télématiques, France Télécom convient du niveau de la tarification d'accès (les « paliers ») à percevoir sur l'utilisateur, ainsi que de la répartition des recettes correspondantes, entre lui-même en qualité d'opérateur, et le fournisseur du service.

L'utilisateur, pour sa part, est chargé sur sa facture téléphonique de sa consommation d'unités téléphoniques, les transactions étant regroupées dans les différents paliers correspondant aux services qu'il a consultés.

Autrement dit, le principe revient à facturer, pour le compte d'un fournisseur, le prix d'un service calculé non pas sur la base d'un tarif intrinsèque, mais en fonction du temps de connexion de l'acheteur du service, dont la durée est forcément variable d'un acheteur à l'autre, ne serait-ce qu'en raison de son habileté à naviguer dans les arborescences

plus ou moins complexes construites par les fournisseurs de services...

Au-delà de la solution apportée au règlement de transactions en ligne (on conçoit qu'un tel système est valable essentiellement pour régler des transactions de faible montant), le Service kiosque est exemplaire de l'importance de l'offre de valeur ajoutée apportée là par France Télécom aux deux acteurs dont il est, en tant qu'opérateur, l'intermédiaire technique :

- à son abonné, il apporte l'avantage d'un système de « relevé de compteur », post payé, multi-prestataires et d'une grande simplicité de fonctionnement et de facturation ;
- au fournisseur de services, il apporte une solution au double problème de la gestion d'une base clients et du recouvrement des créances sur ses clients, services sans lesquels bien des services télématiques n'auraient sans doute jamais vu le jour, faute d'un modèle économique valable[8].

Les tentatives de monnaie numérique

L'ambition de ses promoteurs était de créer *ex nihilo* une nouvelle forme de monnaie, entièrement électronique, dite « numérique ou digitale », constituée de pièces virtuelles, composées de « 0 » et de « 1 », informatiques et stockées au sein d'une mémoire électronique. C'est le substitut électronique de la monnaie fiduciaire dont elle constitue le stade ultime de la dématérialisation et pour laquelle les banques pourraient offrir une parité avec l'argent classique.

DigiCash a sans doute été la tentative la plus célèbre : le cyberbuck fonctionnait sur le même principe que l'argent liquide.

Pour l'utiliser, il fallait ouvrir un compte dans une banque virtuelle et l'alimenter en « vraie » monnaie par une transaction carte « classique ». À partir de son porte-monnaie de cyberbuck, l'acheteur pouvait faire, en ligne, des retraits et obtenir de la monnaie électronique représentée par des « pièces », générées par des algorithmes mathématiques puissants et contenant la somme à transférer, la signature de l'émetteur (la banque virtuelle), l'identifiant du compte client, le tout étant crypté. Chaque « pièce » ne pouvait être générée qu'une seule fois. Cette monnaie digitale, stockée sur le disque dur, pouvait être échangée comme de l'argent liquide.

L'expérimentation des cyberbucks n'a guère dépassé le cadre de la Mark Twain Bank of St Louis (Missouri).

Il en a été de même de la tentative de *cyber-coins* imaginés par CyberCash.

Une valeur sûre : les cartes bancaires[9]

Une étude effectuée en juin 2002 par Ipsos Médiangles auprès de 11 000 internautes visiteurs de sites commerciaux a mis en évidence la

suprématie de l'utilisation des cartes bancaires : 81 % des acheteurs en ligne avaient payé en donnant (peut-être non sans quelque appréhension !), leur numéro de carte bancaire...

C'est un fait, les systèmes opérationnels aujourd'hui utilisent essentiellement les cartes bancaires comme moyen de paiement, y compris, dans certains cas, nous le verrons plus loin, dans les systèmes utilisant le téléphone comme terminal de paiement.

Cette situation n'est pas surprenante si l'on veut bien considérer la grille de lecture que nous avons proposée en première partie.

En effet, les grands réseaux internationaux de cartes comme Visa, Master Card et, à un degré moindre, American Express (qui affiche cependant des ambitions certaines[10] sur le e-commerce), JCB (au Japon) ou Discover (aux États-Unis), représentent :

- un réseau mondial d'émission, au moins pour les premiers cités : sans doute de l'ordre d'un milliard et demi de porteurs. En France, les seules cartes émises par les banques d'obédience du GIE des cartes bancaires ornent le portefeuille de 84 % de nos concitoyens (90 et 91 % pour les tranches de 25-34 et 35-49 ans) ;
- un réseau mondial d'acceptation : près de 15 millions de commerçants dans 300 pays ;
- une image forte de confiance et de notoriété qui dépasse largement l'image propre de chacun des 20 à 25 000 établissements bancaires et financiers qui y participent ;
- des normes communes (Iso, EMV...), permettant une automatisation des processus ;
- des infrastructures incomparables sur le plan technique grâce auxquelles, et contrairement à ce qui se passe avec le chèque, le processus d'autorisation permet un paiement en temps réel, assorti d'une garantie de bonne fin, pour autant qu'en soient respectées les modalités d'utilisation.

Il est non moins vrai que les cartes ont été lancées dans une vision « paiement de proximité » et que ces modalités d'utilisation doivent être adaptées au nouvel environnement que constitue le e-commerce.

Une première étape a été rapidement franchie avec l'adoption du protocole SSL (Secure socket layer), qui utilise la technologie de la cryptographie à clés publique et privée et l'authentification développée par RSA Data Security. Ce protocole de transmission est implémenté et utilisé dans les principaux navigateurs.

La version 2 permet seulement à l'internaute d'authentifier le serveur et de crypter les données sensibles (numéro de carte notamment) envoyées à ce dernier et de contrôler l'intégrité des messages.

C'est à ce processus que la plupart des sites dits « sécurisés » se réfèrent aujourd'hui.

Une version 3 existe et permetttrait d'identifier également l'internaute, pour autant cependant que ce dernier soit muni d'un certificat personnel (et des clés associées), délivré par une autorité de certification compatible avec celle qui a délivré le certificat et les clés correspondantes au marchand.

Deuxième étape, c'est la définition d'un protocole de sécurisation des applications proprement bancaires, le protocole SET (Secure electronic transaction).

Développé conjointement par Visa, MasterCard, GTE, IBM, Microsoft, Netscape, SAIC, TERISA System et Verisign, SET met en œuvre une signature numérique émise par le logiciel du client, c'est-à-dire la signature numérique des données de commande envoyées au commerçant et la signature des données de paiement envoyées à la banque du commerçant : SET permettait ainsi de sécuriser les échanges sur l'Internet et d'authentifier à la fois les commerçants et les porteurs *via* leurs banques respectives.

SET répondait déjà à presque toutes les fonctions sécuritaires attendues d'un système de paiement « sûr », protégeant les internautes contre les commerçants imposteurs et les commerçants contre l'utilisation frauduleuse de numéros de cartes ou le risque de répudiation de la transaction. De plus, cette solution, qui reposait sur l'utilisation de logiciels pouvait être utilisée aussi bien avec des cartes à pistes magnétiques que des cartes à puce, ce qui permettait d'assurer une interopérabilité quasi planétaire, à l'image de l'interopérabilité qui existe entre les cartes à pistes et les cartes à puce en paiement de proximité.

Enfin, SET, protocole développé en collaboration entre les grands réseaux interbancaires de cartes, permettait aux banques de se positionner au cœur de la chaîne de confiance constituée autour de la sécurisation.

Et pourtant, 150 banques seulement, réparties sur 38 pays, s'étaient engagées dans sa mise en œuvre, ce qui était loin de constituer une taille critique suffisante pour espèrer en faire un standard du paiement sécurisé. Autrement dit, SET n'a jamais pu dépasser le stade « pilote ».

Pourquoi cet échec ? C'est sans doute le critère de la « simplicité » qui est en cause : l'un des principaux reproches faits à SET est en effet la complexité (et le coût...) d'implémentation du logiciel chez les internautes et chez les commerçants, dont beaucoup, parmi les principaux acteurs, considèrent encore que l'utilisation de SSL est suffisante dès lors qu'on s'adresse à des marchands connus et ayant pignon sur rue.

Ce qui alourdit également l'utilisation de SET, c'est que tous les contrôles se font en procédure *on line*, notamment le contrôle des certificats utilisés par les acteurs en présence, ce qui induit un allongement des délais de traitement des transactions.

Troisième étape : le « must » de cyber-comm. Forte de sa double

expérience de la carte à puce et du Minitel Magis, la communauté bancaire française avait entrepris d'étendre au paiement en ligne, la sécurisation forte que représente le contrôle du code confidentiel en mode local.

Deux projets avaient ainsi vu le jour, le premier C-Set, sous l'égide du GIE des cartes bancaires, le second, e-Comm, à l'initiative de quelques banques, ces deux projets ayant fini par « converger » dans le projet cyber-comm.

Porté par une vingtaine d'associés de renom[11], le projet reposait à la fois sur la standardisation du protocole SET (on a vu ce qu'il en a été...) et le déploiement de lecteurs de carte à puce.

Sur le papier, cyber-comm avait tout pour séduire : par rapport au protocole classique SET, cyber-comm utilisait en effet la puce pour les procédures d'authentification, d'identification (par le contrôle du code), de scellement et d'archivage, fonctions réalisées en quelques fractions de secondes dans la carte. De plus, l'internaute pouvait s'authentifier et s'identifier à partir de n'importe quel terminal équipé d'un lecteur, alors que dans le protocole SET de base, les éléments d'authentification et d'identification étaient stockés dans le disque dur de son ordinateur.

La question du lecteur (personne ne voulait financer l'investissement initial...) et l'échec du protocole SET ont eu raison des ambitions d'un projet auquel les fabricants de matériels ont cru un moment, si l'on en juge par les annonces faites, par HP ou Compaq en particulier, d'équiper leurs claviers d'un lecteur carte à puce...

Quatrième étape : l'état actuel de la question... Les grands émetteurs de cartes ont repris leur copie et un certain nombre de banques françaises ont décidé de proposer à leurs clients l'e-carte-bleue. Visa et Master Card travaillent désormais chacun sur leur modèle : SPA pour Mater Card et VAP (Visa authentification program) pour ce qui est de Visa. Un accord de « convergence » est cependant acquis aujourd'hui.

Le programme Visa, par exemple, commercialisé sous le vocable « Verified by Visa », repose sur la notion de « 3D » (Three domain model) et la distinction à opérer entre trois domaines : celui de l'émetteur de la carte, celui de l'acquéreur des transactions et enfin celui de l'interopérabilité, passerelle indispensable entre les différents protocoles utilisés sur le marché.

Dans sa version 3D Secure, dont on peut penser qu'elle va s'imposer, le schéma de fonctionnement est relativement simple : le porteur de carte remplit son bon de commande en ligne, indique son numéro de carte bancaire qui sera transmis crypté au site marchand.

Le serveur du marchand se connecte au service Verified by Visa, qui, à partir du numéro de la carte du porteur, est en mesure de lui retourner

l'URL d'authentification de la banque émettrice. Le porteur est ensuite redirigé vers celle-ci afin de s'identifier par les moyens sécuritaires mis en place par sa propre banque (mot de passe, ou tout autre processus agréé).

Enfin, la banque émettrice adresse au commerçant une preuve de l'identité du porteur et la transaction se poursuit ensuite selon les circuits classiques.

Ainsi « avalisée », la transaction ne peut plus être répudiée par le porteur de la carte et la banque émettrice est responsabilisée vis-à-vis du commerçant, qui retrouve la garantie dont il bénéficie pour les transactions « de proximité ».

Rendues obligatoires sur le réseau Visa en avril dernier pour toute transaction effectuée sur Internet en Europe, ces démarches d'authentification seront étendues, à partir du mois d'avril 2003, à toutes les transactions internationales.

Pourtant, à ce jour, très peu de sites marchands utilisent encore le schéma 3D Secure, ce qui laisse planer un doute sur les perspectives réelles de cette nouvelle étape...

L'e-carte-bleue est une carte virtuelle dynamique, processus qui consiste à se faire délivrer, par sa banque, lors d'une connexion sécurisée (aujourd'hui par *login* et mot de passe, demain, pourquoi pas ?, par contrôle du code confidentiel sur un lecteur *ad hoc*...), un numéro aléatoire (*random number*) et spécifique à chaque transaction pour en effectuer le règlement.

Le principal mérite de cette solution, développée par France Télécom, Orbiscom et le Groupement carte bleue, est d'éviter la circulation des coordonnées de la carte « physique » et la constitution, par les commerçants, de fichiers de cartes valides.

Un certain nombre de banques et établissements financiers (notamment Société Générale, Caisse d'Épargne, La Poste, le Crédit Lyonnais...) proposent ce nouveau service (généralement payant) auquel auraient déjà souscrit environ 35 000 de leurs clients.

D'autres banques devraient suivre.

Les plates-formes d'intermédiation

La carte bancaire est, comme nous venons de le voir, le premier moyen de paiement direct sur les réseaux. Mais de nouveaux intermédiaires s'interposent de plus en plus souvent dans la relation entre le client, le marchand, et les moyens de paiement bancaires traditionnels, carte, prélèvement, chèques...

Ces nouveaux acteurs peuvent être classés en quatre grandes familles :
- des FAI (fournisseurs d'accès à l'Internet) tels que AOL, Wanadoo, MSN ou encore Tiscali ;

- des grands portails de services et de commerce P to P (*person to person*) tels que Yahoo ou eBay ;
- des opérateurs cellulaires, Orange, SFR ou Bouygues Télécom en France ;
- des plates-formes indépendantes offrant des solutions de paiement.

Ils offrent trois types de services :
- le service *wallet server* ou « portefeuille » ;
- le service de transfert de fonds, basé sur les e-mails ;
- le PMV (porte-monnaie virtuel) qui concerne principalement les paiements de petit montant et les micro-paiements.

Le « service de portefeuille »

Il consiste à stocker, pour le compte d'un client, l'ensemble de ses données personnelles (numéro de carte ou de compte bancaire, adresses de livraison et de facturation...), et à les transmettre aux sites marchands lors d'une transaction.

Ce service peut être typiquement rempli par tous les sites et opérateurs dont la fonction est d'assurer l'entrée du client sur le réseau.

Deux exemples :

- *Passport*. Le compte Passport de MSN (Microsoft Network) est ouvert en déclarant une ID et un code secret, choisis par le titulaire. Il permet à ce dernier de stocker autant de cartes de crédit ou de débit qu'il le souhaite, assorties chacune d'une adresse de facturation et de livraison qui peuvent être dans chaque cas différentes. Lorsque l'usager visite un site marchand et s'apprête à passer commande, il clique sur l'icône Passport qui ouvre la page d'accueil du site. Il doit alors s'identifier et « signer », puis choisir dans son *wallet* la carte avec laquelle il souhaite effectuer ce paiement. Microsoft se contente de transmettre sous une forme standardisée et une liaison sécurisée les informations nécessaires à l'achat : numéro de carte, adresses de facturation et de livraison. Il est laissé à la discrétion du marchand d'accepter ou de refuser la carte de paiement proposée. C'est l'une des composantes de la nouvelle stratégie Internet dont Bill Gates est personnellement en charge. C'est dire l'importance qu'il y attache, mais aussi les inquiétudes que provoque ce projet auprès des défenseurs du respect de la vie privée des citoyens, à telle enseigne que Microsoft a retiré ce service de son site MSN, de crainte de nouvelles poursuites judiciaires...
- *Yahoo ! Express Achat*. Le principe est identique, à quelques nuances près : Le Yahoo ! *wallet* n'a sélectionné que les cartes des grands réseaux (Visa, Master Card, Discover, American Express) et ne permet d'acheter biens et services que chez les seuls marchands (mais ils sont 10 500...) enregistrés dans le site Yahoo ! Shopping[12].

Il est à souligner que l'on retrouve là, en fait, mais à l'échelle de

systèmes « privés » la même problématique sécuritaire que celle qu'ont à gérer les grands émetteurs de cartes, à l'échelle beaucoup plus complexe de réseaux interbancaires.

Le service transfert de fonds

Le chef de file le plus significatif de ce type de service est sans conteste Paypal, qui est un système de paiement entièrement basé sur Internet et l'e-mail. Il permet d'envoyer de l'argent au destinataire de son choix, pour autant que ce dernier dispose lui-même d'une adresse e-mail. Paypal est avant tout un système destiné au transfert entre particuliers mais son rachat par le géant de la vente aux enchères e-Bay justifie qu'une place lui soit donnée dans ce panorama.

Le fonctionnement en est simple :
- ouverture d'un compte (nom, adresse de domicile et e-mail suffisent) ;
- fourniture d'un numéro de carte bancaire sur laquelle seront débitées les sommes envoyées (plafonnées à 200 $, avec extension possible à 2 000 $) ;
- attribution d'un *login* (l'adresse e-mail et d'un mot de passe) ;
- confirmation de l'ouverture du compte par e-mail de Paypal qui fournit une URL permettant d'accéder au site.

Les procédures utilisent les techniques de sécurisation standard d'Internet et tous les échanges sont cryptés par SSL avec une clé de 128 bits.

Le bénéficiaire est informé par e-mail de Paypal qu'une somme est à sa disposition. Il peut, mais n'y est pas tenu, ouvrir lui-même un compte chez Paypal pour se faire créditer ou demander à recevoir un chèque correspondant.

Enfin, Paypal est aussi opérationnel sur PDA Palm et sur téléphone mobile.

Le porte-monnaie virtuel ou PMV

Il concerne principalement les paiements de petit montant et les micro-paiements qui procèdent d'une problématique particulière : s'agissant en effet de transactions d'un montant parfois de quelques centimes d'euros ou de quelques euros, le coût de traitement à l'unité de telles transactions deviendrait exorbitant par rapport au montant à recouvrer.

La meilleure solution imaginée à ce jour consiste à agréger les petits montants...

Le système bancaire, du fait de sa structure de coûts et de son modèle économique a laissé l'initiative[13] à d'autres acteurs mieux positionnés sur la chaîne transactionnelle pour répondre aux besoins nouveaux liés au marché du téléchargement, dont nous avons déjà souligné qu'il devrait exploser avec la banalisation du haut débit.

C'est une opportunité évidente pour des intermédiaires tels que : opérateurs télécom, FAI ou portails..., qui entretiennent des relations permanentes avec les internautes, d'enrichir leurs services.

Le principe en est simple : l'intermédiaire ouvre un compte, identifié (numéro d'abonné, par exemple) et destiné à enregistrer des flux financiers : de ce fait, son accès doit être sécurisé (généralement par ID et mot de passe) : un processus, somme toute, très classique...

Au-delà de ce principe, deux schémas sont possibles :

- un schéma « prépayé » : le client alimente son compte par tout moyen (y compris par une transaction carte), et les micro-paiements ultérieurs viennent s'imputer au fur et à mesure sur la provision ainsi constituée. C'est le cas, par exemple, du journal *Le Monde*, pour l'achat en ligne d'articles ;
- un schéma « postpayé », dit aussi « relevé des compteurs » dans lequel les micro-paiements sont stockés puis rajoutés à la facture périodique de l'opérateur Télécom, du FAI ou du fournisseur de services. C'est le cas par exemple du service W-Ha, qui s'appuie sur des partenaires fournisseurs d'accès à Internet (Wanadoo, Club-Internet), des journaux (*L'Équipe*...), des opérateurs mobiles (Orange), ou encore des banques en ligne. W-Ha organise avec ses partenaires la facturation de l'utilisateur final et le versement à l'éditeur de son chiffre d'affaires[14 15].

Le paiement sur téléphone mobile : un nouveau venu qui doit faire ses preuves

Transformer les téléphones mobiles en terminaux de paiement pourrait constituer une excellente solution de paiement en ligne, que convoitent d'ailleurs les opérateurs dans leur quête à la valeur ajoutée.

Sur le plan commercial, la densité de la pénétration des mobiles dans la population en fait un instrument particulièrement attractif.

Sur le plan de la sécurité, la carte SIM du téléphone GSM est de même technologie que celle des cartes bancaires et fournit un identifiant fort, capable dans ses dernières versions de gérer plusieurs applications ; enfin le réseau cellulaire fournit d'origine une transmission cryptée.

Ajoutons que les *smart phones* de demain emporteront une puissance de traitement importante, assureront la gestion des données personnelles et permettront de se connecter à des sites d'information et de commerce en ligne, sur lesquels, bien entendu, le problème du paiement se posera.

Bref tous les éléments semblent réunis pour faire des mobiles des candidats valables au titre d'outils de paiement.

Deux alternatives se présentent aujourd'hui : la première consiste à implanter les applications bancaires dans le mobile ; la seconde fait de l'opérateur mobile un intermédiaire de paiement qui exploite son

propre identifiant (les données de la carte SIM) et qui gère des comptes et PMV pour le compte de ses abonnés.

Porter l'application bancaire sur le mobile

Une première voie de développement a consisté à greffer un lecteur de carte bancaire sur le téléphone mobile. La seconde privilégie le portage de l'application bancaire dans une puce du mobile.

Greffer un lecteur de carte : la solution la plus « logique » avait pour ambition d'intégrer un lecteur de carte au dos du téléphone mobile de manière à pouvoir lire en local la carte bancaire.

En France, deux projets pilotes ont vu le jour au cours de l'an 2000 : Movi Plus Paiement développé par les Banques Populaires avec Sagem ; Iti-Achat, ou CB Mobile, projet interbancaire en partenariat avec, notamment France Télécom et Motorola pour la fourniture des terminaux.

L'ergonomie en est simple : le client communique son numéro de téléphone mobile au commerçant qui transmet alors une demande de paiement à la banque. Par SMS, la banque envoie un « ticket » sur le mobile du client et l'invite à introduire sa carte dans le *slot* du terminal, puis à composer son code secret qui est ainsi vérifié en mode local. Un accord est alors transmis à la banque, également sous forme de SMS, et celle-ci transmet alors les messages de confirmation au marchand et au client.

Le système Iti-Achat a également le grand mérite de déconnecter l'acte d'achat du paiement proprement dit, rendant ainsi possible son utilisation dans les différents canaux de vente à distance : centre d'appels de sociétés de vente par correspondance, Minitel ou Internet.

Hormis la France, deux autres régions ont expérimenté les téléphones avec lecteur intégré, la Scandinavie et Singapour. Mais, quel que soit le pays, ces tentatives se sont soldées par un échec dont il est difficile d'analyser les causes. Ce qui est certain, c'est que les opérateurs, pourtant motivés, n'ont jamais reçu le soutien promotionnel nécessaire de la part des banques, auxquelles incombaient les efforts de communication auprès de leurs clients et la constitution d'un réseau de sites d'acceptation digne de ce nom.

Portage de l'application bancaire dans une puce du mobile : c'est l'alternative à la « greffe » d'un lecteur qui peut reposer sur l'insertion de deux puces dans le téléphone ; l'une, la SIM, appartenant au réseau télécom, l'autre, la WIM (Wireless identification module), gérant l'application bancaire : numéro de carte, code secret, vérification locale, clé de cryptage...

Quelques modèles de téléphones dual chip sont en expérimentation en Scandinavie et au Japon. L'une des principales difficultés de ce

modèle est d'ordre juridique et commercial : qui distribue la puce bancaire et l'installe dans le terminal ? Ce doit être logiquement la banque, mais comment gérer plusieurs cartes bancaires différentes ?...

Intégrer l'application bancaire dans la carte SIM

La carte SIM de l'opérateur est - ou sera bientôt - capable d'embarquer et de gérer, avec une sécurité forte, plusieurs applications ainsi que d'interpréter des *applets* Java chargés en ligne. Dès lors, une seule puce pourrait couvrir tous les besoins.

Mais les difficultés commerciales se posent de manière encore plus aiguë que dans le cas précédent. À qui appartient cette puce unique et qui en est responsable ? Par qui serait-elle être distribuée ?

Comment organiser la collaboration avec le système bancaire... ou avec les autres opérateurs ? !

Coopération ou compétition ? !

Bien sûr, il ne nous appartient pas, dans le cadre de cette présentation, de répondre à ces questions...

Au terme de cet aperçu, nous avons conscience que nous aurions sans doute pu évoquer quantité d'autres systèmes... Par exemple, les cartes prépayées anonymes que l'on gratte comme un TacoTac (l'eroticard) (sic) d'easyCode ou le Ticket Surf, dernière née de France Télécom... Ou encore MobilPago, fruit du partenariat entre une banque et un opérateur télécom, partis à la conquête du monde, comme un certain héros de la littérature espagnole...

Cela étant, nous espérons avoir mis en évidence qu'il existe aujourd'hui des moyens relativement sérieux de pratiquer l'e-commerce, même si l'on décèle encore beaucoup de tâtonnements de la part de leurs promoteurs.

Nous retiendrons également que, sans une volonté politique forte des acteurs, les critères purement techniques sont insuffisants pour faire émerger les solutions standard de demain.

Enfin, l'e-business favorise incontestablement la montée d'autres acteurs que les banques, dont l'émission et la gestion des moyens de paiement sont l'une des fonctions fondatrices. Mais celles-ci disposent cependant d'atouts importants pour résister au risque de désintermédiation qui pèse sur elles, en particulier au travers de leur participation aux réseaux internationaux Visa et Master Card.

Internet s'infiltre dans l'ensemble du tissu économique.

Cet extraordinaire phénomène de société, né des possibilités offertes par la technologie, ne fait sans doute que commencer et les progrès qui se réalisent chaque jour sous nos yeux (haut débit, convergence TV/ Internet, UMTS...) continueront à ouvrir de nouveaux marchés à de nouveaux produits.

Ce ne sont certes pas les systèmes de paiement qui vont les créer. Par contre, ceux-ci devront les accompagner et apporter aux acteurs les processus qui permettront, en toute sécurité, de « parachever » toute transaction commerciale par sa bonne fin financière.

Ouverte au quatrième millénaire avant Jésus-Christ , l'histoire de la monnaie et de la banque continue...

NOTES

1 À ce chiffre il conviendrait toutefois d'ajouter le poids du chiffre d'affaires encore réalisé par les 25 000 services Minitel, dont le caractère « ringard » dénoncé par certains ne saurait faire oublier son rôle de pionnier dans le développement du commerce en ligne.

2. Le Gbde a également relevé : la lutte contre la cyber-criminalité, la réduction du fossé numérique, la résolution de l'épineux problème de la fiscalité, la protection de la propriété et intellectuelle et enfin le développement de l'administration électronique, dans la mesure où il appartient aux gouvernements de donner l'exemple pour le développement de l'e-business.

3. L'utilisation de certificat est aujourd'hui, dans les faits, limitée à la certification des commerçants et des plates-formes commerciales qui veulent faire du paiement sécurisé : la clé publique qu'il contient est en effet indispensable à la mise en œuvre des protocoles de type SSL permettant également le scellement et le cryptage.

4. Quelques exemples :
- Labelsite, promu par la Fevad et la FCD (Fédération du commerce et de la distribution) ;
- Web trust, véritable sceau de l'Ordre des experts comptables et commissaires aux comptes, délivré après audit et faisant l'objet d'un contrôle régulier ;
- Web Trader, label délivré, également après audit, par la Confédération de la consommation, du logement et du cadre de vie ;
- Fia-Net va plus loin en proposant de rembourser 50 000 F à tout internaute qui constaterait une fraude sur un site labellisé par Fia-Net ;
- Labels que constitue aussi, pour un site, son hébergement par une référence « de confiance » : France Télécom, pour les sites de Télécommerce, BNP Paribas pour les sites hébergés par Mercanet, ou la Société générale, pour les sites hébergés par Sogennactif. Ce dernier exemple montre que les banques s'essaient timidement à mettre en jeu le capital confiance dont elles bénéficient généralement.

5. On notera, au passage, que la possibilité de proposer une telle assurance suppose un niveau de risque « acceptable », sinon son coût, lui, apparaitraît vite inacceptable !

6. C'est pourquoi, par exemple, l'utilisation de la fonction porte monnaie électronique Monéo ne requiert pas le contrôle du code, qui alourdirait le processus de paiement.

7. On dit que les promoteurs de la carte bleue avaient eux-mêmes failli renoncer à l'aventure après quelques années décevantes et coûteuses !!

8. En téléphonie mobile, les prochaines générations (GPRS et l'UMTS) permettront de nouvelles applications de ce type de solution en passant d' une facturation au temps de connexion à une facturation au nombre d'octets transmis.

9. Le terme de cartes bancaires est pris ici dans son appellation générique et ne concerne pas seulement les cartes bancaires CB, soumises à l'autorité du GIE des cartes bancaires CB.

10. American Express Travel Group estime « d'ici quatre ans, Internet représentera 50 % de notre chiffre d'affaires dans le monde ».

11. Les principales banques françaises, des groupements comme Visa, Carte Bleue, Cartes Bancaires, des industriels comme Alcatel, Bull, Gemplus, Oberthur...

12. Les deux systèmes reposent sur l'utilisation d'une « adresse », constituée par l'adresse e-mail ou un numéro d'abonné, et d'un code secret (8 caractères chez Passport), baptisé Security Key chez Yahoo !

13. Il convient tout d'abord de ne pas confondre le PMV dont il est ici question, et le PME ou porte-monnaie électronique Monéo support « physique » dont l'usage est en cours de généralisation en France dans le cadre des petits paiements de proximité (Parkings, automates, ...).

14. Il n'y a pas, en fait, de paiement en ligne, puisque le paiement est reporté à l'envoi de la facture périodique, mais ce cas de figure n'en méritait pas moins d'être évoqué ici. Il résulte d'un sondage récent effectué par Le Journal du Net que près de 11 % des internautes sont conquis par la formule.

15. ... mais près de 45 % préfèrent la carte bancaire, y compris pour des applications de petit montant...