

Extrait de

Internet, guide stratégique et pratique
pour l'entreprise

par

Jean Haguet

© Reproduit avec la permission des éditions
Masson,

Paris, juin 1996, 352 pp

Les transactions

Parallèlement aux problèmes de sécurité, l'Internet représente un défi pour les transactions commerciales en ligne. Aujourd'hui, le réseau sert surtout de support de promotion et de publicité. Les clients, une fois ferrés, commandent les produits en passant par les circuits habituels. La majorité des serveurs commerciaux s'en tiennent encore à cette approche. Mais tout l'intérêt de l'Internet est de permettre la réalisation de transactions en ligne, effectuées de bout en bout sur le réseau, c'est-à-dire instantanées et automatisées. Ce défi s'organise sur trois fronts :

- Si le réseau n'est pas sûr, comment garantir la confidentialité des transactions ?
- Comment clients et marchands peuvent-ils s'authentifier mutuellement ?
- Et comment intégrer ces nouvelles formes de transactions dans la gestion de l'entreprise ?

Vous serez probablement surpris par le nombre et la variété des systèmes déjà proposés pour résoudre ces difficultés. Trois modèles se dégagent. L'argent électronique prend la forme de codes uniques chiffrés et passe d'un disque dur à un autre via l'Internet. Le second modèle s'appuie sur une liaison directe entre le client et le marchand. Le troisième tente d'éviter la transmission de données sensibles à travers le réseau en proposant une intermédiation.

Les différents modèles font face aux contraintes qui caractérisent les réseaux ouverts comme l'Internet. Il convient de les identifier dans un premier temps. Puis nous décrirons les divers systèmes de paiement mis au point à ce jour, en les classant par modèle. Les termes techniques sont définis dans le glossaire (annexe 6).

15.1. LE COMMERCE ELECTRONIQUE SUR RESEAUX OUVERTS

On distingue cinq contraintes essentielles: doser le neuf et l'ancien; intégrer les transactions au système bancaire; assurer l'intermédiation; chiffrer et authentifier; gérer les transactions en ligne. Nous allons les passer en revue l'une après l'autre.

15.1.1. Doser le neuf et l'ancien

L'Internet contribuera sans doute à révolutionner la pratique du commerce – au moins sur le long terme. Toutefois, cette révolution sera plus lente que certains éditoriaux le claironnent. En outre, le commerce obéit à des constantes. La caractéristique première des transactions sur l'Internet est donc un mélange de neuf et d'ancien. Pour déterminer où doit passer la ligne de front, il faut réfléchir en deux temps :

- Quelles procédures se rapprochent de celles du monde réel? Et comment opérer ce rapprochement ?
- Quelles procédures constituent une nouveauté ? Dans ce cas, comment les maîtriser ?

L'Internet crée un risque nouveau: les transactions en ligne, effectuées uniquement sous forme électronique, peuvent ne laisser aucune trace. Des marchands mal intentionnés seront tentés d'échapper à la fiscalité ou à la réglementation de leur lieu d'implantation, de même qu'aux contrôles douaniers ou administratifs. Ils essaieront aussi de frauder en utilisant de fausses identités ou adresses, voire des moyens de paiement volés (des numéros de cartes bancaires notamment).

Il est donc souhaitable que les contrôles étatiques normaux s'appliquent aux transactions. Car la condition sine qua non du développement du commerce sur l'Internet est la confiance: marchands et clients ne participeront pas à ce nouveau marché s'ils ne sont pas protégés des abus. Par conséquent, les systèmes de paiement doivent intégrer un certain nombre de services permettant d'exercer ces contrôles: par exemple, des tickets horodatés établissant la preuve qu'une transaction a eu lieu, ou un système d'authentification des acteurs de la transaction. Les structures de contrôle existantes devront faire face au nouveau défi lancé par l'Internet; pour le relever, des moyens inédits sont requis.

Pour autant, les contrôles ne doivent pas être un obstacle au développement du commerce électronique sur l'Internet. La réglementation actuelle doit faire preuve de suffisamment de souplesse pour accepter dès aujourd'hui ces transactions. Par ailleurs, réglementer immédiatement ce nouveau marché partout où l'on croit déceler des brèches potentielles serait une erreur: il convient d'abord d'observer l'évolution du secteur avant de le tuer dans l'œuf. C'est l'attitude que les autorités américaines ont adoptée. Toutefois, des auditions d'experts ont déjà eu lieu au Congrès afin d'identifier les faiblesses de l'Internet et de se tenir prêt à intervenir rapidement. Les lois actuelles peuvent suffire en attendant éventuellement de nouvelles.

L'Internet s'appuie en outre sur les circuits de distribution actuels pour les biens «physiques». Personne n'a encore trouvé le moyen de faire passer du vin ou des voitures à travers les «tuyaux» du réseau: il faut encore s'adresser à un détaillant ou à un concessionnaire, même s'ils se trouvent à quelques milliers de kilomètres. Les produits sont ensuite livrés de manière traditionnelle. Seule la communication et le paiement auront lieu sur l'Internet. En revanche, l'Internet constitue

en lui-même un réseau de distribution pour les produits numérisables (informations, logiciels, livres, vidéos, services, documents spécialisés, etc.). Selon la nature des produits, les circuits de distribution prendront donc des formes connues et d'autres nouvelles.

Sur le plan de la sécurité, tout peut se passer en ligne jusqu'au moment de communiquer les informations sensibles (le numéro de carte bancaire par exemple). On peut ensuite envisager de recourir aux moyens de communication traditionnels: téléphone, fax, courrier postal. Certaines entreprises américaines demandent même aux clients désirant utiliser le courrier électronique d'envoyer deux messages distincts: l'un contenant le numéro de la carte, l'autre la date d'expiration. Ainsi, les programmes de sniffing¹ sont trompés et n'interceptent pas les messages. Et si seulement un des deux messages est capté, l'information n'est pas utilisable. Cela suppose bien sûr pour l'entreprise une gestion des messages électroniques afin de rapprocher les deux informations.

Pour effectuer les transactions en ligne de bout en bout, les données sensibles sont souvent chiffrées. La cryptographie asymétrique, grâce aux signatures électroniques, sert également à authentifier les acteurs de la transaction et à assurer l'intégrité et la non-répudiabilité des messages transmis. Ces moyens, ou tout au moins leur utilisation massive, constituent une nouveauté dans la sphère commerciale.

Enfin, qui dit transaction dit paiement. L'Internet voit certes apparaître de nouveaux intervenants proposant des services spécifiques (certification de la transaction, clearing, authentification mutuelle du client et du marchand, fourniture des relevés de compte, intégration de l'EDI, etc.). Mais pour le paiement proprement dit, le réseau doit s'appuyer sur le système bancaire.

15.1.2. Intégrer les transactions au système bancaire

Contrairement à ce que l'on pourrait croire, l'Internet représente plus une chance qu'une menace pour les banques et les institutions financières en général. Pour commencer, rares sont les apôtres des transactions en ligne sur l'Internet qui ont jamais eu l'intention de développer un système parallèle à celui des banques. Même Digicash, chantre de l'argent électronique, n'a pas l'intention d'émettre lui-même cet argent. Il souhaite vendre la licence de son système aux banques.

Ceci s'explique par une exigence primordiale: la confiance. Les transactions sur l'Internet, pour se développer, doivent inspirer confiance à la fois aux clients et aux marchands. Or, ils auront tendance à se méfier d'acteurs nouveaux, venus de nulle part, qui leur proposent de prendre leur numéro de carte bancaire ou toute autre information sensible. Si entreprises et consommateurs savent que des banques connues garantissent la

¹Action d'intercepter des données en transit sur l'Internet. Le pirate poste un programme qui repère certains types d'informations et les capture systématiquement.

validité d'un système de paiement, ils seront plus enclins à vendre ou acheter sur le réseau. Le critère géographique a d'ailleurs son importance: la confiance sera d'autant plus grande que les banques seront connues, donc bien implantée localement. La virtualité a ses limites!

En outre, il coûterait trop cher de créer de nouvelles structures. Il est bien plus simple et confortable pour les galeries commerciales virtuelles de s'appuyer sur le système bancaire en place. Les banques peuvent d'ailleurs apporter leur propre clientèle, qu'elles ont constitué au prix de longs efforts. Les aspects réglementaires et légaux créent une motivation supplémentaire. Les banques savent traiter les problèmes administratifs ou les contentieux. Elles savent aussi gérer les risques commerciaux (recouvrement, assurances, etc.). En outre, elles permettent d'assurer le risque financier induit par l'utilisation des cartes bancaires (fraudes, vols). Il est possible que ce risque soit plus important aujourd'hui avec l'Internet qu'avec la transmission de numéros de carte bancaire par téléphone. Mais la perception de ce risque est aujourd'hui plus importante que la réalité: le réseau doit encore inspirer confiance au plus grand nombre.

Enfin, pour une bonne part, les transactions en ligne sur l'Internet reposent sur les cartes bancaires et les cartes de crédit donc, par définition, sur le système bancaire. Cela est vrai pour les systèmes fondés sur la transmission du numéro de carte bancaire mais aussi pour ceux passant par des portemonnaies électroniques. Quel meilleur partenaire, dans ce cas, qu'une banque? Visa et Mastercard, avec Microsoft, ont d'ailleurs mis au point un système de paiement sur l'Internet qui insiste particulièrement sur l'intégration au réseau bancaire.

Les banques doivent fournir un effort d'innovation pour mettre au moins un système de paiement, pour intégrer l'Internet dans leur dispositif de clearing ou pour passer de nouvelles alliances avec les partenaires connaissant bien le réseau. Cela exige, au départ, qu'elles prennent l'Internet au sérieux. Nous espérons que ce livre les y incitera. L'Internet est au moins un laboratoire de la société d'information du futur. Il nous semble qu'elles ne peuvent pas se permettre, à plus ou moins longue échéance, de l'ignorer.

15.1.3. Assurer l'intermédiation

L'intermédiation consiste à se placer entre le client, le marchand et le système bancaire pour faciliter la transaction. Ce rôle caractérise les systèmes du troisième modèle. Il peut être joué par une société spécialisée ou par une banque. Mais il faut avouer que les banques sont au mieux des partenaires dans les systèmes proposés à ce jour.

Les sociétés d'intermédiation sont souvent de nouveaux acteurs sur le marché, alliés à une ou plusieurs banques (par exemple Globe ID et la Compagnie bancaire). Elles apportent principalement deux choses: des services et des technologies. Les services intègrent plus ou moins de valeur ajoutée:

- authentification des acteurs,
- confirmation de la transaction,

- certification de l'acte,
- traitement de l'opération, clearing,
- redistribution des bénéfices (rétribution),
- gestion de porte-monnaies électroniques,
- fourniture de relevés de compte,
- archivage.

D'autre part, les sociétés d'intermédiation offrent parfois des logiciels ad hoc: logiciels clients pour les consommateurs, logiciels serveurs pour les marchands. Les premiers sont toujours gratuits, les seconds sont souvent payants. Elles proposent également des programmes de chiffrement, intégrés aux logiciels ou aux services qu'elles fournissent. Et les relevés de compte peuvent être transmis aux marchands par EDI. Ces technologies sont malgré tout moins cruciales que les services spécialisés offerts par les sociétés d'intermédiation. Un système comme celui de First Virtual ne repose sur aucune technologie particulière; il s'agit simplement d'une orchestration astucieuse des événements composant la transaction. Globe ID apporte juste ce qu'il faut de technologie en plus pour être meilleur; notamment pour permettre la réalisation des transactions en temps réel (voir plus bas).

15.1.4. Chiffrer et authentifier

Les transactions en ligne sur l'Internet recourent au chiffrement et aux procédés d'authentification. Les logiciels de chiffrement utilisent la plupart du temps la technologie RSA (voir chapitre 14), éventuellement combinée avec la cryptographie traditionnelle. Beaucoup voient dans le chiffrement le moyen de transmettre en toute sécurité les numéros de carte bancaire. Toutefois, les systèmes de paiement les plus en vue (Cybercash, First Virtual, Globe ID) refusent de transmettre ces informations trop sensibles à travers le réseau, chiffrées ou non. Open Market, Cybercash et Globe ID le proposent pour l'ouverture du «compte» mais ce n'est qu'une option. Ensuite, ne sont chiffrés, selon les systèmes, que les mots de passe, les identifiants ou autres ordres de paiement. First Virtual n'utilise pas la cryptographie.

Les normes S-HTTP et SSL (Secure Web) et le système Netcash (pour l'achat de coupons) exigent en revanche la transmission du numéro de carte bancaire au moment de l'achat. Par définition, les procédés d'argent électronique reposent sur la cryptographie. Les codes uniques qui représentent des unités monétaires peuvent être volés comme des billets de banques normaux. Ils doivent donc être protégés lors de leur transfert. Nous traitons la cryptographie dans le chapitre 14.

L'authentification mutuelle des clients et des marchands peut s'appuyer sur les signatures électroniques créées grâce à la cryptographie asymétrique. Mais des procédés plus classiques permettent aussi d'authentifier les acteurs de la transaction. First Virtual utilise le courrier électronique pour demander des messages de confirmation aux clients et aux marchands, ainsi que des identifiants spécifiques.

Avec les signatures électroniques, le chiffrement a tout de même l'avantage d'assurer l'intégrité des données transmises. De cette manière, il est impossible de les modifier lorsqu'elles sont interceptées par des pirates, à moins d'invalider les signatures électroniques. De plus, l'émetteur de ces données ne peut pas modifier le contenu d'un message qu'il a envoyé, ni répudier ce message (nier qu'il en est l'auteur). Nous avons décrit les signatures électroniques dans le chapitre 13.

La plupart des systèmes de transaction ont le souci de rendre les procédures de chiffrement transparentes, pour les clients comme pour les marchands. Il ne faut pas compter voir le grand public et toutes les entreprises se verser dans les détails du fonctionnement de la cryptographie. Avec Globe ID par exemple, les clients entrent des informations dans les champs d'un questionnaire interactif, puis le logiciel fait le reste.

15.1.5. Gérer les transactions en ligne

Les procédures doivent non seulement être transparentes, il faut aussi – idéalement – qu'elles soient automatisées. La vitesse de traitement est essentielle car les clients aiment

que tout soit réglé tout de suite. Lorsque les transactions en ligne n'assurent pas l'immédiateté, elles perdent beaucoup de leur intérêt. En automatisant le processus, le système de paiement donne au client l'impression qu'il effectue un achat instantané, comme dans un magasin traditionnel. Ceci est d'autant plus vrai pour les produits numérisables, livrables instantanément.

Certains systèmes de paiement offrent aussi des services de gestion. Les marchands peuvent ainsi déléguer l'enregistrement et l'archivage de toutes les transactions. Les sociétés d'intermédiation sont à même de présenter des preuves de paiement ou des relevés de compte. Elles peuvent aussi intégrer directement les transactions dans le système comptable des marchands grâce à l'EDI. C'est la solution choisie par Globe ID. On peut même envisager des transactions reposant sur des paiements différés et conditionnés par une confirmation. En effet, il arrive parfois que des transactions ne soient conclues qu'après un certain délai. Par exemple, un client réservant un billet d'avion donnera ses coordonnées bancaires au voyageur; mais celui-ci ne débitera le montant que s'il a pu obtenir les conditions désirées et si le client approuve cette transaction. Dans ce cas, le système de paiement devra garder pendant ce délai la preuve de la commande du client et obtenir les confirmations nécessaires du client et du voyageur. La transaction sera réalisée lorsque les confirmations seront apportées.

Partant des cinq contraintes que nous venons de décrire, plusieurs modèles de transaction sur l'Internet ont été proposés. Nous avons dessiné des schémas qui, pour chaque modèle, situent les différents acteurs et résument les différentes étapes de la transaction. Ces schémas sont conçus pour pouvoir être superposés afin de faciliter les comparaisons. Notez que les liens ou flèches en **gras** indiquent la transmission sur l'Internet d'un numéro de carte bancaire chiffré. Mais il ne s'agit souvent que d'une option: le téléphone, le fax ou le courrier sont des alternatives possibles. Nous le préciserons pour chaque modèle.

15.2. L'ARGENT ELECTRONIQUE

Dans le monde réel, il existe de nombreux moyens de paiement: liquide, chèques, virements et prélèvements bancaires, cartes de débit, cartes de crédit², travelers' cheques, etc. Il en sera de même dans le cyberspace. Parmi les moyens de paiement envisagés pour les réseaux, le plus révolutionnaire est probablement l'argent électronique.

15.2.1. Simple, pas cher, anonyme

²Les Américains ne parlent que de cartes de crédit car les cartes de débit sont peu répandues aux Etats-Unis. Néanmoins, les cartes bancaires françaises Visa, Mastercard ou autre (qui sont des cartes de débit, différé ou non) sont tout à fait utilisables sur l'Internet.

L'argent électronique (ecash) se veut aussi simple à utiliser que de la monnaie. Il se présente sous la forme d'une série unique de nombres validée par une banque, pour laquelle une valeur monétaire est donnée. La plupart des systèmes d'argent électronique sont fondés sur des pièces (coins), dont la dénomination (valeur) varie. Chaque série de nombres représente une pièce de monnaie et porte un numéro de série qui la rend unique. Les pièces sont stockées sur le disque dur du client, voire sur une carte à puce. Les numéros de série sont stockés sur une banque de données accessible à toutes les banques.

Pour acheter, le client transfère les pièces à travers le réseau vers l'ordinateur du marchand. Les données correspondantes sont évidemment chiffrées. Elles sont en outre authentifiées par la signature électronique de la banque du client. Les banques sont en effet seules habilitées à émettre de l'argent électronique aux titulaires de comptes classiques. Les banques décident d'adopter ou non l'argent électronique. Dans le cas favorable, elles doivent mettre en place un système d'émission et d'encaissement. Ce système, qui repose sur un logiciel spécifique, s'intègre complètement à leurs opérations habituelles. L'argent électronique n'est qu'un moyen de paiement de plus.

On peut envoyer de l'argent électronique à un marchand, comme à n'importe quel utilisateur privé. Cet utilisateur peut ensuite dépenser cet argent à son tour ou le déposer sur son compte en banque. Toutefois, les pièces ne sont utilisables qu'une seule fois. Si Pierre donne de l'argent électronique à Paul, celui-ci ne peut pas le donner à Marie sans passer par sa banque: la banque de Paul lui donnera de nouvelles pièces avant qu'il puisse les envoyer à Marie. Par ailleurs, l'argent électronique fait de tous les utilisateurs des marchands potentiels: n'importe qui peut vendre sa production littéraire ou ses services de consultant, avec un minimum de moyens et pour un coût très bas.

La circulation de l'argent électronique est réglée par des logiciels ad hoc. Les procédures sont transparentes aux yeux des consommateurs et des marchands. Cela confère à l'argent électronique une grande simplicité d'utilisation. De plus, cela évite la transmission de numéros de carte bancaire sur le réseau. Grâce à l'automatisation, permise par les logiciels, et au nombre réduit d'opérations pour chaque transaction, le coût de l'argent électronique est très faible. Il est donc tout à fait indiqué pour les petits montants, de quelques centimes à quelques centaines de francs. On peut même envisager à terme de régler des montants infinitésimaux (une fraction de centime). L'argent électronique se prête donc particulièrement bien à la vente d'informations - à la page ou, si besoin est, au paragraphe.

Surtout, l'argent électronique est potentiellement anonyme. Digicash a mis au point une solution cryptographique permettant de générer des «signatures aveugles» (blind signatures): les banques fournissent des pièces à un client sans être capable par la suite de «remonter» au client (voir plus bas).

15.2.2. Une solution controversée

L'argent électronique est encore controversé. Pour beaucoup, c'est irréaliste et dangereux; pour ses partisans, c'est le moyen de paiement de l'avenir, un aboutissement inévitable. L'argent électronique est au moins un cas d'école fort intéressant car il pose la question de l'anonymat dans les transactions électroniques en général. Contrairement au métal et au papier, les bits ont la particularité d'être facilement copiables, à la perfection et à l'infini. Potentiellement, ils laissent des traces partout où ils passent. Si l'argent électronique se généralise, n'importe qui (votre voisin, votre concurrent, le fisc, des malfrats) pourra faire ce que la loi Informatique et Libertés interdit: espionner votre vie privée, dresser votre profil de consommation afin de lancer des mailings systématiques, etc.

Mais les détracteurs de l'argent électronique anonyme y voient une menace pour l'ordre public. Ils craignent que les criminels s'en servent pour transférer anonymement des fonds, faire du marché noir, blanchir de l'argent ou échapper au fisc. Dans le cas de Digicash, le payeur est anonyme mais le bénéficiaire ne l'est pas puisqu'il doit impérativement passer par une banque pour déposer ou re-dépenser l'argent. L'évasion fiscale est donc impossible. Et le marché noir ne pourrait en profiter qu'avec la complicité d'une banque. D'autre part, les clients qui le désirent peuvent apporter la preuve de leurs paiements. Les criminels qui accepteraient de l'argent électronique seraient identifiables avec l'aide rétrospective d'un de leurs clients, affirme Digicash.

L'argent électronique est vu par les banques avec une certaine méfiance. La technologie risquerait de remettre en cause leur position: une nouvelle société pourrait distribuer de l'argent électronique et créer ainsi de la monnaie. Digicash a beau affirmer ne pas vouloir émettre de l'argent électronique et laisser ce rôle aux banques, d'autres entreprises pourraient en décider autrement. Les banques craignent également les conséquences de l'anonymat (pourtant, aucun lien n'est établi aujourd'hui entre un billet de banque retiré au guichet et l'identité du client). Enfin, le cadre réglementaire autour de l'argent électronique n'est pas encore définie. Banques centrales et gouvernements commencent juste à se pencher sur la question. Une nouvelle législation serait peut-être nécessaire avant l'émission du premier cyberfranc. Une phase expérimentale permettrait sans doute de mieux maîtriser les enjeux de l'argent électronique. Pour beaucoup, celui-ci ne verra donc pas le jour avant longtemps.

Dans ce débat, il faut avouer que l'argent électronique déploie des charmes irrésistibles. Certes, de nombreuses questions restent sans réponse. Mais l'argent électronique se prête trop bien aux transactions en ligne: ça doit marcher un jour.

15.2.3. Digicash

Digicash est une entreprise américaine fondée par David Chaum, un spécialiste de cryptographie. Son centre d'opération est à Amsterdam, grâce à une filiale néerlandaise. La protection de la vie privée est le credo de Chaum. Il estime que l'argent électronique exige un choix de société pour le XXI^e siècle,

entre «(...) d'un côté, une surveillance et un contrôle sans précédent sur la vie des hommes; de l'autre, l'assurance de la parité entre les individus et les organisations». Ce choix «ne peut être fait qu'une seule fois», ajoute Chaum. Sa crainte est de voir les organisations de toutes sortes (entreprises, administrations, gouvernements, etc.) profiter de la «traçabilité» des moyens de paiement électroniques pour s'immiscer systématiquement dans la vie quotidienne des citoyens.

Son but n'est pas de créer la monnaie idéale des criminels ou de l'économie souterraine, mais simplement de fournir aux consommateurs un moyen de paiement électronique élégant et aussi confidentiel que les billets de banque. Chaum a découvert un moyen mathématique de préserver l'anonymat des détenteurs d'argent électronique, pour autant que l'on ne cherche pas à forcer les gens à décliner leur identité. Sa méthode permet également de prouver mathématiquement ce principe. En d'autres termes, son système permet d'assurer aux détenteurs d'argent électronique que les banques ne peuvent pas remonter à eux, à moins qu'ils acceptent eux-mêmes de se faire connaître. Cependant, l'argent électronique resterait contrôlé par les banques et s'intégrerait dans les circuits économiques en toute légalité. D'ailleurs, l'ambition de Chaum est de vendre aux banques des licences de son système (il détient les brevets indispensables au système Digicash). Il ne cherche pas à se substituer aux banques en devenant à son tour un émetteur de monnaie, bien qu'il en soit techniquement capable.

L'argent électronique de Digicash utilise des pièces et fait participer les trois acteurs habituels (clients, marchands et banques). Ceux-ci doivent disposer des logiciels adéquats et se tenir prêt à accepter cette forme de paiement. Digicash utilise la technologie RSA pour le chiffrement. Tous les acteurs de la transaction possède une et une seule paire de clés. Le logiciel gère les pièces que Pierre possède sur son disque dur. Lorsque Pierre veut retirer de l'argent électronique de son compte bancaire, son logiciel Digicash envoie à sa banque un code (un nombre choisi au hasard) qui constitue une sorte de pièce «vierge» (blank coin). Le code est caché dans une «enveloppe» digitale. La banque vérifie d'abord que le compte de Pierre est créditeur. Puis elle décide d'apposer sa signature électronique non pas sur la pièce directement mais sur l'enveloppe. De cette manière, la banque ne peut pas lire le code à l'intérieur. L'enveloppe agit un peu comme du carbone et la signature de la banque s'applique sur la pièce.

Cette signature aveugle confère à la pièce sa valeur monétaire, garantie par la banque. Celle-ci débite alors le compte de Pierre. Lorsque Pierre reçoit l'argent électronique, son logiciel retire l'enveloppe. Pierre est le seul à pouvoir l'enlever. Le fait de retirer cette enveloppe n'altère pas la signature électronique de la banque. Pierre a désormais dans son porte-monnaie de l'argent anonyme. En cas de perte (provoquée par un problème informatique par exemple), les pièces sont remboursables à l'instar des travelers' cheques.

La figure 15.1 montre la simplicité de l'acte d'achat. Lorsque Pierre veut acheter un produit, il l'indique au serveur du marchand qui lui adresse une demande de paiement. En cliquant sur un bouton de l'interface Digicash (une petite fenêtre restée ouverte dans un coin de son écran), Pierre transfère les

pièces correspondant au montant. Le logiciel Digicash de Pierre crée une combinaison de pièces pour former le montant exact. Le logiciel du marchand se connecte alors à la banque, qui vérifie: (1) que les pièces sont valables, (2) que ces pièces n'ont jamais été compensées auparavant par une banque. Si quelqu'un tentait d'utiliser la même pièce une deuxième fois, son identité serait révélée. Les pièces une fois acceptées, le marchand choisit de les garder dans son porte-monnaie ou de les déposer sur son compte bancaire.

L'opération est la même pour les transferts de particulier à particulier. On peut d'ailleurs envoyer de l'argent électronique par e-mail. A chaque fois, une vérification par la banque est effectuée - ce qui le différencie de l'argent liquide. Du point de vue de la banque, l'argent électronique ne ressemble pas tout à fait à du liquide non plus. Quand Pierre retire des billets de banque, ils sont aussitôt débités de son compte. Lorsqu'il prend de l'argent électronique, ce dernier est inscrit au passif de la banque. Il retourne à l'actif au moment où il est déposé.

Digicash a d'abord lancé un essai grandeur nature en octobre 1994. Un million de Cyberbucks furent émis par Digicash, qui pour l'occasion jouait le rôle d'une banque. Plus de la moitié avait été retiré en septembre 1995. Cette unité monétaire fictive ne pouvait pas être échangée contre des devises existantes mais elle permettait tout de même d'acheter de réels produits auprès des quelque 70 commerçants qui les acceptaient. Chaque volontaire recevait 100 Cyberbucks sur son compte «bancaire». Il pouvait les stocker dans son porte-monnaie grâce au logiciel fourni gratuitement en téléchargement.

Depuis le 23 octobre 1995, de l'argent électronique Digicash est émis par une banque américaine de Saint-Louis, Mark Twain Bancshares. Dans un premier temps, la banque a plafonné les dépôts d'argent électronique à 200 dollars. Le système fonctionne comme décrit ci-dessus.

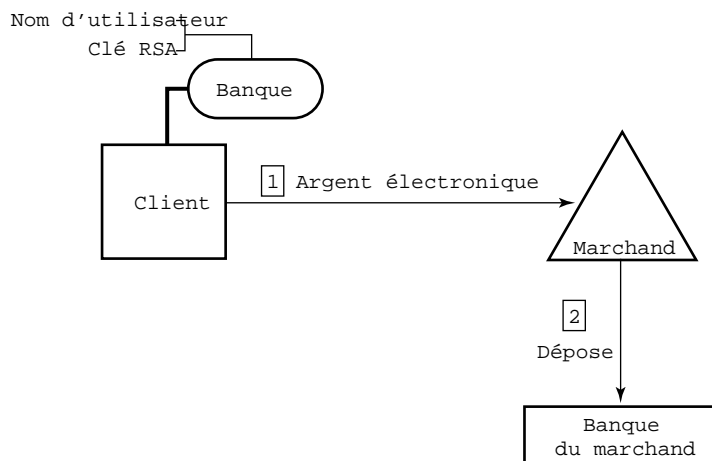


Fig. 1 - Le système de transaction Digicash

15.2.4. Netcash

Développée par Software Agents Inc., la solution Netcash n'utilise pas des pièces mais des coupons. Les clients achètent les coupons auprès d'une «banque» ad hoc appelée Netbank. Pour ce faire, ils communiquent leur numéro de carte bancaire sur le réseau ou par courrier postal. Les coupons sont en fait constitués d'un code spécifique qui ressemble à ceci:

Pour plus d'information, envoyez un message à cette adresse:
netbank-info@agents.com

Le marchand reçoit un coupon par courrier électronique ou à travers le Web. Il l'envoie à son tour à la Netbank qui l'honorera et en virera le montant sur le compte bancaire du marchand. Les coupons ne sont valables qu'une seule fois. Ils ne constituent pas une monnaie en tant que telle. La Netbank n'est donc pas une banque mais simplement une entreprise proposant des coupons à faire valoir sur des produits.

Le problème essentiel de Netcash est son manque de fiabilité. Le dispositif de sécurité n'est pas encore parfait et des escrocs pourraient fabriquer de faux coupons.

15.2.5. Cartes à puce

L'argent électronique peut résider sur une puce logée dans une carte plastique tout comme sur un disque dur. Digicash n'exclut d'ailleurs pas cette solution complémentaire. Le même principe se traduit toutefois différemment dans la pratique. La carte à puce requiert en effet un lecteur, qu'on peut placer dans les parcmètres, les téléphones, les distributeurs de boissons, les transports publics ou... les ordinateurs. Contrairement aux cartes de téléphone, ces cartes sont rechargeables: lorsque le crédit est épuisé, il faut la glisser dans un appareil spécial puis entrer ses coordonnées bancaires et le montant que l'on souhaite déposer sur la puce. En outre, elles ne s'appliquent pas à un seul bien ou service: elles sont polyvalentes.

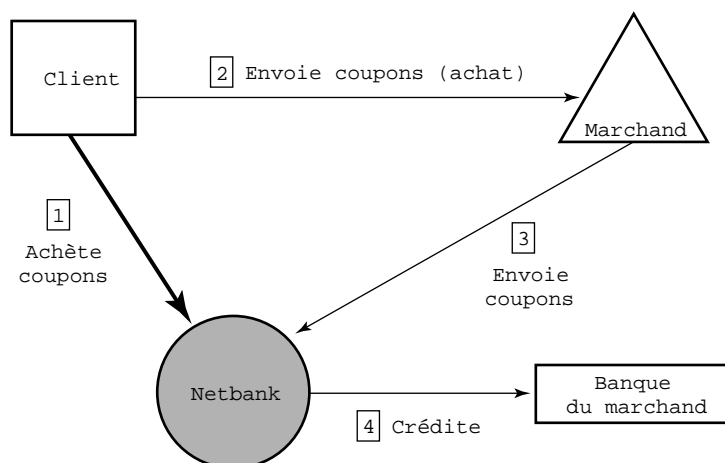


Fig. 2 - Le système de transaction Netcash

Une banque britannique, la Natwest (National Westminster Bank), en partenariat avec British Telecom et la banque Midland, a créé le consortium Mondex. Les trois partenaires ont été

rejoints par des banques canadiennes et du Sud-Est asiatique. Leur but est de développer une solution d'argent électronique à partir de cartes à puce «intelligentes». La carte Mondex accepte (pour l'instant) cinq devises. L'utilisateur peut débiter ou créditer son compte d'un montant contenu dans la puce. Celle-ci garde la trace des transactions effectuées, avec le nom du bénéficiaire de chaque paiement. Toutefois, les informations que recèle la puce sont chiffrées. Des voleurs peuvent dépenser la somme contenue dans la puce mais ils ne peuvent ni la recharger, ni accéder aux données bancaires du titulaire de la carte. Car l'argent électronique Mondex est anonyme. Tout comme pour l'argent liquide, le risque se limite donc à la somme que l'on transporte sur la carte. Une expérience grandeur nature a été lancée en juillet 1995 à Swindon, en Angleterre. Elle implique 40 000 consommateurs et 1 000 commerçants.

Sur le réseau, Mondex serait utilisé à peu près selon le même principe que Digicash. La différence est que Mondex nécessite un appareil spécifique relié à l'ordinateur, qui remplace le logiciel de Digicash. Ce nouveau périphérique agit un peu comme un portefeuille: pour acheter sur l'Internet, il faut y glisser la carte et demander à l'appareil (à travers l'interface logicielle qui l'accompagne) de transférer les fonds de la puce vers l'ordinateur du marchand. L'appareil doit aussi servir de guichet automatique personnel, à domicile ou depuis les locaux de l'entreprise. On y glisse la carte à puce pour retirer de l'argent électronique de son compte bancaire ou en déposer.

15.3. LA LIAISON DIRECTE CLIENT-MARCHAND

Certains systèmes de paiement prônent la transmission pure et simple des coordonnées bancaires en ligne, moyennant bien sûr une batterie de garde-fous. Le chiffrement des informations sensibles, notamment des numéros de carte bancaire, est au cœur de ces dispositifs.

15.3.1. La reproduction d'un achat classique

L'idée essentielle de ces systèmes de paiement est de transposer sur l'Internet les opérations classiques effectuées lors d'un achat. A la différence de l'argent électronique, le client n'utilise pas du liquide mais une carte bancaire, voire un prélèvement bancaire. Le client communique au marchand son numéro de carte ou ses coordonnées bancaires; le marchand obtient le paiement auprès des banques puis envoie le produit au client. L'avantage de cette formule est de créer un lien direct entre clients et marchands, sans passer par des intermédiaires.

Cette formule recèle toutefois un danger: les coordonnées bancaires sont exposées sur le réseau. Des pirates risquent de placer des programmes qui captent systématiquement tout ce qui peut ressembler, par exemple, à un numéro de carte bancaire. Les données sont évidemment chiffrées mais la «casse» récente d'une clé privée de la version exportée du browser de Netscape montre que des systèmes élaborés ont aussi leurs faiblesses. Il est vrai qu'en vertu des restrictions américaines sur les exportations de logiciels de chiffrement, cette version n'utilise la cryptographie traditionnelle que sur 40 bits (au lieu de 56 bits aux États-Unis).

15.3.2. Secure Web (SSL et S-HTTP)

Secure Web est un kit d'outils permettant d'intégrer deux protocoles de sécurisation des transactions, SSL (Secure Sockets Layer) et S-HTTP (Secure HTTP³). Ces deux protocoles, concurrents de prime abord, sont techniquement complémentaires. SSL a été mis au point par Netscape Communications Corp. en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. Il sécurise les transactions entre le Netscape Navigator (le browser) et le Netsite Server (le logiciel serveur vendu par la firme). S-HTTP est issu du consortium Terisa Systems, fondé par RSA et Enterprise Integration Technologies (EIT) et rejoint par America Online, Compuserve, Prodigy et IBM. S-HTTP est promu par CommerceNet, un autre consortium créé par EIT, dont le rôle est d'encourager le commerce sur l'Internet.

En fait, les deux protocoles peuvent se combiner. S-HTTP ne s'applique qu'aux transactions sur le Web. SSL intervient sur une couche logicielle supérieure, de sorte qu'il s'applique à plusieurs protocoles: Gopher, FTP, Telnet, HTTP et S-HTTP lui-même. S-HTTP constitue une extension du protocole HTTP et protège les documents. SSL, lui, sécurise non seulement le document mais aussi le canal que les données vont emprunter. Or, pour maîtriser le canal, il faut que point de départ et d'arrivée respectent les mêmes normes propriétaires: SSL ne fonctionne qu'avec Netscape Navigator à un bout et Netsite

³HTTP (*HyperText Transfer Protocol*) est le protocole utilisé pour le transport des données sur le Web.

Server de l'autre. De son côté, S-HTTP est compatible avec n'importe quel logiciel.

Lorsque la complémentarité des deux protocoles est apparue, Netscape a rejoint Terisa, permettant l'élaboration de Secure Web. Avec ce kit, les marchands acceptent les transactions utilisant l'un ou l'autre des protocoles. L'intérêt des marchands est de toute façon d'utiliser tous les systèmes de paiement possibles afin de vendre au plus grand nombre. Aucun intermédiaire n'intervient dans la transaction. Clients et marchands se reposent sur la technologie pour s'authentifier, chiffrer les données composant la transaction, en assurer l'intégrité et confirmer le paiement. La transaction s'opère donc très simplement, comme l'indique la figure 15.3.

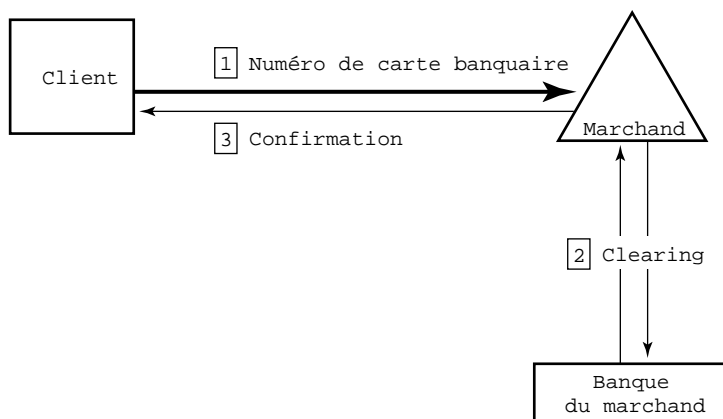


Fig. 3 - Le système de transaction Secure Web

SSL utilise un moteur de chiffrement RSA. Les données sont chiffrées et authentifiées grâce à des signatures électroniques. Lorsque le client est en présence d'un serveur Netsite, son browser Netscape le signale de deux manières : une petite clé apparaît en bas à gauche de l'écran (elle apparaît brisée dans les autres cas) et une ligne bleu barre le haut de la fenêtre de visualisation (en dessous du champ de l'URL). Le client est dès lors censé entrer ses coordonnées bancaires en toute quiétude. Les partisans de S-HTTP affirment qu'il est plus sûr que SSL. Cela reste invérifiable alors que, contrairement à SSL, le protocole n'est pas encore sur le marché à l'heure où nous écrivons.

15.3.3. Visa et Mastercard

Après des tentatives isolées, Mastercard et Visa ont décidé de travailler de concert pour encourager l'utilisation des cartes bancaires sur le réseau. Il existe 300 millions de cartes Mastercard et 442 millions de cartes Visa dans le monde. Les deux concurrents ont trouvé des partenaires prestigieux : GTE, Microsoft, IBM, Netscape, SAIC, Terisa Systems et Verisign. Ensemble, ils ont mis au point une norme commune appelée SET (Secure Electronic Transaction) destinée à sécuriser les transactions par carte bancaire sur des réseaux ouverts comme

l'Internet. Les spécifications ont été publiées en février 1996 sur l'Internet. Des tests étaient prévus pour le printemps, la mise sur le marché pour le dernier trimestre de 1996.

Visa et Mastercard sont partis de deux constats: les Internautes craignent de communiquer leurs coordonnées bancaires, même chiffrées; or l'intérêt pour Visa et Mastercard consiste à inciter les consommateurs à utiliser leur carte bancaire. La solution trouvée est simple: il suffit de substituer le numéro de la carte bancaire par un certificat numérique fondé sur un système cryptographique asymétrique RSA (voir chapitre 14). Un marchand peut d'une part authentifier le client, d'autre part s'assurer qu'il est solvable. Le système d'authentification VisaNet a été retenu.

Le client obtient sa clé en utilisant un logiciel spécifique qui sera intégré dans les browsers. Il entre son numéro de carte bancaire dans le programme. Celui-ci rend un fichier que le client doit envoyer à Visa (ou Mastercard). La compagnie renvoie un certificat contenant une clé qui demeurera gravée dans le logiciel. Lors de chaque transaction, le client demandera au logiciel d'envoyer sa clé au marchand. Celui-ci vérifiera que la clé est valide auprès de la banque du client. Le paiement s'effectue ensuite de manière normale. Le marchand et la banque devront disposer des outils logiciels nécessaires. L'objectif est de rendre la norme SET aussi courante que les cartes bancaires elles-mêmes. Pour un pirate, la seule façon de frauder serait d'obtenir le numéro de la carte bancaire ou de cambrioler l'ordinateur du client.

Au total, la transaction se déroule pratiquement dans les mêmes conditions qu'avec les protocoles SSL ou S-HTTP. Netscape a d'ailleurs décidé d'intégrer le logiciel à son browser. Mastercard envisage en outre d'interdire l'usage d'une de ses cartes sans ce logiciel. Des autorités de certification seront seules habilitées à distribuer les certificats numériques.

15.4. L'INTERMEDIATION

L'argent électronique n'est pas encore prêt et les numéros de cartes bancaires ne doivent pas être transmis sur le réseau. De plus, les cartes bancaires ne conviennent pas au règlement de petits montants. De manière générale, elles entraînent des coûts trop importants. Il fallait donc trouver d'autres solutions. De nouvelles sociétés sont ainsi apparues pour proposer des systèmes de paiement adaptés aux réseaux ouverts comme l'Internet. Ces systèmes exigent tous la présence d'un intermédiaire entre le client et le marchand. Ils sont aujourd'hui considérés comme les systèmes les plus sûrs. En outre, les services spécialisés offerts par les sociétés d'intermédiation facilitent la gestion des transactions en ligne.

15.4.1. Une intermédiation complexe

On pourrait dire qu'il y a intermédiation dès que les clients ou les commerçants doivent ouvrir un «compte» auprès d'une société spécialisée avant d'effectuer des achats. Mais la

définition ne serait pas assez précise. L'Internet Shopping Network, par exemple, demande à ses clients de ne livrer les coordonnées de leur carte bancaire qu'une seule fois, en échange d'un code personnel. Ce code est présenté lors de l'achat en lieu et place de la carte bancaire. Pour autant, on ne peut pas dire que l'ISN joue les intermédiaires. Les First Virtual ou autre Globe ID utilisent le même procédé mais pour le compte d'autrui (des marchands). Surtout, leur rôle est beaucoup plus large. L'intermédiation sur l'Internet consiste en fait à:

- gérer des identifiants,
- garantir l'identité des acteurs et l'intégrité des données,
- proposer un système de paiement sécurisé,
- servir d'interface avec le système bancaire,
- apporter une gamme de services à valeur ajoutée.

Les identifiants livrés par les intermédiaires donnent accès non pas à une galerie marchande (comme l'ISN) mais à un système de paiement. Les clients désirant utiliser le système de First Virtual, par exemple, vont ouvrir un «compte» auprès de la société. Celle-ci enregistrera les coordonnées bancaires du client et lui donnera un identifiant. Les clients peuvent alors se rendre dans tous les magasins virtuels acceptant le système de paiement de First Virtual. Les marchands identifient les clients auprès de First Virtual grâce à ce code personnel. Mais le rôle de l'intermédiaire va bien au-delà. Il permet aux clients et aux marchands de s'identifier mutuellement, de confirmer la transaction, de proposer un système de chiffrement pour protéger les données composant la transaction, de fournir éventuellement un logiciel spécifique au système de paiement, d'effectuer tous les paiements auprès des banques ou des centres de compensation, d'archiver les éléments de la transaction en vue de constituer des preuves ou de livrer des relevés de compte aux marchands, etc. La gamme des services varie d'un intermédiaire à l'autre.

15.4.2. Open Market

L'offre d'Open Market est globale. Cette société de Cambridge (Massachusetts) veut offrir tout les outils dont les entreprises ont besoin pour faire du commerce sur l'Internet. D'abord, Open Market fournit logiciels et services pour créer son magasin virtuel. Un autre logiciel, Commerce Connexion, permet de communiquer en toute confidentialité avec le système de paiement d'Open Market, l'Integrated Commerce Service. Ce dernier assure la sécurité des transactions et offre des mécanismes de paiement. Il apporte même un service de gestion de la clientèle (système automatisé d'assistance client, aide à la gestion des requêtes d'information, etc.).

En outre, son système de paiement est conçu pour accepter tous les dispositifs de sécurité: protocole S-HTTP, procédures d'authentification diverses (allant des mots de passe aux signatures électroniques), procédures d'autorisation des transactions (en fonction de listes de clients autorisés ou de l'accord de la banque du client), service d'audit (enregistrement des événements), «empreintes digitales» permettant de tatouer les documents et d'éviter une diffusion

non autorisée. Les marchands ont la possibilité d'adapter le niveau de sécurité en fonction du montant des transactions. Le système de paiement s'adapte à toutes les configurations de serveurs, à tous les montants (du centime aux dizaines de milliers de francs) et à toutes les formes de paiement (cartes de débit, de crédit, prélèvements bancaires, etc.). Il permet en outre de vendre les produits selon de multiples formats: biens physiques, informations au volume ou par abonnement. Open Market accepte le paiement en devises, ainsi qu'en crédits de services ou en frequent fliers miles⁴.
<http://www.openmarket.com/>

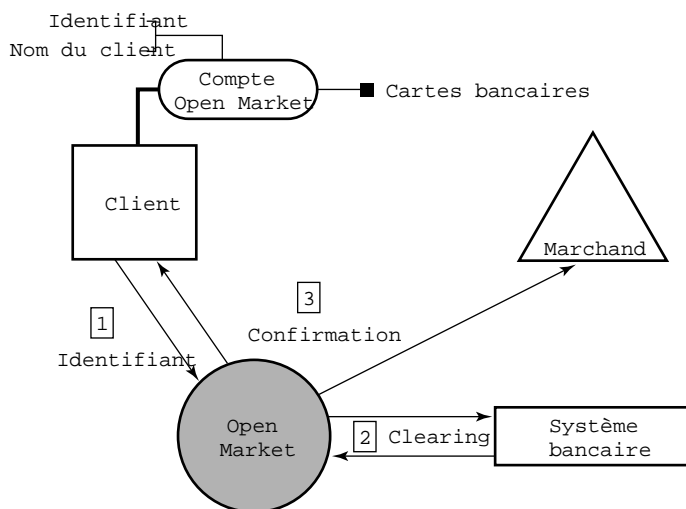


Fig. 4 - Le système de transaction Open Market

Les clients ouvrent un compte unique qui sert à tous les achats effectués dans les magasins équipés du logiciel serveur Commerce Connexion. Ils communiquent leurs coordonnées bancaires en ligne s'ils le désirent, ou bien par téléphone ou par fax. Ils peuvent fixer des limites de dépenses ou définir certains privilèges (abonnements, appartenance à des clubs, etc.) qui affectent le prix des produits. Lors d'un achat sur le serveur d'un magasin virtuel utilisant Commerce Connexion, le client envoie son identifiant (lié à une carte bancaire). Le serveur d'Open Market effectue le paiement après vérification. Le processus d'autorisation des cartes de crédit est en temps réel. Il confirme ensuite la transaction au client et au marchand. Celui-ci ne voit jamais le numéro de carte bancaire du client. Sur le plan du paiement proprement dit, c'est la forme d'intermédiation la plus simple.

15.4.3. Cybercash

Cybercash est une solution encore plus intéressante, dont le sort dépendra de l'adhésion qu'elle remporte auprès des

⁴Bonus réservés aux personnes voyageant fréquemment par avion.

banques. L'entreprise de Reston (Virginie), non loin de Washington, fut créée par Bill Melton, fondateur de Verifone (système de vérification des cartes de crédit dans les points de vente) et Dan Lynch, le fondateur du salon professionnel Interop (le plus grand salon mondial sur les réseaux informatiques et l'intégration). Elle réunit du beau monde: Trusted Information Systems (TIS), un fabricant de logiciels (de gardes-barrières entre autres), EIT, RSA, sans compter un partenariat avec la Wells Fargo. Cybercash est opérationnel depuis 1995.

Le client reçoit un logiciel gratuit qui lui permet de se connecter directement aux serveurs de paiement Cybercash, reliés au réseau bancaire. Ces serveurs sont sécurisés afin d'assurer l'étanchéité entre le réseau bancaire et l'Internet. Le client se sert d'abord du logiciel pour donner les coordonnées d'une ou plusieurs cartes bancaires à un serveur Cybercash. Ces données voyagent une seule fois sur l'Internet. Le client définit au cours de l'opération sa «Persona», qui comprend un identifiant et un mot de passe. Le marchand doit être autorisé à recevoir des paiements par carte bancaire. Cybercash ne l'aide pas à créer son magasin. Surtout, la banque du marchand doit accepter les requêtes en provenance de Cybercash.

Une fois dans un magasin utilisant le système Cybercash, le client fait savoir au marchand qu'il est prêt à acheter. Le marchand lui envoie une demande de paiement (voir la figure 15.5). Le client envoie au marchand sa Persona, choisit une des cartes bancaires enregistrées auprès de Cybercash et clique sur le bouton «Pay». Le marchand ajoute à ce message ses propres données et fait suivre le tout au serveur de paiement de Cybercash. Le serveur valide ou non la transaction et la traite en liaison avec les banques ou centres de compensation. En cas de succès, elle confirme la transaction au marchand, qui la finalise avec le client. Le paiement s'effectue automatiquement: le tout ne demande qu'une minute à partir du moment où le client clique le bouton «Pay». En général, les fonds sont disponibles le lendemain sur le compte du marchand, selon Cybercash.

<http://www.cybercash.com/>

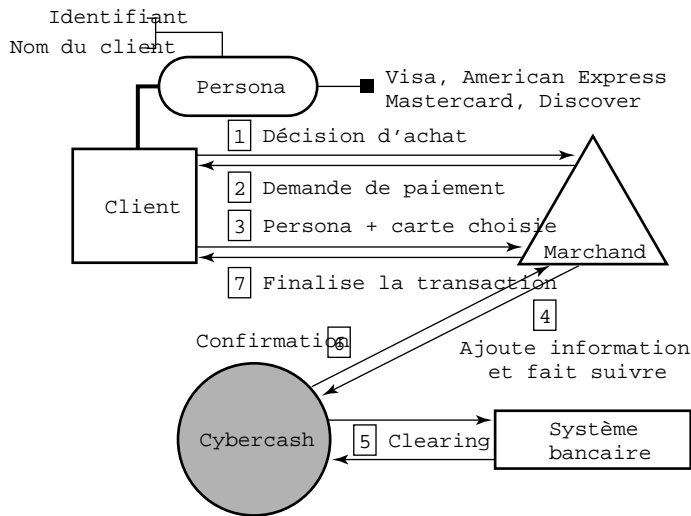


Fig. 5 - Le système de transaction Cybercash

Toutes les données transmises sur l'Internet sont chiffrées avec beaucoup d'efficacité: cryptographie traditionnelle DES sur 56 bits, avec des clés RSA longues de 768 bits. Les signatures électroniques utilisent la technologie MD5 et des clés RSA de 768 bits⁵. Les marchands aussi reçoivent un logiciel Cybercash gratuit qui leur permet d'obtenir instantanément les autorisations pour débiter les cartes bancaires, de traiter les transactions et de communiquer avec leurs banques. Le système est anonyme car les marchands ne voient pas le numéro de carte bancaire du client (sauf si la banque impose cette option). Le serveur Cybercash, lui, ne traite que les informations ayant trait au paiement, non au produit faisant l'objet de la transaction. D'ailleurs, seules les banques décident des mouvements de fonds; Cybercash ne joue que les intermédiaires. Cybercash a lancé fin 1995 le Money Payments Service afin de laisser les particuliers transférer de l'argent entre eux par courrier électronique, même lorsqu'une seule personne est titulaire d'un compte Cybercash. Ce service équivaut à un virement de compte à compte et ne repose pas sur les cartes bancaires. Bien entendu, les marchands peuvent eux aussi tirer avantage de ce service. Le but est double: favoriser le commerce avec les marchands qui n'ont pas le logiciel Cybercash; permettre au marchand d'être payés en liquide plutôt qu'avec une carte de crédit. De plus, un service Mini Payments doit introduire une forme d'argent électronique: les clients auront à leur disposition un portefeuille rempli de pièces, à l'instar de Digicash. Les marchands, eux, pourront vendre de l'information pour de très petits montants. Il semblerait que Cybercash soit autorisé à percevoir des intérêts sur les avoirs déposés dans ce portefeuille.

15.4.4. First Virtual

⁵Voir chapitre 14.

First Virtual est sans doute la solution la plus astucieuse de toutes. Le système combine légèreté des moyens et sécurité optimum. L'entreprise, installée à Washington, regroupe un homme d'affaires et trois gourous de l'Internet. Le premier, Lee Stein, avocat et comptable, conseille les firmes d'Hollywood. Il est PDG de First Virtual. Marshall Rose, un spécialiste de gestion de réseaux, est le chef d'orchestre. Nathaniel Borenstein, le principal auteur du protocole MIME, qui permet d'envoyer des fichiers binaires par courrier électronique, gère les aspects techniques. Einar Stefferud, un spécialiste de courrier électronique, s'occupe du développement. Le quatuor a passé des alliances avec de solides partenaires. First USA Bank traite les transactions impliquant des cartes de crédit. Northern Trust, une autre banque, s'occupe des prélèvements bancaires. EDS (plus précisément sa division Bank Card Processing) gère les données financières et prend en charge la compensation. D'autres grands noms comme Reuters ou Apple ont choisi First Virtual pour vendre leurs produits.

La particularité de First Virtual est qu'il ne recoure à aucun moment ni à la cryptographie, ni à un logiciel ad hoc. Cette simplicité est l'un de ses points forts. Comment parvient-il à ce miracle? Comme dans tous les systèmes d'intermédiation, les clients doivent au préalable ouvrir un compte auprès de l'intermédiaire. First Virtual met à disposition un serveur vocal: les clients communiquent leur numéro de carte bancaire par téléphone et reçoivent immédiatement un identifiant. Les marchands ouvrent eux aussi un compte, lié à un compte bancaire. Ensuite toutes les données sensibles, stockées sur un ordinateur séparé, sont isolées de l'Internet. EDS, qui gère cet ordinateur depuis l'Ohio, est d'ailleurs le seul intervenant à avoir accès aux numéros de cartes bancaires des clients. Les numéros de cartes bancaires n'ont aucun contact avec le réseau.

Les transactions passent par le courrier électronique et consistent essentiellement à authentifier les acteurs avant de procéder au paiement. La figure 15.6 résume les opérations. Au moment d'acheter, le client envoie son nom et son identifiant au marchand. Celui-ci entreprend la procédure d'authentification en présentant ces renseignements à First Virtual. Ce dernier vérifie que le client a un compte. First Virtual envoie alors un message au client (1) pour lui montrer que le marchand est bien autorisé et (2) pour lui demander de confirmer son achat (par un message indiquant yes, no ou fraud). De cette manière, l'intermédiation permet l'authentification mutuelle client-marchand. Une fois que le client confirme l'achat, First Virtual fait procéder au paiement. La transaction est ensuite confirmée au marchand. Pour faciliter la gestion de toutes ces allées et venues, les messages en provenance de First Virtual affichent, dans la zone «Subject» un identifiant unique à chaque demande de confirmation. First Virtual débite le compte bancaire des clients dès que les sommes, cumulées ou non, dépassent 10 dollars. De cette manière, le coût des transactions reste raisonnable.

<http://www.fv.com/>

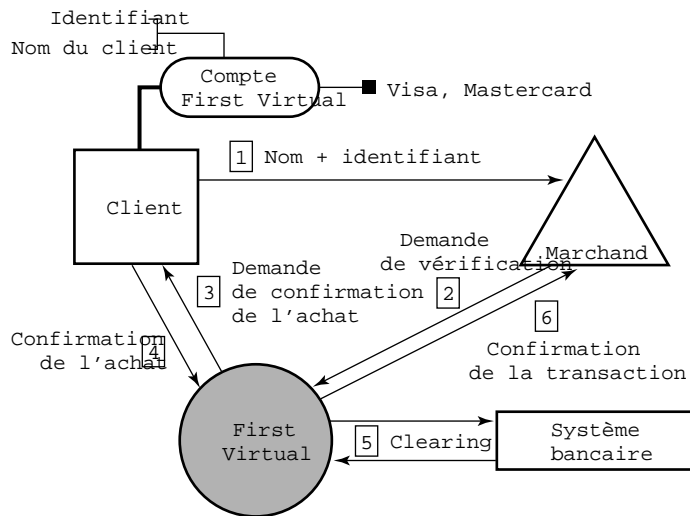


Fig. 6 - Le système de transaction First Virtual

Même si des pirates interceptent les messages, ils ne peuvent pas exploiter les identifiants. La seule façon de lier un identifiant à une carte de crédit serait d'avoir accès à l'ordinateur où sont entreposées toutes les données sensibles; autrement dit, de commettre un cambriolage. Quelqu'un qui utiliserait l'identifiant d'autrui ne risque pas d'arriver à beaucoup de résultat: le vrai titulaire du compte refuserait la transaction au moment où First Virtual lui demanderait de confirmer l'achat. La confirmation de l'achat par le client est d'ailleurs au cœur du système.

La politique «Essayez avant d'acheter» de First Virtual entraîne un troisième risque. Les clients peuvent en effet lire un document, ou des extraits, avant de l'acheter (une philosophie proche de celle des logiciels shareware). Certains pourraient en profiter pour prendre le document sans le payer. Or First Virtual, qui surveille l'utilisation des comptes, s'apercevrait assez vite des abus et annulerait leur compte. Bien sûr, on ne peut pas créer un nouveau compte avec la même carte bancaire. Quant au photocopiage de documents dûment achetés, le problème est le même que dans la vie réelle. Enfin, ceux qui refuseraient de solder leurs factures de carte de crédit verraient leur compte suspendu; puis, plus tard, leur carte de crédit probablement annulée par la compagnie émettrice.

D'un point de vue légal, les clients doivent accepter le principe selon lequel le message qu'ils envoient pour confirmer leur achat constitue un contrat. De même, les messages de confirmation envoyés par les marchands sont des preuves. C'est une condition à laquelle ils ne peuvent échapper s'ils désirent utiliser le système. Ceci dit, tous les intervenants sont libres d'utiliser la cryptographie.

Pour le client, l'ouverture d'un compte coûte 2 dollars. Pour le marchand, on distingue trois types de charges:

- 10 dollars à l'ouverture du compte,
- 29 cents plus 2% du montant de la transaction pour chaque transaction,

- 1 dollar de frais de traitement pour chaque paiement.

Avant de toucher à ces recettes, First Virtual laisse d'abord les banques et ses partenaires se rétribuer. Cela est d'autant plus logique qu'il n'est pas maître de l'argent qui circule. First Virtual ne touche donc l'argent qu'en dernier. De leur côté, les marchands fixent leurs prix librement. Comme les clients, ils restent complètement anonymes s'ils le désirent. De toute façon, les procédures d'authentification assurent aux uns et aux autres qu'aucun escroc ne se cache derrière un produit.

Le système a quelques inconvénients. Il ne convient pas aux biens physiques; il n'est destiné qu'à vendre de l'information. First Virtual encourage d'ailleurs tous les utilisateurs à devenir des marchands pour vendre des publications spécialisées, des guides de toutes sortes, de la poésie, des conseils professionnels, etc. La firme met à leur disposition un magasin, l'Infohaus, où ils peuvent louer un espace. Par ailleurs, les transactions ne sont pas effectuées en temps réel. Les échanges de messages prennent un certain temps, souvent 24 heures. Si le marchand peut se permettre d'automatiser les échanges de messages, le client n'en a pas les moyens et doit prendre la peine de répondre.

15.4.5. Globe ID

Cocorico: le meilleur système de paiement sur l'Internet est tout de même français. Tout au moins, Globe ID est la solution la plus ambitieuse, la plus complexe et en même temps l'une des plus proches de la réalité de tous les jours. L'avenir dira si elle remporte le succès escompté.

Le système de paiement Globe ID a été mis au point par GC Tech, en collaboration avec Edelweb, une société de service fondée par des chercheurs de l'INRIA, et. Dirigé par Gérard Dahan, GC Tech est une émanation de Seppia (conception de CD-Roms), de Waldo (conseils financiers) et de BPA, créée par d'anciens chercheurs de l'INRIA (notamment Philippe Brun et Paul-André Pays). Globe ID est le système utilisé par Globe Online, une galerie commerciale où se retrouvent plus de trente actionnaires français. Parmi ceux-ci, on trouve La Tribune Desfossés (LVMH), Le Monde, Libération, Dafsa, la Compagnie Bancaire, Encyclopaedia Universalis, Euro RSCG ou encore La Centrale des Particuliers. Le serveur pilote est lancé depuis le 15 septembre mais les choses sérieuses devaient commencer début 1996 avec la mise en service du système de paiement Globe ID.

Les transactions sont d'une totale transparence pour le client, d'où la sensation d'une transaction directe avec le marchand. En fait, Globe ID est l'intermédiaire incontournable, la plaque tournante du système. Il emprunte d'ailleurs un modèle transactionnel spécifique, le Clearing in the Middle Transaction Model (CMTM). C'est même le seul cas avec Open Market où client et marchand n'ont aucune relation directe. La figure 15.7 montre que tout passe par Globe ID.

Le système Globe ID repose sur des porte-monnaies virtuels (PMV). Il s'agit en fait d'un avoir que le client dépose au préalable et qui est débité au fur et à mesure de ses achats.

En fait, on peut distinguer deux techniques (en dehors de l'argent électronique) pour débiter des petits montants pour un coût minimum: soit ces petits montants sont cumulés puis débités à partir d'un certain seuil (c'est la solution retenue par First Virtual), soit ils sont débités immédiatement depuis un avoir. Globe ID a choisi la seconde technique.

Avant d'ouvrir un PMV, le client doit télécharger une interface gratuite. Ce logiciel doit être largement distribué auprès du public et des entreprises pour assurer le succès de Globe ID et de Globe Online. L'ouverture du PMV est également gratuite. Elle peut s'effectuer instantanément, en ligne; dans ce cas, les coordonnées bancaires sont chiffrées (technologie RSA) et envoyées à travers l'Internet. Si les clients n'ont pas confiance en ce moyen, ils peuvent passer par le téléphone ou le courrier postal. Le PMV est lié à une ou plusieurs cartes bancaires. Le client a la possibilité de personnaliser ses cartes bancaires, en leur donnant des noms, afin de ne pas les confondre. Des techniques de dédoublement assurent qu'à une carte correspond bien une seule personne. Lorsque le PMV est créé, le client reçoit pour chaque PMV (il peut en avoir plusieurs) un numéro de porte-monnaie et un code confidentiel.

Les clients sont susceptibles de payer de deux manières: soit de gros montants par carte, soit de petits montants débités de l'avoir. A l'ouverture du PMV, le client effectue deux opérations: il donne son numéro de carte bancaire et les autres informations nécessaires, puis verse sur le PMV un montant de son choix, inférieur à 500 francs. En fait, il y a trois formules de paiement possibles, selon le montant des achats:

- moins de 100 francs: débit du PMV,
- entre 100 et 500 francs: PMV ou carte bancaire au choix,
- plus de 500 francs: carte bancaire.

Grâce au logiciel fourni, le client peut consulter l'état de son PMV et y déposer de nouvelles sommes à tout moment. Il lui est également permis de retirer tout ou partie de son avoir. La somme est en effet bloquée sur un compte à la Compagnie Bancaire. Celle-ci ne peut pas se rémunérer sur ce stock d'argent. Par ailleurs, on peut envisager des PMV au sein d'une entreprise. Un disponible serait laissé à la disposition des employés dûment autorisés.

Armé de son PMV, le client fait du lèche-vitrine sur Globe Online. Lorsqu'il repère un produit intéressant, il clique dessus. S'il se déclare prêt à l'acheter, Globe ID lui confirme clairement la nature exacte du produit, l'origine (le marchand) et le montant. De cette manière, le marchand est authentifié. Le client achète en donnant son numéro de porte-monnaie et son code confidentiel. Il est donc authentifié à son tour. Son PMV est aussitôt débité du montant de la transaction. Globe ID traite la transaction avec le réseau interbancaire instantanément. Par la suite, il reverse de 80% à 95% des recettes au marchand selon la nature des produits. La marge est répartie entre Globe Online, Globe ID et GC Tech. Les informations achetées de cette manière restent à la disposition du client pendant deux jours.

<http://www.globeonline.fr/>

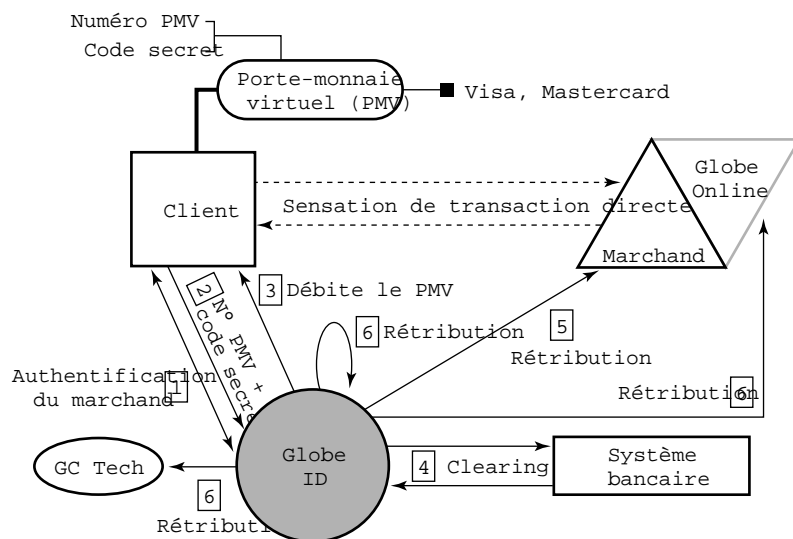


Fig. 7 - Le système de transaction Globe ID

Globe ID (comme Globe Online) a des ambitions mondiales: il traite toutes les devises et toutes les cartes de crédit. Le client a même le choix de la devise pour son PMV, quels que soient sa nationalité et son lieu de résidence. Globe ID actualise toutes les 6 heures un tableau de devises. Pendant toute cette période, ce tableau sert de référence à la compensation entre devises. La Compagnie Bancaire promet un taux de change intéressant. De son côté, Globe Online parle cinq langues: français, anglais, allemand, espagnol et japonais. La galerie commerciale doit s'étendre en Europe et en Amérique du Nord. Des contacts ont été pris au Brésil et au Japon.

Les marchands, quant à eux, déterminent librement leur stratégie commerciale et leurs prix. Il leur est même possible de fixer des prix différents pour le même produit en fonction du lieu de résidence du client. Par exemple, un parfum peut ne pas être facturé au même prix au Français et au Japonais, afin de respecter la logique des marchés. Les relevés de compte, retraçant les transactions qui ont eu lieu, sont transmis aux marchands par EDI (norme Edifact) s'ils le désirent. La Compagnie Bancaire s'engage d'ailleurs à traiter 25 transactions simultanées par seconde. Chaque transaction sera traitée en 0,4 seconde.

On le voit, l'essentiel du rôle de Globe ID n'est pas simplement de servir d'intermédiaire dans le paiement: il est d'apporter des services à valeur ajoutée. Le cœur du dispositif consiste à certifier l'acte que constitue la transaction. Pour cela, l'authentification des acteurs est plus importante que le chiffrement des données transmises. Globe ID s'assure en outre de la volonté de ces acteurs de participer à la transaction. Il veille aussi à garantir l'intégrité des données et leur non répudiabilité (les auteurs ne peuvent dénoncer ce qu'ils ont transmis car les données ne sont pas modifiables une fois envoyées). Seulement après, Globe ID effectue le paiement, en

relation avec le Compagnie Bancaire. Il ne s'arrête pas là: il archive toutes les transactions et les maintient à la disposition des participants. Il est ainsi capable de produire preuves en cas de litiges entre clients et marchands.

15.4.6. Netbill

Nous voulions aussi vous présenter Netbill, une solution expérimentale proposée par l'université Carnegie-Mellon de Pittsburgh, celle-là même qui donna naissance au search engine Lycos (voir chapitre 8). Le souci de ce système est non seulement de permettre les petits montants pour la vente d'informations (biens numérisables) mais surtout de s'assurer que les clients ne pourront utiliser les produits que lorsque le paiement sera effectif. En effet, ils pourraient lire le document et ne pas l'acheter (ce qui arrive avec First Virtual). Pour ce faire, le système utilise des porte-monnaies que les clients alimentent depuis un compte bancaire ou une carte de crédit. Netbill entretient un serveur de paiement connecté aux institutions financières existantes.

Au départ, clients et marchands doivent ouvrir un compte auprès de Netbill. Le système utilise un protocole de transaction permettant le dialogue entre deux bibliothèques logicielles: le «chéquier» du client et la «caisse» du marchand. Ces bibliothèques contiennent tous les critères et toutes les procédures nécessaires à la transaction. Elle sont incluses dans deux logiciels, l'un pour le client, l'autre pour le marchand, qui fonctionnent avec le Web.

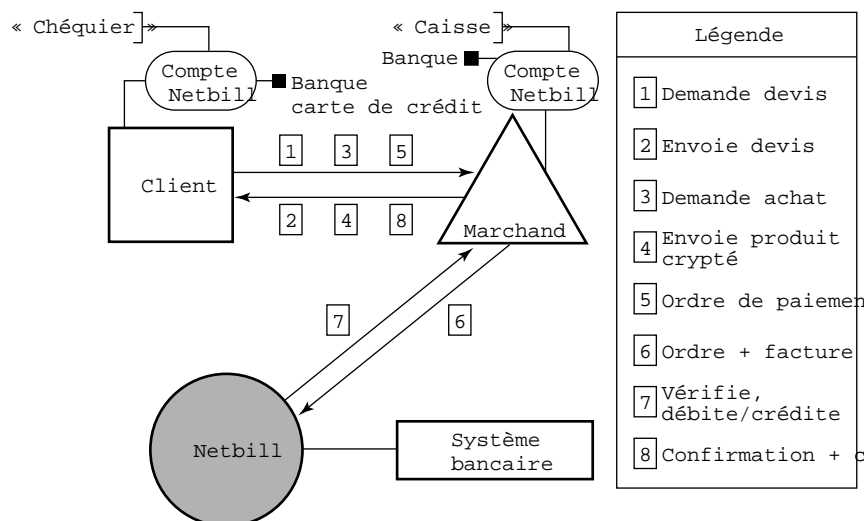


Fig. 8 - Le système de transaction Netbill

Comme indiqué dans le schéma ci-dessous, les relations s'établissent avant tout entre le client et le marchand. Le premier, à la vue d'un produit, demande un devis au second. Celui-ci renvoie un devis, puis le client demande le produit s'il est satisfait. Le marchand lui envoie le produit mais

chiffré, de sorte qu'il est inutilisable sans une clé. Le client renvoie alors un ordre de paiement très officiel qui constitue un engagement ferme. Le marchand le fait suivre au serveur Netbill. Celui-ci effectue le paiement, débite le compte Netbill du client et crédite celui du marchand. Il confirme ensuite la transaction à ce dernier. Alors seulement, le marchand fait parvenir au client la clé permettant d'utiliser le produit.

<http://www.ini.cmu.edu/NETBILL/>

La sécurité est assurée tout au long de la transaction par le chiffrement systématique de toutes les données. Le système intègre un certain nombre de subtilités, telle la différenciation du prix en fonction de privilèges (adhésion à un club, abonnement, achats en volume, prix variant selon l'heure, etc.). Le montant dans l'ordre de paiement (étape 5), calculé par le chéquier du client, doit correspondre à celui calculé par la caisse du marchand. Dans le cas contraire, le produit est repris par le marchand ou la transaction s'interrompt. Le serveur Netbill maintient toutefois le contrôle de la transaction. Il décide de la suite à donner à la transaction. Le nombre d'échange de données pourrait le fragiliser: un problème technique risquerait de nuire à la transaction. Mais il est conçu de telle sorte que la cohérence des transactions est toujours assurée. Netbill fournit en outre des instruments de comptabilité pour la gestion des comptes du client et du marchand. Les coûts marginaux de transactions sont très bas grâce à l'automatisation, aux frais financiers réduits (grâce aux avances consenties par clients et marchands au moment d'ouvrir leur compte), à la certification de la livraison des produits (qui réduit le nombre de litiges), etc...

15.5. LE BILAN

Les solutions techniques sont désormais à peu près au point et plusieurs systèmes de paiement vont se départager dans les années à venir. Elles sont toutefois très variées et pas toujours concurrentes. Clients et marchands peuvent tout à fait utiliser plusieurs systèmes, tout comme on paie dans le monde réel de diverses manières. Une chose est sûre toutefois: grâce à ces systèmes, le commerce électronique sur l'Internet ne peut désormais que se développer.

Les obstacles qui restent seront contournés et le marché s'adaptera aux contraintes intangibles. L'une des conséquences à long terme de ce développement sera sans doute la mondialisation accrue des échanges. l'Internet, réseau planétaire, nous conduit-il vers le marché atomique mondial? Cette tendance doit probablement être intégrée dans la stratégie de votre entreprise. Mais ce n'est pas la seule. Avant de clore ce livre, il nous reste à dégager dans le chapitre 16 les pistes d'avenir que l'on peut déceler aujourd'hui.