

Université Du Centre

Institut Supérieur De Gestion De Sousse

Master Spécialisé :

Commerce International et Technologie de l'Information

Module : Commerce électronique

Dossier De Recherche :

Le Paiement Sur Internet

Préparé par : **BOUBAKER Nobel El Houssine**

Année universitaire 2002/2003



“It’s e-business or out of business”

O’LEAVY

Kathy

Table des matières

Introduction	4
Les différents modes de paiement électronique	5
<i>Les cartes bancaires</i>	5
<i>Les chèques</i>	6
<i>Le paiement par monnaie électronique</i>	6
<i>Le paiement par compte intermédiaire</i>	8
<i>La nouvelle génération de paiement sur Internet</i>	9
Les qualités d'un procédé éligible pour le paiement électronique	14
<i>Identifier et authentifier le vendeur</i>	15
<i>Confidentialité de la transaction</i>	15
<i>Intégrité du procédé</i>	16
<i>Non-répudiation</i>	16
<i>Contrôle d'accès</i>	17
Les techniques actuelles de sécurité du e-paiement	17
<i>Les procédés de cryptages</i>	18
<i>La signature électronique</i>	23
<i>Les certificats électroniques</i>	24
<i>L'identification</i>	25
<i>La datation</i>	28
<i>Le protocole SSL</i>	28
<i>Le protocole SET</i>	29
Conclusion	33
<i>Bibliographie</i>	35

I) Introduction

Après avoir révolutionné les moyens de transmettre l'information, Internet vient révolutionner les pratiques commerciales avec le commerce électronique, que ce soit pour le commerce B to B ou B to C et surtout en offrant la possibilité de transmettre de l'argent. En effet, les différentes pratiques commerciales et modes de paiement ayant cours dans le monde réel peuvent trouver une traduction complète ou partielle dans le monde Internet.

Il est fort intéressant de noter que malgré les contraintes de sécurité sur Internet et surtout celles relatives au paiement électronique, la valeur ajoutée du commerce électronique est incontestable et consiste à :

- ✓ Assurer une ouverture au marché mondial puisque les sites marchands sont accessibles par tous les internautes dans les quatre coins du monde ;
- ✓ Garantir une présence continue 24 heures / 24 et 7 jours / 7 puisque le site marchand est accessible à tout moment ;
- ✓ Offrir un meilleur service aux partenaires et fournisseurs en rendant abordable la documentation technique et commerciale sur Internet ;
- ✓ Réduire les coûts par suppression des intermédiaires.

Le but de ce dossier est de présenter une typologie des types de paiements sur Internet, exposer les exigences auxquelles doit répondre un procédé de paiement électronique fiable et en fin présenter les solutions techniques de sécurité permettant à Internet d'accueillir les paiements.

II) Les différents modes de paiement électronique

Les modes de paiement sur Internet sont les suivants :

- Paiement par carte bancaire (Visa, MasterCard, EuroCard, American Express, ...)
- Règlement par chèques ;
- Paiement par monnaie électronique (E-cash, Digicash, Millicent, ...)
- Règlement par compte intermédiaire (KLELine : Klebox, ...)
- La nouvelle génération de services de paiement sur Internet.

1. Les cartes Bancaires (cartes de crédit)

Les cartes de crédit se présentent aujourd'hui comme le moyen le plus privilégié sur Internet pour tous les commerces à distance. Elles sont les seuls à offrir des garanties de paiement aux commerçants du monde entier. Les géants américains Visa, MasterCard et American Express sont des références supranationales certaines. Visa l'affirme sans retenue : «Visa est la carte de paiement la plus employée dans le monde ... et ce qui se rapproche le plus d'une monnaie commune ».

Il faut noter comme même que les cartes de crédit ne deviendront pourtant jamais un moyen de paiement universel. Les prélèvements qu'elles imposent entre 2 et 5% de la transaction ne sont endurés qu'en l'absence d'une

alternative plus économique. Ce coût est justifié par l'absence d'un contrôle immédiat sur la situation bancaire du titulaire de la carte.

Le principal frein au développement du paiement électronique par carte bancaire est la peur de communiquer son numéro de carte sur la toile. C'est d'ailleurs pour cette raison que les trois quarts des transactions existant sur le Web sont payées par chèque.

2. Les chèques

Les chèques sont d'un usage courant en Europe et au Japon, car une réglementation stricte en garantie le paiement. Inversement, les cartes de crédit n'y sont que pour les transactions internationales ou à distance. Dans le cas du chèque européen, la garantie est offerte au commerçant, non par l'organisme de gestion des cartes, mais par un groupement bancaire institutionnel. Cela revient finalement au même.

On mentionnera donc plus les chèques dans la suite, on parlera simplement 'd'instructions de paiement' ce qui recouvre aussi bien la signature d'un chèque que la présentation du numéro d'une carte.

3. Le paiement par monnaie électronique (Porte-monnaie électronique)

C'est un mode de paiement en débit immédiat permettant un paiement sans intermédiaire du compte de l'acheteur à celui du commerçant. C'est en fait la reproduction sur le marché électronique d'un virement bancaire. On effectue également une opération de débit lors d'un retrait d'argent liquide. Cela peut se faire par Internet, si l'argent en question tombe dans un porte-monnaie électronique.

Le porte-monnaie électronique en question est une mémoire portative, implantée sur une carte à puce, une carte PCMCIA, une disquette, un CD-ROM ou tout ce qu'on pourra inventer... . Cette mémoire, réputé inviolable, conserve le compte d'un argent fictif. Ce mode de paiement est le plus simple conceptuellement et le plus pertinent en théorie.

En fait d'argent, le porte-monnaie électronique peut également contenir des jetons à usage unique comme dans les cartes de téléphone. A la différence cependant des cartes de téléphone jetables, un porte-monnaie électronique digne de ce nom est rechargeable indéfiniment. On remplit son porte-monnaie par opération de retrait bancaire ou bien il se remplit tout seul par crédit tournant. L'argent électronique peut également passer d'un porte-monnaie à un autre et surtout le titulaire d'un porte-monnaie électronique peut convertir aisément son argent fictif en argent réel et vis versa. Le porte-monnaie électronique peut donc fonctionner en mode débit et en mode crédit.

L'avantage de ce système est celui de l'argent liquide : Il ne nécessite pas d'autorisation de paiement, donc pas de transaction immédiate avec un système distant.

Pour faciliter ce type d'opération, une infrastructure matérielle et logicielle doit être mise en place avec surtout une réforme des systèmes d'information bancaires, qui doivent dès lors répondre à un afflux de transactions de toutes provenances, à servir immédiatement et sûrement.

Enfin, le porte-monnaie électronique est un procédé d'avenir, car son coût décroissant, le rendra rentable à moyen terme. Sachant que cette évolution n'inquiète guère les organismes de cartes bancaires, car ils sont déjà en mesure de proposer eux aussi ce mode de paiement.

4. Le paiement par compte intermédiaire

Le règlement par compte intermédiaire est d'une grande souplesse d'utilisation et permet d'effectuer des achats de faibles montants sans pénaliser le commerçant, à l'instar d'un porte-monnaie réel. C'est un vrai nouveau service qui est proposé, adapté au marché du commerce électronique. La mise en œuvre est plus longue qu'avec les solutions traditionnelles, mais une fois en place, elle permet de gérer avec souplesse ses achats.

Les choses se présentent de la façon suivante :

❶ Le client visite un magasin, il fait ses courses, comme dans toute boutique virtuelle classique, mais au moment de paiement, le magasin lui demande s'il est ou non déjà client. Si l'acheteur potentiel est déjà client, il n'aura pas besoin à redonner son numéro de carte ni sa date d'expiration, puisqu'il est identifié par son nom de membre et le mot de passe de son choix ;

❷ S'il n'est pas client, le magasin lui propose de télécharger un formulaire et de le remplir ;

❸ Le client envoie au serveur intermédiaire ce formulaire comprenant une série de renseignements sur lui-même, le ou les comptes bancaires qu'il faudra débiter lors des futurs achats, la ou les cartes de crédit qui seront reconnues comme valables dans les transactions futures et enfin son code secret.

En retour le serveur intermédiaire, après les vérifications électroniques d'usage auprès des banques détentrices des cartes et des comptes concernés, fera parvenir au nouvel inscrit son numéro personnel de portefeuille virtuel ;

④ Dès lors le client peut valider ses achats. En passant commande le commerçant identifie son client par son nom, avec vérification automatique de la validité du mot de passe. Le commerçant envoie un véritable ticket de caisse électronique au serveur intermédiaire (KLELine par exemple) qui se charge de le transmettre à son tour au client ;

⑤ Lorsque le serveur intermédiaire soumet le ticket de caisse du commerçant au client, ce dernier est personnellement identifié par un numéro personnel de portefeuille électronique et le code secret de son choix. Si alors le client valide son achat, il ne peut pas y avoir de doute de sa volonté d'effectuer cet achat. En effet, pour les achats de petit montant un porte-monnaie électronique est utilisé. Le serveur intermédiaire demandera automatiquement au client l'utilisation de l'une de ces cartes ou de son porte-cartes pour alimenter son porte-monnaie électronique et pour couvrir les montants importants des achats.

Ce mode de paiement est très performant en terme de sécurité pour les deux parties à savoir l'acheteur et le commerçant. Le client ne fait circuler ses numéros de carte au commerçant et ne risque pas de se faire piéger par des sites pirates. Le commerçant sait que son client est identifié par l'organisme bancaire. La carte ne peut pas venir d'un vol récent pas encore enregistré dans les bases de données des banques.

5. La nouvelle génération de paiement sur Internet

Etant donné que le portefeuille électronique est le fruit d'un véritable contrat passé entre l'organisme financier et son détenteur, ce système permet un certain nombre de souplesses difficiles à imaginer dans tout autre contexte.

La souplesse du service permet de demander un relevé auprès du serveur intermédiaire, d'ajouter une carte, de remplir le porte-monnaie, de changer le code secret, de vider le porte-monnaie, de retirer une carte et faire un changement d'adresse.

Les serveurs intermédiaires proposent aussi un moyen de paiement multi-devises. Tout internaute peut faire des achats en ligne ; la société intermédiaire se charge des calculs des taux de change sur des sites de partenaires étrangers quelle que soit la devise de son pays et lui permet de connaître les différents prix de sa devise.

Il est aussi proposé des options de paiements échelonnés :

a. L'option de paiement à la carte propose différents modes de paiement en ligne adaptés aux spécificités de chaque secteur d'activité.

b. Le paiement par versement d'acompte : Lors de l'acte de paiement sur la toile, l'internaute ne règle qu'une partie du montant total de son achat. Le solde est débité par la suite, à un commerçant en accord avec l'internaute. Exemple : Le secteur du tourisme. Ce service est fortement sollicité par des tour-opérateurs et des services de réservation hôtelière. Le versement d'un acompte formalise la réservation.

c. Le paiement avec débit différé : Lors de l'achat le serveur intermédiaire interroge les réseaux cartes en temps réel, sans débiter le client. Le débit effectif sera déclenché à la livraison ou à tout moment défini par le commerçant en accord avec son client. La législation de certains pays n'autorisant pas le débit avant la livraison, cette fonction peut s'avérer

indispensable. En effet, ce mode de paiement est une option permettant de s'assurer qu'un produit est disponible.

d. Le paiement d'un forfait de consommation : commerçants et clients s'entendent en ligne sur les modalités d'un forfait de consommation : durée, coût total, coût maximal de chaque transaction. Flexible, ce mode de paiement permet par exemple à un client d'acheter un journal en ligne pendant une certaine durée, sans obligation de l'acheter chaque jour mais en choisissant librement sa fréquence.

e. Le paiement par prélèvement régulier : Le client donne une fois pour toutes l'autorisation à son serveur intermédiaire d'effectuer à un intervalle régulier un débit fixe, pour une durée donnée. Exemple : le paiement mensuel d'un fournisseur d'accès à Internet.

f. Le paiement selon le budget alloué d'un administrateur à un certain nombre de collaborateurs : (Exemple : Klebox corporate ; voir <http://www.Kleline.fr>) Cette version de paiement en ligne est destinée aux entreprises, aux administrations et aux associations. Elle permet à administrateur d'allouer des budgets à un certain nombre de collaborateurs, selon leurs besoins. Cette méthode fonctionne comme un compte bancaire en ligne. L'administrateur envoie un chèque à son serveur intermédiaire pour que son compte soit crédité, et que son serveur intermédiaire puisse à son tour créditer les porte-monnaies des collaborateurs. L'administrateur veille à que le solde de son compte soit toujours suffisant pour permettre la mise à jour automatique (généralement mensuel) des porte-monnaies. Au départ, l'entreprise qui achète désigne le budget mensuel alloué à chacun de ses collaborateurs et ses filiales à l'étranger, qui leur permettra d'effectuer des achats en quelques clics de souris auprès des fournisseurs et commerçants

opérant chez le même serveur intermédiaire. Chaque début de mois, le porte-monnaie électronique de chaque collaborateur est remis au niveau du budget alloué.

Cette opération est automatique, l'entreprise doit seulement penser à vérifier le niveau du solde de son compte administrateur. A chaque début de mois, ce niveau doit être égal à l'ensemble des compléments versés aux collaborateurs.

Exemple : une entreprise décide d'allouer 10000 € de budget porte-monnaie par mois à un collaborateur ou à une de ces filiales ; des achats de 2000 € ; 70 € ; 4520 € ; 65 € ; pendant le mois ramèneront le solde de son porte-monnaie à 3345 €. En début de mois suivant, ce solde sera remis au niveau que l'entreprise a décidé, 10000 € : le serveur intermédiaire crédite le porte-monnaie de votre collaborateur de 6655 € et débite le compte de l'entreprise de ce montant et cela pour chaque collaborateur.

L'administrateur suit les opérations de ces collaborateurs en temps réel, il peut faire accès au relevé des achats. Les collaborateurs réalisent leurs achats sur Internet en toute liberté, dans la limite du budget alloué, et de leur autorisation carte.

g. Le serveur Payline pour le règlement par carte bancaire : Payline a été conçu pour fournir aux commerçants sur Internet une solution de paiement utilisant les circuits et procédures déjà banalisés et permettant le paiement sécurisé avec les cartes bancaires.

Le principe de manœuvre est le suivant :

❶ Un client final fait ses achats chez un commerçant sur Internet, il passe la commande et valide sa facture ;

❷ Le commerçant transmet en mode sécurisé les données techniques de cette facture : référence, montant au serveur Payline. Dans le même temps, le client est routé sur le serveur Payline en mode sécurisé. Il entre son numéro de carte bancaire et la date d'expiration de celle-ci. A aucun moment le client final ne donne son numéro de carte de crédit ni la date de validité au commerçant. Ce dernier n'a donc aucun moyen de prélever à nouveau de l'argent à ce client une fois que cette affaire est réalisée ;

❸ Le serveur Payline contrôle la carte et fait une autorisation auprès de la banque du porteur de la carte ;

❹ Le serveur Payline informe le commerçant ainsi que le client final c'est à dire le porteur de la carte du résultat de transaction en mode sécurisé. Le client final est renvoyé sur le site Marchand du commerçant ;

❺ Le soir, le serveur Payline effectue une remise des transactions auprès de la banque du commerçant.

Le grand privilège de ce système est que chaque partie en présence garde sa propre banque et personne ne doit changer ses habitudes. Dans certains cas à condition de laisser son navigateur afficher ces messages, le client final est prévenu du passage vers le serveur sécurisé, ce qui lui donne confiance au moment de payer avec sa carte de crédit.

h. Les réponses de demain : Aux Etats Unis, la société Miros a lancé une technique reposant sur la *biométrie* qui est une formule d'identification de l'utilisateur par ces caractères physiques personnels.

Pour l'utiliser, il suffit de disposer d'une simple Web-caméra au-dessus de son micro-ordinateur et au moment de la connexion, logiciel compare les images qu'il reçoit à celles qu'il avait déjà numérisées dans sa base de données.

La société Net Nanny, spécialisée dans le filtrage d'accès aux sites Web aux Etats Unis vient de développer un système de reconnaissance de frappe au clavier. Après apprentissage, le logiciel est capable d'identifier sans risque d'erreur la personne qui utilise l'ordinateur.

Il n'est donc plus besoin de mot de passe ou autre puisque c'est l'utilisateur lui-même qui est reconnu. Ce logiciel, toujours en phase d'essais, est, d'après la société Net Nanny, tellement infailible, qu'il pourra servir aux distributeurs de billets, aux contrôles d'accès, etc. Mais, dans ce panorama d'outils de paiement sur le Web, qu'elles sont les exigences auxquelles doit répondre un procédé de qualité pour le paiement électronique ?

III) Les qualités d'un procédé éligible pour le paiement électronique

Ce qui peut paraître paradoxal lorsqu'il s'agit du règlement d'un achat sur le Web, les deux parties ont la même peur. Le client a peur de payer et de rien recevoir, le commerçant a peur de livrer et de ne pas être payé. Donc, une méthode de qualité pour le paiement électronique doit apporter la confiance

et doit sécuriser les deux parties tout en gardant le maximum de souplesse et de confort dans l'utilisation.

Globalement, tout système sécurisé de paiement doit répondre à ces critères de base :

1. Identifier et authentifier le vendeur et garder l'anonymat de l'acheteur vis à vis du commerçant : Il s'agit de garantir que le catalogue de produits diffusé sur la toile appartient bien à un marchand dont l'identité est validée par tiers de confiance. Il faut donc que le commerçant propriétaire du site marchand soit référencé auprès d'un organisme digne de foi, qui se porte garant vis à vis de l'acheteur et offre une voie de recours en cas de litige.

Vis à vis du commerçant, l'acheteur ne souhaite pas nécessairement se faire connaître. Cela permet d'éviter que le commerçant exploite un registre de ces clients. Il y a également un enjeu légal, car un problème crucial de liberté publique se pose sitôt qu'un organisme s'arroge la prérogative d'identifier les personnes physiques. Cet enjeu est décuplé avec le passage à la télématique, qui permet de collecter et fusionner les informations en provenance de sources multiples. La législation de certains pays, tels les Etats de l'Union européenne est à cet égard explicite et impose un monopole de l'état civil.

2. Confidentialité de la transaction et des renseignements bancaires : La substance de la transaction ne doit être connue que de l'acheteur et du commerçant. Mais, il est impératif que l'acheteur doit être en mesure de conserver un document valable juridiquement ' Trace de la commande ', certifiant de façon définitive toutes les caractéristiques de la transaction : identité des parties, substance, montant et dates.

Le seul souci légitime du commerçant est d'être payé. Le système doit donc être en mesure de fournir cette garantie tout en masquant la situation du compte de l'acheteur. La position des organismes internationaux de carte bancaire est ici avantageuse, car ils peuvent masquer jusqu'à la provenance géographique des fonds.

Pour des raisons de sûreté, l'acheteur ne souhaite pas non plus que son identité bancaire soit révélée au commerçant. Les systèmes électroniques peuvent présenter à cet égard un avantage sur les systèmes actuels de cartes et de chèques et procurer la même confidentialité que l'argent liquide.

3. Intégrité du procédé : Les acheteurs et les commerçants doivent avoir confiance dans le procédé qu'ils utilisent. Dans le contexte d'Internet et de l'informatique domestique, il faut compter avec des fréquentes défaillances des systèmes informatiques.

Il est impératif que les transactions soient atomiques, c'est à dire qu'elles s'effectuent en totalité et à l'entière satisfaction des parties ou pas du tout. Toute entorse à ce principe ; souvent désigné intégrité de la transaction ; ruinerait la crédibilité du procédé.

L'intégrité assure aussi qu'aucune modification est apportée aux données et surtout à la trace de la commande. Le mot modification englobe en fait, la duplication, l'insertion, l'effacement d'une partie de l'information et le changement dans l'ordonnancement des informations.

4. Non-répudiation : Elle permet d'éviter à ce que l'une des deux parties nie la transmission ou la réception de l'information lors de procédé de commande d'échange de données ou de paiement électronique sur le Web.

5. *Contrôle d'accès* : Assure que seulement des personnes autorisées peuvent obtenir accès lors du paiement. L'objectif de ce critère est de protégé les informations.

Un problème se pose à ce niveau puisque les organismes financiers opérant à l'international ont quelques obligations, en particulier dans la lutte contre le blanchissement d'argent. Certains Etats (en fait, les organismes de contre-espionnage) désirent également être en mesure de surveiller tous les échanges qui s'effectuent au travers de leurs frontières !

Mais quels sont les mécanismes et les techniques utilisées pour garantir la sécurité du paiement électronique sur Internet ?

IV) Les techniques actuelles de sécurité du e-paiement

Sur Internet, circulent des paquets qui suivent des circuits de routage de machines (host en Anglais) en machines. Chacune de ces machines effectue ce routage avec des logiciels standards aux spécifications bien connues. Le chemin varie en fonction de la disponibilité des machines et des connexions. C'est ce que fait la robustesse d'Internet.

Il est impossible de garantir que les paquets échangés entre deux correspondants ne sont pas interceptés ni altérés. Le problème prendra plus d'ampleur quand il s'agit de communiquer des choses sérieuses comme l'argent. En fait, il existe des solutions et des procédés techniques permettant à un échange d'informations confidentielles de respecter les qualités que j'ai déjà précisé dans la deuxième partie de mon dossier.

Les techniques qui seront évoquer dans cette troisième partie sont : Les procédés de cryptages, la signature électronique, la certification électronique, l'identification, la datation, le protocole SSL et en fin le protocole qui a été développé conjointement par Visa et MasterCard, avec la participation des ténors de l'informatique parmi lesquels Microsoft, IBM et Netscape à savoir le protocole SET.

1. Les procédés de cryptages

La cryptographie c'est la science de préserver la confidentialité des messages alors que la cryptanalyse est l'art de décrypter des messages chiffrés.

Les systèmes cryptographiques sont classés selon trois dimensions :

- Type d'opérations employées pour obtenir le texte chiffré (cyphertext en anglais). Tous les algorithmes sont basés sur les principes suivants : substitution, transposition, combinaison de la substitution et la transposition dans des étapes successives, et les transformations mathématiques ;
- Le nombre de clefs utilisées : clef unique ou cryptage conventionnel et clefs différentes ou cryptage asymétrique ;
- La façon dont le plain texte est traité : (Block cypher et stream cypher). Dans le chiffrement par bloc le message est découpé en blocs de 8, 32, 64 bits et chaque bloc est chiffré indépendamment de la valeur des autres blocs (DES, RSA, IDEA, RC2). Dans le chiffrement en contenu le message est découpé en blocs de 8, 32, 64 bits mais chaque bloc est chiffré en fonction de la clé **mais aussi** de la valeur du bloc précédent et/ou suivant (RC4, SEAL, WAKE).

Les cryptosystèmes se divisent en deux grandes catégories selon leurs techniques, mais aussi selon leurs usages. On a d'un côté les algorithmes de cryptages par blocs ou cryptages symétriques (cryptosystèmes conventionnels), d'un autre les cryptages asymétriques (cryptosystèmes à clef publique).

a. Cryptages par blocs ou cryptages symétriques

Un cryptage par blocs (block cipher, en anglais) est un algorithme qui transforme un bloc de données de taille fixe (en général un mot de 64 bits) en un bloc de même longueur. Cette propriété est essentielle pour des applications réclamant une bande passante garantie.

Les procédures de ce type de cryptage sont des algorithmes symétriques, ce qui signifie que le cryptage et le décryptage s'effectuent par la même fonction.

Les cryptages par blocs sont réalisés selon des modes dépendant des applications. Dans un flot de données, on ne se contente généralement pas de crypter les blocs de données un par un. On utilise souvent les données d'un bloc pour modifier le suivant. On peut par exemple appliquer un OU EXCLUSIF entre les deux. Cela complique nettement la tâche d'un espion, car même s'il trouve la clef, il doit remonter au départ de l'échange pour le décrypter.

Parmi la foule de procédés de cryptages symétriques ces dernières années, qui ont chacun leurs avantages et leurs spécialités. En voici quelques-uns : DES (Data Encryption Standard), Triple DES, IDEA (International Data Encryption

Algorithm, Lai et Al 1992), SAFER (Secure And Fast Encryption Routine, Massey 1993), SKIPJACK et BLOWFISH (Schneir 1993).

Cas de l'algorithme DES : l'algorithme symétrique « Data Encryption Standard » a été élaboré chez IBM, puis fut adopté comme norme de cryptage par l'administration américaine en 1977. C'est à ce jour l'algorithme de cryptage le plus répandu.

Le cryptage DES de base utilise une clef de 56 bits. Il s'effectue en 16 passes de rotation et 3 transpositions sur des mots de 64 bits. En presque vingt ans, cet algorithme a fait l'objet de nombreuses tentatives de forçage. La méthode brutale (essaie de toutes les clefs) requiert évidemment 2^{55} essais en moyenne ce qui le rend impraticable à l'heure actuelle. On est parvenu à le percer en 1994 en partant d'un échantillon connu de 2^{43} mots.

Sur l'implantation matérielle, l'algorithme DES est capable de crypter ou décrypter entre 300 Mbits et 3 Gbits/seconde. Il est donc éligible pour crypter et décrypter sans surcoût des échanges permanents tels les échanges sur un réseau ou sur un bus.

Pour améliorer la puissance de DES, on fait recours au cryptage multiplexe utilisant DES avec des clefs multiples : **Triple DES** utilise 3 clefs secrètes.

b. Cryptages asymétriques

Un cryptage asymétrique est un algorithme pour lequel, cryptage et décryptage sont des fonctions différentes et qui fait intervenir deux clefs différentes. En fait, les procédés du type DES sont également appelés

procédés « à clef privée » car la confidentialité des informations est conditionnée au secret qui entoure la clef de cryptage.

L'inconvénient du procédé symétrique est que la clef doit être communiquée à son interlocuteur dès que l'on souhaite transmettre un message crypté. Il faut donc disposer d'un canal très sûr pour la transmission de la clef. Il faut de plus, changer de clef à chaque nouvel échange.

Les procédés asymétriques sont, par opposition, appelés « à clef publique » car ils sont conçus pour que l'une des deux clefs (la clef publique) puisse être révélée sans compromettre l'autre (la clef secrète). La clef secrète n'a jamais besoin d'être communiquée par son détenteur. La même clef peut être par conséquent être employée pendant longtemps ; les spécialistes conseillent d'en changer tous les deux ans.

RSA est le plus célèbre et le plus répandu des algorithmes asymétriques. Il a été inventé en 1978 par Ron Rivest, Adi Shamir et Leonard Adelman. Une implantation matérielle actuelle du logiciel BSAFE de RSA Data Security Crypte offre un débit de 300 kbits/ seconde.

En logiciel, l'algorithme DES est 100 fois plus rapide que le cryptage RSA. Sur une implantation matérielle, il est entre 1000 et 10000 fois plus rapide (entre 300 Mbits et 3 Gbits/ seconde). Au fur des progrès des algorithmes et des composants, la performance de DES progressera plus rapidement que celle de RSA, car DES se compose d'opérations plus purement informatiques.

Du fait de ce rapport de performances, les échanges de données de tous les protocoles de communication sécurisés se feront selon des cryptages symétriques par blocs tels que DES. L'usage des algorithmes asymétriques

sera ponctuel, on ne les emploiera que pour transmettre des données courtes, de quelques octets, tels que les clefs privées et les signatures électroniques. De nombreux algorithmes asymétriques font chaque année leur apparition lors des conférences : ElGamal, Crypto, Eurocrypt et Asiacrypt.

Les agences gouvernementales Américaines (la NSA « National Security Agency » et le FBI) établissent un seuil à ce qu'elles appellent les cryptages forts. Le seuil est fixé par la formule 40/512 qui indique une longueur maximum de 40 bits pour les clefs de cryptage symétrique et de 512 bits pour le cryptage asymétrique. Ce seuil est supposé correspondre aux puissances de calcul dont dispose la NSA, mais il semble insuffisant à bien des spécialistes même pour des applications commerciales. Ils recommandent plutôt un niveau de 80/768.

Les systèmes réalisant des cryptages forts peuvent néanmoins être diffusés à condition d'être intégrées à certains types d'application, parmi lesquelles les applications strictement financières. Les producteurs américains de logiciels pourront donc diffuser mondialement des produits intégrant ces technologies, ils en auront d'ailleurs l'exclusivité. A titre d'exemple, on peut citer le cas de la compagnie CyberCash qui a ouvert la voie en obtenant le droit d'exporter son système qui incorpore un cryptage RSA à 768 bits.

En effet, les algorithmes de cryptages sont considérés par les autorités américaines comme des technologies sensibles et font l'objet de restrictions à l'exportation. Les logiques commerciales et stratégiques s'opposent dans un débat qui est loin de se clore.

2. La signature électronique

Le concept de signature électronique a été introduit par Diffie et Hellman en 1992. Si le détenteur de clefs asymétriques publie une de ces clefs asymétriques publiques et s'engage à garder l'autre secrète, ce qui lui est possible car il n'a jamais besoin de la révéler, le cryptage d'un document électronique réalisé par cette clef asymétrique privée constitue une signature juridiquement acceptable de ce document. On authentifie le document en le décryptant par la clef asymétrique publique. La probabilité d'erreur est minime surtout avec des clefs sur 768 bits.

Le détenteur d'une clef asymétrique privée peut être tenu pour responsable de tout cryptage réalisé avec elle. Soit il en est l'auteur, soit il a commis une imprudence. Dans un cas comme dans l'autre, il en assume les conséquences. C'est le principe de non-répudiation ou appelé aussi non-désaveu. A contrario, un désaveu est toujours possible quand la signature n'est pas secrète, comme c'est le cas avec les numéros de cartes de crédit et même les signatures manuscrites.

La signature électronique d'un document n'est généralement pas le cryptage de tout le document mais d'une forme abrégée du message, de taille fixe, appelée : **L'empreinte électronique** « Digest en Anglais ». Cette empreinte est réalisée par une fonction de hachage à sens unique.

Plusieurs fonctions de hachage sont couramment employées. Les qualités demandées à une fonction de hachage sont :

- Grande dispersion : Un petit écart entre deux documents doit créer un grand écart entre deux messages.

- Absence de collisions : Deux documents différents ne doivent avoir aucune chance de donner la même empreinte. Il doit être impossible de point de vue informatique, de générer deux documents ayant la même empreinte.

- Inversion impossible : Il ne faut pas que l'on puisse recréer le document à partir de l'empreinte

MD5 et SHA-1 sont les deux fonctions de hachage les plus populaires.

3. Les certificats électroniques

La certification d'un document électronique signé débute par l'examen du certificat de l'auteur présumé du document.

Le certificat est un document d'identité électronique attestant du lien entre une identité et une clef publique. Un certificat mentionne au minimum l'identité en question et la clef publique qui lui est associée. Il peut également mentionner une date d'expiration et un numéro en série. Le certificat est signé électroniquement par l'autorité émettrice, qu'on appelle aussi « autorité certifiante », en anglais « Certifying Authority / CA ». Cette autorité est un organisme ayant intérêt quelconque à se porter garant de certaines identités. Parmi les autorités certifiantes, on trouve VeriSign, Thawte, Entrust, Baltimore, Gemplus et Matra...

Pour vérifier la clef d'un interlocuteur, on va consulter son certificat, puis vérifier la signature du certificat. Vérifier cette signature c'est faire usage de la clef publique de l'autorité émettrice du certificat. En fait, la fabrication d'un certificat se fait sur l'initiative de l'intéressé. Celui-ci fabrique une paire

de clefs asymétriques et transmet la clef publique à l'autorité certifiante. L'autorité s'assure par un moyen quelconque de l'authenticité de l'identité qui lui transmet cette clef, et produit en retour un certificat.

Comme tout document d'identité, les certificats n'ont ni plus ni moins de crédibilité que l'autorité émettrice. Cette crédibilité tient en particulier aux méthodes qu'emploie l'autorité pour s'assurer de l'identité du producteur de la clef et des protections dont elle entoure sa propre signature (sa clef secrète).

La règle veut qu'une autorité certifiante digne de foi publie ses procédures d'identification. Elle peut par exemple ne délivrer de certificat qu'en main propre et sur présentation de pièce d'identité. Le site de la compagnie VeriSign propose une gamme de produits reliés aux certificats électroniques.

4. L'identification

Avant d'entamer un échange sécurisé sur un réseau, on va s'assurer une bonne fois de l'identité de son correspondant et partager ensuite avec lui une clef symétrique (privée) qui permettra de crypter par blocs la suite des échanges. Les deux se font dans la même phase, dite d'identification (*authentication* en anglais).

Le premier système à implanter une identification des participants à un réseau ouvert fut *Kerberos*. Il est d'ailleurs le seul qui soit d'usage courant aujourd'hui. Kerberos fut développé par l'équipe du projet *Athena* en se basant sur le protocole de Needham et Shroeder à clef secrète. Ce protocole, un peu ancien (1978) proposait une méthode d'identification basée sur la présence

d'un service central de distribution de clefs, lequel distribue des clefs secrètes à ses clients.

Kerberos reconnaît l'identité des clients par des méthodes fiables. Il a été conçu pour permettre de gérer l'accès des ressources par des machines non sécurisées à travers un réseau non sécurisé. C'est ainsi qu'il est implanté dans le UNIX, dans le Andrew File System et certains dérivés de NFS. Avec kerberos, un client désirant accéder à un serveur va demander au serveur de clefs la recommandation, appelée « ticket de session », qui lui permettra d'accéder à une ressource donnée pour un temps limité.

Kerberos est élastique car il comporte une notion de domaines dont chacun possède son serveur de clefs qui peuvent se connecter entre eux pour étendre le service. Kerberos a la capacité d'étendre les notions classiques pour un ordinateur unique ou pour un réseau local de contrôles d'accès et de profils d'usager à un ensemble de machines sur Internet.

Kerberos n'intègre pas de services de signature, permettant la certification permanente de documents, il peut néanmoins être employé pour administrer l'accès à des services. La nécessité de disposer de serveurs de clefs et de protéger ceux-ci contre d'éventuelles atteintes à la sécurité, fait que Kerberos est mieux adapté à un ensemble de domaines administrés (réseaux locaux et Intranet) qu'au réseau Internet.

On décrit ci-dessous un schéma d'identification de base. Tous les schémas employés sont des variantes de celui-ci. Partant de deux interlocuteurs Alice et Bob (deux personnages incontournables de toute littérature sur le cryptage) qui ont chacun un couple de clefs asymétriques, attestés par des certificats qu'ils se sont échangés :

- a. Bob (par exemple) expédie à Alice un document qu'il crée pour l'occasion et qu'on appelle un défi (*Challenge* en anglais). Soit **D** ce défi ;
- b. Alice va signer **D** par sa clef secrète. C'est à dire qu'elle génère une empreinte **E(D)**, qu'elle crypte avec sa clef secrète **CSA** pour former la signature électronique **SE(D) = CSA(E(D))** ;
- c. Alice génère une clef symétrique **CC**, avec laquelle elle crypte la signature de **D**, soit **CC(SE(D))** ;
- d. Elle transmet à Bob, le cryptage précédent accompagné de la clé symétrique **CC**, crypté par la clef publique de bob **CP**. Soit dans l'ensemble { **CC(SE(D))** ; **CP(CC)** }. La portion **CP(CC)** est appelée l'enveloppe électronique du message ;
- e. Bob décrypte l'enveloppe par sa clef privée et y trouve la clef **CC** avec laquelle il est en mesure de décrypter le document signé. Il peut vérifier l'identité de son interlocuteur en employant la clef publique d'Alice pour décrypter la signature et vérifier qu'il obtient bien l'empreint de défi ;
- f. Bob renvoie **D** à Alice, crypté par la clef Symétrique **CC** démontrant ainsi qu'il est celui qu'il prétend.

Après cet échange, Bob et Alice peuvent communiquer secrètement par des messages cryptés selon **CC**.

5. La datation

Pour dater un document, on utilise le principe de la signature en aveugle (*Blind signature*). Une signature en aveugle est une signature pratiquée sur un document par une identité qui n'a pas accès au contenu de ce document.

On peut ne présenter au signataire aveugle qu'une empreinte du document. Le signataire va la chiffrer par sa clef secrète, ce qui produit une signature valable pour le document d'origine. Il existe aussi des procédés pour *voiler* le document, le donner à crypter, puis retirer ensuite la voile et récupérer un document crypté par le signataire aveugle.

Il y a une foule d'applications comme les signatures de groupe, celles des autorités certifiantes par exemple. Pour dater un document, on va le faire signer en aveugle par un service de datation. Le cryptage asymétrique de ce service change à chaque instant et de façon aléatoire. Toutes les clefs publiques correspondant à chaque époque sont notoires et sont archivées. Pour vérifier la datation d'un document, il suffit de retrouver quelle clef publique était en vigueur à la date supposée. Le site de la compagnie *Surety Technologies* propose des systèmes de datation.

6. Le protocole SSL (*Secure Socket Layer*)

Le protocole SSL a été développé par Netscape pour offrir sécurité et confidentialité sur Internet. Ce protocole permet d'identifier clients et serveurs dans une connexion de type socket. SSL a bien entendu été implanté sur le navigateur Netscape. En fait, le mot Socket peut être défini comme la combinaison d'une adresse IP avec un numéro de port. Le protocole SSL

s'applique au niveau de la couche TCP/IP et il chiffre les communications entre le navigateur et les serveurs.

SSL s'inscrit comme une couche intermédiaire du protocole de communication (niveau session). Elle n'est pas liée à une application en particulier. Elle permet donc de sécuriser tout protocole existant d'application Internet, que ce soit HTTP, SMTP, Telnet, FTP ou NNTP et ce, sans modifier les logiciels.

Au démarrage de la session, le protocole SSL identifie le client et le serveur, puis négocie les paramètres de cryptage. Durant la session SSL assure la confidentialité et la fiabilité des échanges, par des techniques de cryptage et d'identification des messages. Au cours de la phase d'identification, le serveur expédie ses certificats et indique ses algorithmes de cryptage de prédilection. Le client génère ensuite une première clef, dite *clef maîtresse*, qu'il crypte par la clef publique du serveur avant de la lui expédier. Le serveur se fait connaître en retournant un message crypté par la clef maîtresse. Les échanges qui suivent sont cryptés par des clefs dérivées de la clef maîtresse.

L'identification du client est facultative. Le serveur expédie au client un message quelconque et le client s'identifie en retournant sa signature électronique sur ce message, accompagnée de ses certificats. SSL ne gère de signature que sur les messages prévus dans la phase d'identification.

7. Le protocole SET (Secure Electronic Transaction)

Le protocole SET a été développé conjointement par Visa, MasterCard, Microsoft, IBM et Netscape. En effet, le protocole SET est une spécification

technique qui vise à sécuriser au moindre coût les transactions par carte bancaire sur les réseaux ouverts tels Internet.

SET est indépendant du transport. Il peut par exemple fonctionner sur le Web en interactif. Pour ce faire, les messages de SET sont définis en tant que type MIME (Multipurpose Internet Mail Extension). Les transactions peuvent être très longues. Elles sont identifiées par un numéro unique repris dans tous les messages.

Les participants de SET (commerçants et acheteurs) possèdent deux couples de clefs asymétriques : un pour la signature des documents, un autre pour l'échange des clefs pendant la phase d'identification. On parle de clefs de signature et de clefs de cryptage. Les concepteurs de SET se sont en effet rendus compte que les deux usages des clefs asymétriques rencontraient des contraintes très différentes. En particulier :

- La clef publique de cryptage est employée pour crypter, la clef publique de signature pour décrypter ;
- Les clefs de cryptage peuvent avoir à être présentées en cas d'enquête ;
- Les clefs de signature sont plus cruciales. Elles doivent être plus fortes et mieux protégées. Personne ne doit obtenir votre clef secrète de signature.

Les certificats de SET représentent respectivement la carte de l'acheteur et l'autocollant apposé sur la vitrine du commerçant. Le certificat de l'acheteur ne mentionne pas le numéro de carte, ni aucun numéro de compte. Ceux-ci sont présents, mais voilés et seul le banquier peut les dévoiler.

SET innove avec le procédé dit de la signature duale, qui est employé pour faire une offre d'achat. Grâce à ce procédé, l'acheteur envoie simultanément son offre au commerçant et les instructions de paiement à la banque, en tenant compte des deux contraintes ci-dessous :

- Les deux sont mutuellement conditionnés, car le paiement ne doit être effectué que si l'offre est acceptée par le commerçant et la commande n'est effective que si la banque approuve le paiement ;
- Le contenu de la commande doit être caché à la banque et les instructions de paiement doivent être cachées au commerçant.

Pour éviter des aller retours complexes, une manœuvre élégante a été créée qui exploite les propriétés des empreintes électroniques.

Les deux messages (**O** = offre et **I** = instructions) sont réduits en deux empreintes électroniques **E(O)** et **E(I)**. Les empreintes sont concaténées puis réduites en signature **SC({E(O), E(I)})** par la clef publique de l'acheteur **C**. C'est la signature duale.

L'acheteur transmet l'offre au commerçant et les instructions à la banque. Il joint chacun des documents l'empreinte de l'autre et la signature duale. Ainsi, le message { **O**, **E(I)**, **SC({E(O), E(I)})** } est envoyé au commerçant et { **I**, **E(O)**, **SC({E(O), E(I)})** } est envoyé à la banque.

Les deux destinataires peuvent s'assurer de l'authenticité du message qu'ils reçoivent. Si le commerçant accepte l'offre, il transmet son acceptation à la banque, accompagnée de l'empreinte de l'offre. La banque est en mesure de faire le lien avec les instructions.

Le procédé réellement utilisé par SET est simplifié par rapport au procédé théorique ci-dessus, car aucun message n'est transmis de l'acheteur à la banque. Celle-ci est en mesure de reconstituer les mêmes instructions de paiement (**I**) à l'aide des informations bancaires sur l'acheteur et du prix présenté par le commerçant. Elle vérifie les intentions de l'acheteur en comparant l'empreinte des instructions **E(I)**.

SET entérine les normes de fait et effectue des choix définitifs. DES est employé pour le cryptage des messages. Les enveloppes électroniques forment une variante du format « PKCS#7 » de RSA. SET compte imposer ce format comme nouveau standard. Les signatures suivent les standards de RSA. Les empreintes sont réalisées par l'algorithme SHA-1 et les certificats sont au norme X.509.

La faiblesse de SET est qu'il s'agit d'un système à usage unique (paiement par carte). Le système ne permet pas de modifier le scénario ni d'y introduire de nouveaux intervenants. Cette caractéristique fait l'affaire des financiers. Les systèmes proposés par les informaticiens optent naturellement pour des transports sécurisés, ce qui élargit le champ d'applications. Néanmoins, les perspectives de SSL sont moins claires, car elles visent un champ d'applications encore plus vaste, qui déborde du Web.

V) Conclusion

L'arrivée d'Internet a littéralement révolutionné le monde des affaires. Réduisant temps et distances, ce nouvel outil de travail donne accès à une multitude de renseignements, en plus faciliter la communication partout à travers la planète, à toute heure du jour ou de la nuit, sept jours par semaine.

Cette nouvelle donnée dans le monde des affaires a ouvert la porte au commerce électronique, lequel élargit les marchés et les opportunités et convient tant aux grandes entreprises qu'aux petites et moyennes entreprises.

Pour les entrepreneurs d'aujourd'hui, le commerce électronique est un passage obligé pour faire partie du monde des affaires de demain. Les entreprises ont tout intérêt à effectuer le virage puisque les économies d'échelle et les possibilités d'affaires sont énormes.

Cependant dans le commerce électronique, les entreprises sont obligées à jumeler le savoir-faire et la technologie. Avant de passer à l'action, chaque entreprise est invitée à bien connaître ses besoins et ces objectifs et à préparer sa planification stratégique.

En général les entreprises et les consommateurs sont préoccupés par la sécurité des transactions commerciales sur le Web. En fait, Internet n'est qu'un média. C'est une extension du monde réel. Il est normal qu'on y trouve tas de gens intéressés et des commerçants honnêtes ; et aussi des voleurs et des menteurs. Sauf que dans le monde réel nous avons appris des réflexes.

Dans ce dossier j'ai présenté les moyens de paiement électronique disponible, les critères de fiabilité d'un processus de paiement et les techniques utilisées

par les banques et les informaticiens pour sécuriser les transactions entre les cyberconsommateurs et les sites marchands.

Le fait de savoir toutes les méthodes de paiement sur Internet et les protocoles de sécurité ; nous permet d'apprendre les réflexes nécessaires pour éviter la plupart des pièges du monde virtuel.

Enfin, il est primordial de mentionner que le passage lors du paiement électronique par un organisme intermédiaire digne de foi (serveur Kline, serveur Payline, autorité certifiante,...) tout en chiffrant les informations lors des transactions avec les clés disponibles et quel que soit le moyen de paiement est la solution la plus fiable. En effet, cette solution offre une voie de recours en cas de litige, elle permet de garder une trace de la commande et la veille sur la bonne conclusion de la transaction. Il faut noter toutefois que l'intervention d'un intermédiaire n'est pas gratuite mais elle permet d'en éviter la *plupart des risques*, car le risque zéro n'existe pas. Dans le commerce traditionnel non plus, d'ailleurs...

Bibliographie

ATI : Brochure publicitaire : Le commerce électronique, 2000.

Bernard MONTEH : article dans Micro hebdo : Vie numérique, mode d'emploi, Août 2002.

Chedly FEHRI : Cours de commerce électronique, Master spécialisé : commerce international et technologies de l'information à l'ISG de Sousse, 2002.

Habib YOUSSEF : Cours systèmes de télécommunication, Master spécialisé : commerce international et technologies de l'information à l'ISG de Sousse, 2002.

Laurent CARANI : Etude du paiement sur internet. Maîtrise : systèmes répartis de l'université du Québec à Montréal, Avril 1996.

Ludovic DE NAYER : Article dans Objet Multimédia : Le business sur le Web, 1999.

Malek BELARBIA : Cours de commerce électronique, Maîtrise en commerce international à l'ISG de Sousse, 2000.

Nadia BENNANI & Roumen ANDONOV & Didier DONSEZ : Eléments de cryptoanalyse.

Nadia BENNANI & Didier DONSEZ : Sécurité des systèmes d'information.

Réseau des SADC du Québec : Etude de commerce électronique, un outil d'affaires internationales, Mars 2001.