Edition Côte d'Azur

les ABM News

Les Aventuriers du Bout du Monde

N° 74N

Novembre 1999

Numéro spécial

Le commerce électronique et la sécurisation des paiements

E D I T O

A l'occasion du 4ième salon Capcyber je vous ai réalisé un numéro spécial entièrement consacré au commerce électronique.

Promis par les experts à un brillant avenir, soutenu par le gouvernement français, le commerce électronique se développe de jour en jour.

Près de 150.000.000 d'utilisateurs d'Internet dans le monde, des milliards de dollars qui circulent nécessitent des systèmes de sécurisations de paiements.

Certains systèmes de paiements sont très sophistiqués et utilisent la carte à puce, mais sont réservés, à ce jour qu'à un nombre limité d'utilisateurs, d'autres systèmes utilisent principalement le cryptage SSL..

Je vous ferai découvrir dans ce numéro deux systèmes de paiements sécurisés sur Internet Télécommerce et Paybox, deux systèmes que préconise le Crédit Agricole Provence Côte d'Azur.

Ce numéro est le premier consacré au commerce électronique et nous vous tiendrons informés de son évolution dans de prochains numéros de notre revue.

Yves Roger Cornil

www.cote-dazur.com/capca
www.cornil.com
yves.cornil@wanadoo.fr
yves.cornil@crpca.credit-agricole.fr

Les ABM *c'est le journal des clubs Microcam,* clubs de micro-informatique du Crédit Agricole.

dépôt légal 641 Rennes
ISSN 0295-938

MICROCAM06
111, Avenue Emile Dechame
B.P. 250
06708 Saint-Laurent-du-Var cedex
Mel: mcam06@worldnet.net

MICROCAM
19, rue du Pré-Perché
2025 X
35040 Rennes cedex
Mel: microcam@wanadoo.fr

Directeur de la publication :
Yves-Roger CORNIL

Maquette :
Bertrand Lemenant

Numéro réalisé par**:**

Yves Roger Cornil.

Extraits de LMB Actu et Internet Actu.
Frédéric Loos (IBS).
Site Télécommerce du Cédicam.
Reproduction: Service ERC-CRCAM Provence Côte d'Azur

Apple Performa 5300, Apple Select 360, HP Scanjet 5p, Adobe PhotoShop,Adobe PageMaker,Capture 4.2.,

N°74N

SOMMAIRE

Le Commerce Electronique et la sécurisation des paiements sur Internet.

Généralités sur Internet

Internet est un réseau mondial d'ordinateurs interconnectés (Web, toile) accessible, généralement, par l'intermédiaire d'un fournisseur d'accès au prix d'une communication locale.

Internet c'est:

- plus de 60.000.000 d'ordinateurs connectés aux Etats Unis.
- plus de 147.000.00 d'utilisateurs dans le monde en 98.

Les Etats-Unis mènent en nombre d'internautes avec 80 millions.

La France vient en septième position avec 2,79 millions, derrière l'Australie, le Canada, l'Allemagne, l'Angleterre, le Japon et les USA.

L'Europe totalise 36,2 millions d'internautes.

Au 15 janvier 1999, l'association française des fournisseurs d'accès (AFA) compte 1.280.000 abonnements individuels en France, correspondant à 11,2 millions d'heures de connexion mensuelles par le réseau téléphonique commuté (hors connexions par câble ou par liaisons spécialisées).

En trois mois, les abonnements ont progressé de 33% (+320 000) et le nombre d'heures de connexions de 40% (+3 200 000 heures). Par ailleurs, l'AFPI (association française des professionnels de l'Internet) rejoint l'AFA et, à cette occasion l'AFA, devient l'association des fournisseurs d'accès et de services Internet.

source: Le Micro Bulletin Actu 146 - 17 février 1999

Quels composants et combien ça coûte?

Que faut-il pour se connecter à Internet?

Un micro-ordinateur (PC ou Macintosh) pour un prix d'environ 10.000 F.

On peut trouver selon les périodes, et plus particulièrement dans la grande distribution des offres de PC à 4.990F ou 1990F plus 2 ans d'abonnement chez un fournisseur d'accès, voire même gratuit si vous aimez la pub ou que vous vous engagiez à acheter sur Internet un certain chiffre d'affaires (USA).

Ajoutez suivant les configurations :

- un modem connecté sur le port série de l'ordinateur ou une carte interne; le prix oscille entre 600F à 1.500F. Il existe des offres spéciales par exemple Wanadoo + Olitec à 290F.

- un système d'exploitation moderne (Windows 95 ou 98, MacOS 8.x, Unix). on peut constater la montée en puissance du système d'exploitation UNIX gratuit LINUX.

- un logiciel de navigation Netscape Communicator ou Microsoft Internet Explorer. Ces logiciels évoluent rapidement; début novembre 99 la version 5.0 est disponible pour Internet Explorer et 4.7 pour Netscape Communicator, aussi bien pour les plateformes Windows que MacOs.

- un abonnement à un fournisseur d'accès (Wanadoo, Nice Matin, Club-Internet ...) donnant accès à des communications lo-

cales, prix de 55F à 99F); on trouve certains abonnements gratuits, mais attention au coût des télécommunications (2,23 la minute pour certains gratuits !!!).

Personnellement j'utilise un abonnement Wanadoo à 75 F (avec l'offre Olitec à 290F) plus un abonnement gratuit à Free et encore un abonnement pour mon site avec un nom de domaine personnel (www.cornil.com).

- les communications téléphoniques :

15 F de l'heure le jour, 7,50 F le soir; réduction de 40% si Primaliste Internet à partir de 22 heures.

Depuis quelques semaines vous pouvez prendre le Libre Accès France Télécom; il s'agit d'un forfait de 100F par mois pour 20 heures de connexions.

Les mondes de la micro-informatique, de l'Internet et des communications évoluent très vite, aussi bien sur les puissances des ordinateurs, du nombre d'utilisateurs connectés et des prix.

Les principales fonctionnalités d'Internet

Consultations de pages (surf) grâce à un navigateur (les Canadiens disent butineur); les butineur les plus connus sont Netscape Communicator (ou Netscape Navigator suivant la version) et Microsoft Internet Explorer. Ces logiciels sont gratuits et le plus utilisé est à ce jour est Internet Explorer.

Messagerie électronique (Mel en français, E-mail en anglais) avec la possibilité de joindre des documents (texte élaboré, tableur, image, programme ...). Les logiciels de messagerie les plus connus sont Microsoft Outlook Express, Eudora, Netscape Messenger ...). Il existe des messageries qui fonctionnent à partir d'un navigateur (tel que Hotmail par exemple.

Transfert de fichiers (FTP, File Transfert Protocol) pour récupérer des films en format QuickTime ou AVI, des sons, des images, des programmes (une mise à jour d'un logiciel par exemple ou des pilotes pour un péripérique particulier ...).

Le FTP est utilisé aussi pour mettre à jour vos propres pages (ou une fonction FTP comprise dans un logiciel de création de page).

Un peu de technique.

L'information circule sur le Net (comprenez Internet ou le Web) selon le protocole de commutation de paquets TCP/IP.

L'adresse peut être sous la forme d'une suite de 4 nombres consécutifs séparés par un point (185.44.60.1 par exemple) ou sous une dénomination plus explicite (www.credit-agricole.fr).

La transformation entre le nom (qu'on appelle généralement nom de domaine) et les numéros TCP/IP est réalisé par un serveur de nom appelé DNS.

Les suffixes du DNS indiquent une activité (.com pour commercial, .org pour une organisation ...) ou un pays (.fr pour la France, .uk pour le Royaume Uni, .be pour la Belgique ...)

Chaque page consultable sur Internet a une adresse précise nommée URL (Uniform Resource Location).

Dans les navigateurs, l'adresse est sous la forme:

http://nom1.nom2.nom3

Exemples:
http://www.cote-dazur.com/capca
http://www.augfrance.com/
http://www.augfrance.com/Microcam06
http://yves.cornil.free.fr

Le commerce sur Internet

Il existe plus de 50.000 sites français à vocation commerciale. A la fin de 1998, 3,3 milliards de F avaient été dépensés par les internautes dans l'hexagone contre 1,2 milliards en 1997. (source LMB Actu)

Selon une récente enquête du cabinet d'études Stratégie Internet, les sites marchands ont plus que doublé leur audience en un an: 200.000 Français, soit 10% des internautes, ont déjà acheté en ligne. Le chiffre d'affaires mensuel moyen des sites marchands est de 50.000 francs. Le commerce électronique permet aux petits et moyens commerces d'être présents sur tous les marchés mondiaux, (source AFP/12/01/99).

Le cabinet d'études Dataquest prévoit que les ventes en ligne vont tripler cette année pour la période de Noël par rapport à l'année dernière. Les marchands en ligne se réjouissent d'avance du chiffre d'affaires de 12 milliards de $US annoncé par Dataquest. En 1998, ce chiffre était de 4,5 milliards de $US. "Les Etats-Unis domineront avec 70% des ventes en ligne. L'Europe suivra avec 15,5%, tandis que la zone Asie-Pacifique représentera 7% du commerce électronique, cette saison", déclare le cabinet d'études. (source Internet Actu du 21/10/99)

Il y a en France une volonté politique de développer l'Internet en France (discours d'Hourtin en août 97) ainsi que le commerce électronique (rapport Francis Lorentz).

Une baisse des prix des micros déja constaté en France devrait accélérer le mouvement, mais il faudrait continuer à baisser de façon significative le coût des télécommunications pour assurer un vrai décollage de l'Internet en France.

Qui vend sur Internet ?

Secteur d'activité qui veut:

- se diversifier
- créer une activité commerciale nouvelle; on voit se développer des commerces qui n'existent que sur Internet. C'est un moyen de toucher des clients nouveaux, en particulier dans les pays qui n'ont pas le minitel.
- augmenter ses marges commerciales; pas de frais de catalogues, la saisie est faite par le client.

Les secteurs porteurs :

- biens, services, information normalisé, en particulier l'informatique (Dell, Apple...), voyages (DegriffTour ...),
- loisirs, spectacles, livres, cédéroms (Amazon , FNAC, Furet du Nord, Boxman ...)

images de marque: cadeaux, alimentation, vins .... et même des voitures

Le commerce inter-entreprises tend à se dévopper fortement, surtout outre atlantique.

Les critères : prix, service, disponibilité.

Comment vendre sur Internet ?

Une entreprise passe généralement par plusieurs phases avant d'ouvrir un site marchand:

- simple connexion pour découvrir l'Internet, visiter de sites pour trouver éventuellement des idées.

- ouverture d'une vitrine "institutionnelle" pour présenter l'entreprise, les produits, les services et sutout être confronté à la mise à jour fréquente des informations sur Internet.

- vente de produits avec 2 modes de paiements :

- off line (chèque, contre remboursement) .

- transmission du numéro de CB par fax

- en ligne (saisie directe du numéro de carte sur l'Internet par le client).

Vendre sur l'Internet est un nouveau métier; l'entreprise doit maîtriser les techniques de la Vente Par Correspondance (VPC) et ces nouvelles méthodes doivent s'exercer dans un contexte mondial, sauf si l'entreprise se limite à l'hexagone ou à certains pays.

Le commerçant doit faire appel à des professionnels pour la création des pages (graphistes, informaticiens) et ainsi que pour l'hébergement de son site.

Les risques de fraudes sur Internet

Différents cas de fraudes peuvent se présenter sur Internet:

- Réutilisation de numéros de cartes volées.
- Capture au fil de l'eau par le réseau TCP/IP.
- Attaque de serveurs commerçants pour récupérer des numéros de cartes valides.
- Faux numéro de cartes, générés par des serveurs; les numéros de cartes peuvent correspondre à une carte existante.
- Création de fausses enseignes (en clair le commerçant n'existe pas).

Le régime de la VPC (Vente par Correspondance) s'applique et en cas de constation d'un paiement par un client, le préjudice est supporté par le commerçant

Comment sécuriser le paiement par carte sur Internet?

Un système de paiement sécurisé , devra, au minimum vérifier

- qu'il n'y a pas d'opposition sur la carte,
- le numéro de carte ne circulera pas en clair sur le réseau, il devra donc être crypté pendant le tranfert entre le poste du client et le poste du commerçant . Ce cryptage est assuré par le navigateur par le système SSL (Secure Socket Layer) de Netscape. Le cryptage pourra porter sur une clé plus ou moins longue (40 bits, 64 bits ou plus). Le gouvernement français a libéralisé il y a quelques mois les contrainres réglementaires du cryptage.

Le paiement sécurisé pourra passer par un intermédiaire, par exemple les systèmes Paylaine (SG2), Cybercash (Sligos), Kleline (Compagnie Bancaire), Paybox System (IBS) ou utiliser un système propre à la banque.

La réponse des banques pour sécuriser les paiements sur Internet.

En 1997 les réseaux MasterCard et Visa (400 millions de cartes et 12 millions de commerçants) ont mis en place un système sécurisé.

Il s'agissait d'un paiement par carte, sécurisé, entre acteurs monétiques (SET, Secure Electronic Transaction).

Sans rentrer dans le mécanisme complexe mis en place, il y a délivrance d'un certificat, stockage sur le disque dur du client ou sur une disquette; la protection est assurée par un mot de passe et le numéro de carte est chiffré.

Quant au Groupement Carte Bancaire (25 millions de porteurs, 500.000 commerçants) il a mis en place fin 1997 un paiement par carte, très sécurisé appelé C-SET (Chip Secure Electronic Transaction), le chip étant la puce de la carte bancaire .

Le système était fait pour permettre aux acteurs du paiement de s'authentifier réciproquement (le client et le commerçant) lors d'un paiement en utilisant des certificats délivrées par les banques et stockés sur la puce de la carte du client.
La protection du certificat, et donc la sécurisation du paiement est assuré par la frappe du code confidentiel de la carte bancaire.

Ce système nécessitait un lecteur sécurisé fabriqué par Bull. C'est une sorte de TPE qui se connectait sur le port série du PC ou du Macintosh.

Le numéro de carte n'apparaît jamais, ni sur le réseau, ni dans le micro-ordinateur, ni chez le commerçant.

La somme à valider s'affiche sur le lecteur, comme sur un TPE (pour éviter qu'un programme type «cheval de Troie» modifie la somme affichée sur l'ordinateur du client.

Il y a interopérabilité entre Set et C-Set.

Au niveau des appellations commerciales le premier système s'appelait E-Comm et le second Cybercard. Le Crédit Agricole avait opté pour Cybercard et avait lancé une campagne de tests sur une centaines de commerçants et quelques milliers de clients.

Vous devez vous demander pourquoi je parle au passé de ces deux opérations de sécurisations franco-françaises E-comm et Cybercard (encore que sur les noms il y aurait à redire), c'est parce que les deux systèmes sont en cours de convergence pour donner Cyber-Comm.

Un premier test devrait avoir lieu dans la semaine du 24 novembre et la mise sur le marché devrait avoir lieu en février 2000. Un nouveau lecteur de carte utilisant le protocole USB serait utilisé.

La première version délivrée serait pour les plateformes Windows, pour MacOs il faudrait attendre plus tard.

QUEST-CE QUE LE COMMERCE ÉLECTRONIQUE?

Il s'agit de toute forme de vente à distance utilisant des médias électroniques. A ce titre, la vente par Minitel, ou le téléachat font partie du commerce électronique. Mais c'est bien entendu l'Internet qui représente le plus fort potentiel dans ce domaine, du fait de son caractère mondial, du nombre d'utilisateurs connectés, et de la richesse et de la souplesse qu'offre le Web. Documents multimédia, hypertexte, simplicité des mises à jour ...tout concourt au développement de nouvelles activités commerciales et à la création de nouveaux.
métiers.

QUELS SONT LES AVANTAGES DE L'INTERNET POUR LES CONSOMMATEURS ET LES VENDEURS?

L'Internet permet à des millions d'Internautes et un nombre considérable d'entreprises de se rencontrer 24 h / 24h, sans contrainte de temps ou de distance. Comparaison des produits, des services, des prix, personnalisation des relations avec la clientèle, fidélisation... On le voit, les atouts d'Internet sont considérables et permettent à une entreprise de disposer d'un nouveau canal de distribution, et de multiplier les ouvertures vers l'extérieur. Elle doit apprendre à s'adapter à ce nouveau contexte, et intégrer l'Internet dans sa stratégie.

QUELQUES CHIFFRES.

Parcque Internet ne dépend d'aucune organisation, il est difficile d'avoir des chiffres fiables sur le nombres d'internautes dans le monde ainsi que le chiffre d'affaire réalisé. Cependant on peut citer quelques chiffres à titre indicatif.

- plus de 147.000.00 d'utilisateurs dans le monde en 1998.

Les Etats-Unis mènent en nombre d'internautes avec 80 millions.

L'Europe totalise 36,2 millions d'internautes et le nombre d'internautes en France avoisinne les 3 millions.

Au 15 janvier 1999, l'association française des fournisseurs d'accès (AFA) comptait 1.300.000 abonnés.

Le cabinet d'études Dataquest prévoit que les ventes en ligne vont tripler cette année pour la période de Noël par rapport à l'année dernière. Les marchands en ligne se réjouissent d'avance du chiffre d'affaires de 12 milliards de $US annoncé par Dataquest. En 1998, ce chiffre était de 4,5 milliards de $US. "Les Etats-Unis domineront avec 70% des ventes en ligne. L'Europe suivra avec 15,5%, tandis que la zone Asie-Pacifique représentera 7% du commerce électronique, cette saison", déclare le cabinet d'études.

(source Internet Actu du 21/10/99)

QUEL MODE DE PAIEMENT CHOISIR SUR INTERNET?

Internet permet une très grande diversité d'échanges économiques. Dans ce contexte, le moyen de paiement le plus adapté pour acheter sur le Net est incontestablement la carte bancaire CB, MasterCard ou Visa. Plus de 900 millions de cartes sont en circulation dans le monde, qui permettent dès aujourd'hui des paiements au plan national ou international. Et la simplicité du paiement, tant pour l'acheteur que pour le vendeur, la promettent à un bel avenir sur ce réseau.
Depuis fin 1997 il est possible, pour certains priviligiés, avec un lecteur de carte à puce de payer dans des conditions proches du commerce traditionnel (cf article sur Cybercard). Les toutes petites transactions seront bientôt facilitées, grâce notamment au porte-monnaie électronique.

Télécommerce

C'est quoi Télécommerce?

Télécommerce est une offre intégrée de commerce sur Internet, opérée par France Telecom et le Crédit Agricole (ajoutez maintenant la BNP et le Crédit Lyonnais) qui permet de gérer les fonctions essentielles nécessaires à la vente sur le Net :

- La mise en valeur de la boutique et aide à la vente,
- La gestion des paiements,
- La gestion du back office.

Si le commerçant ne dispose pas encore d'un site sur Internet, il est possible de lui proposer, en option, des solutions de front office :

- création de boutique,
- hébergement,
- accès à Internet.

Que fait-on avec Télécommerce?

Les fonctions gérées par Télécommerce concernent :

- La mise en valeur de la boutique et l'aide à la vente:

- Site www.telecommerce.fr
- Référencement dans les sites d'audience de France Telecom sur le Web, et notamment sur Wanadoo et Voilà.
-Création d'un label Télécommerce, et actions de communication des partenaires
- Possibilité de gérer des fonctions de type coupons électroniques, et demain d'autres solutions de fidélisation

- La Gestion des paiements

- Paiement par Carte Bancaire, carte Eurocard/ MasterCard ou Visa, avec des solutions diverses et évolutives, gérées par le Crédit agricole;
- Ouverture demain à d'autres solutions de paiement.

- La gestion du back office

- Gestion du bon de commande, du reçu
- Déclenchement de la livraison en ligne (vente de biens en ligne)
- Archivage des transactions
- Suivi des commandes
- Déclenchement du règlement, à la demande du marchand
- Réclamations
- Gestion d'abonnements (vente de biens en ligne).

Le paiement et Télécommerce

L'intérêt de la carte bancaire dans Telecommerce.

La carte bancaire est l'instrument privilégié de paiement sur Internet. En effet, du fait de l'existence des réseaux Eurocard / MasterCard ou Visa, c'est le produit le plus adapté au caractère mondial de l'Internet, les opérations empruntant des circuits internationaux sûrs et rodés.

Par ailleurs, elle facilite les achats d'impulsion, la communication du numéro de carte bancaire par le client étant très simple. .Enfin, elle vous permet de simplifier le suivi des ventes : le paiement se réalisant en même temps que la commande, vous n'avez pas à

QUEST-CE QUE LE COMMERCE ÉLECTRONIQUE?

Il s'agit de toute forme de vente à distance utilisant des médias électroniques. A ce titre, la vente par Minitel, ou le téléachat font partie du commerce électronique. Mais c'est bien entendu l'Internet qui représente le plus fort potentiel dans ce domaine, du fait de son caractère mondial, du nombre d'utilisateurs connectés, et de la richesse et de la souplesse qu'offre le Web. Documents multimédia, hypertexte, simplicité des mises à jour ...tout concourt au développement de nouvelles activités commerciales et à la création de nouveaux.
métiers.

QUELS SONT LES AVANTAGES DE L'INTERNET POUR LES CONSOMMATEURS ET LES VENDEURS?

L'Internet permet à des millions d'Internautes et un nombre considérable d'entreprises de se rencontrer 24 h / 24h, sans contrainte de temps ou de distance. Comparaison des produits, des services, des prix, personnalisation des relations avec la clientèle, fidélisation... On le voit, les atouts d'Internet sont considérables et permettent à une entreprise de disposer d'un nouveau canal de distribution, et de multiplier les ouvertures vers l'extérieur. Elle doit apprendre à s'adapter à ce nouveau contexte, et intégrer l'Internet dans sa stratégie.

QUELQUES CHIFFRES.

Parcque Internet ne dépend d'aucune organisation, il est difficile d'avoir des chiffres fiables sur le nombres d'internautes dans le monde ainsi que le chiffre d'affaire réalisé. Cependant on peut citer quelques chiffres à titre indicatif.

- plus de 147.000.00 d'utilisateurs dans le monde en 1998.

Les Etats-Unis mènent en nombre d'internautes avec 80 millions.

L'Europe totalise 36,2 millions d'internautes et le nombre d'internautes en France avoisinne les 3 millions.

Au 15 janvier 1999, l'association française des fournisseurs d'accès (AFA) comptait 1.300.000 abonnés.

Le cabinet d'études Dataquest prévoit que les ventes en ligne vont tripler cette année pour la période de Noël par rapport à l'année dernière. Les marchands en ligne se réjouissent d'avance du chiffre d'affaires de 12 milliards de $US annoncé par Dataquest. En 1998, ce chiffre était de 4,5 milliards de $US. "Les Etats-Unis domineront avec 70% des ventes en ligne. L'Europe suivra avec 15,5%, tandis que la zone Asie-Pacifique représentera 7% du commerce électronique, cette saison", déclare le cabinet d'études.

(source Internet Actu du 21/10/99)

QUEL MODE DE PAIEMENT CHOISIR SUR INTERNET?

Internet permet une très grande diversité d'échanges économiques. Dans ce contexte, le moyen de paiement le plus adapté pour acheter sur le Net est incontestablement la carte bancaire CB, MasterCard ou Visa. Plus de 900 millions de cartes sont en circulation dans le monde, qui permettent dès aujourd'hui des paiements au plan national ou international. Et la simplicité du paiement, tant pour l'acheteur que pour le vendeur, la promettent à un bel avenir sur ce réseau.
Depuis fin 1997 il est possible, pour certains priviligiés, avec un lecteur de carte à puce de payer dans des conditions proches du commerce traditionnel (cf article sur Cybercard). Les toutes petites transactions seront bientôt facilitées, grâce notamment au porte-monnaie électronique.

gérer des dossiers en instance, dans l'attente de l'arrivée d'un chèque ou virement.

Une solution de paiement sur Internet fiable, pérenne et évolutive

La sécurisation des échanges sur Internet via SSL est actuellement un standard du marché. Dans le cadre de Telecommerce, elle permet de chiffrer la transmission du numéro de carte bancaire, et d'assurer l'authentification du site du commerçant, ce qui représente une garantie pour l'acheteur.

Le paiement par carte bancaire, géré par le Crédit agricole, donne lieu à une demande d'autorisation systématique. Il apporte au commerçant une solution de paiement efficace, permettant de disposer d'un potentiel d'acheteurs de plus de 900 millions de personnes dans le monde.

Une formule évolutive

Aujourd'hui, Télécommerce accepte les paiements par carte CB, Eurocard/ MasterCard ou Visa. D'autres formules de paiement seront progressivement intégrées: paiement avec carte à puce et lecteur de carte, paiement via le protocole SET, etc...Et pour répondre à tous les besoins, des solutions permettant de gérer de tout petits paiements, mais aussi des formules de crédit à la consommation, seront intégrées au fur et à mesure de leur disponibilité. La présence du Crédit Agricole dans Télécommerce est, pour les clients, la garantie d'une intégration progressive et simple de solutions de paiement permettant de couvrir toutes leurs attentes.

Vous êtes consommateur.

Télécommerce intègre une solution de paiement sur Internet fiable, pérenne et évolutive.

Les trois atouts de Télécommerce pour vous, consommateur sur Internet, résident :

- dans la simplicité: vous êtes titulaire d'une carte bancaire, CB, MasterCard ou Visa, vous avez la possibilité de payer auprès de tout marchand Télécommerce sans formalité;
- dans l'authentification du site du commerçant : l'agrément Télécommerce est une véritable garantie;
- dans le chiffrement du bon de commande et du numéro de carte : Télécommerce offre une réelle confidentialité et une totale intégrité. Une fois l'achat réalisé, votre numéro de carte sera stocké, non pas sur le site du commerçant, mais directement sur la plate-forme Télécommerce, dans une base de données, extrêmement protégée par des barrières infranchissables (système de firewall).

Vous êtes marchand.

Il est possible d'établir une comparaison entre les fonctions nécessaires pour vendre dans le cadre du commerce de proximité, et leur équivalent sur Internet. Ces fonctions se répartissent entre " Avant Vente " (le front office), et " Après Vente " (le back office).

L'offre de base de Télécommerce est à cheval sur ces deux types de fonctions. Et si la création de la boutique, son hébergement et l'accès à Internet ne font pas directement partie de Télécommerce, le Crédit agricole pourra proposer au marchand des solutions permettant de couvrir ce type de besoin.

1 - L'Internaute navigue dans la boutique de marchand et choisit ses articles.
2 - Le site du marchand lui transmet, en ligne, le bon de commande électronique.
3 - L'Internaute le valide, saisit ses coordonnées, ainsi que celles de sa Carte Bancaire. L'ensemble est chiffré, et routé automatiquement vers la plateforme Telecommerce. La plateforme vérifie les informations reçues, et se connecte au Crédit Agricole pour le trairement du paiement.
4 - Le Crédit Agricole gère la demande d'autorisation via les circuits interbancaires, et transmet la réponse à la plateforme 5.
6 - La réponse est stockée sur les bases de données de la plate-forme Télécommerce
7 - La réponse est transmise à l'Internaute, en ligne avec la référence de la transaction. Elle est communiquée au marchand, suivant des modalités convenues au préalable (e-mail, fax ...)
8 -
9 - Le Crédit Agricole traite ensuite le paiement, et l'introduit dans les circuits de compensation interbancaires.
10 - Après règlement par la banque de l'Internaute, le Crédit Agricole crédite lecompte du commerçant.

Saisie des coordonnées du client

Affichage du récapitulatif de la commande et saisie de numéro de carte et date de validité. Notez que le cadenas (en bas, à gauche) est fermé, indiquant que nous sommes en présence d'une page sécurisée par SSL.

1,2,3 Spresso
Reçu électronique

Nous vous remercions pour votre commande, votre paiement a été accepté par le système de paiement partenaire.
Votre commande est réalisée et suivie à l'aide de Télécommerce, un service de France Télécom.

N° de commande	N° du magasin	Date
100008	400398	15 mars 1999

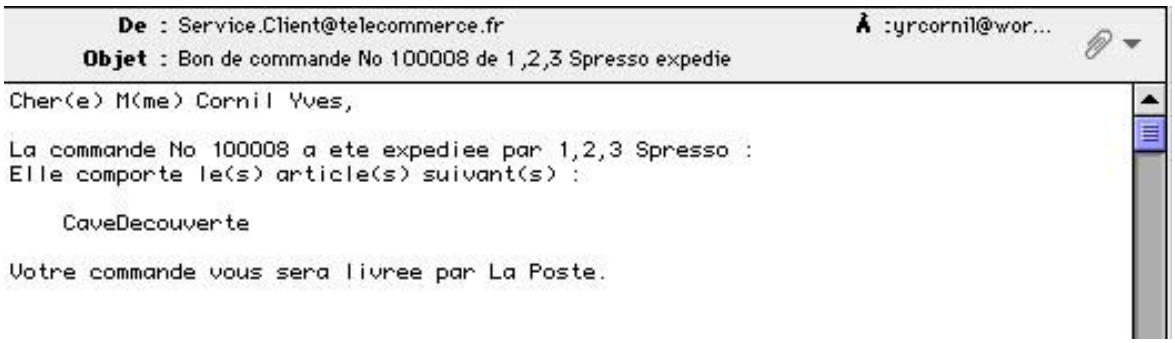
N° de transaction bancaire : 35465

Confirmation de l'acceptation du paiement.

Pour conserver une trace de votre commande et suivre l'état de votre livraison indiqué sur ce reçu, vous pouvez :

- imprimer / sauvegarder ce reçu,
- ou de préférence, l'ajouter à votre liste de signets (bookmarks, favoris);
- Si vous vous êtes inscrit au préalable à Télécommerce, ce reçu serait disponible dans votre Service Client Télécommerce. Cliquez ici pour vous inscrire.

Acheté par	Colis à livrer à	Payé à
Cornil Yves Credit Agricole 111 avenue Emile Dechame 06708	Cornil Yves Credit Agricole 111 avenue Emile Dechame 06708 06 St Laurent du Var	1,2,3 Spresso CMC Malongo ZI 9ème rue 06513 Carros France metropolitaine



De : Service.Client@telecommerce.fr
À :yrcornil@wor...
Objet : Bon de commande No 100008 de 1,2,3 Spresso expedie

Cher(e) M(me) Cornil Yves,

La commande No 100008 a ete expediee par 1,2,3 Spresso :
Elle comporte le(s) article(s) suivant(s) :

CaveDecouverte

Votre commande vous sera livree par La Poste.

Email de confirmation reçu par le client.

Pour goûter à Télécommerce
(et aux cafés Malongo)

www.123spresso.com

Télécommerce en douze points.

En adhérant à Télécommerce, le marchand sait sur le plan commercial :

1 - Que le consommateur, quel que soit son pays d'origine, achète sur son site Web en toute confiance et qu'il n'a pas de logiciel spécifique à télécharger. Le marchand bénéficie de l'apport d'affaires du label Télécommerce.

2 - Que Télécommerce lui assure la promotion de son site sur les sites d'audience de France Télécom, site Télécommerce, Wanadoo, Voilà, pour en optimiser la fréquentation.

3 - Qu'il est un des premiers marchands en France à disposer, en standard, d'une solution de coupons électroniques de réduction.

4 - Que France Telecom met en place des programmes pour l'aider à fidéliser ses clients et leur faire parvenir des promotions personnalisées, et lui permettre de bénéficier de toutes les fonctions avancées d'Internet appliquées au merchandising : technologies push, moteurs de recherche, hauts débits.

5 - Que Télécommerce lui proposera un choix d'options de plus en plus large ; micropaiements, service logistique clé en mains, multilinguisme, centre d'appels Télécommerce.

sur le plan logistique :

6 - Qu'il bénéficie du service le plus complet : Télécommerce calcule les taxes et les frais de port, enregistre et conserve la trace des commandes, le renseigne sur l'état de ses commandes 24h sur 24h.

7 - Que chaque paiement par carte bancaire fait l'objet d'une demande d'autorisation à la banque et qu'il dispose donc de toutes les garanties de paiement dans le cadre de la réglementation s'appliquant à la Vente à Distance.

8 - Qu'il dispose à tout moment d'une capacité illimitée de traitement des commandes en cas d'affluence sur sa boutique.

sur le plan technique :

9 - Qu'il peut s'appuyer sur le réseau de professionnels de l'Internet agréés Télécommerce, pour l'aider à créer et exploiter son site Web.

10 - Qu'il dispose avec le service Télécommerce d'un outil simple et performant de paramétrage de sa boutique et d'un numéro d'appel pour toute assistance.

11 - Qu'il n'a pas à investir sur des outils techniques de sécurisation, de paiement et de " back-office ".

12 - Que la plate-forme Télécommerce intègrera les dernières innovations en matière de sécurisation des paiements et ce, sans impact sur le coût de traitement des transactions.

Paybox

Le paiement par Carte Bancaire.

Aujourd'hui, on estime que plus de 147.000.000 d'utilisateurs d'Internet dans le monde (cf ABM 74N page 4). 3,3 milliards de francs ont été dépensé par les internautes en 1998 (cf ABM 74N page 6).

Le mode de paiement le plus utilisé sur Internet est et restera assurément la carte bancaire.

Les paiements par carte bancaire peuvent être réalisés de 2 façons:

- **Paiement de Proximité**: par carte à puce uniquement, avec saisie et contrôle du code confidentiel. Ceci nécessite un lecteur de carte à puce sur le site de l'achat, en présence de l'acheteur. C'est ce type de paiement que l'on fait dans un magasin, un supermarché ou à une pompe à essence.
- **Vente Par Correspondance ou à distance** (VAD/VPC): utilisation du numéro embossé sur la carte, et de la date d'expiration (AA/MM). Cette méthode ne nécessite pas la présence de l'acheteur et du vendeur sur le même site. Le numéro de carte peut être communiqué par l'acheteur au vendeur via différents moyens (courrier, fax, téléphone et...**Internet**).

Nous avons vu précédemment qu'il était possible de s'équiper d'un lecteur sécurisé (Cybercard, E-Comm, cf ABM 74N page8) mais que ces matériels sont encore au stade expérimental. D'autre part tous les pays n'utilisent pas encore la carte à puce (les Etats Unis en particulier) ce qui limite ainsi le champs d'utilisation des lecteurs sécurisés à puce, ce qui n'empêcherait pas les commerçants français de proposer des solutions hautement sécurisées aux clients français.

Depuis plusieurs années, la vente par correspondance utilise la carte bancaire par des moyens traditionnels. Des millions d'acheteurs communiquent chaque jour leur numéro de carte par téléphone, courrier, télécopie, sans autre garantie que la confiance accordée au vendeur.

L'internet est un nouveau support du commerce tout à fait adapté à l'utilisation de la carte bancaire en mode VAD/VPC.

Il est déjà possible de payer en ligne sur l'Internet, sans code confidentiel, avec un niveau de sécurité et de confidentialité bien supérieur aux moyens classiques, depuis n'importe quel ordinateur relié au Web, sans équipement ou logiciel spécifique, ce qui représente un marché gigantesque accessible aujourd'hui!.

Cependant l'étendue nouvelle des marchés au niveau mondial amène des risques potentiels de fraude (cf ABM 74N page 7) au détriment des porteurs de cartes bancaires et donc obligent les commerçants à utiliser des systèmes de paiements qui soient sécurisés.

Des techniques comme **SSL** (Secure Socket Layer) permettent de crypter très efficacement les données sensibles comme un numéro de carte bancaire.

Développée par Netscape, cette technologie permet de crypter la totalité des échanges entre deux ordinateurs reliées à l'Internet. Elle utilise une clé de cryptage à 40 bits (et 128 bits, autorisé depuis peu en France).

Dans le cas d'une opération de paiement, SSL sert à crypter le numéro et la date d'expiration d'une carte, saisi sur le clavier de l'acheteur, avant son envoi vers le système de télépaiement.

Ce système ne requiert aucun logiciel ou matériel particulier sur l'ordinateur du porteur (acheteur), en dehors des outils de navigation Internet disponibles sur le marché.

A ce jour, plus de 80% des commerces sur Internet utilisent SSL pour sécuriser leurs paiements.

La récente disponibilité de SSL avec des clés 128 bits renforce encore la sécurité, et peut repousser la nécessité de passer au paiement avec code confidentiel.

Les objectifs d'IBS.

En 1998, IBS, avec plus de 10 ans d'expérience en monétique, s'est engagé dans la réalisation d'un système de paiement sur Internet permettant d'offrir une solution simple aux acteurs du commerce électronique :

- Aux **commerçants** voulant vendre des produits ou services sur Internet, souhaitant sécuriser et gérer leurs transactions de paiement, en gardant leur banque actuelle, sans investir lourdement sur un marché qui émerge.
- Aux **hébergeurs, gérants de galeries virtuelles, fournisseurs d'accès, créateurs de sites**, souhaitant intégrer à leurs offres un service de paiement sécurisé simple à mettre en oeuvre et sans surcoût important pour les hébergés.
- Aux **établissements bancaires,** désirant répondre aux besoins de leurs clients commerçants, tout en gardant une monétique traditionnelle, utilisant des protocoles bancaires normalisés et des contrats standards (vad/vpc).
- Aux **acheteurs potentiels sur l'Internet**, soucieux de la sécurité et de la confidentialité de leurs paiements.

Depuis Septembre 1998, IBS propose un TPE Virtuel, (Terminal de Paiement Electronique) conçu spécifiquement pour accepter les paiements réalisés sur l'Internet, appelé PAYBOX.

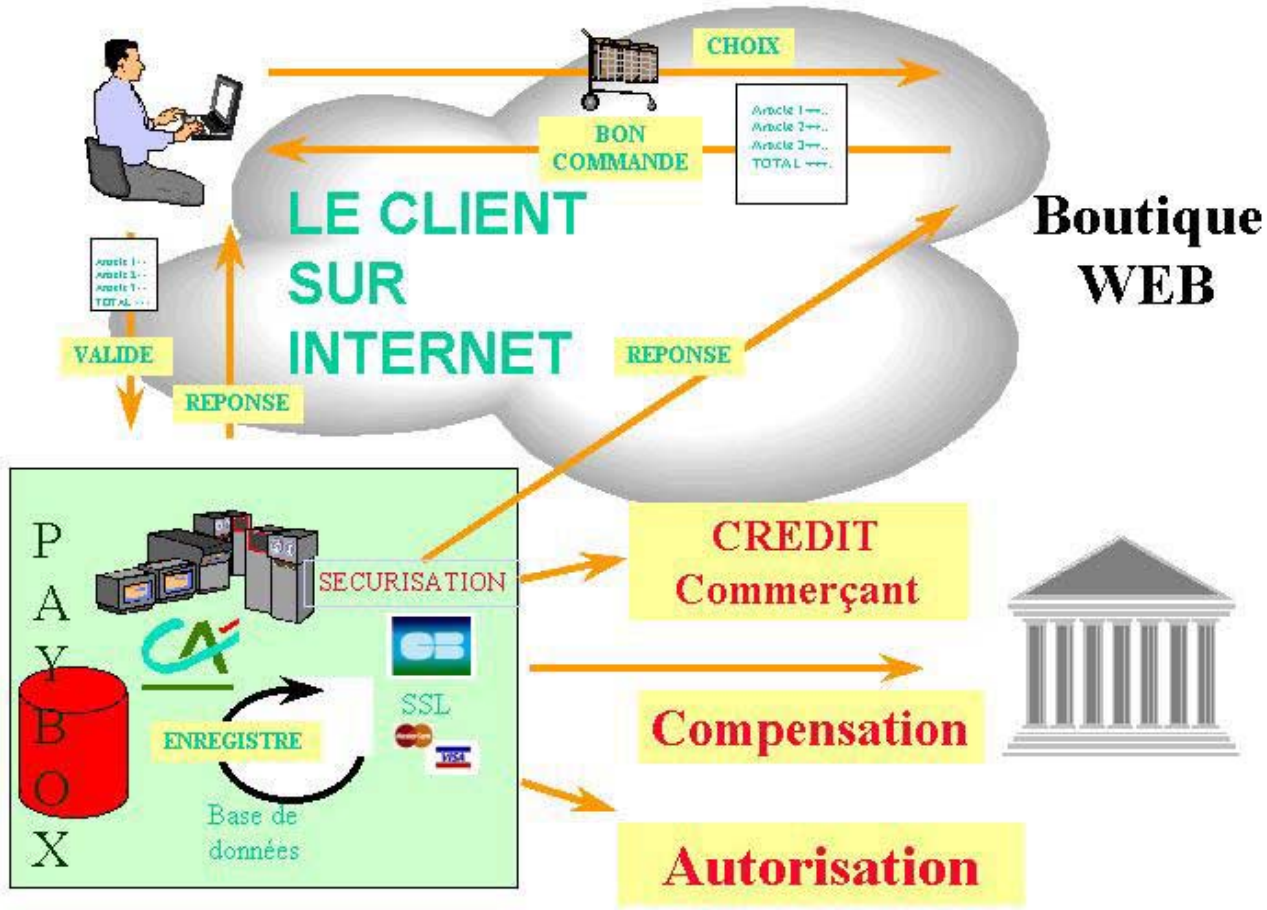
D'un point de vue fonctionnel, il est strictement identique, pour le commerçant, la banque et l'acheteur, à un TPE en mode VAD/ VPC (Vente A Distance/ Vente Par Correspondance):

- Pour le commerçant, il suffit de demander l'ouverture d'un contrat VAD/ VPC à sa banque habituelle, pour être directement crédité sur son compte (aucune autre ouverture de compte n'est nécessaire). Le service de paiement sécurisé PAYBOX s'intègre facilement sur son site Internet.

- Pour la banque, PAYBOX est vu comme un TPE en mode VAD/VPC, parmi les 700.000 TPE du parc français. Il se connecte aux centres de télécollecte et d'autorisation de n'importe quelle banque, en utilisant les protocoles normalisés CBSA, CBPR (et CBPR Euro), définis par le Groupement des Cartes Bancaires (GCB).

- Pour l'acheteur (porteur de la carte bancaire), aucun logiciel spécifique n'est requis. PAYBOX lui assure également que son numéro de carte bancaire n'est connu que de PAYBOX (pas du commerce), et que le commerce auquel il s'adresse a été authentifié préalablement par IBS.

Réalisation d'un achat avec Paybox



1) Depuis son ordinateur équipé d'un navigateur Web, le client se connecte par Internet au commerce de son choix. Il sélectionne les articles ou les services qu'il désire acheter. En général, une boutique virtuelle sur Internet utilise un logiciel simulant le remplissage d'un 'caddy': le client choisit ses articles et les dépose dans un panier.

2) Lorsque la sélection est terminée, l'utilisateur donne au commerçant les informations nécessaires à l'expédition de sa commande: Nom, adresse postale, téléphone et adresse e-mail. Ceci se fait habituellement par l'intermédiaire d'un formulaire 'en ligne' que le client remplit.

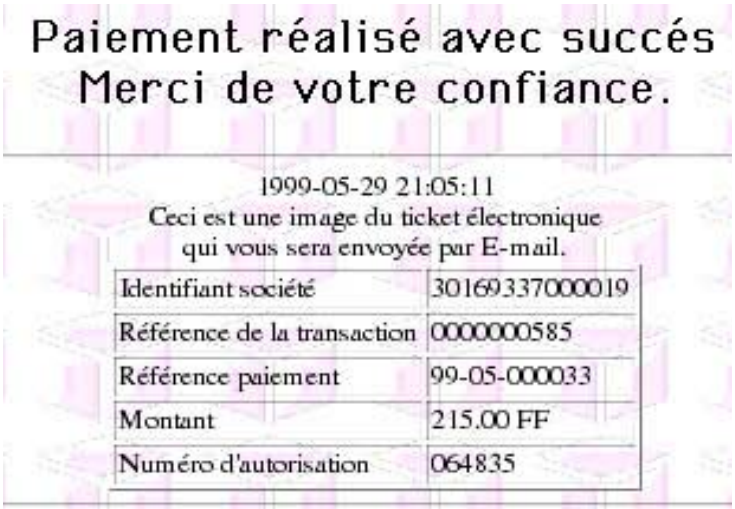
4) Le client n'a plus qu'à confirmer l'acceptation ou le refus de sa commande. Il peut éventuellement la modifier. Lorsque tout est conforme à son choix, il peut alors cliquer sur un bouton qui va activer l'opération de paiement (ici le bouton paiement sécurisé).
A ce stade, le logiciel de la boutique virtuelle du commerçant possède toutes les informations utiles pour réaliser une vente, à l'exception du numéro de carte bancaire. Certaines de ces informations vont être 'transférées' sur le serveur **PAYBOX** d'IBS: numéro et montant de la commande, devise, e-mail du client, n° de commerçant... Ceci est assuré par un petit programme IBS (module CGI) installé sur le serveur du commerçant. Ce programme 'renvoie' l'acheteur sur la page d'accueil du serveur **PAYBOX**.

ETAPES 5 A 7: Saisie du numéro de carte et demande d'autorisation.

La liaison entre l'acheteur et le serveur **PAYBOX** est établie en HTTPS, protocole sécurisé avec SSL, qui crypte l'ensemble des informations échangées.
Cette protection protège les données envoyées par l'Internet et garantit à l'acheteur que son numéro de carte bancaire ne peut être intercepté en clair par un tiers durant son transfert vers le serveur sécurisé **PAYBOX**.

5) La page d'accueil de **PAYBOX** informe l'acheteur sur son achat: présentation du nom du commerçant (ce qui garantit que le commerce a été authentifié), montant et devise de l'achat (Franc ou Euro). Chaque commerce peut avoir une page d'accueil différente, personnalisable pour mieux s'intégrer au style de la boutique (fond, couleurs, logos...). Les seuls élements constants sont les zones de saisie du numéro de carte et de la date d'expiration.

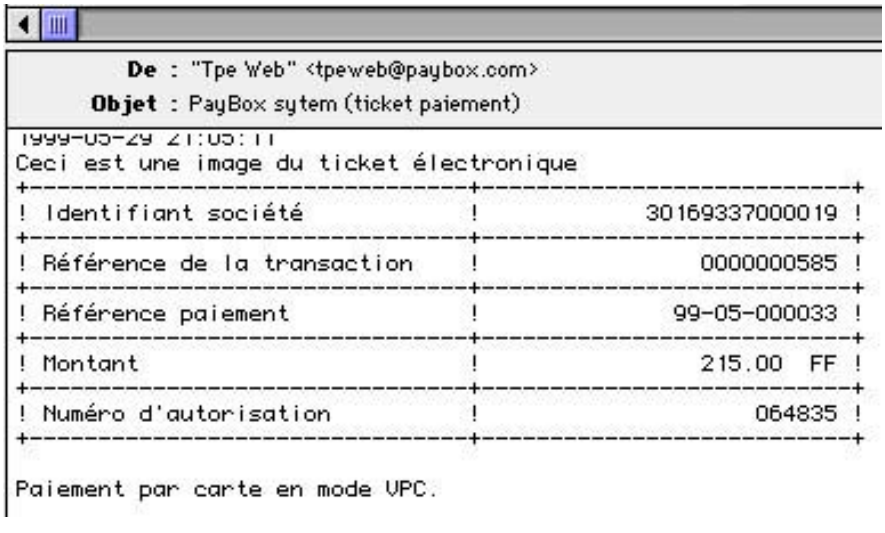
6) Lorsque le numéro de carte a passé un premier niveau de contrôle (clé de Luhn, oppositions, etc.), le serveur **PAYBOX** émet une demande d'autorisation vers le centre de la banque à laquelle est affiliée le commerçant. Ceci est réalisé par Transpac, en utilisant les protocoles bancaires normalisés, comme CBSA.



7) Le centre d'autorisation de la banque renvoie un numéro d'autorisation ou un refus. Si le paiement est accepté, **PAYBOX** effectue alors les opérations suivantes:

- affichage du ticket de paiement sur l'écran de l'acheteur (option)
- envoi du ticket de paiement par e-mail à l'acheteur et au commerçant
- En option, connexion directe en HTTP vers le serveur commerçant pour renvoyer les informations sur le paiement (n° autorisation, montant, référence commande).

Le numéro de carte n'est par contre JAMAIS renvoyé au commerçant.



L'acheteur est ensuite automatiquement redirigé vers le serveur du commerçant, où il peut reprendre le cours de sa visite.

ETAPE 8: Télécollecte vers la banque du commerçant.
Cette opération se fait en général une fois par jour. Elle consiste pour **PAYBOX** à envoyer vers la banque les transactions de paiements dûment autorisées et enregistrées durant la journée, pour qu'elles soient créditées sur le compte du commerçant. Cette télécollecte est effectuée automatiquement, en fonction des paramètres donnés par la banque, au travers du protocole normalisé CBPR (ou CBPR Euro). Durant cette opération, les listes d'oppositions sont également renvoyées à **PAYBOX**. Un ticket de compte-rendu de télécollecte est renvoyé par e-mail au commerce. Il indique le total des transactions envoyées à la banque.

A noter également la possibilité pour le commerçant de se connecter sur le serveur **PAYBOX** pour contrôler et visualiser en direct les paiements effectués sur son site . Il peut ainsi gérer les paiements différés, annuler des paiements ou lancer manuellement la télécollecte vers sa banque. Cet accès au 'Back Office Commerçant' est protégé par mot de passe.

L'OFFRE DE SERVICE PAYBOX

Pour un commerçant, l'utilisation du TPE virtuel **PAYBOX** implique:

- la signature d'un contrat VAD/VPC avec sa banque,
- l'installation sur le site commerçant d'un programme fourni par IBS,
- un abonnement pour accès au serveur **PAYBOX**; ce contrat est signé dans les agences du Crédit Agricole Provence Côte d'Azur.

A la suite de la signature de ce contrat, le Crédit Agricole(BAN/BTE6) attribue au commerçant un numéro d'adhérent (ou de 'site') à 7 chiffres et un numéro de machine (ou de 'rang') à 2 chiffres. Ces deux numéros sont utilisés par **PAYBOX** pour l'authentification du commerçant durant les opérations d'autorisation et de télécollecte.

INSTALLATION D'UN SCRIPT CGI SUR L'ORDINATEUR DU COMMERÇANT.

Ce programme, installé sur le serveur du commerçant, assure l'établissement de la communication entre l'acheteur et le serveur **PAYBOX** d'IBS une fois que le porteur a validé sa commande et confirmé sa volonté de payer. C'est la seule partie de logiciel «livré» par IBS.

Ce module est un exécutable CGI (Common Gateway Interface) qui est appelé par le logiciel Web du commerçant lorsque le porteur appuie sur un bouton «Paiement» défini dans une page HTML prévue à cet effet. Le numéro du commerçant, le numéro de commande, son montant, la devise utilisée et l'e-mail de l'acheteur sont alors cryptés et envoyés au serveur **PAYBOX** d'IBS, au travers d'une session SSL sécurisée.

Les modules CGI pour utilisation de **PAYBOX** sont fournis dans les versions suivantes:

- Windows-NT
- UNIX SCO
- AIX
- LINUX
- SOLARIS
- IRIX
- (D'autres systèmes peuvent être pris en compte).

Ces modules sont directement disponibles sur le site d'IBS avec la documentation d'installation et d'utilisation.

Ils sont immédiatement opérationnels.

En utilisant le numéro de commerce-test fourni dans la documentation, le commerçant et/ou son hébergeur peut intégrer le module IBS dans les pages HTML de sa galerie, effectuer tous les tests souhaités sans aucune intervention d'IBS ou du Crédit Agricole.

Pour passer en production, il suffit simplement de signer le contrat d'abonnement **PAYBOX** par l'intermédiaire d'une agence du Crédit Agricole et de remplacer le numéro de commerce-test par celui attribué par la banque. La galerie du commerçant devient opérationnelle immédiatement.

Une fois installé, ce module dialogue en HTTP (et HTTPS) via l'Internet avec le logiciel navigateur Web du porteur et le serveur **PAYBOX** d'IBS. A noter qu'un même serveur (site) peut héberger plusieurs commerçants (galeries). Dans ce cas, le module IBS n'est à installer qu'une seule fois. Toutefois, chaque commerce nécessite un paramétrage particulier pour différenciation (chaque commerce se voit attribuer un numéro de TPE virtuel unique).

Rien à installer sur l'ordinateur du client.

Pour accéder à l'Internet, aux galeries marchandes et au serveur de paiement **PAYBOX**, l'acheteur doit simplement disposer d'un navigateur Web acceptant les connexions SSL, sur n'importe quel type de station et/ou de système d'exploitation.

Aucun autre logiciel spécifique (plug-in) au télé-paiement n'est nécessaire.

Ces caractéristiques sont disponibles sur tous les navigateurs disponibles à ce jour.

L'accès au serveur Paybox.

PAYBOX, installé dans les locaux d'IBS, est uniquement dédié au paiement électronique sur Internet. Ce serveur, relié en permanence à l'Internet, assure les opérations suivantes:

- **Identification** des sites Web des commerçants affiliés demandant un paiement.

- **Décodage et contrôle** des informations reçues du site commerçant authentifié (montant, devise, n° commerce, etc.)

- **Affichage** d'une page sécurisée (SSL) pour la saisie du n° et de la date d'expiration de la carte par le porteur. Cette page est **personnalisable** (couleurs, fond, logos, polices) pour chaque commerce.

- **Contrôles** préalables de validité du n° de carte avant demande d'autorisation.

- **Analyse comportementale** pour détection de fraude potentielle.

- **Connexion** (via Transpac) vers le **serveur d'autorisation** concerné (protocole CBSA)

- Si paiement autorisé, **envoi du ticket de paiement** au porteur et au commerçant par e-mail

- En option, **envoi** des mêmes informations **par liaison directe HTTP** entre **PAYBOX** et le serveur du commerçant (sans passer par le navigateur du porteur)

- **Redirection** (automatique ou manuelle) du porteur vers le(s) pages(s) du serveur commerçant (3 retours possibles: après 1°: paiement effectué 2°: paiement refusé 3°: paiement annulé)

- Gestion des **paiements différés**: le commerçant a la possibilité de différer les paiements (de 0 à 99 jours). La durée du différé peut être différente pour chaque paiement.

- Chaque jour (via Transpac), **envoi automatique des transactions de paiement** vers le serveur de télécollecte de la **banque** du commerçant (protocole CBPR ou CBPR Euro).

- Emission d'un **ticket de compte rendu** de télécollecte vers le commerçant (par e-mail), contenant le total des paiements effectués dans la journée.

Un processus de sécurité très sophistiqué.

Une processus particulier, développé par IBS, permet à **PAYBOX** de surveiller en temps réel le comportement du porteur, notamment pour éviter l'utilisation du serveur de paiement comme testeur de numéros de carte générés automatiquement, ou pour d'autres types d'attaques:

- recherche de BIN par incrément, dérivation ou masque
- multiplication des essais avec différentes dates d'expiration
- adresses (IP) porteurs aléatoires
- carte «nomade», etc...

D'autres contrôles sont aussi réalisés par **PAYBOX**: clé de Luhn, dates d'expiration, contrôles dans les listes d'opposition. Si un numéro de carte passe tous ces contrôles, il y a alors demande d'autorisation systématique sur le serveur d'autorisation de la banque du commerçant (via Transpac).

En cas de détection de fraude, **PAYBOX** refuse toute nouvelle demande de paiement de la part du porteur dans la session en cours. Le porteur doit alors soit recommencer la totalité du processus d'achat, en repartant vers le serveur du commerce, soit attendre 24 heures avant de pouvoir réutiliser PAYBOX, soit arrêter et redémarrer son navigateur, ce qui évite l'utilisation d'automate. Un système d'alerte avertit également le service technique d'IBS.

Les confirmations de paiement sont envoyées par **PAYBOX** au commerçant et au porteur par e-mail. Cette méthode permet d'informer commerçant et porteur par un deuxième canal (SMTP), dans le cas où les liaisons Internet (sessions) seraient interrompues (encombrement, rupture communication, faute de routage, panne du PC du porteur, etc..).

A noter qu'en option **PAYBOX** peut aussi renvoyer un compte-rendu de paiement par un autre canal, à savoir un module CGI installé sur le serveur du commerçant, sans passer ou utiliser le navigateur du porteur (acheteur). Ceci garantit que le commerce est toujours informé d'un paiement, même lorsqu'un acheteur ne revient pas sur le site commerçant.

Liaison de Paybox avec les serveurs bancaires.

Les liaisons entre le serveur de paiement **PAYBOX** et le centre d'autorisation ou le centre de télécollecte sont de type X.25, via les protocole CBSA et CBPR (ou CBPR Euro). Cette technique simplifie l'accès vers les serveurs d'autorisation et de télécollecte et permet une rupture totale de protocole, de service et de média entre l'Internet et l'établissement bancaire. Cette protection assure une étanchéité parfaite entre le monde Internet et l'environnement monétique bancaire.

Le Back office du commerçant.

Tout commerçant abonné au service **PAYBOX** peut accéder au 'tableau de bord' de son TPE virtuel.

Ce tableau de bord, appelé 'back-office commerçant' est un ensemble de pages protégées sur le site Web d'IBS. Elles permettent au commerçant d'effectuer les opérations suivantes:

•**Visualisation/Impression** des paiements effectués sur les 3 derniers mois

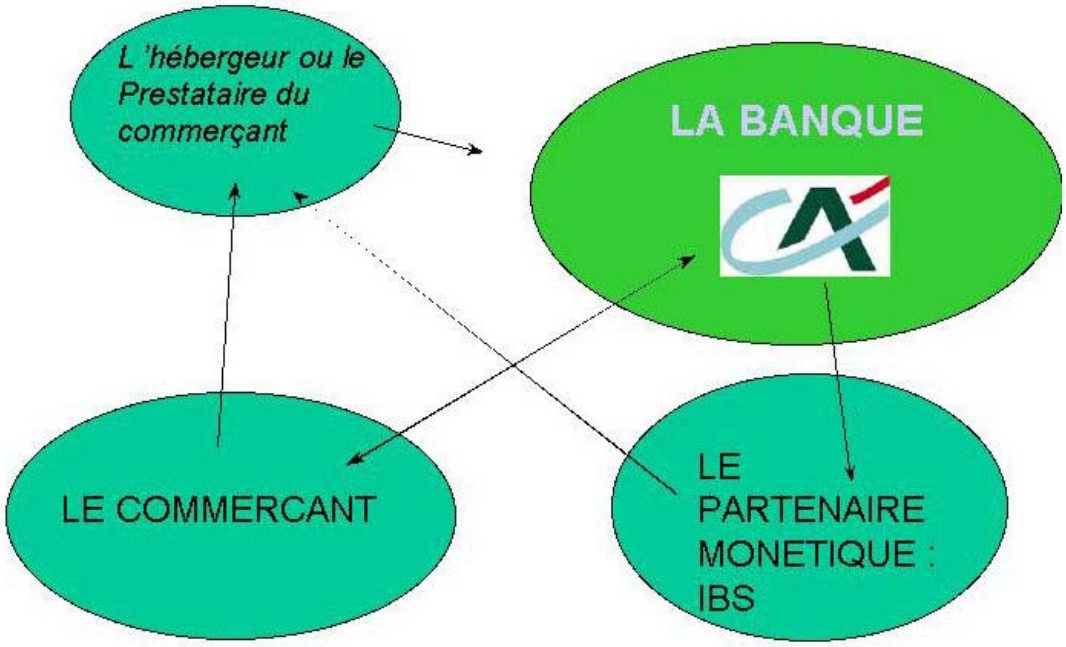
•**Annulation** d'un paiement

•**Mise en recouvrement d'un paiement différé** (envoi du paiement à la banque avant date d'échéance prévue initialement)

•**Lancement d'une télécollecte** en manuel vers la banque (avant l'heure prévue)

•**Visualisation** des informations et autres paramètres du commerce.

Il suffit pour cela au commerçant de se connecter sur le site www.paybox.com avec le navigateur de son choix, et de rentrer le nom et le mot de passe qui lui ont été attribué par IBS.

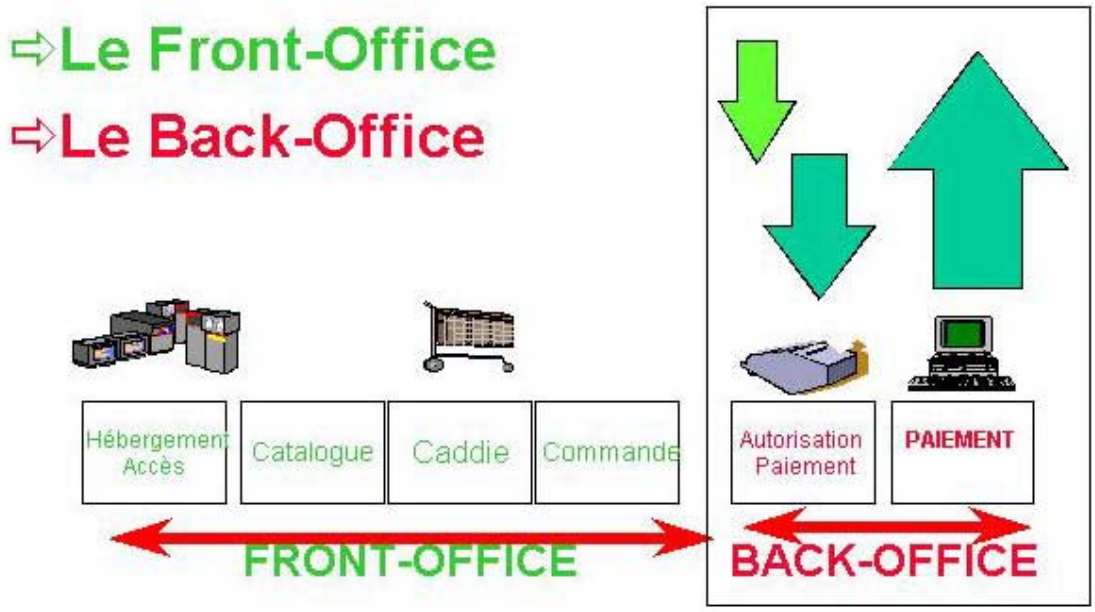


Liaisons entre les différents intervenants

Pour goûter à Paybox (et à la Lerina):

www.abbayedelerins.com

Front office - Back office



A plusieurs reprises nous avons abordés les termes de Back office et de Front office.

Dans le commerce électronique on appelle front-office les composants suivants:

- création de la boutique. Ceci est fait en utilisant le langage HTML ou des logiciels générant du code HTML. On y incluera la gestion du catalogue, c'est à dire la présentation des articles.

- Hébergement de la boutique; ceci est fait par un fournisseur d'accès.

- La gestion du bon de commande, c'est à dire la valorisation de la commande en fonction des articles choisis, tel que l'on ferait à la caisse du super marché en mettant les article dans le caddie puis en payant. La gestion du bon de commande se fait par l'intermédiaire d'un formulaire et de langages spécialisés tels que Jav ou Javascript.

Le Back-office consiste lui à gérer la demande d'autorisation de paiement à la banque et à réaliser le paiement proprement dit, c'est à dire le crédit du commerçant et le débit du client.

C'est dans ce dernier domaine qu'interviennent les acteurs pour concourir au paiements, et plus particulièrement la banque et l'intermédiaire télématique (si nécessaire).

Le protocole SSL

(Secure Socket Layer)

Baitan - Berger - Maia

Aujourd'hui la solution la plus répandue pour sécuriser les transactions est SSL (Secure Socket Layer, créé par Netscape).
Son succès s'explique par sa simplicité d'utilisation et par son intégration dans tous les navigateurs du marché : vous remarquerez en bas à gauche de votre navigateur Netscape une petite clé, qui devient automatiquement entière si le serveur qui vous envoit les informations utilise SSL.

SSL (Secure Socket Layer) est un protocole de communication d'information qui permet d'assurer l'authentification, la confidentialité et l'intégrité des données échangées.
Ce protocole utilise un moyen de cryptographie reconnu : l'algorithme à clé publique RSA (du nom de ses concepteurs - Rivest - Shamir - Adleman -).

Une clé RSA est le résultat d'opérations entre nombres premiers.

Le but recherché par les entreprises commerciales est un moyen permettant une communication sûre avec leurs clients, et plus précisément, une façon sûre d'obtenir le paiement des biens/services vendus.

Dans un tel cadre commercial, les données qui sont primordiales de protéger lors de la transmission sont constituées des informations concernant la carte de crédit du client (généralement). Dans le cas de vente de contenu électronique ou de service électronique il faut également protéger la transmission de ces données. La libre circulation non-protégée de ces données grugerait une partie des ventes des marchands.
Les transactions commerciales qui s'effectuent sur Internet sont généralement ponctuelles. C'est-à-dire qu'elle ne sont ni régulières, ni périodiques. Un système de cryptographie permettant d'assurer ce type de communication doit tenir compte de ces éléments.
Le browser Navigator de la compagnie Netscape Communications Corporation utilise l'implantation du protocole SSL. Ce protocole effectue la gestion des clés et l'authentification du serveur avant que les informations ne soient échangées.

Processus

Le processus est le suivant :

Un utilisateur quelconque utilise le logiciel Netscape client et entre en communication avec un logiciel serveur de type commercial.

Le serveur possède déjà sa paire de clés publique/privée. C'est cette paire de clés qu'il utilise dans ses communication avec tous les logiciels clients.

Le logiciel client, une fois reconnu par le logiciel serveur, génère une paire de clés publique/privée.
Le logiciel client demande au logiciel serveur de lui fournir sa clé publique (celle du serveur).
La clé publique du client est aussitôt encryptée avec la clé publique de serveur et transmise au serveur.

Le serveur décode le message avec sa clé privée serveur et authentifie la clé publique de l'utilisateur.
Le serveur envoie ensuite au logiciel client une confirmation, encryptée, du bon déroulement de l'opération.

Toutes les informations suivantes qui seront transmises entre l'utilisateur et le serveur commercial seront désormais encryptées. De plus, il n'y a que ce serveur qui est en mesure de communiquer avec cet utilisateur puisqu'il n'y a que ce serveur qui connaît la clé publique de cet utilisateur.

L'utilisateur et le serveur commercial peuvent maintenant échanger toutes les données voulues de façon sûre.
L'ensemble de ce processus est maintenant complètement transparent pour l'utilisateur.

Avec ce protocole, une nouvelle paire de clés est générée à chaque établissement de la communication entre le logiciel client de l'utilisateur et le logiciel serveur. La communication est donc entièrement sûre, mais en aucun cas le serveur commercial ne peut s'assurer de l'identité de l'utilisateur à l'autre extrémité.

Une façon de résoudre ce problème, est de joindre à ce processus un système de validation, comme par exemple un numéro d'identification personnel (NIP) qui s'obtient par une inscription préalable.

FONCTIONNEMENT

Le système repose sur l'algorithme RSA (Rivest, Shamir et Adleman, les trois concepteurs comme indiqué plus haut), un standard utilisé pour le cryptage des données et la signature de messages électroniques. Cet algorithme est très utilisé pour l'authentification et le cryptage des données dans le domaine informatique.

Deux paires de clés - une pour le verrouillage et l'autre pour le déverrouillage - à 40 bits sont utilisées.
Chaque paire est composée d'une clé publique et d'une privée. La clé publique est faite afin d'être distribuée alors que la clé privée n'est jamais distribuée, elle est toujours gardée secrète. Les données qui sont cryptée avec la clé publique peuvent seulement être décryptées avec la clé privée. Et inversement, les données qui sont cryptée avec la clé privée peuvent seulement être décryptées avec la clé publique. C'est cette asymétrie qui fait que la clé publique est si utile.

<u>Démonstration par l'exemple</u>
(L'exemple ci-dessous provient du site Netscape)

L'authentification est la procédure de vérification d'identité, pour que chacun soit sûr que l'autre soit bien celui qu'il prétend être. Dans l'exemple suivant la notation {SOMETHING} KEY signifie que {SOMETHING} a été crypté ou décrypté en utilisant une clé KEY.

Imaginons que Alice (A) désire authentifier Bob (B). B a une paire de clés, une publique et une privée. Il révèle à A sa clé publique. A génère un message aléatoire et l'envoie à B:
A @ B RANDOM-MESSAGE

Bob utilise sa clé privée pour crypter le message reçu et le retourne à Alice :
B @ A {RANDOM-MESSAGE} BOB'S-PRIVATE-KEY

Alice reçoit le message et le décrypte en utilisant la clé publique révélée précédemment. Elle compare le message décrypté avec l'original qu'elle a envoyé à Bob ; s'ils correspondent, elle sait qu'elle est entrain de parler à Bob.

Un imposteur n'aurait pas pu connaître la clé privée de Bob et par conséquent serait incapable de crypter correctement le message envoyé à Alice pour validation.
Une fois qu'Alice a authentifié Bob, elle peut alors lui envoyer des messages que seul Bob peut décoder.
A @ B {SECRET} BOB'S-PUBLIC-KEY

Seule la clé privée de Bob est capable de décoder le message. Et par conséquent, même si quelqu'un d'autre est entrain d'observer la communication entre Alice et Bob, il ne peut pas déchiffrer ce message.

NB: Il est a savoir que Alice et Bob sont des prénoms utilisés dans presque tous les livres traitant de la cryptologie.

Certificats

Un certificat est un document électronique qui atteste qu'une clé publique est bien liée à une organisation ou personne. Il permet la vérification de la propriété d'une clé publique pour prévenir la contrefaçon de clés publiques.

Un certificat contient généralement une clé publique, un nom ainsi que d'autre champs pour identifier le propriétaire, une date d'expiration, un numéro de série, le nom de l'organisation qui contresigne le certificat et la signature elle-même. Le format des certificats est définie par la norme X509.

Le certificat est donc une attestation que les informations qu'il contient sont exactes. Pour cela, le certificat doit être généré par un tiers de confiance, c'est-à-dire un organisme indépendant qui contrôle la véracité de ces informations. Le CA (Certifying Authority, autrement dit l'organisme certificateur) donne la crédibilité au certificat.

Il existe typiquement deux types de certificats utilisés avec SSL : pour serveur et pour client. Techniquement ils utilisent le même format mais diffèrent par l'information qu'ils contiennent.

Ainsi un certificat coté client sert à identifier un utilisateur, il contiendra donc des information sur cet utilisateur.

Coté serveur, le certificat a pour but d'authentifier le serveur et l'organisme qui l'exploite.

C'est ce type de certificat dont vous avez besoin pour mettre en place un serveur "sécurisé" HTTPS.

Il ne sera pas expliqué ici comment obtenir un certificat serveur. Il existe plusieurs fournisseurs de certificats serveurs SSL. Pour plus d'informations sur ce sujet, consulter le site de Netscape et celui de SSL hosting.

Certificat pour client

Un certificat client est un certificat qui identifie l'utilisateur d'un navigateur web, et qui a vocation à identifier avec certitude un unique individu.

Ce certificat est basé sur une clé publique/privée qui est stockée par le navigateur (à l'avenir, cette clé sera probablement sur carte à puce). De la même façon qu'un certificat pour serveur n'a pas de sens tant qu'il n'est pas authentifié par un tiers, le certificat client à besoin d'être signé.

On peut différencier deux types de certificats suivant leurs signatures: les certificats signés par un serveur ou un organisme local (par exemple l'entreprise qui exploite un serveur SSL) et les certificats signés par un tiers certificateur reconnu de tous.

Les certificats signés par un organisme local prennent tout leur sens dans la cadre d'un intranet/extranet. Ainsi certaines entreprises au lieu de donner des couples username/password à leurs employés leur font générer une clé SSL qu'ils vont ensuite signer.
Il suffira alors d'indiquer au serveur de n'accepter les connexions SSL que de possesseurs de certificats signés par l'entreprise.

On peut bien sur aller plus loin et utiliser les champs que contiennent les certificats pour créer des ACLs, et autoriser l'accès à des zones spécifiques du serveur en fonction de l'appartenance à tel ou tel service, par exemple.

Ces certificats signés par une entité locale ont leurs limites dès qu'il s'agit de travailler avec des clients d'origines différentes. Ainsi un consommateur qui utilise des banques et des centres commerciaux SSL se retrouve rapidement avec des dizaines de certificats différents, fournis par chacun des serveurs. Aussi les certificats signés localement ne conviennent pas au grand public.

La solution est que chaque individu souhaitant s'identifier sur plusieurs serveurs utilise un certificat signé par un tiers de certification. Ce dernier aura effectué toutes les vérifications nécessaires pour prouver que le certificat est authentique (qu'il identifie bien la bonne personne). L'individu fournira alors aux serveurs qu'il veut utiliser son certificat personnel signé par le tiers. Le serveur utilisera alors ce certificat pour assurer la sécurité (l'affectera dans les ACLs qui conviennent). L'utilisateur n'aura à stocker qu'un seul certificat (le sien, qui est en quelque sorte sa signature électronique) et n'aura à retenir qu'un seul mot de passe, celui qui protège son certificat.

Ce système simplifie la vie de l'utilisateur, mais aussi de l'administrateur des serveurs. En effet, même si à l'échelle d'une entreprise il est simple d'attribuer avec certitude un certificat à la bonne personne, ce n'est plus le cas pour un magasin virtuel. Comment être sûr à distance que l'on signe le certificat de son client (que l'on n'a jamais vu)?

Ce problème d'attribution des certificats signés se pose dès lors que les acteurs ne sont pas locaux et ne se connaissent pas. Il est donc nécessaire d'utiliser un tiers certificateur. Il existe d'ores et déjà plusieurs tiers qui fournissent des certificats SSL clients, dont Thawte.

SSL ET LES LOGICIELS DE COMMUNICATIONS

SSL est un protocole de communication qui est indépendant du protocole de communication de plus haut niveau qui repose sur lui. Il est donc possible de porter les logiciels de communications usuels (ftp, telnet, http, etc.) sur SSL sans grande modification, et de façon quasiment transparente pour l'utilisateur. SSL peut alors négocier la méthode de chiffrement à utiliser, authentifier les acteurs de la communication, et chiffrer au vol tout ce qui transite par son canal.

Les spécifications de SSL sont publiques, mais son implémentation de référence (SSLREF) n'est pas exportable des USA.

Heureusement, il en existe une implémentation librement accessible à partir de l'Australie. Il existe des patchs pour intégrer SSL aux logiciels de communications usuels: http (Mosaic et NCSA httpd), telnet, ftp, etc.

<u>Sources & divers liens pouvant vous intéresser :</u>

Université de Genève (en Français)
http://cuisung.unige.ch/TechInternet/Securite/SSL.html
Netscape (en Anglais)
http://help.netscape.com/products/server/enterprise/3x/manual/encrypt.htm
Ecole Polytechnique Fédérale de Lausanne (en Français)
http://www.epfl.ch/SIC/SA/publications/FI95/fi-7-95/7-95-page3.html
dernière mise à jour: 22 mai 1998
Baitan - Berger - Maia