MASTER DE SPÉCIALISATION EN INFORMATIQUE ET INNOVATION

Le commerce électronique : questions clés et mise en perspective à travers le développement d'un site

Coppens, Benoît; Hallard, Xavier

Award date:
1999

Awarding institution:
Universite de Namur

Facultés Universitaires Notre-Dame de la Paix, Namur
Institut d'Informatique
Année académique 1998-1999

Le commerce électronique: Questions clés et mise en perspective à travers le développement d'un site

Mémoire réalisé par Benoît Coppens et Xavier Hallard

Mémoire présenté en vue de l'obtention du grade de Maître en Informatique.

Les affaires [...], c'est l'argent des autres.

Dumas (Alexandre), [1824 - 1895], *La Question d'argent,* II, 7, Jean.

Abstract

Le commerce électronique n'est plus aujourd'hui simplement une expression à la mode mais une véritable réalité. Nous proposons dans ce mémoire d'en offrir au lecteur un panorama aussi large que possible en traitant de ses problèmes clés pour déboucher sur un guide d'étapes destiné aux entreprises souhaitant développer leur propre site Web de commerce électronique. La mise en pratique de notre expérience théorique a été effectuée chez VisionShape dont nous avons entièrement reconstruit le site. Au cours de ce rapport, nous offrons la possibilité de saisir l'importance du travail réalisé.

Electronic commerce isn't just a fashionable expression anymore but a well reality. We propose in this thesis to offer readers a view as large as possible of its key problems in order to provide a guidebook for companies wishing to develop their own electronic commerce Web site. The implementation of our theoretical experience has been done with VisionShape which site has been entirely rebuild by us. In this report, we offer the possibility to realise the importance of our work.

Remerciements

Nous tenons à exprimer nos plus vifs remerciements à notre promotrice, Madame Claire Lobet pour sa patience, sa gentillesse, son soutien et ses conseils prodigués tout au long de l'élaboration de ce mémoire.

Nous remercions également Amdahl Corporation et tout particulièrement M. Lloyd Dickman qui ont rendu possible notre stage, en nous donnant l'occasion de travailler dans un domaine connexe au commerce électronique.

Nous tenons aussi à exprimer notre gratitude à Daniel Borrey, directeur général de VisionShape, pour nous avoir permis d'apporter une expérience pratique à notre travail et pour sa disponibilité.

Nous portons également une profonde reconnaissance aux professeurs de l'Institut d'Informatique pour le bagage intellectuel qu'ils nous ont permis d'acquérir.

Tout d'abord, je remercie chaleureusement mes parents qui m'ont donné la possibilité de réaliser mes études et mon stage en Californie ainsi que pour leurs encouragements et leur affection. Tout comme ma marraine, mon parrain et mes grands-parents, ils méritent donc toute ma profonde reconnaissance pour leur soutien et la tendresse qu'ils m'ont procurés durant ces années d'études.

Je n'oublie pas non plus le reste de ma famille et mes amis qui m'ont apporté leur soutien et leur compréhension durant mes études et mon stage.

Enfin, c'est tout naturellement, à toi, Benoît, que reviennent mes derniers remerciements pour tous ces bons moments passés ensemble. Ce mémoire n'est, d'ailleurs, que le reflet de cette complicité unique qui nous unit depuis maintenant quelques années.

Xavier Hallard

Je remercie profondément mes parents qui m'ont donné la possibilité de réaliser mes études. Je souhaite également exprimer ma gratitude à l'ensemble de ma famille qui m'a permis de partir en stage en Californie.

Je remercie également toutes les personnes qui m'ont soutenu et encouragé aussi bien durant la réalisation de ce mémoire que durant les années d'études qui l'ont précédée.

Enfin, à toi, Xavier, merci pour tous les bons moments que nous avons eu l'occasion de passer ensemble durant notre stage et la réalisation de ce mémoire.

Benoît Coppens

Table des matières

Table des figures

Introduction

Le commerce électronique n'est plus aujourd'hui simplement une expression à la mode mais une véritable réalité. Nous avons donc été motivés à l'idée de travailler dans un tel domaine.

C'est dans cette optique que nous avons effectué un stage chez Amdahl Corporation, société californienne située dans la Sillicon Valley dont une des activités est le développement de solutions Mondex. Il s'agit d'un système de porte-monnaie électronique mis au point par MasterCard que nous étudierons plus en détail au cours de ce mémoire.

Notre stage nous a permis de nous familiariser avec les systèmes utilisés pour gérer les paiements électroniques via la carte Mondex tant chez les divers commerçants qu'au travers du réseau Internet.

Avec l'accord et la collaboration d'Amdahl Corporation, entre autres, tous les éléments nécessaires étaient dès lors réunis pour que, dans un premier temps, nous orientions notre mémoire vers une analyse et une comparaison des différents systèmes de porte-monnaie électronique présents et à venir. Nous nous serions alors focalisés sur une comparaison de ces systèmes permettant d'effectuer des achats sur Internet.

Mais progressivement, différentes contraintes nous ont poussés à modifier le sujet de notre mémoire.

- Premièrement, le volume des documents confidentiels mis à notre disposition était plus important que nous ne l'avions prévu.
- Deuxièmement, le déclin du système Mondex que nous avions officieusement ressenti au cours de notre stage, fut confirmé par la fermeture de Mondex USA dans le courant de l'année 1999. Nous étions dès lors moins enthousiastes à l'idée de travailler sur un système souffrant d'un avenir très incertain. D'ailleurs le licenciement ou le départ volontaire de plusieurs collègues de notre département réduisaient les sources utiles et précieuses d'information. Celles-ci tendaient à se restreindre à un strict minimum, mettant encore un frein au choix d'un tel sujet.
- Enfin, la difficulté d'obtenir des informations détaillées auprès de concurrents tels que Banksys avec son système Proton, et Visa avec son système VisaCash et le récent accord de coopération entre ces deux derniers, ne nous offraient que peu d'espoir pour parvenir à fournir une comparaison de qualité, du moins sur le plan technique.

Nous avons donc, en concertation avec notre promotrice, opté pour un sujet connexe et attrayant.

Nos nouveaux objectifs furent alors de réaliser une application en grandeur réelle, à savoir la réalisation d'un site de commerce électronique et ce, après avoir soulevé les différents problèmes liés à une telle application et en les éclairant par une synthèse originale de la littérature.

Ce mémoire a donc pour intention de fournir au lecteur un panorama aussi large que possible des problèmes clés liés au commerce électronique et ce, dans le

but de déboucher sur un guide d'étapes, fruit de notre expérience pratique et des multiples questions soulevées, tant dans la réalisation théorique que pratique de notre mémoire. Ce guide est destiné aux entreprises souhaitant développer leur propre site de commerce électronique.

Nous avons donc, dans le cadre de ce mémoire, effectué le développement d'un site pilote pour l'entreprise VisionShape. Située au États-Unis et possédant un comptoir à Louvain-la-Neuve, il s'agit d'une société essentiellement tournée vers la fabrication et la vente de scanners ainsi que vers le développement de solutions de traitement de l'image.

Dans le premier chapitre *Le commerce électronique*, nous nous efforcerons de proposer au lecteur une vue d'ensemble du commerce électronique. Nous étudierons sa position au sein des divers continents avec cependant une importance plus particulière accordée à l'Europe et à la Belgique. Nous nous attarderons aussi sur les divers facteurs favorables et défavorables que rencontrent, avec le commerce électronique, tant le vendeur que l'acheteur.

Le chapitre 2 *Commerce électronique et sécurité* s'intéressera aux techniques actuelles utilisées pour sécuriser la transmission de données et plus particulièrement les informations de paiement.

Le chapitre 3 *Moyens de paiement* mettra l'accent sur les divers moyens de paiement disponibles sur Internet. A cette occasion, des solutions implémentant ces systèmes de paiement seront analysées.

Le commerce électronique soulève de nombreux problèmes pour le législateur d'aujourd'hui. Quelques moyens pouvant faciliter la législation du commerce électronique et l'attitude des hommes de loi face à ceux-ci seront analysés dans le chapitre 4 *Droit et commerce électronique.*

Le chapitre 5 *Marketing* analysera divers procédés à suivre pour non seulement attirer le client sur un site Web mais aussi pour le fidéliser. Nous parlerons, entre autres, des modes de fonctionnement des sites de recherche et des techniques utilisées pour offrir une personnalisation du site à l'internaute.

Le chapitre 6 *Étude de cas* a pour intention de permettre au lecteur de se rendre compte du travail réalisé auprès de l'entreprise VisionShape. Après une première analyse des problèmes que nous avons rencontrés dans la première version du site, nous proposerons au lecteur la démarche que nous avons suivie et les modifications que nous avons apportées de manière à rendre le site plus convivial et attrayant.

Enfin nous terminerons, dans le chapitre 7 *Vers un guide d'étape*, par un guide reprenant les questions utiles à se poser lors de la mise sur pieds d'un site de commerce électronique.

Chapitre 1: Le commerce électronique

1. Introduction

Après une brève description de l'évolution des usages d'Internet, nous essayerons de définir le commerce électronique.

Ensuite, nous étudierons sa position dans divers continents et nous attacherons une importance plus particulière à l'Europe et, bien entendu, à la Belgique.

Nous chercherons, enfin, à voir quel est l'impact du commerce électronique sur l'économie et ses conséquences sur ces principaux acteurs, à savoir le vendeur et l'acheteur.

2. Évolution des usages d'Internet

Le point de départ d'Internet se situe dans le monde militaire. Dès la fin des années 60, l'armée américaine voulait être sûre que ses ordinateurs mis en réseau puissent échanger, même en cas de conflit, des informations entre eux. C'est pourquoi elle mis sur pied en 1969 le réseau ARPANET.

En 1984, la National Science Foundation voit en Internet un grand moyen de distribution pour ces puissants ordinateurs. C'est ainsi qu'un de ces derniers, situé à San Diego, pouvait être utilisé depuis l'Illinois. L'usage devient gouvernemental et de plus en plus scientifique.

Pendant les années 80, les universités commencent à faire usage d'Internet pour transmettre de l'information: lettres, mémos,...

En 1989, Tim Berners-Lee, employé au CERN, pense à une nouvelle utilisation d'Internet et crée le langage HTML (*HyperText Mark-up Language*) pour l'usage interne du CERN. Sa popularité fut immédiate: le World Wide Web était né.

A partir de 1992, un sérieux trafic commercial envahit Internet. L'usage se tourne plus vers l'informatif et le publicitaire.

C'est en 1993 que Marc Andreesen et son équipe de l'université de l'Illinois conçoivent Mosaïc, l'interface graphique pour le World Wide Web permettant ainsi l'inclusion d'images, de sons, de vidéos,...

Aujourd'hui, le business a découvert Internet et le World Wide Web a grandi à un rythme incroyable. Depuis 1994, Internet s'est ouvert au commerce électronique. Citons en exemple les sites d'Amazon[1] et de Dell[2].

Amazon, leader dans la vente de livres sur Internet, fut créé à Seattle en 1994. En quelques chiffres, Amazon emploie 280 personnes (en mai 1998) et dispose d'un catalogue de plus de 3 millions de titres. Amazon, c'est aussi la création de deux antennes: l'une au Royaume-Uni, l'autre en Allemagne. (**[LORENTZ 98]**)

---

[1] http://www.amazon.com/

[2] http://www.dell.com/

3. Qu'est-ce que le commerce électronique?

3.1. Définition

Le commerce électronique peut inclure toutes les transactions financières et commerciales réalisées de manière électronique, incluant EDI (*Electronic Data Interchange*) ou EFT (*Electronic Fund Transfer*). Cependant, certains le limitent à la vente au détail aux consommateurs pour lesquels la transaction et le paiement se font au travers d'Internet. (**[OCDE 99]**)

3.2. Différenciation

On distingue deux types de commerce électronique suivant les partenaires de l'échange. Il peut s'agir d'un échange entre deux entreprises (business-to-business) ou d'un échange incluant un consommateur final (business-to-consumer).

3.2.1. Business-to-business

[OCDE 99] regroupe le commerce business-to-business en trois formes majeures:

- L'utilisation d'Internet, de pages HTML et de navigateurs;
- Le déploiement d'intranets qui assurent les fonctions "business" de l'entreprise;
- L'extension de l'intranet d'une firme à certains partenaires.

[OCDE 99] considère les trois facteurs suivants comme favorables au développement du commerce business-to-business:

- La réduction des coûts de transaction et l'amélioration du service;
- Une réaction défensive des compétiteurs engagés dans le commerce électronique;
- L'insistance de larges entreprises qui poussent leurs fournisseurs à se connecter à leurs systèmes.

3.2.2. Business-to-consumer

Dans cette catégorie deux types de produits sont à distinguer:

Les produit intangibles

Selon **[OCDE 99]**, cinq grandes catégories se retrouvent dans les produits intangibles:

- le divertissement et l'éducation;
- le voyage;
- les journaux et magazines;
- les services financiers;
- les e-mails.

Forrester Research estime que le divertissement pour adultes représentait en 1996 une part de marché de 10% dans ce type de commerce électronique avec près de $50 millions de chiffre d'affaires. Ce dernier devait tripler l'année suivante. (**[FORRESTER 97a]**) Le gambling en ligne (casinos virtuels) est aussi très à la mode.

Les produits tangibles

Dans les produits tangibles, on retrouve, parmi les produits les plus vendus, les biens électroniques, les livres, les habits, la nourriture/boissons mais aussi les CD's.

Phases de développement du business-to-consumer

Selon **[LIPS et al. 98]**, le commerce électronique connaîtra un cycle d'évolution en 3 phases.

Durant la première phase (*phase d'essai*), le fournisseur et le consommateur tâtonnent, prennent leurs marques, expérimentent les technologies numériques. Ils se contentent de leur appliquer les méthodes prouvées dans les autres médias traditionnels.

La deuxième phase (*phase de croissance*) se traduit par un début de standardisation des interfaces et des standards de présentation des produits au consommateur final.

Durant la troisième phase (*phase de maturité*), on observe la banalisation de l'accès des consommateurs à l'environnement électronique marchand. Un point d'équilibre sera atteint lorsque les deux environnements (physique et électronique), auront trouvé leur place et leur part de marché et commenceront à se disputer les clients l'un à l'autre.

[LIPS et al. 98] estime qu'actuellement, le commerce électronique au niveau mondial se situe entre la première et la deuxième phase.

3.3. En quelques chiffres

Le commerce business-to-business existe déjà depuis le début des années 70 et brasse des milliards de dollars au quotidien. Quant au commerce business-to-consumer, il existe depuis quelques années et est difficilement mesurable.

Débutant de pratiquement 0 en 1995, on estime que le commerce électronique business-to-consumer a rapporté un chiffre d'affaires mondial aux alentours de $26 milliards en 1997. On prévoit un chiffre d'affaires de $330 milliards pour l'an 2001-2002 et $1000 milliards pour l'an 2003-2005. (**[OCDE 99]**)

Il faut néanmoins remarquer que les seules données que l'on possède viennent souvent d'entreprises qui participent au commerce électronique. Leurs résultats ne sont qu'approximatifs.

4. Situation extra européenne

Dans la suite du texte, nous utiliserons "commerce électronique" pour désigner le commerce électronique business-to-consumer.

Les États-Unis furent les initiateurs et sont les plus grands consommateurs de commerce électronique. Pour toutes les catégories majeures du commerce électronique, les États-Unis dirigent typiquement 65 à 85 pour cent des 100 premiers sites. Il existe actuellement plus de 250.000 cyber-entreprises et les États-Unis sont typiquement crédités des 4/5 de l'activité internationale dans le domaine du commerce électronique. (**[OCDE 97]**)

	Booz-Allen & Hamilton	IDC	ActiveMedia
Amérique du Nord	76	87	93
Europe	24	8	5
Asie	0	4	1
Reste du monde	0	1	1
Total	100	100	100

Tableau 1: Part du commerce électronique en 1997 d'après plusieurs sources

On peut constater que l'Asie ne représente que, dans le meilleur des cas, 4% du total mondial. Ce chiffre peut s'expliquer par le coût élevé des communications mais aussi par le peu d'investissements financiers à la suite des multiples périodes financières turbulentes traversées par ce continent. Le Japon demeure le pays le plus avancé en cette matière.

A court terme, **[FORRESTER 97b]** prévoit que la part des États-Unis diminue pour atteindre trois quart de l'activité totale mondiale du commerce électronique.

5. Situation en Europe

Des récentes études effectuées par Gartner Group tentent à démontrer que le retard européen par rapport à la situation américaine peut s'évaluer à 12 à 18 mois.

L'Europe, comme nous pouvons l'observer dans le tableau ci-dessous, pour un continent très industrialisé, doit se rendre à l'évidence: son démarrage dans le commerce électronique est relativement lent.

	1995-96	1996-97	2000-01	2001-02
Bénélux	13		4800	
France	0	4	6100	8367
Allemagne	0	73	9700	16090
Italie	0	1	3900	
Hollande		2		
Pays nordiques	13		6800	
Suède		3		
Scandinavie				6436
Espagne	0	1	1500	
Royaume-Uni	26	9	11000	12872
Reste de l'Europe	13	3	500	20595
Total Europe	65	1200	48800	64360

Tableau 2: Chiffres d'affaires en millions de US$ réalisés par le commerce électronique ([OCDE])

Plusieurs raisons peuvent expliquer un tel retard. Nous allons nous attarder à celles qui nous paraissent les plus importantes.

- Les tarifs élevés en matière de téléphonie;
- Les préoccupations relatives à la vie privée;
- La diversité des langues;
- Les systèmes de taxes différenciés et les monnaies nationales;
- Le manque de conscience des bénéfices potentiels.

Les tarifs élevés en matière de téléphonie

Le prix élevé des communications en Europe représente un véritable frein à l'expansion du commerce électronique.

Gageons qu'avec l'ouverture des marchés et la venue de nombreux concurrents, les tarifs ne seront plus, dans un prochain avenir, source d'une telle lenteur dans le développement européen du commerce électronique.

Les préoccupations législatives et la crainte du consommateur

La crainte des consommateurs se tourne vers l'utilisation abusive des données à caractère personnel à des fins de marketing. Largement analysés dans le chapitre 4 *Commerce électronique et le droit*, les problèmes législatifs sont encore nombreux.

Grâce à l'usage de la cryptographie, une quantité de problèmes législatifs semble se résoudre. Un tel usage permettra, également, d'assurer un haut niveau de confidentialité sur le réseau.

En Belgique, la vente sur Internet est régie par la loi sur la vente à distance. Elle offre un délai de 7 jours au consommateur pour changer d'avis.

Gageons que l'un et l'autre augmenteront la confiance du consommateur face à l'achat en ligne.

La diversité des langues

Un des avantages considérables des États-Unis dans leur expansion rapide de l'utilisation d'Internet et, par conséquent, du commerce électronique est l'emploi d'une même langue, à savoir l'anglais.

Aujourd'hui, l'usage incessant de l'anglais sur le réseau européen limite l'accès à ceux qui comprennent l'anglais.

La diversité des langues sur un même site demande un travail colossal mais elle est une condition indispensable pour dynamiser le commerce électronique.

Les systèmes de taxes différenciés et les monnaies nationales

A l'inverse des États-Unis qui se plaît à voir Internet comme une zone taxe-free, l'Union Européenne cherche quant à elle à taxer les transactions s'effectuant sur un tel médium électronique.

En Europe, il faudra donc s'attacher à éviter la double taxation: celle du pays expéditeur mais également celle du pays receveur, bref des pays prenant une part active dans les transactions électroniques. Outre la taxation des revenus, les droits de douanes sont aussi concernés. Il faudrait donc mettre en place un système de suivi et de contrôle des produits commandés par Internet pour y associer des droits de douane.

A l'heure actuelle, seuls les produits achetés et expédiés de manière traditionnelle sont soumis à des taxes, au contraire des petits colis issus de la commande d'un produit sur le réseau Internet. Ce type commerce est en effet difficilement repérable et son contrôle coûterait plus cher que les recettes qu'il rapporte. (**[INSIDE 98]**)

Fort est à parier qu'avec la venue croissante de nouveaux consommateurs, la tendance pourrait s'inverser. Les vendeurs et les consommateurs devront alors s'attendre à s'acquitter de taxes qui, avec la venue de l'Euro, seront, pour le moins, universelles quant à la devise utilisée!

Manque de conscience des bénéfices potentiels

Enfin, certains auteurs mettent en évidence un manque de conscience des bénéfices potentiels du commerce électronique en Europe.

Face à ce manque de conscience, les autorités européennes ont entrepris un vaste travail de conscientisation notamment au travers de **[COM 97]**:

"Promouvoir l'adoption généralisée du commerce électronique en tant que pratique commerciale courante en Europe, tel est le défi qu'il nous faut relever."

Dans ce bref aperçu des différents freins qui agissent ou ont agi sur le développement du commerce électronique, retenons qu'un certain nombre de leviers devraient permettre d'impulser un mouvement favorable à son développement en Europe:

- Une libéralisation des télécommunications;
- Une mise en place d'un marché unique;
- Une stimulation via l'Euro;
- Un cadre cohérent et réglementaire.

Depuis quelques années donc et, comme nous pouvons l'apercevoir dans la figure ci-dessous, les autorités européennes avancent petit à petit pour offrir un cadre favorable au développement du commerce électronique. C'est au tour principalement des entreprises, aujourd'hui, de poursuivre le mouvement.

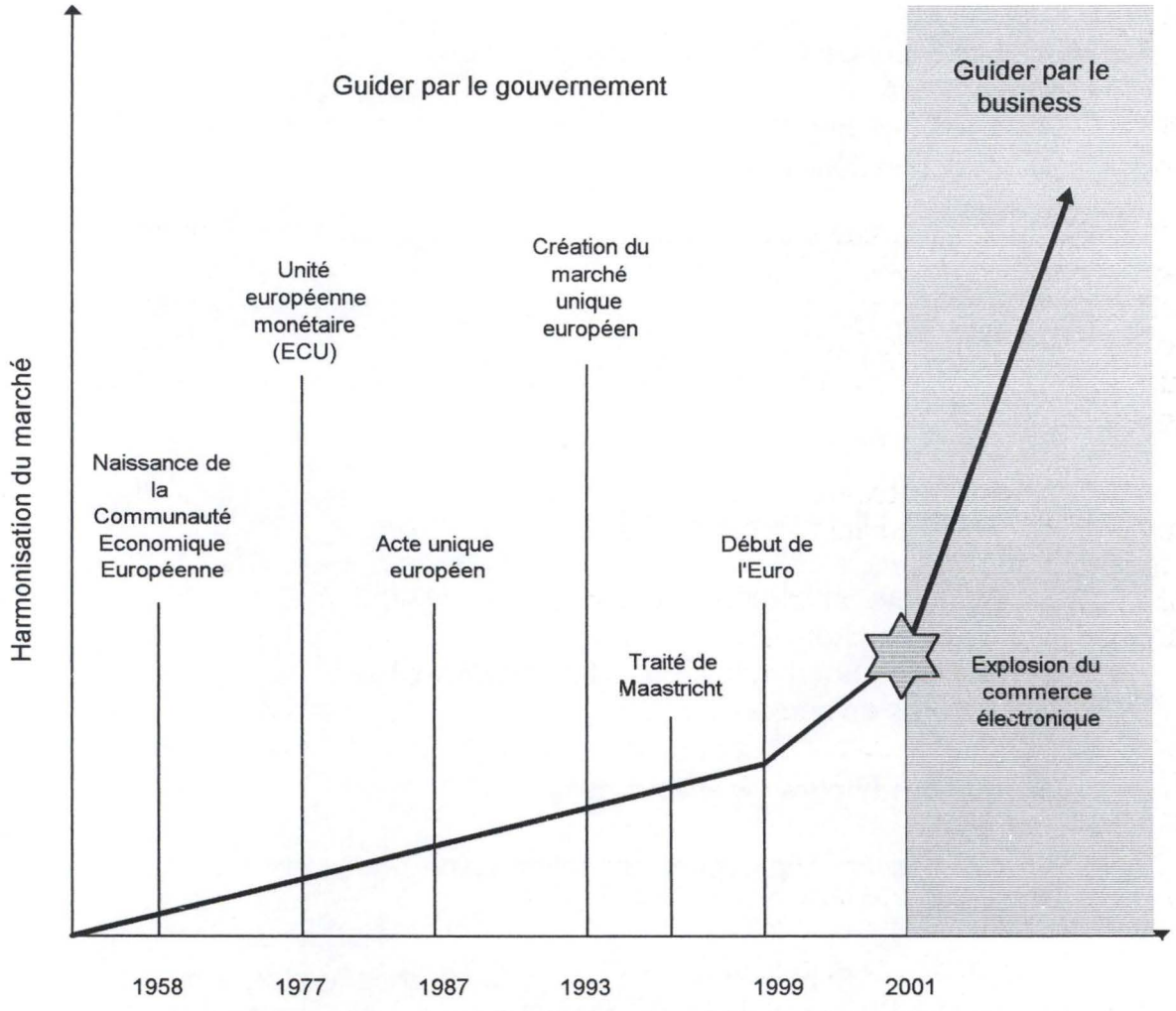


Figure 1: Avancée de l'Europe vers un marché ouvert au commerce électronique [FORRESTER]

6. Situation en Belgique

Même si la Belgique est reconnue comme un pays à la traîne par rapport aux autres pays européens comme l'Allemagne, la Grande Bretagne, la Scandinavie et la France, elle peut se défendre d'être en avance dans certains domaines.

Au 1er avril 1999, **[INSIDE 98]** a répertorié plus de 150 sites de commerce électronique en Belgique. On peut les regrouper en 14 catégories principales. Nous en profitons pour donner l'adresse des sites les plus connus et ce de manière non exhaustive.

- Livres
  - Proxis: http://www.proxis.be/
  - Frontstage: http://www.frontstage.com/
- CD, CD-ROM, DVD
  - Frontstage: http://www.frontstage.com/
- Vêtements:
  - Les 3 Suisses: http://www.3suisses.be/
- Ordinateurs:
  - RedCorp: http://www.redcorp.com/
  - Dell: http://www.dell.be/
- Loisirs
  - Cinebel Ticketing: http://ticketing.cinebel.com/
- Nourriture
  - GB: http://www.ready.be/
  - Delhaize:http://www.caddy-home.be/
- Cadeaux
  - Gift Online: http://www.gift.be/
- Informations
  - Infobel: http://www.infobel.be/
- Internet
  - Advalvas Shop: http://www.shop.advalvas.be/
- Galeries marchandes:
  - Advalvas Shop: http://www.shop.advalvas.be/
- Fournitures de bureau
- Jeux
  - ElliToys:http://www.ellitoys.com/
- Voyages
  - Connection: http://www.connection.com/
- Divers

Signalons que *Shops 2 go to* (http://www.shop2go.to/) est une galerie marchande qui tient à jour la liste complète des sites belges de commerce électronique.

Dans le domaine des paiements électroniques, la Belgique peut se vanter d'être pionnière avec sa solution Proton qui sera analysée de manière détaillée dans le chapitre 3 *Moyens de Paiement*.

Quant aux prévisions, **[IDC 98]** estime que le commerce électronique connaîtra une très forte croissance en Belgique. Le volume des transactions devrait croître de 2.5 milliards à la fin 1998 à 28.5 milliards de francs belges en 2001. La plus importante part de ces transactions seront effectuées par les échanges business-to-business.

7. Impact du commerce électronique sur l'économie

Le commerce électronique est encore relativement neuf et, de ce fait, les analyses de son impact sont souvent basées sur une certaine spéculation ou quelques évidences anecdotiques.

Cependant dans les grandes tendances, il apparaît qu'aujourd'hui, le commerce électronique peut améliorer l'économie mondiale et en accentuer la compétitivité. En bref, elle permet d'en augmenter la croissance à long terme.

Nous allons maintenant nous attarder sur les gains des acteurs principaux, à savoir le vendeur et le consommateur. Nous terminerons par quelques exemples de réussite assez exemplaires.

7.1. Les gains du vendeur

Le commerce électronique permet de toute évidence, par son impact sur la diminution des prix, d'offrir aux entreprises une opportunité pour renouveler les anciens processus et les remplacer par de nouvelles technologies moins onéreuses et de réduire sensiblement les coûts de production.

Les avantages que procurent le commerce électronique aux vendeurs sont multiples:

- Possibilité de disposer de catalogues en ligne;
- Possibilité de publicité;
- Possibilité d'analyse spécifique très importante. Le vendeur est aujourd'hui capable de définir le profil de l'acheteur-type et non plus de spéculer sur une quantité vendue. L'impact sur la publicité est incommensurable et cette dernière en est d'autant plus redoutable!
- Mise à disposition de FAQ (*Frequently Asked Questions* ou *Foire Aux Questions*) pour un meilleur service après vente;
- Gestion des stocks meilleure et plus rigoureuse;
- Amélioration du processus de vente;
- Amélioration de la gestion des transactions;
- Augmentation de l'efficacité commerciale (meilleure capacité de réaction, fiabilité accrue, réduction des coûts);
- Ouverture à un marché mondial.

Ces avantages améliorent considérablement l'efficacité des processus de vente. Un gain incontestable est donc à signaler:

- Dans l'exécution de la vente;
- Dans le placement et l'exécution des commandes;

- Dans le support et le service après vente du consommateur;
- Dans la réduction du staff nécessaire;
- Dans le temps du cycle de la vente.

Signalons toute fois les facteurs défavorables:

- Des coûts supplémentaires et de plus en plus importants nécessaires à une sécurisation des réseaux.
- Les difficultés et les dépenses pour un marchand à accéder au commerce électronique.
- Le coût d'une logistique très personnalisée est souvent onéreux.

7.2. Les gains du consommateur

Les avantages offerts aux consommateurs sont multiples. La liste non exhaustive ci-dessous permettra au lecteur d'en saisir les principaux aspects.

- Proximité. Le consommateur se sent chez lui, dans "son" magasin. La personnalisation est de plus en plus utilisée en marketing et est d'ores et déjà une arme redoutable.
- Facilité de trouver les produits.
- Commodité et simplicité de l'achat.
- Choix innombrable avec des outils de recherche de plus en plus spécialisés et performants
- Comparaison "instantanée" des diverses offres pour un même produit et une information souvent complète.
- Facilités de paiement avec une livraison simple et relativement rapide.
- Économies dont le consommateur est finalement le premier bénéficiaire.
- Accessibilité 24h/24, 7j/7. America OnLine[3] (AOL) rapporte que pratiquement 40% des achats électroniques effectués via leur site se déroulent entre 22h00 et 10h00.

Les facteurs défavorables sont:

- L'achat du matériel, même si l'on constate un coût de plus en plus accessible pour des ordinateurs de plus en plus puissants.
- Les coûts des communications même si ceux-ci sont en diminution. La moyenne calculée par l'OCDE pour 20 heures de communication est tombée de $68 à $20 en l'espace de quelques années.
- Le peu de confiance dans les marchands, leur fiabilité et leur stabilité.
- L'aspect du manque de respect de la vie privée.
- La multiplicité des sites et la difficulté de navigation.

7.3. Exemples

Micron Computers rapporte un gain énorme de productivité dans leur service après-vente. En effet, il estime que les standardistes passent en moyenne deux

[3] http://www.aol.com/

minutes au téléphone avec une personne qui a surfé sur son site Web et vingt minutes pour les consommateurs traditionnels. (**[KEHOE 98]**)

Auto dealers établit les mêmes constatations: il dépense environ $25 pour gérer une offre établie au travers du commerce électronique et parfois plusieurs centaines de dollars dans des transactions courantes (face-à-face) (**[ECONOMIST 98]**)

MCI rapporte que l'utilisation du commerce électronique pour acheter des PCs réduit son cycle d'achat d'ordinateurs de 4 à 6 semaines à 24 heures! (**[MARGHERIO 98]**)

La comparaison de Dell par rapport à Compaq est très illustratrice: la vente des produits Compaq en utilisant les canaux de distribution traditionnels engendre un bénéfice de $16 millions sur une vente de $5.7 milliards (premier quadrimestre 1998). Dell, utilisant principalement Internet pour vendre ses produits, avec un chiffre d'affaires inférieur de $3.9 milliards, engendre un bénéfice supérieur à Compaq: $305 millions! (**[RANDOLPH 98]**)

8. Conclusion

Une question subsiste: l'européen aura-t-il la mentalité nécessaire pour s'ouvrir aux multiples portes de la communication électronique?

Au regard du développement du Minitel en France, on peut supposer que l'européen suivra un même parcours. La France a mis un certain temps avant de se familiariser avec ce nouvel état d'esprit tout comme le fera sans doute l'Europe avec le commerce électronique.

Le commerce électronique sera, dès sa phase de maturité, certainement la *killing application* attendue. En effet, nombreuses sont les personnes qui aujourd'hui déjà, se connectent sur Internet dans le but principal de faire des achats en ligne ou, du moins, de s'informer sur diverses offres commerciales.

De plus, et comme nous le verrons dans les chapitres suivants, par l'évolution du système juridique et technique et sa volonté de diminuer les craintes de l'utilisateur, par des moyens de paiements de plus en plus adaptés à ses besoins et par un environnement plus attractif et personnalisé, la tendance serait de répondre par l'affirmative à la première question.

Chapitre 2: Commerce électronique et sécurité

1. Introduction

Lors d'une connexion sur Internet, dans le but de surfer ou de faire des achats, quatre composants interviennent:

- le navigateur du client;
- le protocole de transmission;
- le serveur Web du marchand;
- le système d'exploitation au-dessus duquel tourne le serveur Web.

Ces quatre composants comportent chacun des lacunes au niveau de la sécurité.

Le commerce électronique pose des problèmes de sécurité, essentiellement en ce qui concerne la transmission des données sur Internet. C'est pourquoi, dans ce chapitre, nous nous intéresserons particulièrement à ces derniers.

Quant aux problèmes liés aux autres composants (trous de sécurité dans les navigateurs, protection des systèmes et base de données du marchand, etc.), ils ne concernent pas spécifiquement le commerce électronique et étaient déjà présent avant l'apparition de celui-ci. C'est pourquoi nous n'aborderons pas ce sujet ici.

Internet est un canal de communication non sécurisé. Lors de la transmission d'un message, celui-ci va, depuis son origine (par exemple un client) et jusqu'à sa destination (par exemple un marchand), passer par plusieurs machines intermédiaires inconnues. Ces dernières pourraient être des espions et donc intercepter, lire, détruire ou modifier les messages. La mise en place d'une connexion sécurisée est donc une nécessité.

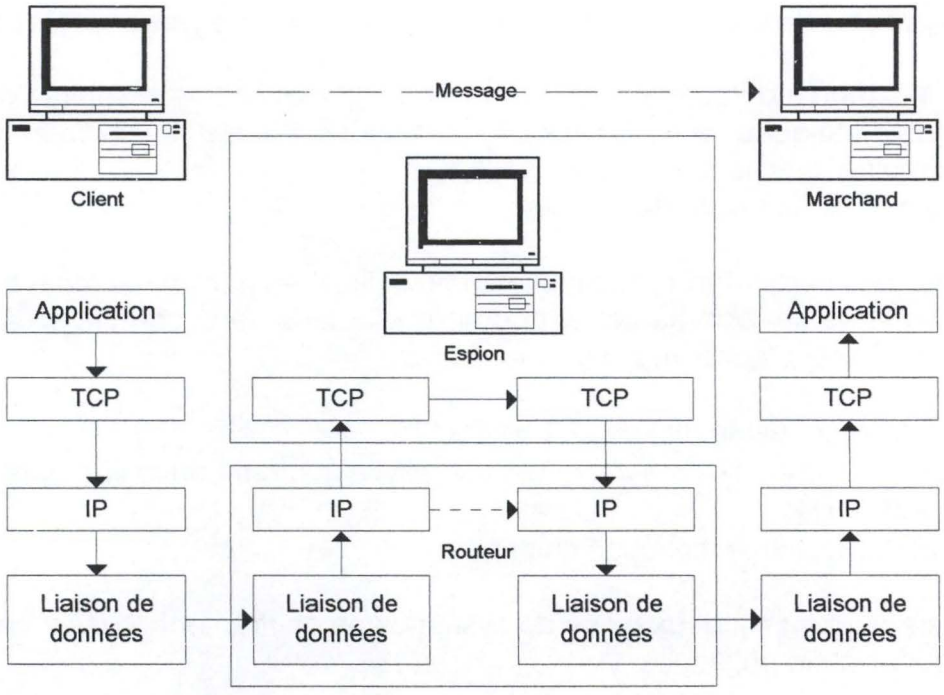


Figure 2: Transmission d'un message

Nous commencerons par un bref rappel du chiffrement, de la signature digitale et du certificat digital. Nous aborderons ensuite les protocoles de sécurisation des transactions SSL et SET. Nous terminerons par analyser le bénéfice au commerce électronique des cartes à puce.

2. Le chiffrement

La rédaction des paragraphes de ce point se base sur **[HUBIN 95]**, **[GHOSH 98]** et **[KOSIUR 98]**.

2.1. Introduction

Lorsque l'on évoque le mot cryptage, on pense avant tout à une sorte de code secret qui interdit aux personnes non autorisées de lire les messages. Notons tout d'abord que le mot cryptage est à bannir. Il est en effet préférable d'utiliser le terme de chiffrement. Bien que l'aspect privatif du chiffrement est important, il ne constitue qu'un des quatre aspects particulièrement importants pour le commerce électronique. Ces aspects sont:

- Authentification: permet à un client de s'assurer que le marchand auquel il envoie les détails de sa carte de crédit est bien la personne qu'il dit être. Cela peut également permettre au marchand de vérifier si le client avec lequel il traite est bien le propriétaire réel de la carte de crédit utilisée.
- Intégrité: permet de s'assurer que le message transmis n'a pas été altéré par une tierce personne durant sa transmission.
- Non répudiation: permet d'empêcher un client ou un marchand de nier avoir reçu ou envoyé un message particulier.
- Aspect privatif: permet de s'assurer qu'une tierce personne ne sera pas capable de prendre connaissance des messages transmis.

Les éléments principaux d'un système de chiffrement sont le message à chiffrer, l'algorithme de chiffrement, la clé et le message chiffré (ou cryptogramme).

- L'algorithme de chiffrement (ou crypto-système) est un ensemble de règles mathématiques qui définissent comment le texte à chiffrer doit être combiné avec la clé.
- La clé est une suite de chiffres.

Ces termes seront fort probablement mieux illustrés par un exemple simple: si nous prenons le terme 'commerce' et que nous ajoutons deux caractères à chaque lettre, le terme devient 'eqoogteg'. Dans ce cas-ci:

- 'commerce' est le message à chiffrer;
- 'ajouter x caractères à chaque lettre' est l'algorithme de chiffrement;
- '2' est la clé;
- 'eqoogteg' est le message chiffré.

Il existe aujourd'hui deux types de systèmes de chiffrement utilisés: ceux à clé partagée et ceux à clé publique.

2.2. Chiffrement à clé partagée

Le chiffrement à clé partagée, encore appelé chiffrement à clé unique ou chiffrement symétrique, implique l'utilisation d'une seule clé qui est partagée par l'expéditeur et le récepteur du message.

Après avoir créé le message, l'expéditeur le chiffre avec la clé partagée et l'envoie au récepteur qui le déchiffre alors en utilisant une copie de la même clé que celle utilisée pour le chiffrement. On peut schématiser ce système ainsi:

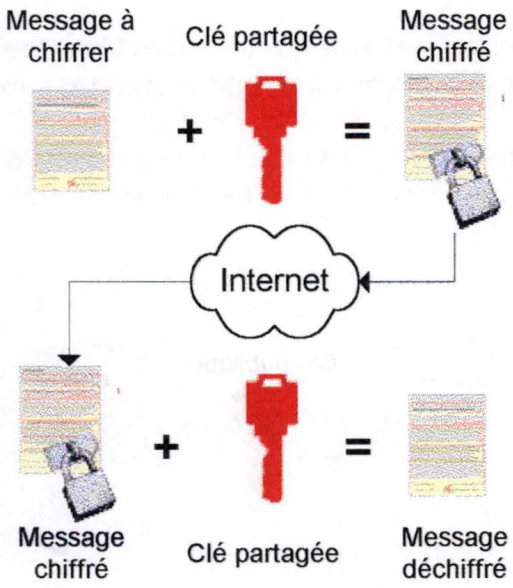


Figure 3: Chiffrement à clé partagée

Une méthode de chiffrement largement utilisée est le ***D**ata **E**ncryption **S**tandard* (DES). Cette méthode fut publiée en 1974 par le NBS (***N**ational **B**ureau of **S**tandard*). C'est une version remaniée par IBM et la NAS (***N**ational **S**ecurity **A**gency*) de l'algorithme Lucifer créé par IBM.

Le chiffrement à clé partagée a cependant quelques limites tout particulièrement en ce qui concerne la distribution de la clé. Pour que l'aspect privatif soit conservé, chaque émetteur de messages devra fournir une clé différente à toutes les personnes avec lesquelles il compte communiquer, sinon chaque récepteur potentiel sera en mesure de lire tous les messages, qu'ils lui soient destinés ou non.

Ce système est maniable dans le cas où un nombre restreint de parties sont impliquées. Dans le cas du commerce électronique, qui peut engendrer des communications entre des centaines de client, une telle solution n'est plus adéquate.

Une autre limitation du chiffrement à clé partagée est sa totale incapacité à supporter la non-répudiation. Étant donné que les parties possèdent la même clé, il est tout à fait possible pour une partie de créer un message chiffré avec la clé partagée et faire croire qu'il lui a été envoyé par une autre partie.

Le chiffrement à clé partagée utilisé seul ne convient donc pas pour le commerce électronique. A la place, un système connu sous le nom de chiffrement à clé publique est utilisé.

2.3. Chiffrement à clé publique

Le chiffrement à clé publique, ou chiffrement asymétrique, implique l'utilisation de deux clés: une pour chiffrer le message et l'autre pour le déchiffrer. Ces clés portent le nom de clé publique, désignant celle mise à disposition de tout un chacun, et de clé privée, quand elle n'est connue que de son propriétaire.

Ces paires de clés peuvent être utilisées dans les deux sens afin de permettre l'aspect privatif des transmissions et l'authentification de l'expéditeur.

L'aspect privatif est réalisé par le chiffrement du message avec la clé publique du destinataire. De ce fait, il ne peut être déchiffré que par la personne à qui l'expéditeur le destine grâce sa clé privée.

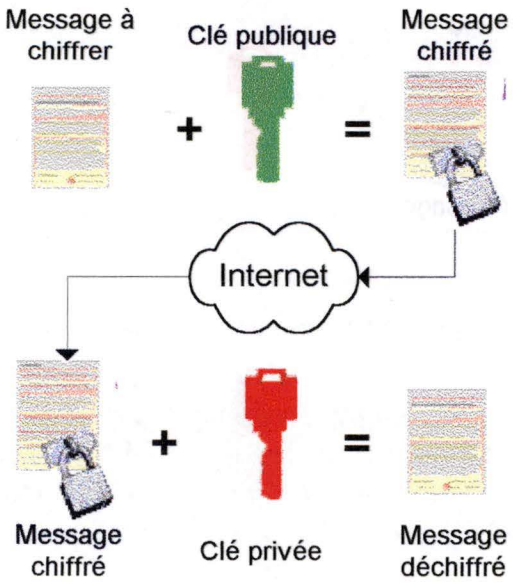


Figure 4: Réalisation de l'aspect privatif

L'authentification est réalisée par le chiffrement du message avec la clé privée de l'expéditeur. De cette manière, le destinataire, ne sachant déchiffrer le message qu'avec la clé publique de l'expéditeur, peut s'assurer de l'identité de celui-ci.

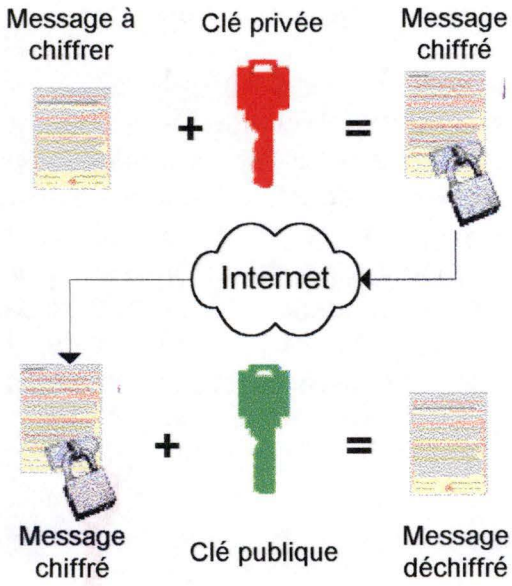


Figure 5: Réalisation de l'authentification

Du fait que la clé publique peut être largement distribuée (par exemple à partir du serveur d'une organisation tierce), le chiffrement à clé publique ne souffre pas du même problème de distribution des clés que les systèmes de chiffrement à clé partagée.

Il est important de remarquer que les deux clés sont liées par une relation mathématique mais que la connaissance d'une des deux clés et/ou d'un message chiffré et/ou déchiffré ne permet pas de retrouver l'autre clé.

L'algorithme de chiffrement le plus connu est fort probablement le RSA, du nom de ces trois auteurs: **R**ivest, **S**hamir et **A**delman.

Le désavantage des systèmes de chiffrement à clé publique est qu'ils sont relativement lents. Ainsi, lorsqu'un système de ce type est utilisé uniquement pour une authentification, il n'est pas nécessaire de chiffrer l'entièreté du message, particulièrement si celui-ci est long. On utilise alors une signature digitale.

2.4. Signature digitale

Une signature digitale est implémentée par un système de chiffrement à clé publique et utilisée pour vérifier l'origine et le contenu d'un message.

Un avantage du chiffrement à clé publique est que le récepteur d'un message préalablement chiffré avec la clé privée de l'expéditeur, et déchiffré avec succès à l'aide de la clé publique de ce dernier, connaît l'identité de l'expéditeur. C'est le principe de l'authentification, sur base duquel fonctionne une signature digitale.

Le message à chiffrer est tout d'abord passé au travers d'un algorithme à sens unique (one-way function). Il en résulte un nouveau message appelé *digest*. Ce

digest est nettement plus petit que le message d'origine. Il n'est pas possible de reconstruire le message d'origine à partir du digest.

Le digest peut être rapidement chiffré avec la clé privée de l'expéditeur. Le message résultant est la signature digitale. Celle-ci sera ajouté au message à envoyer avant sa transmission. Le récepteur du message pourra alors s'assurer de l'identité de l'expéditeur. De plus, il pourra également s'assurer que le message n'a pas subi de transformations lors de sa transmission. Il suffit, pour cela, au destinataire de recalculer le digest. Si celui-ci correspond à celui qu'il a reçu (digest qu'il aura été capable de déchiffrer grâce à la clé publique de l'expéditeur), il saura que le message est intact. En effet, toute modification du message durant sa transmission modifiera de façon imprévisible le digest calculé par le destinataire.

Figure 6: Création d'une signature digitale

L'authentification peut encore être renforcée par l'utilisation d'un certificat digital.

2.5. Certificat digital

Avant de chiffrer et de transmettre une information sensible, il est important de s'assurer que la clé publique utilisée appartient bien à la personne à laquelle l'émetteur destine l'information et non à quelqu'un qui se présente comme telle.

Un méthode possible est l'utilisation d'un organisme de confiance ou d'une **A**utorité de **C**ertification (AC). Les possesseurs d'une clé publique la soumettent à l'AC avec une preuve de leur identité. L'AC émet alors un certificat qu'elle signe avec sa clé privée qui certifie que la clé publique attachée au certificat appartient bien à la partie mentionnée sur le certificat.

Il existe différentes classes de certificat suivant le type de vérification effectuée par l'AC auprès du demandeur de certificat.

- Certificat de classe 1: le certificat digital de classe 1 propose de déposer dans un fonds spécial un nom non ambigu et une adresse électronique. Ce certificat peut être obtenu pour un temps limité, peu importe le domicile du demandeur. Les certificats digitaux de classe 1 sont habituellement gratuits et sont délivrés à titre d'essai.
- Certificat de classe 2: Le certificat digital de classe 2 offre de meilleures assurances quant à l'identité de son propriétaire dans la mesure où il exige que les nom, prénom, adresse et autres données personnelles du demandeur aient été vérifiés par une copie de sa carte d'identité/ passeport/ permis de conduire et sa signature.

- Certificat de classe 3: le certificat de classe 3 offre un haut niveau d'authentification grâce à une procédure de vérification sévère de l'identité du demandeur, ce qui permet son utilisation à des fins professionnelles pour des applications critiques. Ce type de certificat offre une assurance de niveau supérieur quant à l'identité dans la mesure où le demandeur doit se présenter personnellement devant une autorité locale d'enregistrement (ALE).
- Certificat de classe 4: ces certificats existent en théorie mais leurs spécifications n'ont pas encore été finalisées. Ils se différencient des certificats de classe 3 par le fait qu'ils incluent la position de leur propriétaire dans une organisation.

Les certificats digitaux fournissent la base pour sécuriser les transactions électroniques puisqu'ils permettent à l'ensemble des participants de la transaction de rapidement et facilement vérifier l'identité des autres intervenants.

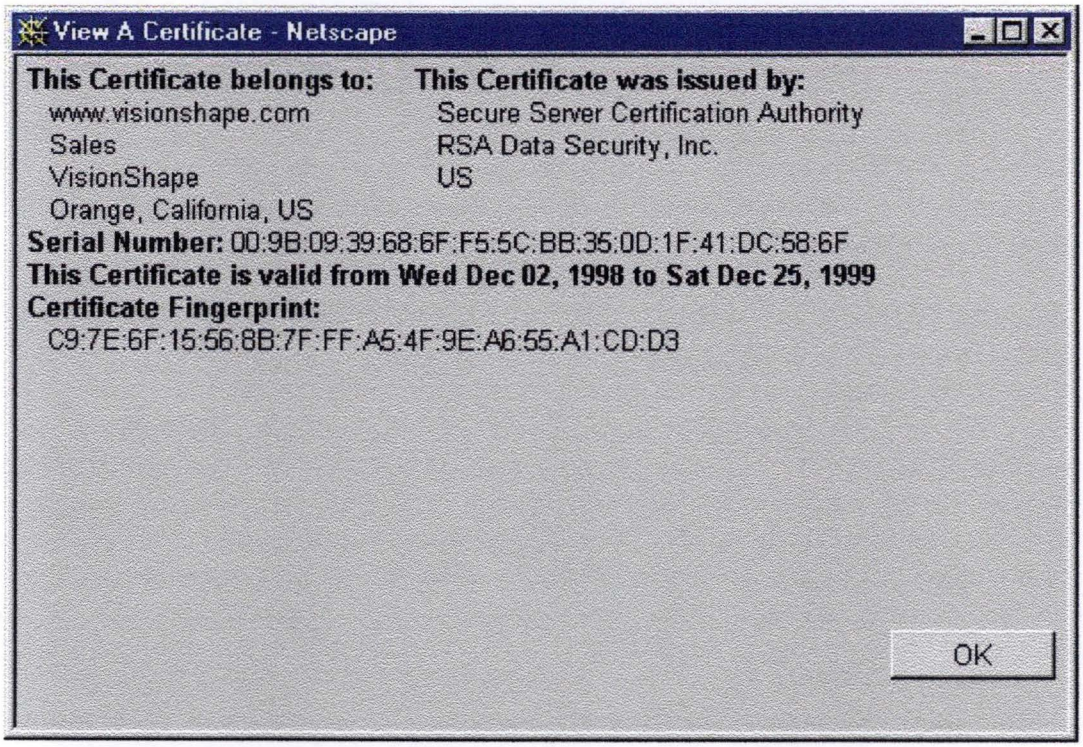


Figure 7: Certificat digital comme il apparaît dans Netscape Navigator 4.x

Analysons les informations fournies par Netscape Navigator lorsque l'on demande l'affichage d'un certificat. Ce certificat reprend l'identité du propriétaire du certificat, l'identité de l'AC qui l'a délivré, sa période de validité, son numéro de série et sa signature. Seule la clé publique du propriétaire du certificat n'apparaît pas.

N'oublions cependant pas que ces certificats permettent uniquement de vérifier l'identité de la partie avec laquelle une connexion sécurisée a été établie. Dans le cas de sites marchands, ils ne présument en rien de la qualité et de la validité du contenu du serveur marchand.

Les Autorités de Certification ont également la responsabilité de maintenir à jour une liste de tous les certificats révoqués. Cette liste permet à un utilisateur de

vérifier si un certificat est toujours valide. Elle ne contient pas les certificats dont la date d'expiration a été atteinte mais bien les certificats révoqués pour d'autres raisons. Il peut par exemple s'agir du certificat d'une société ayant fait faillite.

2.6. Restrictions sur l'exportation de système de chiffrement

Qu'est-ce qu'ont en commun une bombe et un système de chiffrement? D'après la loi américaine, les systèmes de chiffrement sont classés comme des munitions et l'exportation de logiciels contenant des systèmes de chiffrement est contrôlée par les *Defense Trade Regulations* américaines. En général, ces régulations interdisent l'exportation, à partir des États-Unis, de logiciels qui emploient des systèmes de chiffrement avec de longues clés. Il y a cependant quelques exceptions comme, par exemple, les logiciels utilisés dans le seul but de chiffrer des données financières et de les transférer entre des banques approuvées.

En 1992, la *Software Publishers Association* a conclu un accord avec le Département d'État. Cet accord autorise l'exportation de logiciels contenant les algorithmes de chiffrement RC2 et RC4 développés par la société américaine RSA mais seulement si la taille de la clé était limitée à 40 bits (par opposition aux clés de 128 bits disponibles pour une utilisation à l'intérieur des États-Unis). La sécurité d'un algorithme de chiffrement dépend de la longueur de la clé utilisée. Plus la clé est longue, plus il y a de combinaisons possibles et plus le temps nécessaire pour craquer le message chiffré sera long.

Depuis 1992, la vitesse et la disponibilité des ordinateurs ont considérablement augmenté et bien que déchiffrer un message chiffré avec une clé de 40 bits prend encore un temps assez important, cela devient faisable. A l'heure actuelle, il est encore plus facile et productif pour un voleur, de scanner le trafic Internet pour trouver des numéros de cartes de crédit non chiffrés que d'en trouver un chiffré et de le craquer. Cependant, au fur et à mesure que la puissance des ordinateurs augmentera, le temps pour décrypter des messages chiffrés avec des clés de 40 bits continuera de diminuer et les clés de 40 bits ne pourront plus être considérées comme assez sûres pour effectuer des transactions de commerce électronique.

Le tableau ci-dessous reprend le temps moyen nécessaire pour craquer un message suivant la longueur de la clé utilisée et l'investissement en matériel réalisé pour effectuer le déchiffrement.

	Longueur de la clé en bits				
Prix	40	56	64	80	128
$100 000	2 secs	35 h	1 an	70 000 ans	10^{19} ans
$1 million	0.2 secs	3.5 h	37 jours	7000 ans	10^{18} ans
$100 millions	2 millisecs	2 mins	9 h	70 ans	10^{16} ans
$1 milliard	0.2 millisecs	13 secs	1 h	7 ans	10^{15} ans
$100 milliards	2 microsecs	0.1 secs	32 secs	24 jours	10^{13} ans

Tableau 3: Comparaison du temps et de l'argent nécessaires pour déchiffrer un message. [SCHNEIER 96]

Le gouvernement américain a proposé diverses méthodes rendant possible l'exportation de systèmes de chiffrement utilisant des clés plus longues. Ces méthodes sont toutes basées sur des systèmes de récupération de clés permettant, aux agences d'application de la loi, d'obtenir une copie de clés privées, si besoin est, pour déchiffrer certains messages.

Un ordre exécutif (*the Administration of Export Control on Encryption Products*) a pris effet le 1er janvier 1997. Il autorise les vendeurs à expédier, dans le monde entier, des systèmes de chiffrement utilisant des clés de 56 bits mais à la condition ultime que soit ajouté, dans le système, endéans les 2 ans, un système de récupération des clés. Cependant l'industrie a montré une résistance considérable à l'intégration de ces systèmes de récupération, craignant pour la vie privée des individus et des entreprises.

La résolution de ce problème est considérée comme vitale pour l'avenir du commerce électronique mondial.

3. SSL

Les différents paragraphes de ce point sont basés sur les explications de **[GHOSH 98]**

3.1. Introduction

Le protocole SSL (***S**ecure **S**ockets **L**ayer*) fut créé par Netscape. C'est aujourd'hui la méthode la plus utilisée pour sécuriser les transactions sur Internet. De plus, ce protocole est supporté par la majorité des serveurs Web ainsi que par la plupart des navigateurs clients tels que Netscape[4] Navigator et Microsoft[5] Internet Explorer.

SSL offre la possibilité de créer un canal sécurisé entre un client et un marchand. Il permet également d'authentifier le serveur et certifie l'intégrité des données.

- L'aspect privatif est garanti par le chiffrement. Bien que l'information puisse toujours être interceptée par un espion, ce dernier ne pourra la déchiffrer étant donné qu'il n'a pas accès à la clé de chiffrement.
- L'intégrité est aussi assurée par le chiffrement. Si l'information reçue ne peut être déchiffrée correctement, alors le récepteur sait que l'information transmise a été altérée durant sa transmission.
- L'authentification est assurée par l'emploi de certificats digitaux. Ces certificats fournissent une base aux transactions électroniques sécurisées puisqu'ils permettent à tous les participants de la transaction de facilement et rapidement vérifier l'identité des autres participants. SSL 2.0 permet l'authentification du serveur marchand. La version 3.0 y ajoute la possibilité d'authentifier le client.

[4] http://www.netscape.com/
[5] http://www.microsoft.com/

Le navigateur Internet Explorer de Microsoft permet à son utilisateur de connaître la version de SSL utilisée lors de l'établissement d'une connexion sécurisée.

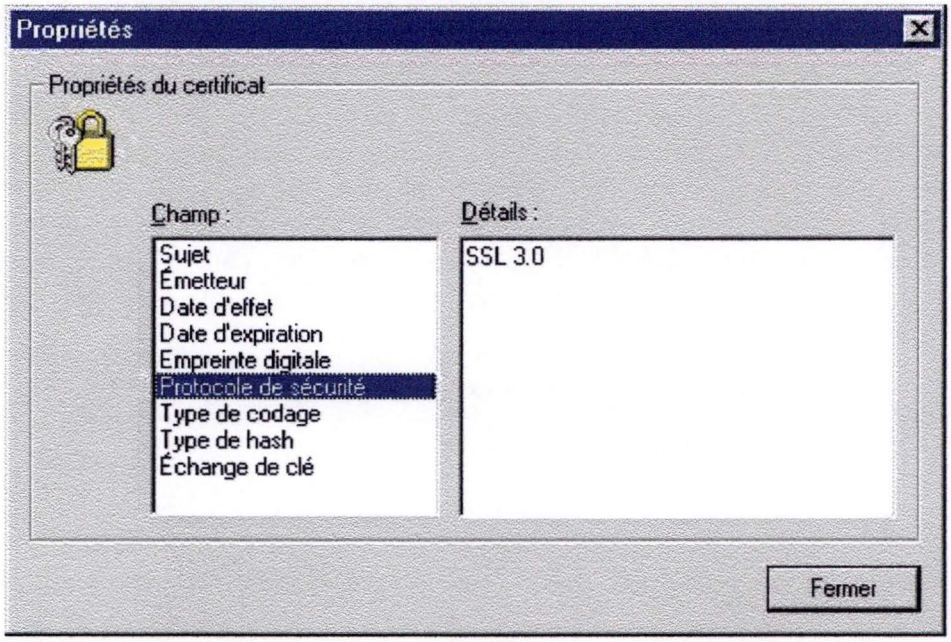


Figure 8: Visualisation dans Microsoft Internet Explorer de la version de SSL utilisée

Mais il nous faut mentionner que SSL se limite à cela. C'est à dire que les données ne sont sécurisées que le long de la ligne de communication et non sur la machine client ou sur le serveur Web.

3.2. Positionnement de SSL

Si l'on reprend le modèle des couches sous-jacent à toute transmission sur un réseau, SSL est simplement une nouvelle couche située juste au-dessus de la couche de transport TCP. Donc en théorie, toutes les applications étant situées au-dessus de SSL, elles pourraient utiliser cette méthode pour sécuriser leurs données. Cependant actuellement seul HTTP utilise SSL.

HTTP	mail	telnet	news	ftp	LDAP	Autres
SSL						
TCP						
IP						
Liaison de données						

Figure 9: Positionnement de SSL

3.3. Le processus de chiffrement

SSL utilise deux techniques différentes de chiffrement: un système à clé partagée et un système à clé publique.

La raison pour laquelle on utilise ces deux techniques se justifie simplement, comme nous l'avons déjà signalé, par le fait que les méthodes de chiffrement à clé publique sont nettement plus lentes que celles à clé partagée.

Au départ le serveur du marchand envoie au navigateur du client son certificat contenant sa clé publique. Le navigateur du client après avoir authentifié le serveur chiffre alors une pré-clé qu'il a créée au hasard avec la clé publique du serveur et la lui envoie. Le navigateur du client et le serveur génèrent alors des clés partagées qui ne sont utilisées que pour la connexion en cours. On les appelle des clés de session. Ensuite et pour le reste de la connexion, le navigateur du client et le serveur du marchand utilisent une méthode de chiffrement à clé partagée en utilisant comme clés celles de session précédemment créées.

3.4. SSL en action

Une connexion SSL est établie à la demande d'un utilisateur. A cet effet, il préfixe l'URL du document souhaité par 'https' en opposition à la manière habituelle qui est d'utiliser 'http'. Par exemple,

http://server.domain.com/index.html

demande que le document index.html soit envoyé par le protocole standard HTTP[6], alors que

https://server.domain.com/index.html

demande au serveur l'envoi du même document par le protocole HTTPS. Le protocole HTTPS est une version modifiée du protocole HTTP qui incorpore SSL.

L'établissement de la connexion sécurisée porte le nom de *SSL handshake*. Le but de cette procédure est de:

- Authentifier le serveur;
- Permettre au navigateur du client et au serveur de sélectionner les méthodes de chiffrement qu'ils utiliseront;
- Authentifier le client le cas échéant;
- Générer les clés de session;
- Établir la connexion sécurisée de type SSL;

Nous examinerons ici les différentes étapes accomplies lors de l'établissement d'une connexion sécurisée dans le cas où l'identité du client n'est pas vérifiée. C'est, en effet le cas le plus courant à l'heure actuelle: la vérification de l'identité du client

[6] Protocole utilisé sur le Web et définissant la façon dont sont formatés et transmis les messages circulant sur Internet. La version la plus répandue est la version HTTP 1.1.

nécessite de la part de celui-ci l'achat d'un certificat auprès d'une Autorité de Certification.

1. Le navigateur du client (dénommé ci-après 'le client') demande au serveur qu'un document lui soit transmis en utilisant le protocole HTTPS. Il envoie par la même occasion au serveur le numéro de la version de SSL qu'il utilise, une suite d'identificateurs de protocoles de sécurité ainsi qu'une chaîne de caractères créée au hasard. Ces identificateurs de protocole de sécurité consistent en:

    - L'identificateur du protocole de chiffrement à clé partagée qui sera utilisé. Microsoft Internet Explorer permet de connaître le protocole choisi.

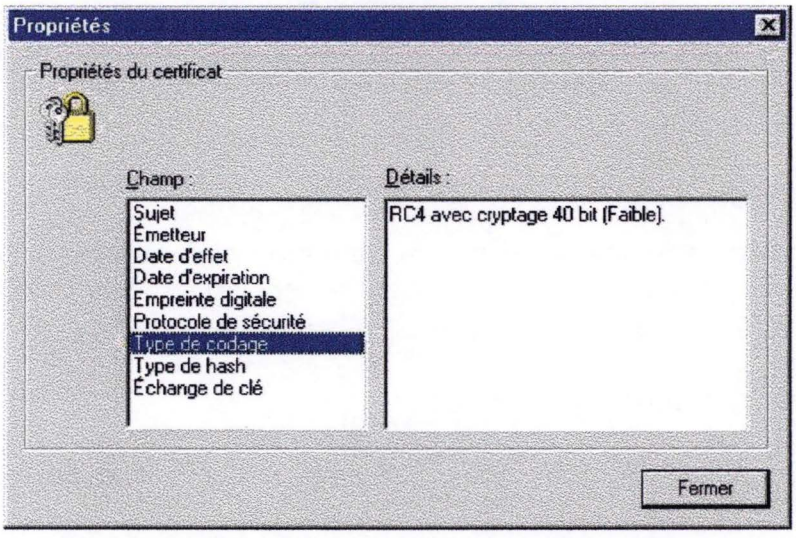


Figure 10: Identificateur du système à clé partagée utilisé

- L'identificateur des algorithmes à sens unique qui seront utilisés pour vérifier l'intégrité des messages. Microsoft Internet Explorer permet à son utilisateur de connaître la méthode employée.

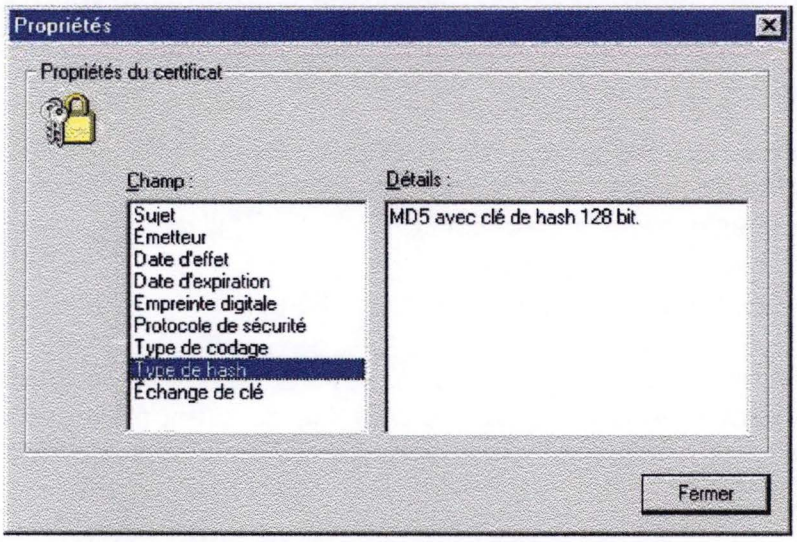


Figure 11: Identificateur des algorithmes à sens unique utilisés

- L'identificateur des algorithmes qui seront utilisés pour créer les clés de session. Microsoft Internet Explorer permet à nouveau de connaître le système choisi.

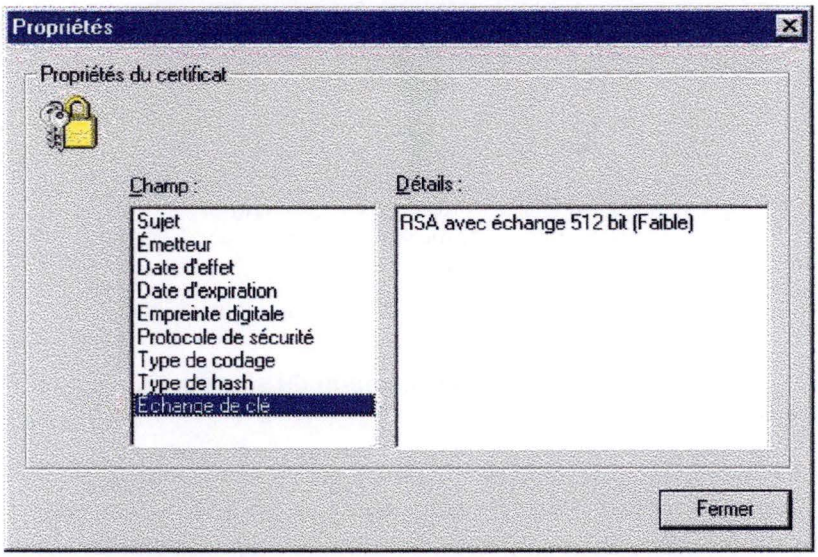


Figure 12: Identificateur du système de création des clés de session

2. En réponse à ce message, le serveur envoie: le numéro de version de SSL qu'il emploie, son certificat au format X.509[7], son accord sur les algorithmes à utiliser proposés par le client et un identifiant de connexion créé aléatoirement. Les algorithmes de chiffrement proposés par le client sont choisis par ce dernier suivant la version de SSL utilisée et les restrictions gouvernementales sur l'exportation des systèmes de chiffrement.
3. Le client authentifie alors le serveur grâce au certificat qu'il vient de recevoir. Il commence par vérifier la date de validité du certificat. Ce certificat est digitalement signé avec la clé privée de l'Autorité de Certification ayant émis le certificat. Le client tente alors de déchiffrer la signature avec la clé publique de l'Autorité de Certification ayant émis le certificat[8]. Si après déchiffrement de la signature, le client obtient le digest correspondant aux informations contenues dans le certificat, alors le serveur est authentifié.

[7] Standard mondialement utilisé pour définir des certificats digitaux

[8] Un navigateur contient le certificat de plusieurs Autorités de Certification lors de son installation. Cela implique que, par défaut, l'utilisateur du navigateur fait confiance à tous les sites Web ayant un certificat signé par ces différentes Autorités de Certification. L'utilisateur a le loisir d'ajouter ou de supprimer de son navigateur des certificats d'Autorités de Certification.

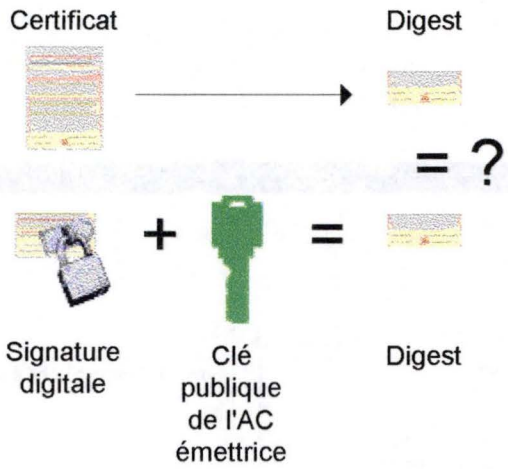


Figure 13: Authentification du serveur

4. Si le serveur est authentifié, le client génère un nombre secret (*premaster key*) qui sera utilisé pour générer les clés de session (*master key*).
5. Ce nombre secret est chiffré avec la clé publique du serveur (qui était contenue dans le certificat du serveur) et lui est envoyé. Dès lors, on n'utilise plus le système de chiffrement à clé publique mais le système à clé partagée. Le nombre secret envoyé au serveur est généré par le client afin d'éviter que le serveur ne réutilise le même nombre pour différentes connexions.
6. A ce moment, les deux machines (le client et le serveur) connaissent le nombre secret généré par le client. Elles connaissent également la méthode à utiliser pour générer les clés de session puisqu'elles se sont mises d'accord en début de procédure. Les deux machines créent ensuite les deux clés de session pour sécuriser la transmission. Étant donné qu'elles utilisent la même méthode, elles généreront les mêmes clés. Une des clés sera utilisée pour chiffrer le trafic sortant du client et entrant dans le serveur tandis que l'autre sera utilisée pour chiffrer le trafic sortant du serveur et entrant dans le client.

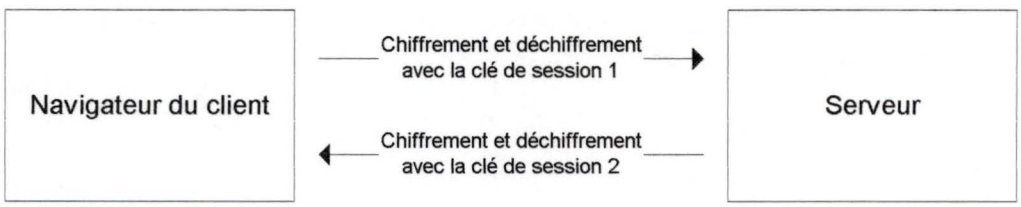


Figure 14: Utilisation des deux clés de session

7. Le navigateur du client envoie alors au serveur, après l'avoir chiffré avec une des deux clés de session, l'identifiant de connexion que le serveur avait créé.
8. Si le serveur, après l'avoir déchiffré, reconnaît l'identifiant qu'il avait créé, il sait qu'une connexion sécurisée a été établie.

9. Par la suite, le serveur envoie au client la chaîne de caractères que ce dernier avait créée en tout début de procédure. Avant de l'envoyer, le serveur chiffre cette chaîne avec l'autre clé de session.
10. Le client vérifie la validité de cette chaîne de caractères après l'avoir déchiffrée. S'il s'agit de la chaîne qu'il avait créée, il sait également qu'une connexion sécurisée a été établie. Rappelons que cette chaîne de caractère avait été envoyée en début de session sous forme non chiffrée.
11. A ce moment là peuvent avoir lieu des transferts d'informations sécurisés basés sur un système de chiffrement à clés partagées connues uniquement du serveur et du client. Le serveur envoie, par exemple, la page demandée en début de procédure par le client.

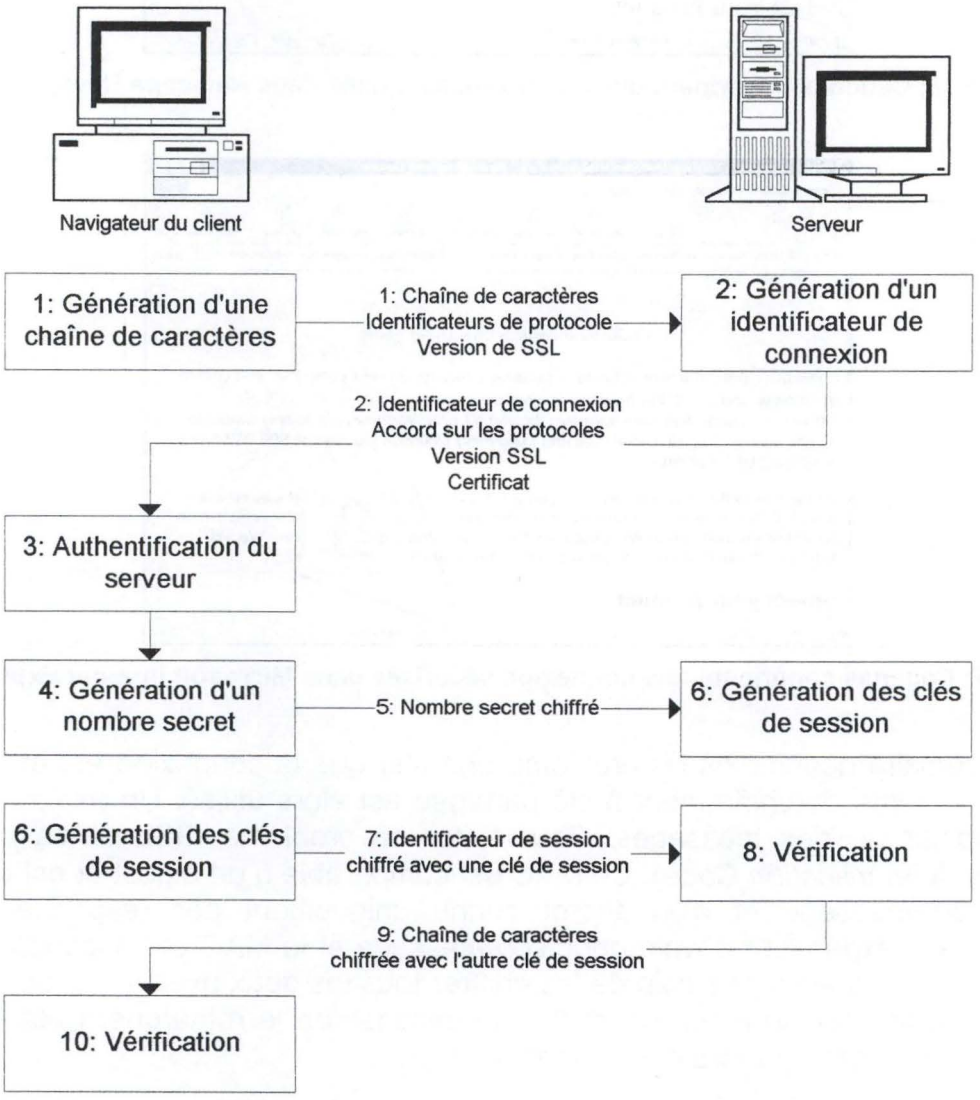


Figure 15: Établissement d'une connexion sécurisée de type SSL

Netscape Navigator et Microsoft Internet Explorer permettent de vérifier aisément si une connexion sécurisée a été établie. Il suffit de vérifier que le cadenas situé en bas de la fenêtre du navigateur soit fermé.

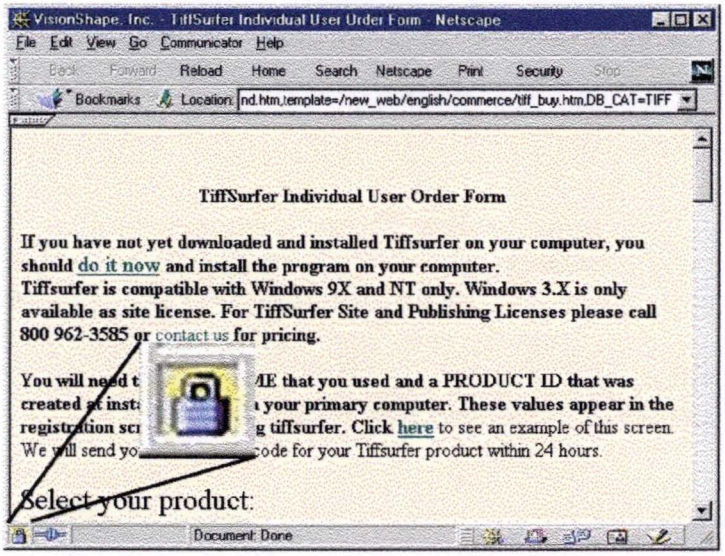


Figure 16: Cadenas confirmant une connexion sécurisée dans Netscape Navigator 4.x

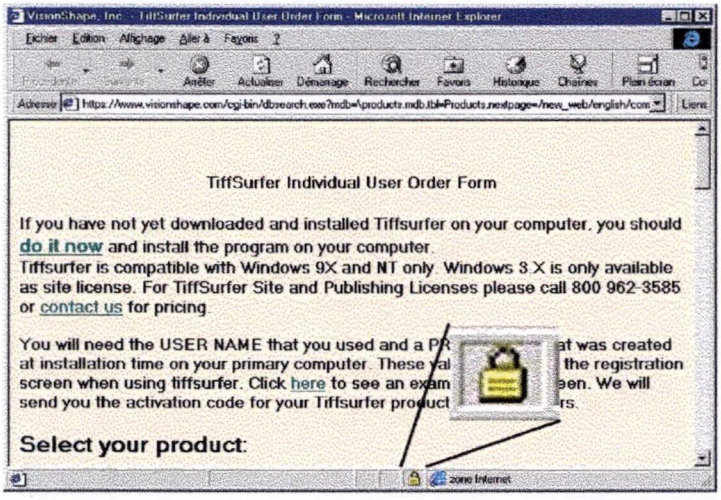


Figure 17: Cadenas confirmant une connexion sécurisée dans Microsoft Internet Explorer 4.x

Il persiste néanmoins un problème une fois que la connexion est établie. En effet, un système de chiffrement à clé partagée est alors utilisé. Un espion pourrait donc modifier un des messages. Pour éviter ce problème, SSL utilise un MAC (***M**essage **A**uthentication **C**ode*). Ce MAC est comparable à un digest et est construit à partir du message et d'un secret connu uniquement par l'expéditeur et le destinataire. L'expéditeur envoie donc son message et le MAC correspondant à son destinataire après avoir pris soin de les chiffrer tous les deux avec la clé de session. Si un espion modifie le message chiffré, le destinataire le remarquera étant donné que le MAC ne correspondra pas au message reçu.

Enfin, pour éviter qu'un éventuel espion ayant capté un message puisse l'envoyer une seconde fois, tous les messages échangés durant la connexion sécurisée se voient attribuer un numéro de séquence contenu dans le MAC.

Une alternative au protocole SSL est le protocole SET, que nous allons décrire un peu plus bas.

3.5. Le spoofing

Malgré toute la sécurité que procure SSL, ce dernier n'empêche pas le spoofing.

Le spoofing est le terme désignant la situation dans laquelle un serveur Web se fait passer pour un autre serveur Web sans que la personne connectée ne s'en rende compte.

Supposons donc qu'un client souhaite se connecter sur le serveur d'un marchand. Il trouve un lien vers ce marchand dans une page HTML située sur un serveur attaquant. Cette page est écrite de telle manière qu'apparaisse à l'écran un lien vers https://www.marchand.com/ (lien établissant une connexion sécurisée vers le marchand) alors que le lien conduit à https://www.attaquant.org/https://www.marchand.com/. De cette manière, le serveur de l'attaquant fait office de proxy[9]. Le client aura l'impression de s'être connecté chez le marchand alors qu'il est toujours connecté chez l'attaquant. Lorsque le client demande la page https://www.marchand.com/index.html, l'attaquant reçoit la demande et la transmet au marchand. Ce dernier envoie alors à l'attaquant la page en question. L'attaquant a alors tout le loisir de la modifier avant de la transmettre au client.

Pour que le client ne se rende pas compte de cette supercherie, l'attaquant possède lui aussi un certificat. De cette manière, la connexion établie entre l'attaquant et le client sera bien une connexion SSL sécurisée. De plus, l'attaquant peut utiliser un scripte écrit en JavaScript afin qu'apparaisse dans la barre d'adresse du navigateur du client l'adresse du serveur marchand (https://www.marchand.com/) et non l'adresse à laquelle le client est réellement connecté (https://www.attaquant.org/https://www.marchand.com/).

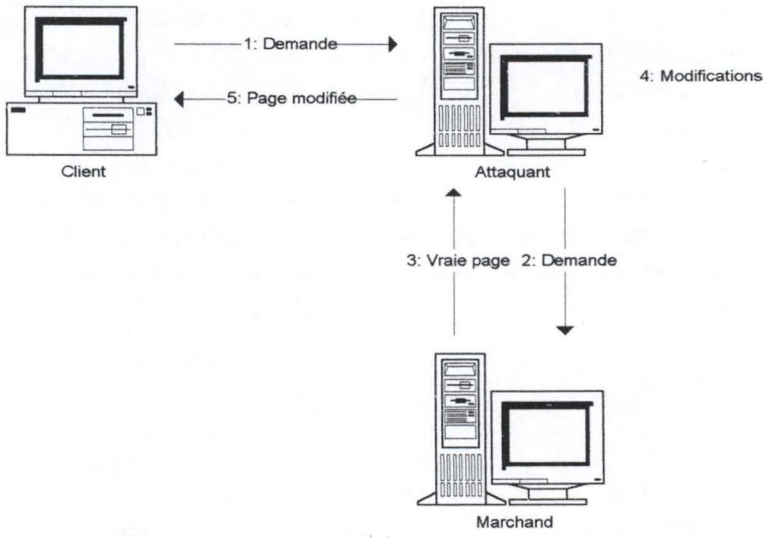


Figure 18: La technique du spoofing

[9] Un proxy est un serveur situé entre une application cliente (telle qu'un navigateur) et un serveur réel. Ce proxy intercepte toutes les demandes envoyées au serveur réel. S'il sait satisfaire la demande, il la satisfait. Dans le cas contraire, il la fait suivre au serveur réel.

La seule solution pour le client de s'assurer qu'un serveur tiers n'est pas en train de faire du spoofing est de désactiver JavaScript dans son navigateur afin de s'assurer que l'URL affichée dans la barre d'adresse est bien l'adresse du site auquel il est connecté et de vérifier l'identité du serveur avec lequel il est réellement connecté, en affichant son certificat.

4. SET

La rédaction des paragraphes de ce point est basée sur **[SET 97]** décrivant le protocole SET. Ces documents disponibles sur le site Web officiel de SET[10].

4.1. Introduction

SET est l'abréviation de ***S**ecure **E**lectronic **T**ransaction*, protocole spécialement développé par Visa[11] et MasterCard[12] pour établir sur Internet des transactions sécurisées à base de cartes de crédit. Lors du développement de SET, Visa et MasterCard ont reçu le soutien et l'aide de GTE[13], IBM[14], Microsoft, Netscape, RSA[15], SAIC[16], Terisa[17], et VeriSign[18].

Il faut tout d'abord remarquer que, contrairement à SSL qui est un protocole visant uniquement à sécuriser la transmission d'informations (quelque soit leur type), SET est un protocole de paiement.

SET utilise des certificats digitaux pour assurer l'identité de tous les acteurs en présence (acheteur, marchand et institution financière). Tout comme SSL, SET permet la vérification de l'identité du marchand par l'utilisation d'un certificat digital. Cependant, SET permet également au marchand de vérifier l'identité de l'acheteur, ici aussi grâce à un certificat digital. Cela permet de rendre l'utilisation d'une carte de crédit volée plus difficile.

SET chiffre également les informations de paiement avant de les faire transiter sur Internet. De par le fait que SET ne chiffre que les données financières de la commande, il est exempté des restrictions américaines sur l'exportation de systèmes de chiffrement et contrairement à SSL, il peut chiffrer les détails d'une carte de crédit avec une clé de 128 bits.

Les autres éléments de la transaction, comme par exemple l'adresse de livraison, les articles commandés, etc. sont déterminés avant que SET n'entre en action. Si le marchand le souhaite, ces informations peuvent être chiffrées avec par exemple SSL.

---

[10] http://www.setco.org/
[11] http://www.visa.com/
[12] http://www.mastercard.com/
[13] http://www.gte.com/
[14] http://www.ibm.com/
[15] http://www.rsa.com/
[16] http://www.saic.com/
[17] http://www.spyrus.com/
[18] http://www.verisign.com/

Un autre avantage de SET est qu'il ne permet pas au marchand d'avoir accès aux détails de la carte de crédit et donc une deuxième source de fraude est enrayée.

4.2. Le processus de chiffrement

Lors d'une transaction utilisant le protocole SET, l'information est séparée en deux groupes:

- L'information relative au client et au marchand: identifiant de la commande, montant de la commande, etc.
- L'information relative au client et à l'institution financière tels que les détails de la carte de crédit.

SET autorise que ces deux types d'information soient inclus dans une seule transaction digitalement signée.

L'information destinée à l'institution financière est chiffrée avec sa clé publique alors que l'information destinée au marchand est chiffrée avec la clé publique de ce dernier. Le marchand n'a donc pas accès aux détails de la carte de crédit.

Hormis ce chiffrement, les deux groupes d'information sont digitalement signés. En fin de compte, ces deux signatures sont combinées en une signature unique qui couvre l'entièreté de la transaction.

4.3. SET en action

Un système SET se compose de trois parties:

- Un porte-monnaie digital installé sur la machine du client.
- Un serveur de commerce chez le marchand.
- Un serveur de paiement auprès de l'institution financière.

Un porte-monnaie digital est un composant logiciel intégré au navigateur Internet. Il peut être automatiquement installé lors de l'installation du navigateur. Durant le processus d'installation de ce porte-monnaie digital, l'utilisateur fournit les détails de sa carte de crédit et obtient un nom d'utilisateur et un mot de passe (PIN, ***P**ersonal **I**dentification **N**umber*) pour sécuriser l'accès au porte-monnaie. Ce dernier doit également obtenir un certificat digital auprès d'une Autorité de Certification. Remarquons que l'utilisateur a besoin d'un certificat différent pour chacune des cartes de crédit contenues dans son porte-monnaie digital.

Pour utiliser le système SET, le client sélectionne ses produits auprès d'un site marchand et choisit ensuite, de payer via le système SET en cliquant sur un bouton situé sur la page Web du marchand. L'application de porte-monnaie digital est de suite lancée. L'utilisateur sélectionne la carte de crédit avec laquelle il souhaite payer. Le porte-monnaie et le serveur du marchand échangent leurs certificats. S'ils sont valides, le porte-monnaie chiffre les détails de la carte de crédit et les envoie avec les détails de la commande. Bien que ces derniers contiennent une version chiffrée des détails de la carte de crédit, le marchand n'y a pas accès. Par contre, ces informations sont transmises au serveur de paiement de l'institution financière qui débitera le compte du client et créditera celui du marchand.

4.4. SET en détails

Afin de faciliter la compréhension du lecteur, nous découperons la transaction en trois étapes:

- La demande d'achat;
- L'autorisation du paiement;
- L'exécution du paiement.

Ces trois étapes font intervenir les acteurs suivants:

- L'acheteur;
- Le porte-monnaie digital de l'acheteur;
- Le serveur du marchand dénommé ci-après le marchand;
- Le serveur de paiement installé dans une institution financière.

4.4.1. Demande d'achat

En parcourant le catalogue du vendeur, l'acheteur sélectionne les articles désirés. Une fois cette étape terminée, il envoie au marchand les autres informations dont ce dernier pourrait avoir besoin (adresse de livraison, méthode de livraison, etc.),à l'exception des informations de paiement. Par la suite, le vendeur envoie à l'acheteur un formulaire reprenant l'ensemble des informations de la commande. Si l'acheteur approuve son contenu, il clique sur un bouton situé sur le formulaire. L'application de porte-monnaie digital de l'acheteur est automatiquement activée et le protocole SET entre en jeu.

Le schéma ci-dessous reprend l'ensemble des étapes ayant lieu durant la demande d'achat. Nous détaillerons par la suite ces différentes étapes.

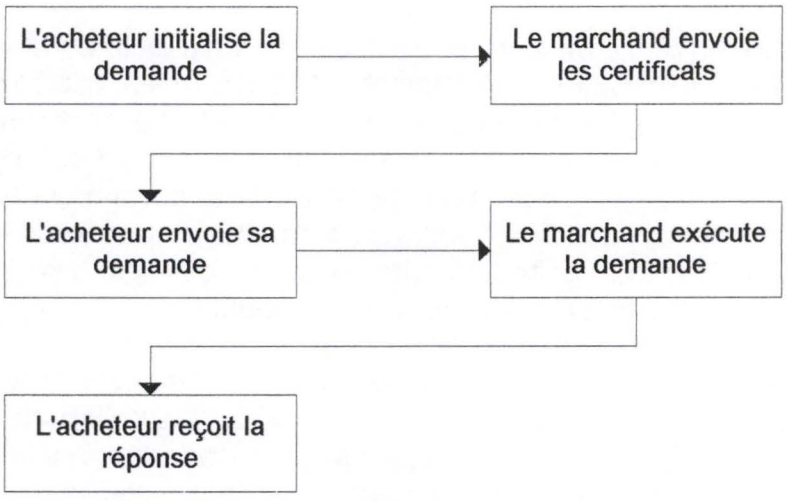


Figure 19: Demande d'achat

Initialisation de la demande

L'acheteur initialise la demande en cliquant sur le bouton du formulaire indiquant qu'il accepte le contenu de la commande. Cette action active l'application de porte-monnaie digital qui prévient le marchand que l'acheteur veut effectuer l'achat.

Envoi des certificats

Lorsque le marchand reçoit la demande, il lui attribue un identifiant de transaction unique. Il envoie au porte-monnaie digital de l'acheteur son certificat digital, celui du serveur de paiement et l'identifiant de la transaction après l'avoir signé avec sa clé privée.

Envoi de la demande

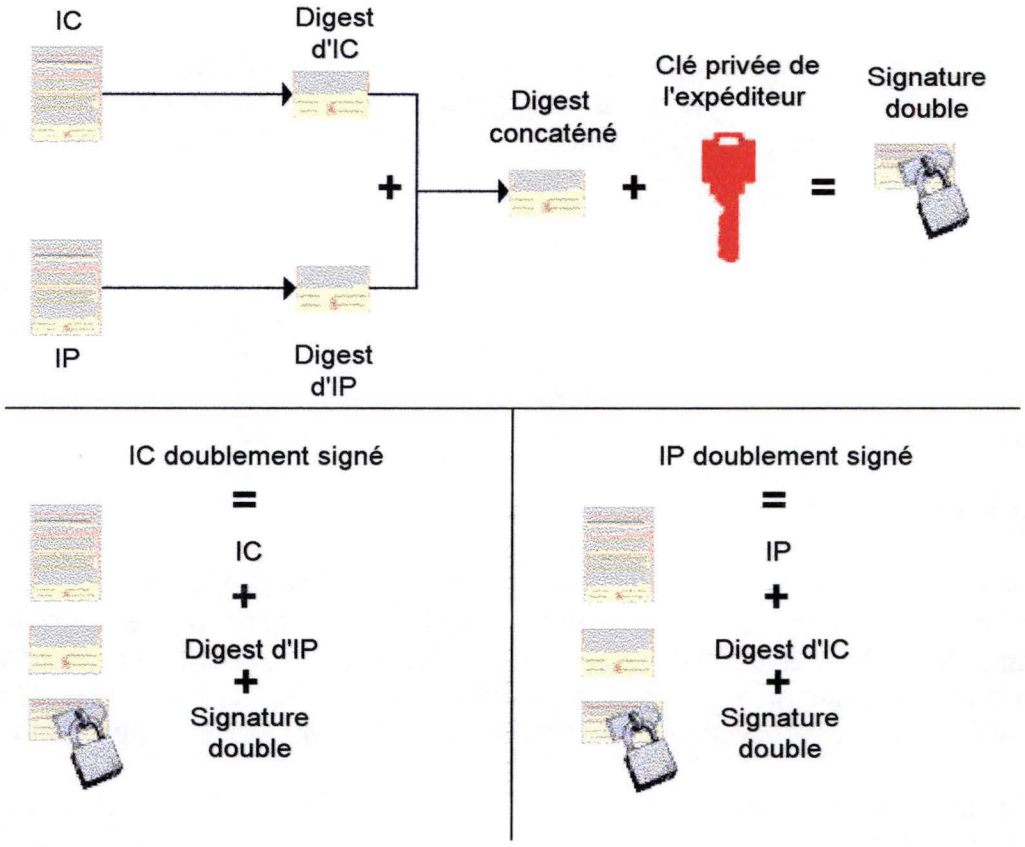
Le porte-monnaie commence par vérifier la validité des certificats reçus. En cas de résultat positif, le porte-monnaie vérifie la validité de la signature de l'identifiant de la transaction. Il utilise à cette fin la clé publique du marchand se trouvant dans le certificat de ce dernier. Cela lui permet de vérifier si l'identifiant n'a pas été altéré durant sa transmission et s'il a bien été envoyé par le marchand.

Par la suite, l'acheteur sélectionne dans son porte-monnaie la carte de crédit qu'il souhaite utiliser.

Le porte-monnaie crée ensuite l'IC (*Informations de Commande*) et l'IP (*Instructions de Paiement*). L'IC contient entre autres le type de carte utilisée (Visa ou MasterCard), le montant de la commande, un résumé de la commande et l'identifiant de la transaction. L'IP reprend, entre autres, les détails de la carte de crédit et l'identifiant de la transaction.

Le porte-monnaie calcule la signature double de l'IC et de l'IP. Il calcule pour cela le digest d'IP et celui d'IC. Il enchaîne les deux digests obtenus et calcule ensuite sur cette base un nouveau digest et le chiffre avec la clé privée de l'acheteur. Rappelons ici que l'acheteur possède un certificat par carte de crédit. On utilise donc la clé privée correspondant à la carte de crédit choisie.

Pour que IC et IP soient doublement signés, on ajoute à IC le digest de IP et la signature calculée à partir de la concaténation des digests d'IP et IC. Quant à IP, on lui ajoute le digest d'IC et la même signature.



Le porte-monnaie génère ensuite au hasard une clé de chiffrement partagée de 128 bits et l'utilise pour chiffrer l'IP doublement signé. Le porte-monnaie chiffre ensuite la clé partagée avec la clé publique du serveur de paiement.

Le porte-monnaie envoie au marchand:

- Le certificat digital correspondant à la carte de crédit utilisée;
- L'IC doublement signé;
- L'IP doublement signé et chiffré avec la clé partagée;
- La clé partagée, chiffrée avec la clé publique du serveur de paiement.

Traitement de la demande

Lorsque le marchand reçoit la demande, il commence par vérifier la validité du certificat de l'acheteur. Il utilise la clé publique de l'acheteur et le digest de IP (contenu dans IC) pour vérifier la validité de la double signature et s'assurer de la non-altération de la demande durant sa transmission.

Par la suite, le marchand exécute la demande et sollicite une autorisation de paiement auprès du serveur de paiement. Cette étape sera décrite dans le point suivant.

Sans attendre la réponse du serveur de paiement, le marchand peut envoyer une réponse à l'acheteur. Ce dernier pourra demander au marchand le statut de son paiement. Le marchand l'informera de l'autorisation ou du refus du paiement.

La demande exécutée, le marchand envoie à l'acheteur son certificat digital et sa réponse digitalement signée avec sa clé privée.

Si la demande d'autorisation du paiement indique que le paiement est accepté, le marchand envoie alors à l'acheteur les articles ou services de sa commande.

Réception de la réponse

Lorsque le porte-monnaie digital de l'acheteur reçoit la réponse du marchand, il commence par vérifier la validité du certificat qu'il reçoit. Il vérifie alors la signature du message grâce à la clé publique du marchand.

Enfin, il exécute des actions variant suivant le contenu du message. Il peut, par exemple, afficher une fenêtre à l'écran indiquant à l'acheteur le statut de sa demande.

4.4.2. Autorisation du paiement

Lors du traitement de la demande, le marchand doit demander au serveur de paiement si le paiement est autorisé. Cette autorisation se déroule en trois étapes:

- Demande de l'autorisation;
- Traitement de l'autorisation;
- Traitement de la réponse.

Demande de l'autorisation

Le marchand commence cette procédure en générant une demande d'autorisation. Celle-ci comporte entre autre l'identifiant de la transaction et le montant de la commande. Il signe cette demande avec sa clé privée. Il crée alors une nouvelle clé partagée avec laquelle il chiffre la demande signée.

Il envoie par la suite au serveur de paiement:

- La demande signée et chiffrée;
- La nouvelle clé partagée chiffrée avec la clé publique du serveur de paiement;
- Son certificat digital;
- Les informations reçues de l'acheteur (le certificat digital de l'acheteur, la clé partagée que ce dernier avait créée et chiffrée avec la clé publique du serveur de paiement et l'IP doublement signé et chiffré).

Traitement de l'autorisation

Le serveur de paiement commence par vérifier la validité des certificats du marchand et de l'acheteur.

Il déchiffre la clé partagée créée par le marchand avec sa clé privée. Celle-ci lui permet de déchiffrer la demande d'autorisation du marchand. Il vérifie la non-altération de la demande grâce à sa signature digitale et à la clé publique du marchand.

Le serveur de paiement déchiffre la clé partagée créée par le porte-monnaie digital de l'acheteur grâce à sa clé privée. Cette clé partagée lui permet de déchiffrer l'IP doublement signé. Il utilise la clé publique de l'acheteur et le digest d'IC (contenu dans IP) pour s'assurer qu'IP n'a pas été altéré durant sa transmission et qu'il a bien été signé par l'acheteur.

Le serveur de paiement vérifie que l'identifiant de transaction contenu dans l'IP de l'acheteur est bien identique à celui contenu dans la demande d'autorisation du marchand. En cas de test positif, le serveur de paiement vérifie que le paiement puisse avoir lieu; c'est à dire que l'acheteur dispose d'un crédit suffisant.

Le serveur de paiement crée une troisième clé partagée qu'il utilise pour chiffrer sa réponse après l'avoir signé avec sa clé privée.

Le serveur de paiement envoie finalement au marchand son certificat digital, la clé partagée (qu'il a créée) après l'avoir chiffrée avec la clé publique du marchand et sa réponse signée et chiffrée.

Traitement de la réponse

Le marchand commence par vérifier la validité du certificat du serveur de paiement. Il déchiffre la clé partagée créée par le serveur de paiement grâce à sa clé privée.

Il utilise cette clé partagée pour déchiffrer la réponse du serveur de paiement. Il vérifie la validité de la signature de la réponse, ce qui lui permet de s'assurer que la réponse n'a pas été altérée lors de la transmission.

Le marchand peut ensuite terminer le processus de demande d'achat.

4.4.3. Exécution du paiement

Le protocole SET permet au marchand de demander l'exécution d'un paiement lorsqu'il le souhaite. De plus, il a la possibilité de demander l'exécution de plusieurs paiements en une seule opération.

L'exécution d'un paiement se fait en trois étapes:

- Demande d'exécution du paiement;
- Exécution du paiement;
- Traitement de la réponse du serveur de paiement.

Demande d'exécution du paiement

Le marchand commence par générer une demande d'exécution de paiement. Celle-ci comprend entre autres le montant de la transaction et l'identifiant de la transaction. Il signe cette demande avec sa clé privée.

Il crée une quatrième clé partagée avec laquelle il chiffre sa demande signée.

Il envoie au serveur de paiement:

- Son certificat digital;
- La quatrième clé partagée après l'avoir chiffrée avec la clé publique du serveur de paiement;
- La demande signée et chiffrée avec la quatrième clé partagée.

Exécution du paiement

Lorsque le serveur de paiement reçoit une demande d'exécution du paiement, il commence par vérifier la validité du certificat du marchand. Il utilise ensuite sa clé privée pour déchiffrer la quatrième clé partagée. Cette dernière lui permet de déchiffrer la demande d'exécution du paiement.

Il vérifie ensuite que la demande n'a pas été altérée (durant la transmission de la demande) et qu'elle émane bien du marchand grâce à sa signature digitale et à la clé publique du marchand.

Il exécute le paiement en débitant le compte de l'acheteur et en créditant celui du marchand.

Il termine en générant une réponse. Il crée au hasard une cinquième et dernière clé partagée avec laquelle il chiffre sa réponse après l'avoir signé avec sa clé privée.

Il envoie finalement au marchand:

- Son certificat digital;
- La cinquième clé partagée après l'avoir chiffrée avec la clé publique du marchand;
- Sa réponse signée et chiffrée avec la cinquième clé partagée.

Traitement de la réponse du serveur de paiement

Lors de la réception de la réponse du serveur de paiement, le marchand commence par vérifier la validité du certificat du serveur de paiement. Il déchiffre ensuite la cinquième clé partagée grâce à sa clé privée. Il utilise cette clé partagée pour déchiffrer la réponse signée du serveur de paiement.

Il vérifie par la signature digitale et la clé publique du serveur de paiement que la réponse n'a pas été altérée durant la transmission et qu'elle provient bien du serveur de paiement.

Le marchand termine le processus en conservant la réponse du serveur de paiement afin de vérifier que son compte est crédité du montant prévu.

5. Cartes à puce

L'utilisation de cartes à puce peut apporter un plus à la sécurité. Avant de voir pourquoi, nous nous proposons de les décrire brièvement.

5.1. Présentation

Une carte à puce est une carte en plastique qui se présente sous la forme d'une carte de crédit (type Visa) à la différence près qu'une puce électronique est incorporée dans la carte. Une carte à puce contient une mémoire de telle sorte qu'elle peut être utilisée à plusieurs fins. Par exemple, elle peut mémoriser des informations personnelles, l'historique des réparations de votre voiture, voire même une somme d'argent.

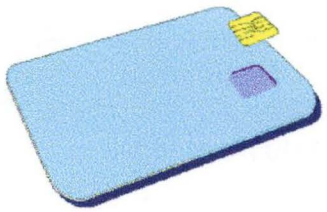


Figure 20: Éclaté d'une carte à puce

Les bénéfices d'une carte à puce sont:

- Capacité d'incorporer un microprocesseur capable d'exécuter différentes tâches, tel le chiffrage de données;
- Capacité de combiner plusieurs mécanismes de paiement dans la même carte;
- Capacité de combiner plusieurs fonctions sur la même carte. Par exemple une application "porte-monnaie électronique" et une application "clé d'accès à des bâtiments";
- Capacité de stockage importante;
- Portabilité;
- Sécurité.

Contrairement aux cartes à puce, les cartes à bande magnétique ne sont pas très sécurisées. Il est actuellement assez facile de se procurer les outils nécessaires pour pirater les données confidentielles contenues sur la bande magnétique. Lorsque de l'argent est stocké sur une carte (tel un porte-monnaie électronique), ce problème devient critique.

Les cartes à bande magnétique nécessitent un système distant pour stocker et traiter toutes les données. Pour qu'une telle carte soit utilisable, elle doit toujours être connectée à un système en ligne. Cela pose peu de problèmes aux États-Unis où les coûts de télécommunication ne sont pas importants. Dans d'autres pays, comme en Belgique, ces coûts sont peu négligeables et il paraît peu économique de

maintenir un lecteur de carte continuellement en ligne afin de procéder aux transactions liées aux cartes de débit et de crédit pour de petits montants. L'utilisation d'une carte à puce est une solution plus économique puisqu'elle permet de traiter et de stocker localement les transactions. Ce n'est qu'en fin de journée que l'ensemble des transactions sont transférées au système bancaire du commerçant.

Enfin, la portabilité est importante et en particulier pour certains types de données (comme par exemple les données vous identifiant et permettant de vous contacter) dans un monde aux dispositifs et périphériques multiples où les informations doivent être consultables à tout moment et en tout lieu. Certains dispositifs, tels les kiosques multimédia, seront connectés sur Internet. D'autres, comme votre agenda électronique ne le seront peut-être pas. Les consommateurs désireront disposer de certaines informations constamment, peu importe le dispositif utilisé, connecté ou non, et son emplacement. Les cartes à puce, avec leur capacité de traitement et de stockage qui évoluent continuellement, constituent une solution pratique pour rendre les données portables et universellement accessibles.

5.2. Principe de fonctionnement

Une carte à puce doit être insérée dans un dispositif appelé **Card Acceptance Device** (*CAD*), qui peut être relié à un ordinateur. Un tel dispositif est aussi appelé **terminal**, **lecteur** ou **interface device** (*IFD*). Ils fournissent tous le même service de base, à savoir l'alimentation électrique de la carte et l'établissement d'une connexion grâce à laquelle se fera l'échange de données. Ce dispositif a une grande importance puisqu'il est le lien, d'une part, entre deux ordinateurs (celui contenu dans la puce et celui avec lequel la puce converse) et, d'autre part, entre l'utilisateur et l'application utilisée.

Outre les différences ergonomiques, il existe plusieurs types de dispositif, variant soit au niveau de la forme, soit au niveau des fonctionnalités. Au niveau de la forme, on retrouve les types suivants:

- Relié par câble;
- Intégré dans le clavier;
- Intégré dans un PC;
- Sous forme d'une carte spécifique pour une utilisation avec un ordinateur portable.

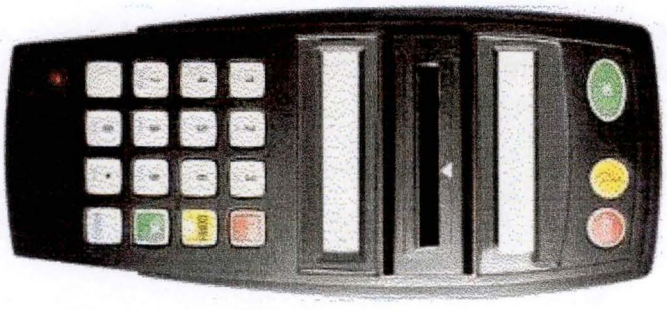


Figure 21: Exemple de terminal relié par câble: un terminal Proton (conçu par Banksys[19])

[19] http://www.banksys.be/

Au niveau des fonctionnalités, on retrouve les particularités suivantes:

- Simple transfert de données;
- Capacité de traitement interne avec clavier et affichage;
- Capacité de supporter plusieurs types de processeurs;
- Capacité de supporter plusieurs protocoles;
- Capacité d'utiliser différents types de cartes: avec ou sans contact.

Lorsque deux ordinateurs communiquent entre eux, ils échangent des paquets de données, construits sur base d'un protocole. De la même manière, lorsqu'une carte à puce communique avec le monde extérieur, elle utilise ses propres paquets de données construits sur base d'un protocole particulier. Ces paquets sont appelés **Application Protocol Data Units** (*APDU*). Un APDU contient soit un message de commande, soit un message de réponse. Dans le monde des cartes à puce, on utilise le modèle maître - esclave où la carte à puce joue toujours le rôle de l'esclave: la carte à puce attend toujours un APDU de commande d'un terminal. Elle exécute ensuite la commande spécifiée dans l'APDU et répond au terminal par un APDU de réponse.

Les tables suivantes indiquent le format des APDU de commande et de réponse. La structure des APDU est décrite dans la quatrième partie de ISO 7816.

En-tête obligatoire				Champs conditionnels		
CLA	INS	P1	P2	Lc	Données	Le

Tableau 4: APDU de commande

L'en-tête décrit la commande sélectionnée. Elle est constituée de 4 champs: la classe (CLA), l'instruction (INS) et deux paramètres (P1 et P2). Chaque champ contient 1 octet.

- CLA: octet de classe. Dans beaucoup de systèmes de cartes à puce, cet octet est utilisé pour identifier une application. En effet, une carte à puce peut contenir dans la même puce plusieurs applications.
- INS: octet d'instruction. Cet octet indique l'instruction à exécuter dans l'application choisie.
- P1, P2: octets de paramétrisation: permet de qualifier l'instruction choisie.
- Lc: indique le nombre d'octets du champ de données de l'APDU de commande.
- Le: indique le nombre maximum d'octets attendu dans le champ de données de l'APDU de réponse.

Champ conditionnel	Queue obligatoire	
Données	SW1	SW2

Tableau 5: APDU de réponse

- SW1, SW2: ces octets indiquent le statut de l'exécution de la commande dans la carte à puce.

En amont, le terminal est connecté à un autre dispositif, soit un PC soit un dispositif en réseau. La manière dont le terminal communique avec ces dispositifs

est définie par un protocole. Ce dernier peut-être propriétaire ou standard (exemple: Multos, OpenCard).

5.3. Domaine d'utilisation des cartes à puce

Les domaines d'utilisation d'une carte à puce sont très nombreux et ne se limitent pas au porte-monnaie électronique. Nous ne mentionnerons ici que les plus importants.

- Stockage de clé de chiffrage;
- Porte-monnaie électronique. Cette application sera étudiée en détails dans le prochain chapitre;
- Stockage d'un profil utilisateur;
- Sécurisation des GSM et des récepteurs satellite;
- Clé d'accès à certains réseaux et bâtiments;
- Stockage de données médicales;
- Carte d'identité universitaire;
- Carte de fidélité;
- ...

Étudions de plus près l'utilisation d'une carte à puce en tant qu'application de stockage d'une clé de chiffrage.

Les protocoles de transactions sécurisés pour le commerce électronique tels que SSL et SET que nous avons détaillés, nécessitent que les clés de chiffrement privées soient stockées de manière sûre.

La méthode de stockage la plus simple est de chiffrer la clé privée avec un mot de passe et de la stocker sur le disque dur de l'ordinateur. C'est la façon dont les programmes tels que Netscape Navigator travaillent. Cette méthode, bien que commode, comporte des risques de sécurité. En effet, si quelqu'un découvre ou intercepte le mot de passe, il pourrait utiliser la clé privée qui était sensée être protégée. Une seconde faiblesse est qu'une fois la clé déchiffrée, celle-ci est stockée dans la mémoire vive de l'ordinateur où elle pourrait être copiée par un programme pirate.

La sécurité peut être améliorée en stockant la clé de chiffrement dans un média amovible comme une disquette. Un attaquant devrait avoir accès à ce média et connaître le mot de passe avant de pouvoir utiliser cette clé secrète. Cependant, cette méthode nécessite encore le déchiffrement de la clé et son stockage dans la mémoire vive de l'ordinateur où elle peut à nouveau être copiée par un programme pirate. Les cartes à puce peuvent fournir une solution très sécurisée pour la génération, le stockage et l'utilisation de clés privées.

Dans son implémentation la plus basique, la carte à puce peut être utilisée pour stocker des clés privées et des certificats digitaux protégés par un mot de passe. La sécurité peut encore être améliorée par l'utilisation d'un microprocesseur installé dans la puce et générant les paires de clés privées et publiques et effectuant le chiffrement. Les données à chiffrer ou à déchiffrer sont alors passées à la carte où le microprocesseur effectue les opérations nécessaires avant de renvoyer à

l'ordinateur les données traitées. De cette manière, la clé privée ne quitte jamais la carte et de ce fait, elle n'est plus vulnérable aux attaques de programmes pirates scannant la mémoire de l'ordinateur à la recherche de clés.

6. C-SET

Le projet de protocole C-SET est une initiative de Banksys et du Groupement des Cartes Bancaires de France. Ce projet est soutenu par la DG III de la Commission Européenne au travers du programme **I**nformation **S**ociety **I**nitiatives for **S**tandardization (ISIS).

Ce projet, basé sur la technologie des cartes à puce et entièrement compatible SET, a pour but de rendre interopérable les différents systèmes de cartes à puce existant au monde. La carte à puce peut être une carte de débit, une carte de crédit ou encore un porte-monnaie électronique (de type Proton, par exemple). De plus C-SET est un protocole qui permet aussi bien les transactions mettant face-à-face l'acheteur et le vendeur que les transactions sur des réseaux ouverts tel Internet.

C-SET a été développé afin que les différents systèmes conformes à C-SET soient:

- Mondialement interopérables;
- Hautement sécurisés;
- Faciles d'utilisation pour les porteurs de carte;
- Financièrement accessibles;
- Conformes aux législations en vigueur au niveaux nationaux et international.

Le protocole C-SET, basé sur une architecture sécurisée sophistiquée, assure un niveau de sécurité sur un réseau ouvert équivalent à celui présent lors d'une transaction face-à-face. Spécifiquement, C-SET permet:

- L'identification du porteur de carte comme utilisateur légitime;
- L'identification du marchand comme marchand légitime;
- La non-répudiation du paiement par l'acheteur;
- La non-répudiation de la commande par le marchand;
- L'authentification de la réponse du serveur de paiement;
- La confidentialité des instructions de paiement;
- La liaison d'un paiement à une commande grâce à l'usage de la double signature.

Le protocole C-SET part de l'hypothèse qu'un PC n'est pas sécurisé. C'est pourquoi l'environnement sécurisé de C-SET se compose de:

Pour le porteur de carte

- Une carte à puce:
  - Contenant l'identité de l'acheteur.
  - Contenant les clés de chiffrement utilisées.

- Un lecteur de carte à puce sécurisé:
  - Forçant l'utilisateur à confirmer de lui-même la transaction.
  - Protégeant la confidentialité du ***P**ersonal **I**dentification **N**umber* (PIN).
  - Assurant que le montant de la transaction apparaît sur l'écran du terminal.
  - En option, empêchant le détournement des applications de chiffrement exécutées à l'intérieur du lecteur.

Pour le marchand

- Un terminal sécurisé préservant la confidentialité des clés de chiffrement utilisées pour l'authentification.
- Un serveur marchand installé dans un endroit sécurisé et préservant l'intégrité des logiciels applicatifs.

Pour le système de paiement

- Un terminal sécurisé préservant la confidentialité des clés de chiffrement utilisées pour l'authentification et la confidentialité des transactions.
- Un serveur de paiement installé dans un endroit sécurisé et préservant l'intégrité des logiciels applicatifs.

Banksys et le Groupement des Cartes Bancaires de France ont été en contact avec l'industrie des cartes de paiement, les organismes de standardisation et les autres organismes intéressés afin de favoriser l'acceptation du protocole C-SET au niveau mondial.

7. Conclusion

Nous terminerons ce chapitre en comparant les trois protocoles étudiés dans ce chapitre, à savoir SSL, SET et C-SET. Nous avons choisi les critères de comparaison suivants:

- Chiffrement des données de paiement: indique si les données de paiement circulant entre le client et le marchand sont transmises de façon sécurisée.
- Accès aux données de paiement par le marchand: indique si le marchand à la possibilité d'accéder aux détails de la carte de crédit du client.
- Utilisation de clés longues: indique si le système autorise l'utilisation de clés de chiffrement de plus de 56 bits.
- Certificat serveur: indique si le protocole impose que le marchand se procure un certificat digital.
- Certificat client: indique si le protocole impose que le client se procure un certificat digital.
- Logiciel client: indique si le client doit, en plus du navigateur, installer d'autres logiciels sur son PC.
- Hardware client: indique si le client doit acquérir un matériel spécifique.
- Protection des clés: indique si le système prévoit un stockage sûr des clés privées (dans une carte à puce, par exemple).
- Solutions disponibles: indique le nombre de solutions disponibles pour les marchands.

	SSL	SET	C-SET
Chiffrement des données de paiement	Oui	Oui	Oui
Accès aux données de paiement par le marchand	Varie suivant les solutions	Non	Non
Utilisation de clés longues	Non	Oui	Oui
Certificat serveur	Oui	Oui	Oui
Certificat client	Non	Oui	Oui
Logiciel client	Non	Oui	Oui
Hardware client	Non	Non	Lecteur de carte
Protection des clés	Non	Non	Oui
Solutions disponibles	Disponible en standard	De plus en plus de solutions disponibles	Très peu de solutions disponibles

Tableau 6: Comparaison des protocoles étudiés

Il est clair que le protocole SET présente certains avantages sur le protocole SSL . En comparaison à SSL,

- Il permet une identification de l'acheteur.
- Le marchand n'a jamais accès aux détails de la carte de crédit.
- Seules les informations de paiement étant chiffrées, SET peut utiliser des clés de chiffrement de 128 bits sans avoir à craindre les régulations américaines sur l'exportation des systèmes de chiffrement.

On peut donc s'étonner de rencontrer de nos jours si peu de sites Web conformes au protocole SET bien que les spécifications du protocole SET furent finalisées dés le début 1997. La raison principale de cette lenteur est l'acceptation pour ainsi dire planétaire du protocole SSL et la complexité et le prix des systèmes SET, même si cette dernière raison a été fortement remise en cause dans **[GARTNER 98]**.

Comparés aux deux autres protocoles, C-SET nous paraît le plus sûr. Contrairement à SET, il permet aussi l'utilisation de moyens de paiement autres que la carte de crédit. Son expansion est freinée toutefois par l'obligation pour l'acheteur de se procurer un lecteur de carte.

Qu'il s'agisse de SET ou de C-SET, ces protocoles nécessitent de la part du client l'acquisition d'un certificat digital. Ce dernier n'est pas gratuit. Son prix pourrait freiner la diffusion de ces protocoles.

Il faut donc se réjouir du fait que la Commission Européenne soutienne C-SET et que Bank Card Company (représentant belge de Visa et MasterCard) encourage en Belgique le développement de solutions conformes au protocole SET.

Chapitre 3: Moyens de paiement

1. Introduction

Nous nous intéresserons dans ce chapitre aux divers moyens de paiement utilisant Internet comme médium. Nous nous limiterons cependant aux moyens utilisés dans le cadre des transactions business-to-consumer.

Ces différents moyens ne sont pas les seuls disponibles. Il est en effet tout à fait possible de commander un article sur un site marchand et de téléphoner au vendeur afin de lui communiquer son numéro de carte de crédit. Tout comme il est possible de régler sa commande par virement bancaire.

Les moyens de paiement dont le Web est le support sont pour la plupart une version électronique des systèmes de paiement que nous utilisons dans la vie quotidienne. La différence fondamentale entre les systèmes de paiement électronique et les traditionnels est que dans le cas des premiers, tout est digital et conçu de manière à être traité électroniquement.

Il existe actuellement deux grands types de systèmes de paiement. Les systèmes de type carte de crédit et les systèmes basés sur la monnaie électronique. Après avoir détaillé ces deux systèmes, nous terminerons, en citant deux autres systèmes plus discrets: le chèque électronique et le paiement par carte de débit.

2. Carte de crédit

2.1. Introduction

Le paiement sur Internet par carte de crédit est certainement le moyen de paiement le plus utilisé. Les ténors dans ce domaine sont Visa, MasterCard et American Express (AMEX). Plus discrets sont les systèmes Diners Club et Discover. En Belgique, les deux seuls organismes capables d'effectuer le clearing pour ces systèmes sont Bank Card Company (BCC) et Citibank. Notons que BCC est une société anonyme prestataire de services financiers dont l'actionnariat est détenu par les banques belges. Ce sont ces dernières qui sont détentrices des licences d'exploitation de Visa et MasterCard et qui chargent BCC d'en exercer la gestion pour leur compte.

Examinons la façon dont se déroule une transaction par carte de crédit dans la vie 'réelle' (non virtuelle). Après avoir choisi ses articles, le consommateur présente sa carte de crédit au vendeur. Ce dernier peut alors vérifier la capacité de l'acheteur à payer sa note en contactant sa banque. En cas de réponse positive de la banque, le vendeur crée un récépissé reprenant toutes les données de la transaction que l'acheteur signe afin de l'approuver.

Régulièrement, le vendeur présente ces récépissés à l'organe créditeur afin de recevoir l'argent qui lui est dû. Quant au consommateur, il reçoit un relevé mensuel reprenant l'ensemble des transactions effectuées le mois précédent. Il ne lui reste plus qu'à rembourser à l'organe créditeur, les achats qu'il a effectués avec sa carte de crédit.

Utiliser sa carte de crédit pour effectuer des achats sur Internet suit le même scénario. Mais sur Internet, des précautions particulières doivent être prises pour assurer la sécurité de la transaction et l'authentification de l'acheteur et du vendeur. Cela a conduit à toute une variété de systèmes pour utiliser les cartes de crédit sur Internet. Deux caractéristiques permettent de distinguer ces diverses solutions: le niveau de sécurité offert et les logiciels nécessaires au consommateur et au marchand.

Dans la suite du texte, nous appellerons:

- La commande: l'ensemble des informations de paiement et de commande.
- Détails de la carte de crédit: il s'agit du numéro de la carte et de sa date d'expiration.
- Informations de paiement: les détails et l'émetteur (Visa, MasterCard,...) de la carte de crédit et le total de la commande. Cet ensemble d'informations correspond aux données utiles à l'organisme de crédit.
- Informations de commande: la liste des articles commandés, leur prix et leur quantité, le total de la commande et l'adresse de livraison. Cet ensemble d'informations correspond aux données utiles au marchand.
- Organe créditeur ou organisme de crédit: compagnies telles que Bank Card Company ou Citibank habilitées à effectuer les opérations de clearing pour les différentes cartes de crédit disponibles sur le marché (Visa, MasterCard,...).

2.2. Le système First Virtual

Un des premiers systèmes permettant l'utilisation sa carte de crédit pour effectuer des achats sur Internet ne nécessitait pas l'envoi de son numéro de carte. C'est pourquoi nous n'en ferons qu'une brève description.

Ce système, dénommé First Virtual Internet Payment System, a été mis sur le marché en 1994 par First Virtual[20] (FV). Il fut développé dans le cadre de la vente de logiciels par Internet.

Dans un premier temps, le consommateur désireux d'utiliser ce système doit s'inscrire chez FV. Pour ce faire, l'utilisateur transmettait par téléphone, par fax ou par voie postale son numéro de carte de crédit à FV. En contrepartie, FV renvoyait un identificateur appelé VirtualPin. Lors d'un achat, les étapes suivantes avaient lieu:

- Le consommateur envoyait sa commande au marchand par e-mail;
- En cas d'acceptation, le marchand demandait à l'acheteur son VirtualPin;
- Le marchand vérifiait chez VF la validité de l'identificateur;
- Si la vérification était positive, l'acheteur pouvait télécharger le produit;
- Le marchand envoyait le détail de la transaction à FV;
- FV demandait confirmation auprès du client;
- Le client envoyait sa réponse à FV.

[20] http://www.fv.com/

Le client avait alors trois réponses possibles:

- YES: le client disposait alors de 90 jours pour rendre le produit sinon il était débité;
- NO: le client était prié de retirer le produit de son système;
- FRAUD: le VirtualPin du client était alors annulé.

Le schéma ci-dessous reproduit le processus complet en cas de confirmation positive du client.

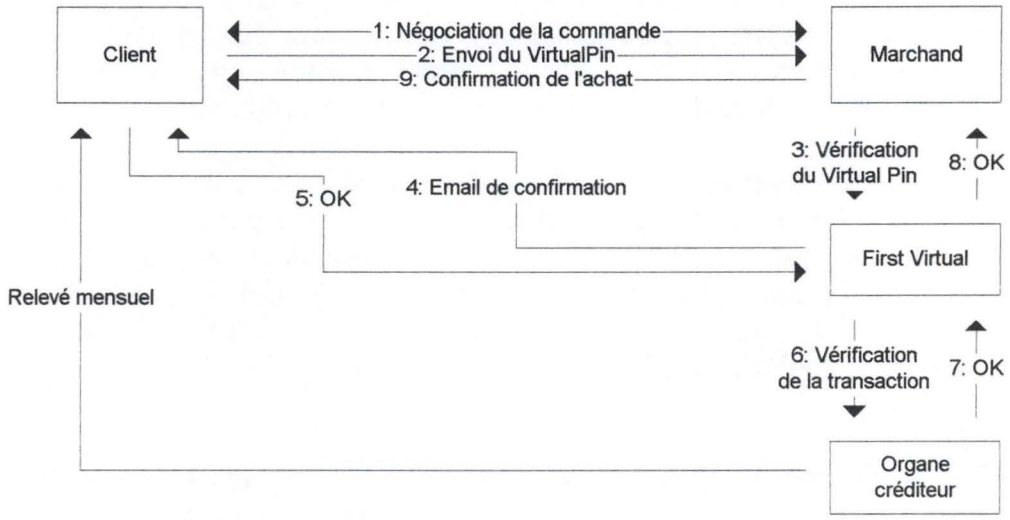


Figure 22: Le système de First Virtual. [KIOSUR 97]

Ce système présente l'avantage d'être extrêmement simple et de se baser sur les infrastructures de clearing existantes. D'un autre côté, le système est tout à fait insécurisé. Les e-mails contenant le VirtualPin peuvent être interceptés. De plus le système se base essentiellement sur l'honnêteté des clients.

2.3. Classement des systèmes

Nous allons maintenant nous intéresser aux systèmes où le numéro de la carte de crédit transite sur le Web lors de chaque transaction.

Les transactions où interviennent une carte de crédit peuvent être classées selon le chiffrement effectué.

Nous pouvons proposer le classement suivant:

1. Toute l'information de la transaction est transmise en clair sur le Web.
2. Seules les informations de paiement sont chiffrées. Le reste de l'information est envoyé en clair.
3. Toute l'information de la transaction est chiffrée avant d'être transmise sur le Web.
4. Toute l'information de la transaction est chiffrée avant d'être transmise sur le Web. Mais le marchand n'est capable de déchiffrer que les informations

de commande. Seule une autorité de confiance est capable de déchiffrer les informations de paiement.

Actuellement, les systèmes de classe 2 et 3 sont les plus nombreux et transmettent pour la plupart leurs informations chiffrées grâce à SSL. Ceux de classe 1 tendent à disparaître alors que ceux de classe 4 émergent. Une solution SET utilisant SSL pour chiffrer les informations de commande est typiquement une solution de classe 4.

Le problème des systèmes de classe 1 est un problème de fraude. Avec ces systèmes, il y a toujours moyen d'être à l'écoute des messages transitant sur le réseau et donc d'intercepter une transmission. Dans le cas d'un système de classe 1, les données de la carte de crédit n'étant pas chiffrées, l'espion peut aisément récupérer le numéro de la carte et l'utiliser à des fins frauduleuses.

Lors d'une transaction avec ce type de système, aucune signature n'est requise. Aucune preuve n'atteste l'achat par le porteur de carte. C'est pourquoi les organismes de crédit se voient obligés de rembourser leurs clients lorsque ceux-ci peuvent prouver que les détails de leur carte de crédit ont été volés. Il est donc fortement déconseillé d'utiliser des systèmes de classe 1 afin d'éviter le vol des détails de sa carte de crédit et donc toutes les méandres administratifs en cas d'utilisation abusive.

Le problème des systèmes de classe 2 et 3 est également un problème de fraude. Dans ce cas-ci, il n'y a plus moyen d'intercepter les informations de la carte sur le réseau. Cependant le marchand a accès à ces données. Il lui est possible d'utiliser ces informations à des fins illicites. Ce problème est également présent dans les systèmes de classe 1.

Nous pouvons schématiser les différentes classes de la manière suivante:

Classe 1: rien n'est chiffré

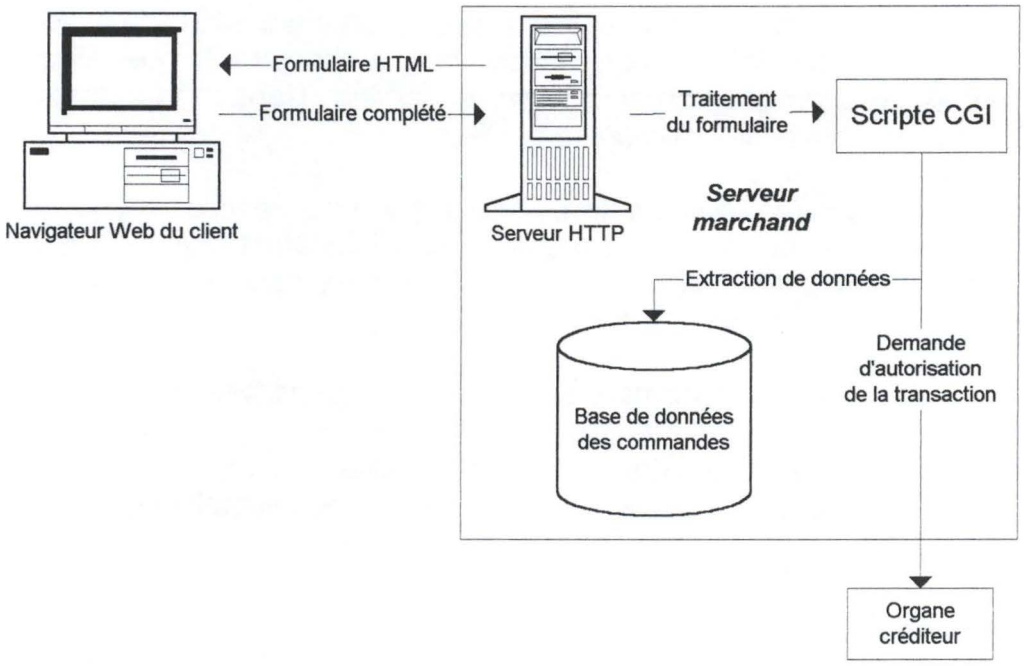


Figure 23: Transmission insécurisée. [KIOSUR 97]

Étapes:

1. Le client demande au serveur Web du marchand un formulaire de commande.
2. Le client rempli le formulaire avec sa commande, ses informations personnelles et de paiement.
3. Il le renvoie au serveur Web.
4. Un scripte CGI traite le formulaire. Il extrait les informations de commande et les stocke dans la base de données du marchand.
5. Le scripte extrait les informations de paiement et les expédie à l'organe créditeur chez lequel le marchand est inscrit afin d'autoriser ou d'annuler la transaction.
6. L'institution financière envoie sa réponse au marchand. Celui-ci confirme ou infirme la commande auprès du client par l'envoi d'une page Web ou d'un e-mail.

Scripte CGI[21]:

CGI, abréviation de ***C**ommon **G**ateway **I**nterface* est un ensemble de spécifications facilitant le transfert d'informations entre un serveur Web et un programme CGI. Un programme CGI est un programme conçu pour accepter et

[21] http://www.pcwebopedia.com/

retourner des données conformément aux spécifications CGI. Ce programme peut être écrit dans n'importe quel langage: C, Perl, Java, Visual Basic, ...

Les programmes CGI sont la façon la plus aisée pour des serveurs Web d'interagir dynamiquement avec un utilisateur. Par exemple, la plupart des pages HTML contenant des formulaires utilisent un programme CGI pour traiter les données contenues dans le formulaire. Cependant, à chaque fois que le scripte est exécuté, un nouveau processus est créé sur le serveur. Dans le cas de sites Web très visités, cela peut ralentir fortement le serveur.

Une autre manière de fournir à l'utilisateur une réaction dynamique est d'inclure des scriptes ou des programmes qui s'exécutent sur la machine de l'utilisateur plutôt que sur le serveur. Ces programmes peuvent être des applets Java, des scriptes Java ou des contrôles ActiveX.

Classes 2 et 3: la totalité de l'information ou une partie est chiffrée

Les étapes sont identiques aux systèmes de classe 1 à la différence qu'avant la transmission des informations, une connexion sécurisée est établie.

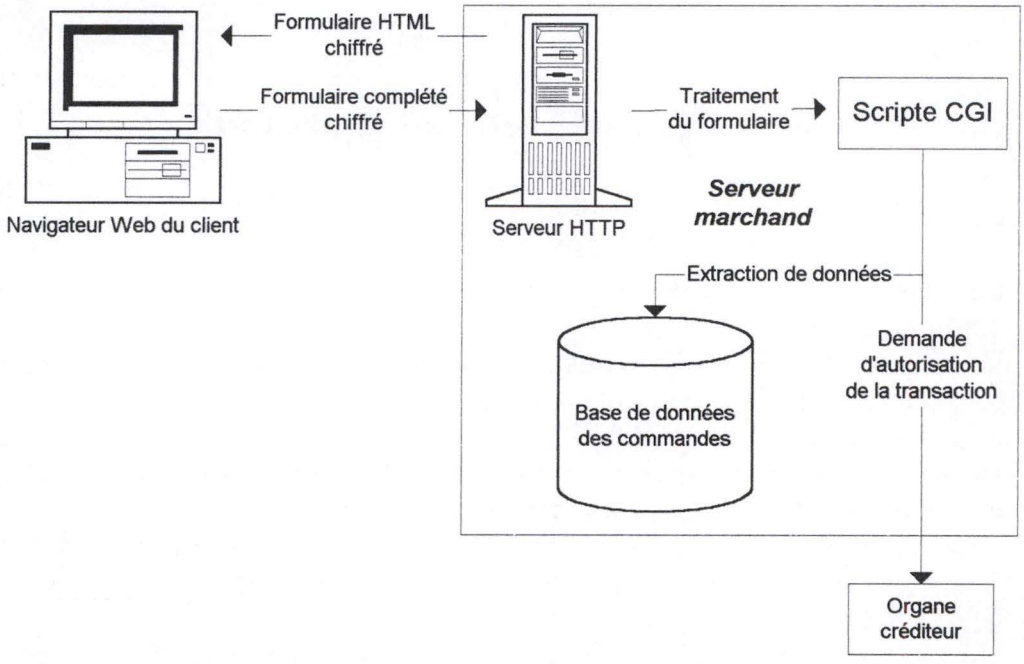


Figure 24: Transmission sécurisée. [KIOSUR 97]

Classe 4: la totalité est chiffrée mais le marchand n'a pas accès aux informations de paiement

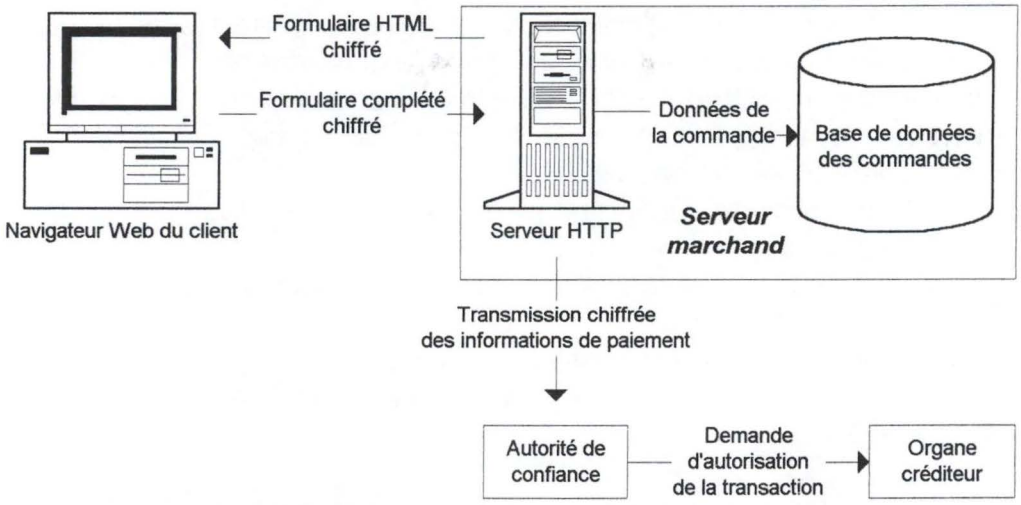


Figure 25: transmission sécurisée et intervention d'une autorité de confiance. [KIOSUR 97]

Les sociétés américaines CyberCash[22] et Verifone[23] ont chacune conçu un système basé sur ce modèle. Elles utilisent le système de porte-monnaie digital (à ne pas confondre avec les porte-monnaie électroniques et virtuels que nous verrons plus tard). Il s'agit d'une petite application située sur la machine du client et contenant l'ensemble des informations de paiement et personnelles du client sous forme chiffrée: numéro de carte de crédit, adresse de livraison, ... Il peut également contenir un certificat digital identifiant le client.

Le système peut être schématisé de la façon suivante:

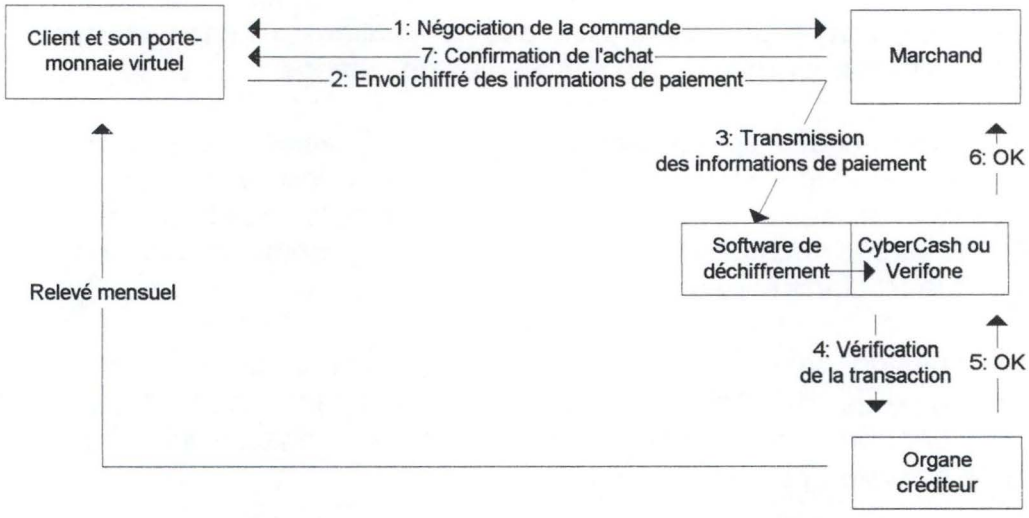


Figure 26: Le système de CyberCash et Verifone. [KIOSUR 97]

[22] http://www.cybercash.com/

[23] http://www.verifone.com/

Étapes:

1. Le client effectue sa commande auprès du site marchand.
2. Le client envoie, par l'intermédiaire de son porte-monnaie digital, les informations de paiement et de livraison le concernant.
3. Le serveur marchand reçoit ces informations sous forme chiffrée. Il déchiffre les informations de livraison et envoie celles de paiement directement chez CyberCash (ou Verifone).
4. CyberCash déchiffre les informations de paiement et les envoie à l'organe créditeur pour vérification.
5. L'organe créditeur effectue la vérification et envoie sa réponse (supposons positive) à CyberCash.
6. CyberCash envoie une réponse positive au marchand.
7. Le marchand envoie à son client une réponse positive reprenant les détails de la vente.

Il faut remarquer que les informations de paiement et de livraison sont chiffrées de manière différente et que seul CyberCash (ou Verifone) possède la clé capable de déchiffrer les informations de paiement.

2.4. Exemple d'implémentation

Nous avons étudié dans le paragraphe précédent les différentes classes de système au niveau conceptuel. Nous allons donc nous intéresser à une solution technique.

Il faut tout d'abord remarquer que, si au niveau conceptuel toutes les solutions d'une même classe se ressemblent, les développeurs ont la liberté d'implémenter leur solution comme ils le souhaitent.

Remarquons aussi que Bank Card Company et Citibank ne sont que des organes de clearing et ne proposent donc pas de solutions. Ils imposent néanmoins le protocole à utiliser pour user de leurs systèmes de clearing.

Nous avons choisi de présenter la solution *Payment Suite* proposée par Element[24], société belge située en Flandre. Notre choix a été guidé par les recommandations de Bank Card Company (BCC). Element compte parmi ses clients AdValvas[25], la galerie marchande de Planet Internet[26] contenant une vingtaine de commerces et le Roularta Media Club[27].

Cette solution permet de régler ses achats par carte de crédit (Visa ou MasterCard) ou par la carte Proton. Nous étudierons la partie du système consacrée au paiement par carte de crédit. Nous reviendrons ultérieurement sur la partie concernant le paiement par carte Proton.

---

[24] http://www.element.be/

[25] http://www.advalvas.be/

[26] http://shopping.planetinternet.be/

[27] http://www.mediaclub.be/

La solution d'Element est une solution de classe 4. Le système permet de supporter plusieurs marchands. Cette solution est donc destinée à être achetée par un hébergeur Internet. Il mettra la solution à disposition de ses clients désireux de vendre via Internet.

Nous nous limiterons ici uniquement à la partie paiement. Nous laisserons donc de côté la gestion des informations de commande tels l'adresse de livraison ou les articles commandés.

Les schémas et explications des paragraphes suivants proviennent de la documentation proposée sur le site Web d'Element.

2.4.1. Types de transaction

Il y a quatre types possibles de transactions qui peuvent être entreprises avec un organisme de clearing (BCC dans notre cas).

- Demande d'autorisation;
- Annulation de l'autorisation;
- Exécution de vente;
- Annulation de la vente.

Demande d'autorisation

Cette étape est toujours la première lors d'une transaction de paiement en ligne par carte de crédit. C'est une demande de réservation du montant de la transaction pour la carte de crédit en jeu.

La première validation effectuée sur le numéro de carte de crédit se fait localement sur le serveur marchand. Il s'agit du test de Luhn. Chaque numéro de carte de crédit possède une relation mathématique. Celle-ci permet de vérifier si un ou plusieurs chiffres du numéro ont été changés. Le test de Luhn évite des appels inutiles vers le réseau de clearing, permettant de ce fait des économies de téléphone.

Si le test de Luhn n'indique pas un mauvais numéro de carte de crédit, un appel est fait vers une application en ligne située sur le serveur de l'organisme de clearing. Cette application vérifie le numéro de la carte et sa date d'expiration. Si ce test échoue, l'autorisation est refusée et l'appel est terminé.

Si le numéro de la carte de crédit et sa validité correspondent, l'application se poursuit et vérifie que le porteur de carte dispose de crédit suffisant pour réserver la somme des achats. En cas de test positif, un numéro d'autorisation est émis. Ce numéro se compose de 6 chiffres et figure sur le récépissé du client.

La réservation de la somme à payer a une durée de vie de 10 jours ouvrables à moins que la transaction commerciale soit annulée par le marchand ou si le marchand en demande l'exécution.

Annulation de l'autorisation

Lorsqu'une demande d'autorisation est approuvée, le serveur de l'organisme de clearing émet un numéro d'autorisation. Dès que le marchand n'a plus besoin de cette autorisation parce qu'il ne livrera pas chez le client les produits ou services commandés, il peut annuler l'autorisation précédemment obtenue. Cela libère la somme réservée et restaure la limite de crédit du client à sa valeur initiale.

Si le marchand oublie d'annuler la transaction endéans les 10 jours ouvrables, la transaction sera automatiquement annulée par l'organisme de clearing.

BCC invite d'ailleurs ses clients à annuler manuellement toutes les autorisations qui ne sont plus utiles et de ne pas attendre l'annulation automatique.

Exécution de la vente

Une fois que les articles commandés ont été envoyés ou que les services ont été délivrés, le marchand peut changer une autorisation en une exécution de vente. Dès ce moment le marchand est crédité. Le client réglera le montant de ses achats lorsqu'il recevra son relevé mensuel.

La loi belge interdit de changer une autorisation en une exécution de vente sans respecter un délai de 7 jours après l'envoi des articles ou la livraison des services commandés. Durant ce délai, le client a le droit de retourner les articles ou services sans être débité.

Si une autorisation est changée en une exécution de vente, le serveur de l'organisme de clearing émet un nouveau numéro de transaction correspondant à la vente. Ce nombre sera différent de celui émis lors de l'autorisation. Dès le changement de l'autorisation une exécution de vente, il n'est plus possible d'annuler la transaction avec une annulation d'autorisation.

Annulation de la vente

Si dans un délai de 7 jours à compter de la réception des produits, les produits et services livrés ne satisfont pas les besoins du client ou si une erreur a été commise, le marchand peut encore annuler l'exécution de la vente. Lorsqu'un marchand annule une exécution de vente, son compte est débité alors que celui du client est crédité.

2.4.2. Le système

Le système tourne sous Windows NT Server et nécessite une base de données Microsoft SQL Server ou compatible ODBC 3.0.

Étapes:

1. Le client envoie, grâce à un formulaire HTML ou à un porte-monnaie digital, son numéro de carte de crédit avec sa date d'expiration au-dessus d'une connexion sécurisée à l'aide de SSL.

2. Un scripte CGI dénommé Visapost traite les données reçues. Il commence par effectuer un test de Luhn. S'il est positif, il enregistre les données de la transaction dans la base de données en chiffrant les données de la carte.
3. La base de données ayant été modifiée, le service carte de crédit se connecte au réseau de BCC via le réseau téléphonique et procède à une demande d'autorisation.
4. La réponse de BCC est enregistrée par le service carte de crédit dans la base de données.
5. Suivant la réponse de BCC, une page HTML confirmant ou infirmant la transaction est envoyée au client.

Le flux des données peut être schématisé de la façon suivante:

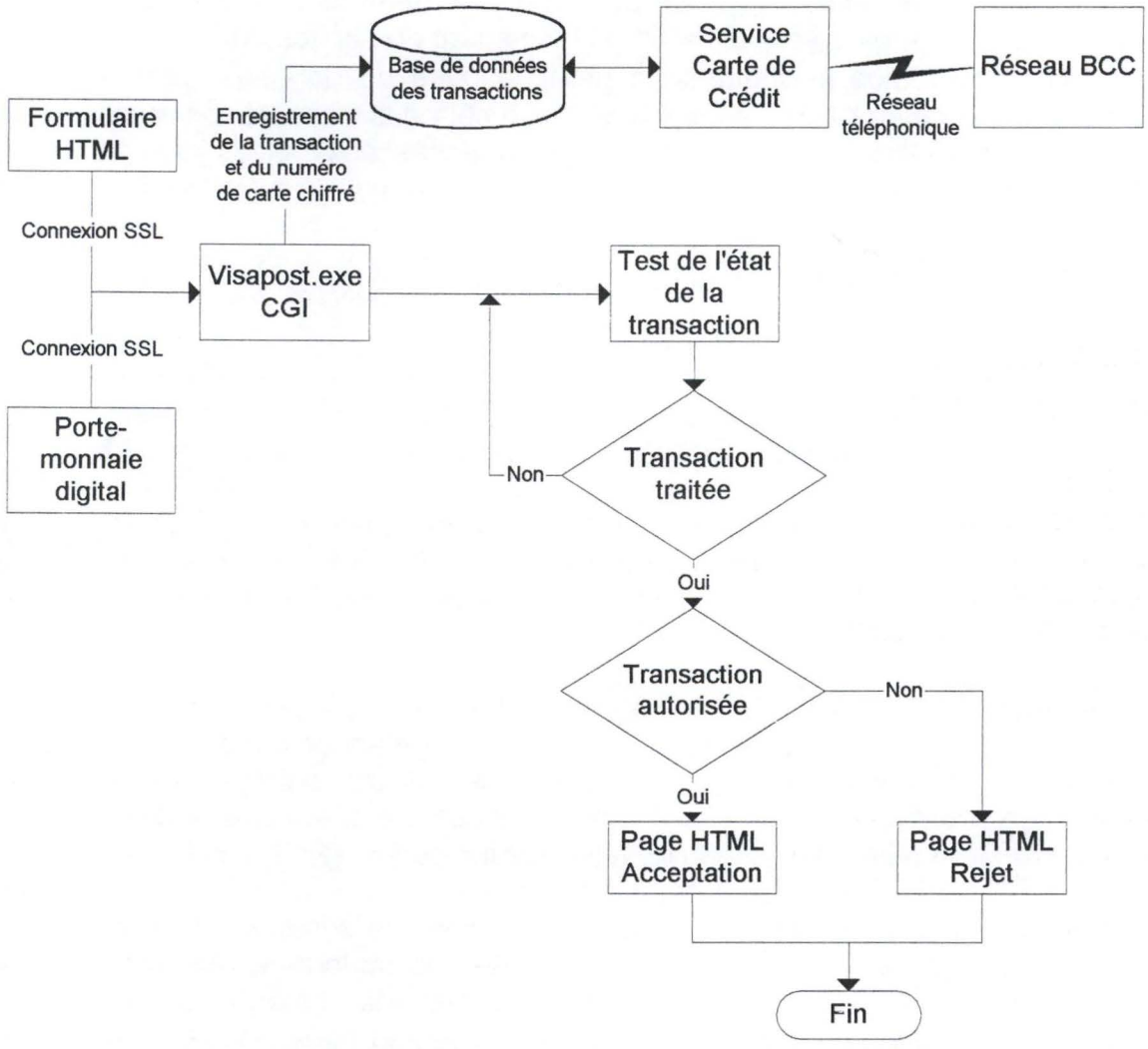


Figure 27: le système d'Element

Pour comprendre l'ensemble du système, il nous faut aussi décrire ce que voit le client sur son écran.

1. Un formulaire est présenté au client lui demandant ses informations de paiement (dans le cas d'une utilisation avec un porte-monnaie digital, une page demande d'effectuer son paiement par ce moyen).
2. Un fois le formulaire envoyé, le client reçoit une page HTML d'attente. Cette page est rechargée automatiquement toutes les 15 secondes jusqu'au moment où la transaction est traitée. Cette page contient une commande qui, à chaque rechargement de la page, teste l'état de la transaction.
3. Une fois la transaction traitée, la page reçue par le client dépend du résultat de la transaction: acceptée ou rejetée.

Aux éléments présents sur le schéma précédent, il faut ajouter deux éléments:

- Un panneau de configuration permettant de gérer le service carte de crédit (paramétrage du service, arrêt ou lancement du service, etc.);
- Un back office permettant de gérer la base de données (permet, entre autre, au marchand, de consulter l'ensemble des transactions réalisées sur son site Web et leur statut sans avoir accès aux détails des cartes de crédit).

3. Monnaie électronique

3.1. Introduction

Il nous faut, avant toute chose, définir la notion de monnaie électronique. Nous retiendrons la définition du Basle Committee on Banking Supervision: **[BASLE 98]**

La monnaie électronique fait référence aux moyens de stockage de valeurs ou mécanismes prépayés en vue d'exécuter des paiements via les terminaux des points de vente, les liaisons directes entre deux appareils ou les réseaux informatiques ouverts comme Internet.

On distingue deux types de produits dits de monnaie électronique: les mécanismes 'hardware', aussi appelés porte-monnaie électroniques qui utilisent un support carte (une carte à puce, par exemple) et les mécanismes 'software', ou porte-monnaie virtuels pour lesquels le produit fonctionne grâce à un logiciel installé sur un PC standard relié à un réseau de télécommunication. **[PETIT 98]**

Comme nous le verrons par la suite, le nombre de systèmes en compétition dans le domaine de la monnaie électronique est très important, que cela soit en termes de vendeurs de solution ou en termes de catégories spécifiques d'implémentation. Chaque catégorie aura ses vainqueurs et ses perdants. Mais il est fort probable qu'il n'y aura pas une solution unique dominante sur le marché, tout comme l'argent liquide, les chèques et les cartes de crédit sont utilisés en parallèle. Jusqu'à présent, les banques (plus particulièrement aux États-Unis) sont restées prudentes et beaucoup d'entre elles ont expérimenté différentes solutions. On s'attend toutefois à ce que les institutions financières aient une influence décisive sur l'adoption de solutions spécifiques de paiement électronique. Celles-ci devront avoir un degré relativement élevé de sécurité, la sécurité étant la préoccupation première

des institutions financières. De plus, l'introduction de réglementations aura un impact important sur le développement et l'adoption de la monnaie électronique.

L'arrivée de la monnaie électronique est le fruit d'une progressive dématérialisation des paiements. En effet, l'argent n'a pas une définition absolue. **[Oll 98]** nous rappelle brièvement l'histoire de l'argent au cours des siècles. Tout a commencé avec le troc où les marchandises représentaient l'argent. Par la suite, un moyen abstrait d'échange apparut sous la forme d'un support ayant, lui-même, une valeur (pièces d'or). Depuis lors, le principal moyen de paiement est basé sur un support n'ayant aucune valeur intrinsèque: les pièces et les billets. Dès le moment où le support était détaché de sa valeur, l'étape suivante fut l'adoption d'un support où la valeur était référencée mais stockée autre part: les chèques. L'étape finale d'abstraction physique est l'ensemble des systèmes basés sur le crédit dont les ténors sont Visa et MasterCard. La particularité de ces systèmes porte sur le transfert réel de l'argent qui n'a pas lieu in situ mais dans le futur. L'étape suivante et émergente est la suppression du support physique et l'introduction d'environnements virtuels et électroniques où la valeur n'est plus liée à des paramètres physiques et où le propriétaire de cette valeur à la capacité de transformer la valeur en différentes formes de manifestations électroniques.

3.2. Propriétés des systèmes de paiement électronique

Il est possible de classer les différents systèmes de paiement électronique d'après leurs caractéristiques. **[Oll 98]** nous propose toute une série de caractéristiques. Notons cependant que ces caractéristiques pourraient s'appliquer à d'autres moyens de paiement que les systèmes de paiement électronique.

- Atomicité: si la transaction a lieu, elle doit avoir lieu dans sa totalité;
- Consistance: toutes les parties impliquées doivent être d'accord sur les termes de l'échange;
- Isolement: les transactions doivent être indépendantes les unes des autres;
- Durabilité: il doit toujours être possible de revenir au dernier état consistant;
- Économie: effectuer une transaction doit être bon marché;
- Extensibilité: le système doit être capable de supporter plusieurs utilisateurs simultanément;
- Interopérabilité: il doit être possible d'échanger de la valeur avec d'autres systèmes;
- Conservation: le système conserve la valeur de l'argent à travers le temps et il est facile d'en conserver ou d'en retirer.

Un autre classement, toujours selon **[Oll 98]**, est basé sur le degré d'informations divulguées lors d'une transaction, à savoir le degré de visibilité par les différentes parties des informations entrant en jeu lors d'une transaction, de manière directe ou indirecte. Les parties en jeu sont le vendeur, l'acheteur, le banquier et l'autorité publique. Les informations significatives sont: l'identification du vendeur et de l'acheteur, la date, le montant et l'article vendu. Par exemple, lors de l'achat d'un pain avec de l'argent liquide, aucune information concernant cette transaction n'est transmise à la banque contrairement à un achat effectué avec une carte de crédit.

Comme nous l'avons déjà mentionné, la sécurité reste un des principaux obstacles à l'adoption de la monnaie électronique. Ces inquiétudes incluent la transmission d'informations personnelles et sensibles sur des réseaux ouverts et non sécurisés, l'anonymat de l'utilisateur et tout autre usage frauduleux des instruments de paiement électronique. La capacité d'exploiter des techniques avancées de paiement électronique à des fins illicites est source inquiétudes pour les gouvernements. D'un autre côté, apporter des clarifications légales appropriées ne pourrait être que bénéfique. Rappelons, enfin, que les mécanismes de paiement électronique existant tendent à se focaliser sur des transactions de faible valeur.

3.3. Porte-monnaie électronique

3.3.1. Présentation

Un porte-monnaie électronique se présente sous la forme d'une carte à puce capable de mémoriser des informations de type monétaire. Il existe différents types de porte-monnaie électronique:

- Rechargeable: capacité d'ajouter à la somme déjà présente dans la puce de l'argent et de l'échanger avec d'autres parties. La carte peut-être rechargée et réutilisée indéfiniment.
- Jetable ou à valeur fixée: la carte n'est pas rechargeable. Habituellement, on retrouve cette caractéristique sur les cartes téléphoniques mais elle peut aussi être utilisée dans le contexte de cartes reçues en cadeau lors, par exemple, d'une action promotionnelle.
- Crédit/Débit: dans ce type de carte, les informations présentes habituellement sur la bande magnétique de la carte sont transférées dans une puce afin de garantir à l'utilisateur une plus grande sécurité. Il est en effet plus simple de découvrir les informations contenues sur une bande magnétique que les informations stockées dans une puce.

Les systèmes de porte-monnaie électroniques ont, par rapport aux pièces et billets, les avantages suivants:

- Coûts de manipulation restreints;
- Sécurité supérieure;
- Ne nécessite pas de change (dans le sens 'monnaie');
- Usage commode;
- Offre de services étendue;
- Paiements à distance plus simples;
- Convient parfaitement aux distributeurs laissés sans surveillance.

3.3.2. Les systèmes disponibles

Plusieurs systèmes de porte-monnaie électronique existent actuellement. Les plus connus sont Proton[28], Mondex[29] et VisaCash[30]. D'autres, comme CAFE ou

[28] http://www.proton.be/
[29] http://www.mondex.com/
[30] http://www.visa.com/

WorldPay, sont plus discrets. Nous nous focaliserons sur la solution Proton, disponible en Belgique depuis 1995. Nous décrirons aussi la solution Mondex, avec laquelle nous avons fait plus ample connaissance lors de notre stage aux Etats-Unis.

3.3.2.1. Le système Proton

Le système Proton se présente sous la forme d'un porte-monnaie électronique de type rechargeable. Avant d'expliquer le fonctionnement du système Proton, nous nous proposons de faire un bref historique du développement de la carte à puce en Belgique.

Développement de la carte à puce en Belgique

Les cartes de crédit étaient au départ purement analogiques. Elles ne comportaient qu'un nombre identifiant gravé sur la carte. La transaction était authentifiée par la signature du porteur de carte. Chaque émetteur de cartes concevait ses propres terminaux. Ceux-ci étaient manuels. Un coup de fil ou un coup d'œil dans un listing était suffisant pour s'assurer qu'aucune opposition n'avait été faite sur la carte et garantissait donc au marchand une transaction sûre. Ce système fonctionne encore de nos jours.

Dans les années 70, de l'information numérique a commencé à être incluse dans les cartes, encodée soit sur une bande magnétique soit dans une puce, technologie qui était à l'époque fort chère et encore immature. En France, les cartes à puce ont obtenu un premier succès grâce à Bull, innovateur dans ce domaine, alors que des systèmes à base de bande magnétique étaient développés en Belgique.

En 1977 et 1978, deux groupes bancaires lancèrent sur le marché belge les systèmes Bancontact et MisterCash. Des centaines de terminaux furent installés dans les stations essence et dans les supermarchés. En 1987, suite à la demande des marchands et des consommateurs, les deux réseaux sont devenus compatibles. En 1989, les deux systèmes fusionnèrent en un réseau unique et une entreprise fut créée pour le gérer. Banksys, dont les principaux actionnaires sont les banques, était née. Le but était de promouvoir un réseau sécurisé, fiable et ouvert, mariant les ressources et les technologies des précédents acteurs. Depuis lors, le nombre de terminaux installés et de transactions n'a cessé d'augmenter.

En 1995, Banksys a fait un pas important vers les cartes à puce en lançant son porte-monnaie électronique: Proton. Aujourd'hui, la majorité des belges possèdent une carte Proton, d'autant plus qu'elle s'intègre à la carte de débit traditionnelle Bancontact/MisterCash.

Figure 28: Le logo Proton

De nombreuses banques étrangères ont acheté des licences Proton et l'on estime aujourd'hui à plus de 30 millions le nombre de porteurs de cartes Proton dans le monde.

Le 29 juillet 1998 a été créé **P**roton **W**orld **I**nternational (PWI) par American Express, Banksys, ERG, Interpay Nederland et Visa International. Le but de cette nouvelle compagnie est de continuer à développer et à licencier les produits Proton à travers le monde. Elle a également annoncé soutenir et implémenter CEPS (***C**ommon **E**lectronic **P**urse **S**pecifications*). CEPS est un ensemble de spécifications permettant l'interopérabilité des différents porte-monnaie électroniques existants. Enfin, PWI recommande et supporte l'usage de Java pour le développement d'applications à destination des cartes à puce.

La raison pour laquelle l'Europe est nettement plus avancée que les États-Unis au niveau des cartes à puce provient de la dérégulation américaine de l'industrie télécom. Cette dérégulation a conduit à une baisse importante des coûts de télécommunication et donc des coûts liés à la vérification en ligne des cartes de crédit et de débit, au point que les commerçants américains acceptent les cartes de crédit pour régler des sommes minimes. A l'opposé, les charges téléphoniques restant importantes en Europe, il paraît inconcevable d'utiliser une carte de crédit pour effectuer des paiements impliquant de petites sommes. D'où l'importance que prennent les cartes à puce comme Proton.

Fonctionnement

Le système est basé sur la réconciliation auprès des institutions financières des transactions effectuées.

Une carte Proton contient une puce de type BULL CP-8 utilisant le DES comme algorithme de chiffrage. La carte peut contenir au maximum 5.000FB. Chaque carte possède un identificateur dénommé PurseID. Cet identificateur se retrouve dans toutes les transactions effectuées avec la carte.

Ludmilla Petit et Alexandra De Vylder nous expliquent dans **[PETIT 98]** de façon claire et détaillée le fonctionnement de la carte Proton:

"

Le chargement de la carte Proton par le titulaire de celle-ci se fait par un transfert à partir de n'importe quel compte à vue que le titulaire de la carte dispose auprès de l'émetteur de la carte Proton. Le chargement nécessite, contrairement au paiement, l'introduction d'un code secret. Ceci permet de ne pas pouvoir recharger une carte perdue ou volée.

Au moment même du chargement, le compte du titulaire de la carte se voit débité. Parallèlement, un compte global (appelé "compte-float") dans le chef de la banque émettrice est crédité de l'équivalent. Ainsi ce compte-float permet à tout moment de donner l'aperçu de l'ensemble des chargements de la clientèle de l'établissement de crédit, diminué de tous les transferts déjà opérés vers les comptes des commerçants qui devaient recevoir un paiement.

Le paiement avec une carte Proton consiste en la transmission de données électroniques de la carte Proton vers le terminal du commerçant qui participe au système. Cette transmission donne lieu sur la carte Proton à un transfert de données (tenues à jour par un système compteur dont est pourvue la carte Proton) et à un autre transfert de données dans le terminal du commerçant. Dans le terminal du commerçant se trouvent deux mémoires:

- *La mémoire du module de sécurité (security-module), qui enregistre pour chaque transaction, le numéro de séquence de celle-ci et le numéro de la carte Proton dont émanent les données électroniques. Ce numéro de carte permet à Banksys de retrouver par la suite l'identité de l'établissement de crédit qui a émis la carte. Banksys ne peut, cependant, en principe pas retrouver l'identité du titulaire de la carte. Le module de sécurité traduit à chaque moment l'état global du compteur du terminal.*
- *Le journal qui enregistre en détail les données de chaque transaction.*

Entre le terminal du commerçant et l'ordinateur central de Banksys ont lieu à des moments déterminés des collections. Il s'agit d'un échange de données entre le terminal du commerçant et l'ordinateur central de Banksys. A l'occasion de ces collections, l'ordinateur central fait à chaque fois une copie du module de sécurité ainsi que du journal du terminal du commerçant. Après copie du journal, les données de celui-ci sont effacées du terminal.

A l'occasion de la collection, l'ordinateur central de Banksys vérifie si la demande de paiement du commerçant est juste (c'est-à-dire si les montants de chaque mémoire du terminal correspondent) et si celle-ci doit donner lieu à un paiement dans le chef du commerçant. Dans le cas où la vérification opérée par Banksys révèle qu'un paiement doit avoir lieu, l'ordinateur central le communique à tout établissement de crédit qui doit effectuer un paiement au commerçant.

A cette fin le journal du terminal du commerçant comprend des sous-rubriques correspondant aux différents établissements de crédit. Chaque sous-rubrique comporte le montant total dont un établissement de crédit donné est redevable sur base des transactions de sa clientèle avec le commerçant en question.

Un module déterminé dans l'ordinateur central de Banksys contacte alors le compte-float de chaque banque et le charge de transférer le montant dû vers le compte du commerçant.

Lorsque la banque opère un transfert en faveur du commerçant, ce dernier est informé par la banque de la période à laquelle le paiement se rapporte. Le commerçant n'a cependant aucun détail sur chacune des transactions, dont l'ensemble forme la somme dont la banque lui est redevable.
"

Pourquoi alors soutient-on que le système Proton n'est pas totalement anonyme? L'établissement de crédit qui reçoit mission d'effectuer un paiement au profit d'un commerçant se voit communiquer le numéro de carte de l'utilisateur. Or, il lui est possible de mettre en relation ce numéro de carte avec un numéro de compte (rappelons-nous que maintenant carte de débit et carte Proton partagent la même

carte!) et donc avec le titulaire de celui-ci. De même, au moment du chargement de la carte Proton, la banque peut facilement identifier le lien entre la puce Proton et le compte bancaire d'où émane le chargement. Le recoupement de toutes ces données peut s'avérer porteur d'informations quant à l'utilisation des moyens de paiement, les habitudes de consommation et goûts personnels de l'utilisateur de la carte Proton.

Remarquons aussi que le système Proton ne permet pas le transfert de carte à carte et de contenir plusieurs devises différentes.

Enfin, le système Proton nécessite de la part de l'acquéreur du système de lourds investissements financiers. En effet, les réconciliations journalières nécessitent d'importantes capacités de calcul.

Sécurité des transactions

Le site que Banksys consacre à Proton[31] nous donne quelques informations quant à la sécurité des transactions effectuées.

Chaque fois qu'une personne effectue une transaction avec sa carte Proton, que ce soit un paiement ou un chargement, les applications de sécurisation de la carte vérifient l'authenticité du terminal de paiement ou de chargement avec lequel la transaction est réalisée. Pour un paiement, par exemple, la carte teste le terminal du marchand et vice versa. Les mécanismes cryptographiques utilisés pour effectuer une telle transaction sont relativement complexes et font appel à des clés de chiffrement dynamiques (c'est-à-dire qui changent avec le temps) et des clés de session uniques différentes pour chaque transaction.

Les messages échangés entre la carte et le terminal du marchand sont donc sécurisés par chiffrement (essentiellement basé sur le triple DES bien que des certificats RSA soient également utilisés). Par conséquent, ces messages ne peuvent en aucun cas être falsifiés. Un terminal reconnaît toujours si une carte est "saine" et si elle contient de l'argent. De même, la carte reconnaît toujours si le terminal du marchand est valide.

Implémentation d'une solution

Nous décrirons une solution de paiement via Internet et non le système développé par Banksys gérant le système dans la vie courante. Comme annoncé plus haut, nous allons décrire la solution développée par Element.

Tout comme dans le cas de la solution carte de crédit, les schémas et explications des paragraphes suivants proviennent essentiellement de la documentation proposée sur le site Web d'Element.

Le système tourne sous Windows NT Server et nécessite une base de données Microsoft SQL Server ou compatible ODBC 3.0.

---

[31] http://www.proton.be/

Le système nécessite du côté client:

- Une carte Proton
- Un terminal CZAM/PC (vendu au prix de 1.990Fb)

Le terminal CZAM/PC est l'interface utilisée pour lire et écrire sur une carte Proton à partir d'un PC.

Figure 29: Un terminal de type CZAM/PC

Le CZAM/PC actuel peut être connecté au PC par l'utilisation d'un port série (8). De nouveaux terminaux utilisant une liaison USB ou intégrés au clavier devraient bientôt faire leur apparition.

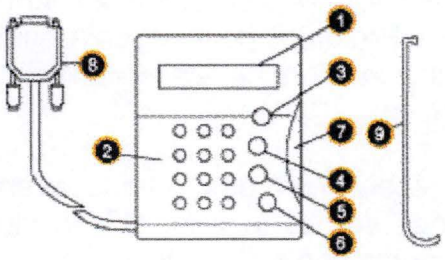


Figure 30: Schéma du CZAM/PC

Le CZAM/PC possède un lecteur de cartes à puce (7), son propre écran alphanumérique (1) et son clavier (2) utilisé pour entrer le code secret de la carte. A côté du clavier, sont disposés quelques boutons supplémentaires: 'STOP' (3), 'CORR' (4), '?' (5) et 'OK' (6).

Le bouton 'STOP' permet d'annuler une opération en cours. La touche 'CORR' peut être utilisée pour entrer à nouveau son code secret en cas d'erreur. La touche '?' permet de connaître le solde de sa carte Proton. Cette touche est très importante lors de l'installation du CZAM/PC. Si en pressant la touche '?', l'écran du terminal n'indique pas le solde de la carte, toute autre opération échouera. Enfin, le bouton 'OK' est utilisé pour accepter une transaction.

Enfin, signalons que le CZAM/PC dispose d'une fixation murale (9).

Parce que sur Internet, le paiement est initié par le PC, le terminal C-ZAM/PC utilisé pour effectuer la transaction doit protéger l'utilisateur d'un virus ou d'une application "Cheval de Troie" sur son PC. Le C-ZAM/PC est donc équipé d'un logiciel qui rend impossible la réalisation d'une transaction sans une intervention directe de

l'utilisateur: le fait d'appuyer sur la touche 'OK'. L'écran du lecteur garantit que le montant correct de la transaction est montré à l'utilisateur. Le clavier du C-ZAM/PC permet quant à lui d'introduire votre code en toute sécurité pour les paiements Bancontact/MisterCash ou pour le chargement en ligne de votre carte Proton sur Internet . Le code ne devrait jamais être introduit sur le clavier d'un PC où vous courez le risque qu'il soit intercepté. Le code est vérifié localement sur la puce et n'est jamais envoyé sur Internet.

Le C-ZAM/PC garantit donc que:

- L'argent ne peut être retiré de la carte Proton sans l'accord de son propriétaire.
- Le montant qui apparaît sur l'écran du C-ZAM/PC est bien le montant qui sera payé ou chargé.
- Le code secret ne peut être saisi sur le PC ou sur Internet lorsque l'utilisateur l'entre dans le C-ZAM/PC.
- Aucune information envoyée sur Internet ou stockée dans le PC ne pourra être utilisée pour retirer de l'argent de la carte ou du compte de l'utilisateur (excepté pour les paiements pour lesquels l'accord de l'utilisateur a été donné avec sa carte et le C-ZAM/PC).

Remarquons enfin que l'utilisateur n'est absolument pas dépendant du poste à partir duquel il paie. Avec sa Proton, il peut payer à partir de n'importe quel(s) PC et/ou terminal C-ZAM/PC à condition de s'assurer de l'intégrité du PC et du C-ZAM/PC.

Cette portabilité représente un des grands avantages de Proton sur les solutions de paiement basées sur du logiciel, qui, le plus souvent, permettent de payer sur Internet uniquement via son propre PC.

Le terminal CZAM/PC est un lecteur de carte générique et peut être utilisé pour effectuer diverses tâches. Les applications du CZAM/PC connues aujourd'hui sont:

- Paiement par carte Proton;
- Chargement de la carte Proton;
- Authentification de l'utilisateur par la carte Proton pour des applications de homebanking;
- Lecteur Bancontact/MisterCash;
- Lecteur de la carte d'identité sociale SIS.

En plus des différents logiciels fournis par Element, le marchand a besoin du CZAM/VMT.

Le CZAM/VMT est une caisse enregistreuse électronique utilisée pour stocker l'argent entre deux collections. Une collection est l'opération durant laquelle l'argent qui est stocké temporairement dans le CZAM/VMT est transféré vers les systèmes de Banksys. Ce transfert se fait sur une ligne téléphonique et par l'utilisation d'un protocole propre à Banksys.

Un CZAM/VMT peut gérer jusqu'à 28 transactions simultanées, c'est-à-dire que 28 clients peuvent payer leur commande en même temps avec leur carte Proton.

Les nouveaux CZAM/VMT seront capables de gérer des transactions en EURO. Ce nouveau modèle sera appelé le CZAM/VMT Multi. Il comportera trois CSM (***C**hips **S**ecurity **M**odule*), chacun étant capable de gérer 16 transactions simultanées. Un CZAM/VMT Multi pourra donc gérer 48 transactions simultanées.

Une infrastructure normale de paiement comportera plus d'un CZAM/VMT. En effet, il n'est pas possible d'effectuer des transactions pendant une phase de collection. Il est donc recommandé d'avoir plus d'un CZAM/VMT. Dans ce cas, il y aura toujours au moins un CZAM/VMT disponible pour effectuer des transactions.

Un CZAM/VMT peut stocker jusqu'à 2000 transactions et contenir une somme allant jusqu'à 100 000 FB.

Exécution de la transaction

Mentionnons tout d'abord que le serveur du marchand se compose de deux éléments: un serveur marchand (le serveur Web auquel est connecté le client) et un serveur de paiement (qui effectue le paiement vers les CZAM/VMT).

1. Le serveur du marchand initie le porte-monnaie digital situé du côté client avec des paramètres spécifiques comme: le montant à payer, l'URL du serveur, le port et le numéro de la transaction, identifiant cette dernière.

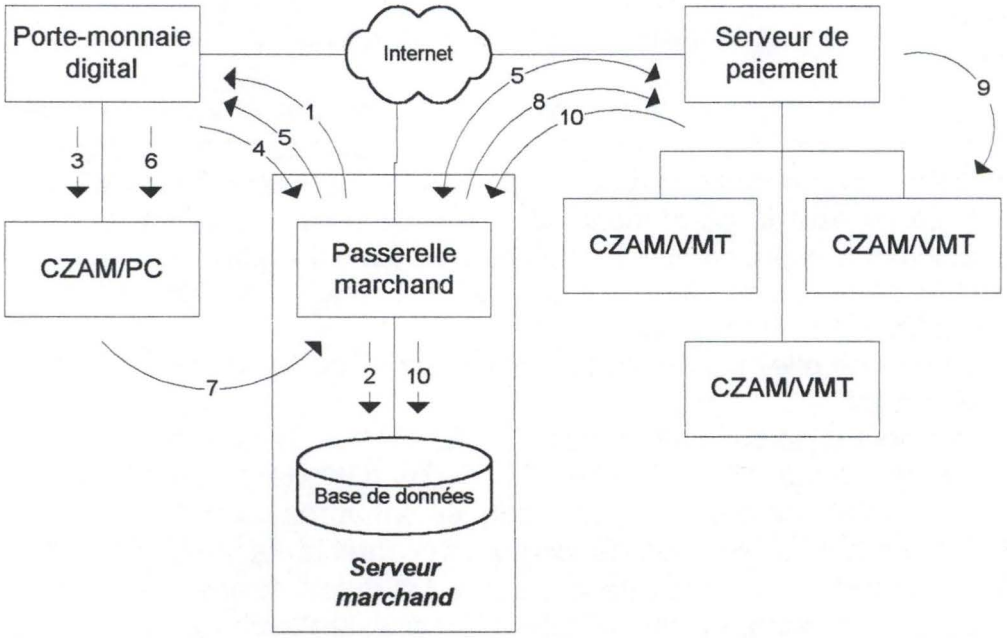


Figure 31: Schéma simplifié de la solution Proton d'Element

2. Le serveur marchand introduit les données de la transaction dans une base de données grâce à la passerelle[32] marchand. Les données de la transaction sont composées de 9 champs. Lors de cette étape, la passerelle ne remplit que les 5 premiers champs. Les 4 derniers seront remplis plus tard.

    - Un entier identifiant le vendeur;
    - Le numéro de la transaction;
    - Le montant de la transaction;
    - La devise de la transaction (les codes monétaires ISO sont utilisés; pour le franc belge, il s'agit du nombre 86);
    - Le statut de la transaction. Sa valeur à cette étape est '-2' et signifie que la transaction est initiée;
    - La date de la transaction;
    - L'heure de la transaction;
    - L'adresse IP du client;
    - L'identificateur de la carte Proton (PurseID).

3. Le porte-monnaie digital du client active le terminal CZAM/PC et demande à l'utilisateur d'introduire sa carte Proton.
4. Le porte-monnaie digital contact la passerelle marchand afin de s'assurer que toutes les données sont correctes, à savoir:

    - Le montant à payer donné par le CZAM/PC est-il correct?
    - Est-ce que le numéro de transaction donné par le CZAM/PC est bien un numéro de transaction existant et dont le statut est '-2'? Si tel est le cas, la passerelle change le statut de la transaction en '-1' et envoie la transaction au serveur de paiement.

5. Le serveur marchand contacte le serveur de paiement. Celui-ci répond au serveur marchand qui à son tour répond au porte-monnaie digital du client. Cette étape permet de créer un processus dans un CZAM/VMT.
6. A ce niveau, le porte-monnaie digital demande au client de confirmer le paiement en pressant le bouton 'OK' de son CZAM/PC.
7. Une confirmation du paiement est envoyée à la passerelle du serveur marchand par le CZAM/PC.
8. La passerelle transfère la confirmation du paiement au serveur de paiement.
9. Le serveur de paiement crédite le CZAM/VMT de la somme payée. Au cas où l'utilisateur ne presse pas la touche 'OK', le processus créé dans le CZAM/VMT sera annulé automatiquement après un certain temps.
10. Finalement le serveur de paiement contacte la passerelle du serveur marchand, lui indique que le paiement a réussi et envoie une confirmation au porte-monnaie digital du client. La passerelle change alors le statut de la transaction en '1', pour indiquer que la transaction est réussie et complète les champs encore vides dans la base de données.
11. Le serveur marchand redirige le client vers une page où figure le résultat de la transaction.

[32] Ensemble de hardware et de software permettant de faire le lien entre des systèmes de types différents.

Opération de collection

L'opération de collection est, comme nous l'avons déjà mentionné plus haut, l'opération durant laquelle l'argent stocké temporairement dans le CZAM/VMT est transféré vers les systèmes de Banksys. Cette opération doit être réalisée au moins une fois par mois et est semblable à l'opération de collection effectuée avec les terminaux situés dans les magasins *réels*.

3.3.2.2. Le système MONDEX

Introduction

Mondex, créé par MasterCard International, est avec Proton et VisaCash, le troisième acteur prédominant dans le monde des porte-monnaie électroniques. Mais contrairement aux autres, basés sur le principe de la réconciliation, le système Mondex exécute les transactions indépendamment d'une institution financière ou d'équipements de réconciliation des transactions. Par là même, Mondex est fort probablement le système qui se rapproche le plus des traditionnels pièces et billets en termes d'usages et de modèles de transactions. L'avantage pour les institutions financières l'acquérant est le peu d'investissement en infrastructure comparé aux systèmes fournissant la puissance de calcul nécessaire à ceux basés sur la réconciliation. L'avantage pour l'utilisateur final est un anonymat total lors de l'exécution de ses transactions. Une fois que des fonds sont extraits d'une institution financière, il n'y a plus le moindre enregistrement des transactions subséquentes si ce n'est les dix dernières transactions sur la carte même et ce, pour la commodité du porteur de carte. L'argent réside ainsi réellement sur la carte: carte perdue, argent perdu!

Mondex offre aussi une série de caractéristiques périphériques non disponibles avec les autres systèmes. La carte peut par exemple être mise par le porteur dans l'état 'unlocked' (utilisable) ou 'locked' (bloquée) pour augmenter la sécurité. La carte peut également contenir 5 porte-monnaie de devises différentes à la fois. Enfin, il est également possible de transférer de l'argent entre deux cartes.

Le département d'Amdahl dans lequel nous avons travaillé nous a permis d'approcher le système Mondex de près. Cependant la majorité de l'information à laquelle nous avons eu accès est confidentielle. Nous ne pourrons donc pas nous étendre longuement sur ce système.

Présentation du système

Le système Mondex a pour principe de faire intervenir deux puces lors d'un transfert d'argent. Ceci permet d'accroître la sécurité puisque l'argent n'est jamais stocké dans une mémoire d'ordinateur, réduisant de ce fait les possibilités de fraude. Le temps nécessaire à l'exécution d'une transaction, plus important que celui nécessaire dans le système Proton, constitue le désavantage majeur de Mondex.

Dans un système monétaire conventionnel, une banque centrale est responsable du battage et de l'émission de valeurs sous forme de pièces et de

billets. Dans le système Mondex, le rôle de la banque centrale conventionnelle est joué par une organisation dénommée *Originator* (initiateur). Cet initiateur a la responsabilité de créer de la valeur électronique dans une devise spécifiée qui est alors distribuée par le réseau bancaire. Mondex, lors du lancement du système, a créé un initiateur pour chacune des monnaies présentes dans le système.

A côté de ce travail d'émission, l'initiateur doit aussi récupérer cette valeur pour ensuite la réémettre ou la détruire. Tout comme pour les systèmes bancaires conventionnels, les procédures de création et de destruction de valeurs sont régies par des régulations strictes. Nous n'avons malheureusement pas eu accès aux documents en expliquant le fonctionnement.

Une fois la valeur disponible dans le système bancaire, les utilisateurs du système peuvent l'utiliser pour effectuer des paiements. Un paiement Mondex implique toujours le transfert sécurisé de l'argent d'une puce à une autre. Les paiements peuvent avoir lieu vers ou depuis une banque, entre consommateurs et marchands ou encore directement entre consommateurs.

Les porteurs de carte peuvent retirer ou déposer de l'argent sur leur compte. Pour le porteur de carte, l'argent est transféré entre son compte et sa carte. En réalité, l'argent électronique est en fait échangé avec le porte-monnaie de la banque. La banque débite ou crédite ensuite le compte de l'utilisateur.

La figure suivante montre un exemple de paiement Mondex. Dans cet exemple, le client charge sa carte depuis son compte via un distributeur. La banque transfère de l'argent électronique de son porte-monnaie vers le porte-monnaie du client. Elle débite ensuite le compte du client et crédite le sien de la valeur transférée. Ce système est tout à fait analogue à celui utilisé lors d'un retrait d'argent liquide à un distributeur.

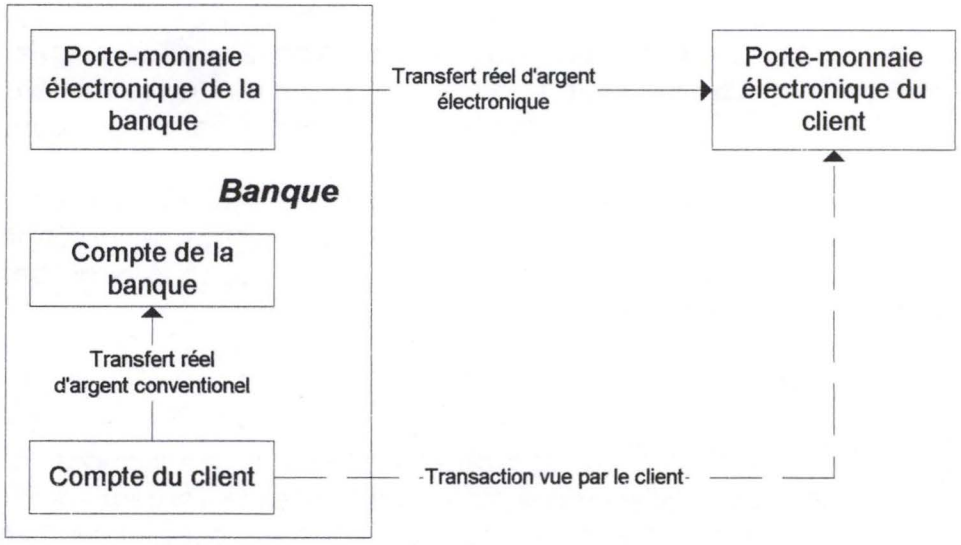


Figure 32: Rechargement d'une carte Mondex

Un autre exemple démontrant la façon dont la valeur Mondex reste intacte est une machine de change qui accepte des billets et des pièces avec en contre partie,

un chargement équivalent de la carte Mondex de l'utilisateur. Dans ce cas, la machine transfère l'argent électronique de son porte-monnaie vers le porte-monnaie de l'utilisateur.

Le schéma suivant détaille le fonctionnement du paiement entre un client et un marchand. Étant donné que le système Mondex ne transfère de l'argent que d'une puce vers une autre puce, le terminal du marchand réalisant la transaction en contient également une. Toutes les communications ayant lieu entre le terminal et les cartes à puce se font d'après un protocole propre à Mondex. Les étapes de la transaction sont les suivantes:

1. Le vendeur introduit dans son terminal (il s'agit d'un lecteur de cartes à puce homologué par Mondex) la somme à payer qui apparaît au consommateur sur l'écran du terminal.
2. L'acheteur introduit sa carte Mondex dans le lecteur de carte à puce du terminal.
3. Le terminal vérifie si la puce contient bien un porte-monnaie électronique Mondex.
4. Le terminal exécute alors plusieurs tests sur les deux porte-monnaie (celui de l'acheteur et celui du vendeur) afin de savoir si le paiement peut avoir lieu. Si ces tests sont positifs, le terminal demande aux deux porte-monnaie d'effectuer le paiement.

Dès que ces étapes ont eu lieu, le paiement peut prendre place. Il consiste en trois étapes:

1. Le porte-monnaie marchand demande la valeur à payer.
2. Le porte-monnaie client envoie cette valeur.
3. Le porte-monnaie marchand accuse réception de la valeur.

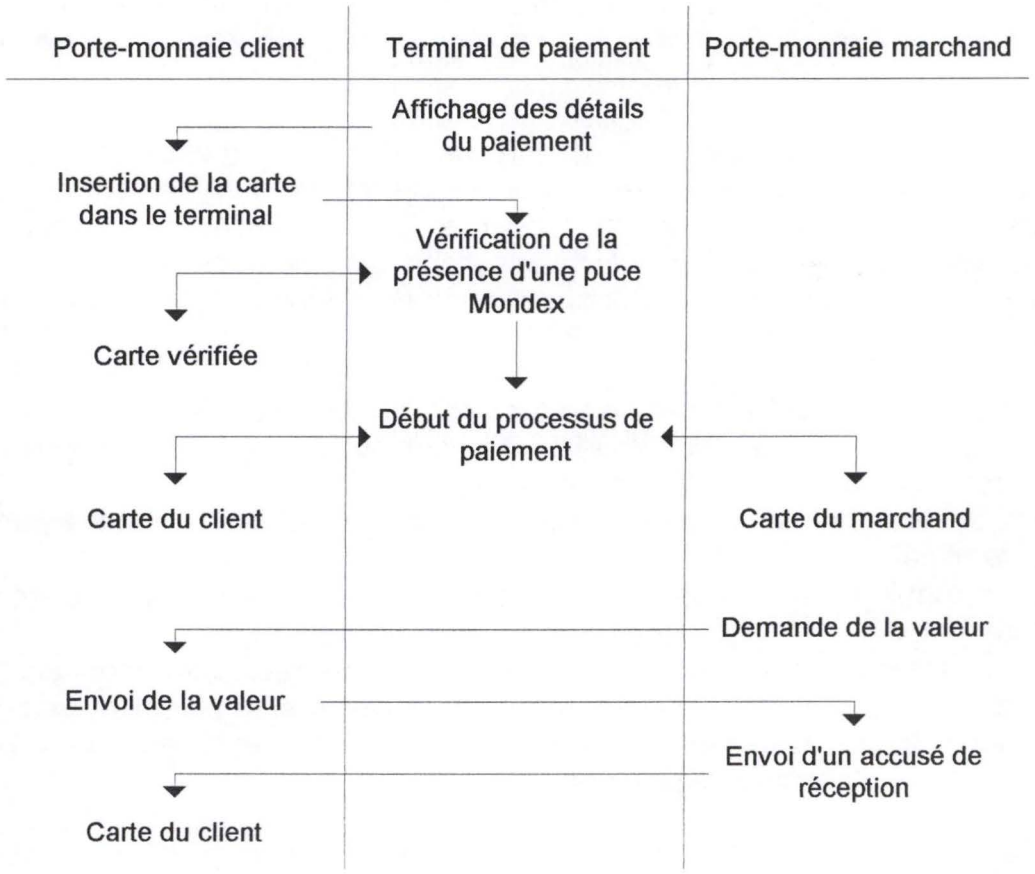


Figure 33: Étapes d'un paiement Mondex

Tout comme l'utilisation de pièces et de billets, l'argent électronique peut être de n'importe quelle devise. Pour chaque devise supportée par Mondex, il existe un initiateur. Chaque porte-monnaie peut contenir plusieurs devises à la fois, chaque devise étant contenue dans des parties séparées du porte-monnaie et appelées 'Pocket'. La valeur contenue dans une 'Pocket' est distincte de la valeur contenue dans les autres 'Pocket'. Le concept, par exemple, d'un franc belge devenant un franc français n'existe pas. Aucune conversion de devise n'intervient à l'intérieur du porte-monnaie. Lorsqu'un paiement a lieu entre deux porte-monnaie, les parties impliquées décident de la devise à utiliser.

La façon dont sont gérées les devises multiples est mieux illustrée par l'exemple suivant:

Soit un bureau de change offrant des facilités de change pour des pièces et billets mais aussi pour l'argent électronique. Un utilisateur dont le porte-monnaie électronique contient £200 veut en échanger 100 contre des francs français. Il devra également s'acquitter d'une commission auprès du bureau de change. Pour effectuer ce change, deux transferts ont lieu:

1. L'utilisateur paye £100 au bureau de change;
2. Le bureau de change déduit £2 de commission, calcule l'équivalent en francs français de £98, et ensuite transfère ce montant depuis sa 'Pocket'

franc français de son porte-monnaie vers la 'Pocket' franc français du porte-monnaie de l'utilisateur.

Le schéma suivant illustre l'opération effectuée.

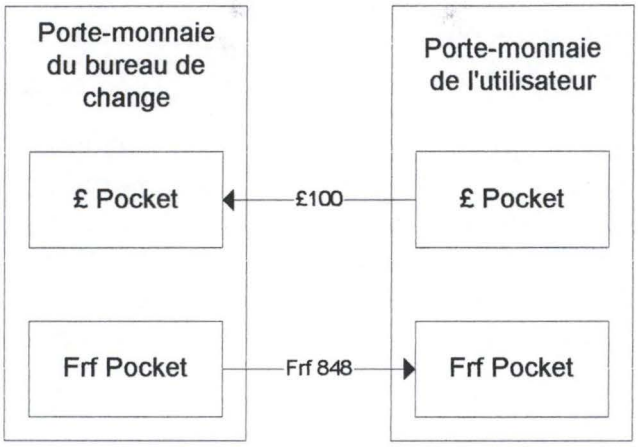


Figure 34: Exemple d'opération de change

Il montre bien que la valeur totale de chaque devise en circulation n'a pas changé après que le change ait eu lieu. Dans cet exemple, le bureau de change a gagné des Livres Sterling alors que l'utilisateur a gagné des francs français. Notons pour terminer que les taux de change et le montant de la commission sont déterminés par le bureau de change et non par Mondex.

3.4. Porte-monnaie virtuel

3.4.1. Présentation

Un système de monnaie électronique n'utilisant pas une carte à puce utilise un fichier pour conserver l'argent. La valeur est contenue dans un fichier chiffré enregistré sur un PC et protégé par un mot de passe. Ainsi, seul son propriétaire y a accès. Ce fichier peut être ou ne pas être transférable sur un autre PC et porte souvent le nom de porte-monnaie virtuel.

Ce fichier contient un ensemble de jetons et chaque jeton représente une certaine somme d'argent. Un jeton n'est rien de plus qu'une suite de chiffres. Une banque, offrant ce type de service, émettra ces chaînes de chiffres tout en débitant votre compte d'un montant égal à celui de l'argent émis sous forme de jetons. La banque valide chaque jeton en lui appliquant sa signature digitale avant de le transmettre à votre PC. Lorsque vous souhaitez dépenser vos jetons, il vous suffit de transmettre au commerçant un nombre de jetons correspondant à l'article acheté. Le commerçant transférera alors ces jetons à sa banque pour en obtenir la contre-valeur. Pour s'assurer que chaque jeton n'est utilisé qu'une fois, la banque conserve le numéro de série de tous les jetons déjà dépensés. Cela évite qu'un consommateur ne dépense deux fois le même jeton ou que le commerçant contrefasse un jeton.

Ce système, basé uniquement sur du software, ne demande aucun hardware spécifique.

Un de ces problèmes majeurs concerne le respect de l'anonymat. En effet, lorsque la banque crée un jeton, elle connaît son numéro de série et la personne à qui elle l'a transféré. Diverses solutions existent néanmoins pour garantir à l'utilisateur son anonymat. Nous étudierons un peu plus loin la solution mise en place par DigiCash.

En toute logique, on s'attend à ce que cela soit les banques qui émettent de l'argent électronique sous forme de jetons. Actuellement, peu le font. Mais les marchands ou d'autres intermédiaires ont également la possibilité d'émettre leurs propres jetons. Jusqu'ici il n'existe pas de solution permettant l'interopérabilité des différents systèmes. Seule l'institution émettrice est capable de racheter les jetons qu'elle a émis. Il n'existe aucune règle ou taux de change entre les différentes institutions émettrices.

3.4.2. Les systèmes disponibles

Plusieurs solutions étaient disponibles sur le marché, comme par exemple la solution e-Coin de la société américaine CyberCash. La plus connue était certainement la solution e-cash de DigiCash. C'est cette dernière que nous décrirons ici car elle est restée la référence au niveau des systèmes de porte-monnaie virtuels. Nous avons employé le passé car CyberCash vient de mettre fin à sa solution e-Coin. Quant à DigiCash, cette société américaine vient d'arrêter ses activités. Il semble qu'à l'heure actuelle il n'existe plus sur le marché de telles solutions.

Le système e-cash de DigiCash est un système à base de jetons et qui utilise un software installé sur un PC pour effectuer la transaction. Les jetons peuvent être générés à partir d'un compte bancaire, déposés sur un compte ou encore transférés à une autre personne. Le jetons sont stockés dans le porte-monnaie virtuel de l'utilisateur dans son PC.

Ce système nécessite l'intervention d'une institution financière lors de toute transaction et ce, dans le but d'éviter des problèmes de fraudes (utilisation à deux reprises d'un même jeton). Malgré l'intervention de cette institution, l'anonymat de l'acheteur est conservé. DigiCash utilise pour cela un système dit d'aveuglement.

Supposons qu'Alice veuille retirer de son compte bancaire $20 sous forme d'un jeton.

1. Grâce au logiciel DigiCash installé sur sa machine, Alice crée le numéro de série de son jeton (et non la banque!). Pour que ce jeton soit utilisable et ait bien une valeur de $20, il faut que la banque le signe avec sa clé privée. Si Alice envoyait le numéro de série à la banque tel quel, la banque serait capable de tracer l'utilisation de ce jeton. L'anonymat serait perdu.
2. Afin d'éviter ce problème, le logiciel installé sur le PC d'Alice crée un nombre aléatoire appelé facteur d'aveuglement.
3. Le logiciel multiplie le numéro de série par le facteur d'aveuglement
4. Alice signe alors ce nouveau nombre avec sa clé privée et l'envoie à la banque en lui demandant de le signer et de lui attribuer une valeur de $20.

5. La banque vérifie alors qu'il s'agit bien d'Alice en utilisant la clé publique de cette dernière.
6. En cas de test positif, la banque signe le nombre avec, parmi ses clés privées, celle qui correspond à une valeur de $20 et renvoie alors le nombre signé à Alice.
7. Alice commence par vérifier la signature de la banque pour s'en assurer l'authenticité.
8. En cas de test positif, il suffit au logiciel d'Alice de diviser le nombre reçu par la banque par le facteur d'aveuglement pour obtenir le numéro de série signé.

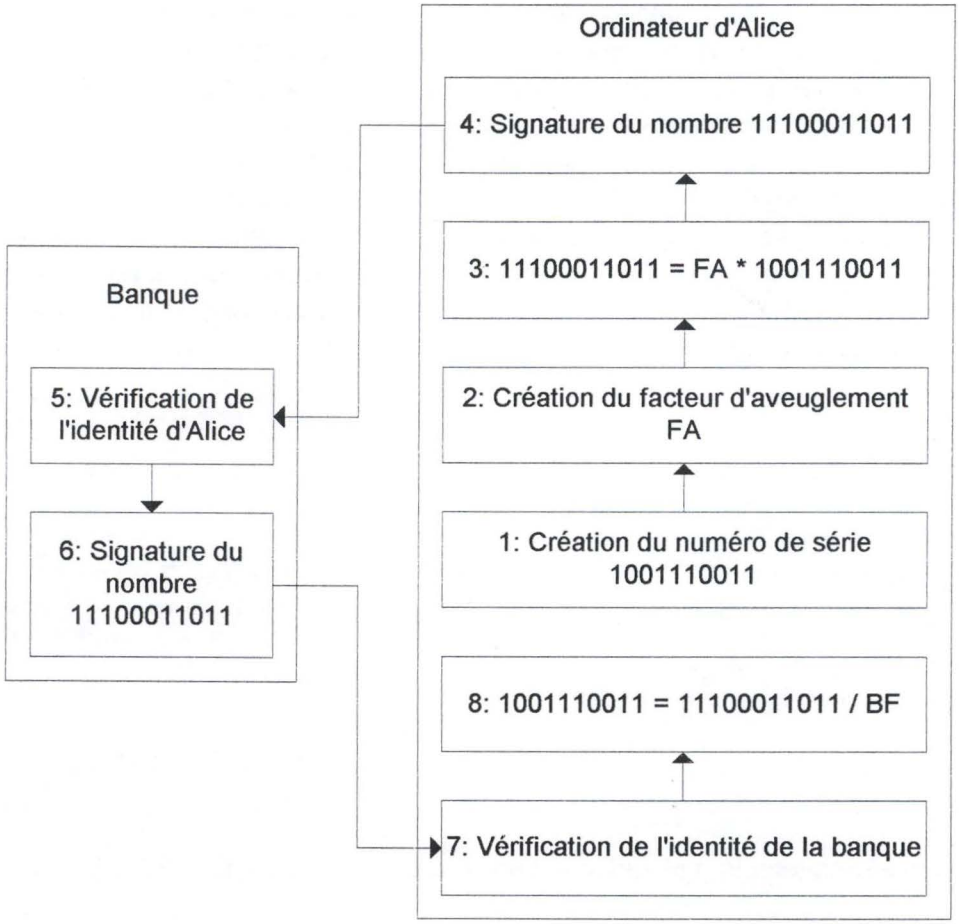


Figure 35: Création d'un jeton dans le système DigiCash. [GHOSH 98]

De par les propriétés mathématiques des algorithmes de signature utilisés, la division du nombre signé par le facteur d'aveuglement n'invalide pas la signature digitale.

Alice possède maintenant un jeton d'une valeur de $20 ayant un numéro de série inconnu de la banque.

Nous terminerons la description du système e-cash de DigiCash en expliquant le processus de paiement.

Alice souhaite transférer à Bob les $20 qu'elle lui doit. Comme dans toutes les transaction du système DigiCash, une banque est impliquée afin de vérifier l'authenticité du jeton utilisé et de s'assurer qu'il n'a pas encore été dépensé.

1. Bob envoie à Alice une demande de $20.
2. Le logiciel d'Alice retire le jeton de $20 du porte-monnaie digital d'Alice et l'envoie à Bob.
3. Bob peut alors vérifier l'authenticité et la valeur du jeton étant donné qu'il a été signé par la banque. Bob doit néanmoins l'envoyer à la banque pour pouvoir être crédité. Cette procédure, réalisée par le logiciel installé sur l'ordinateur, est transparente pour son propriétaire.
4. La banque de Bob vérifie la signature de la banque d'Alice en utilisant la clé publique de la banque d'Alice. Grâce à cette vérification, la banque peut connaître la valeur du jeton et vérifier son authenticité. La banque vérifie également que le numéro de série du jeton ne fait pas partie de la liste des jetons déjà dépensés. En cas de test positif, la banque crédite le compte de Bob de $20. Dès que Bob reçoit l'extrait de compte de la transaction, son logiciel envoie à Alice la notification de la transaction. Le numéro de série du jeton envoyé par Alice à Bob étant différent du nombre signé par la banque d'Alice, la banque est incapable de déterminer la façon dont Alice a dépensé ses $20.

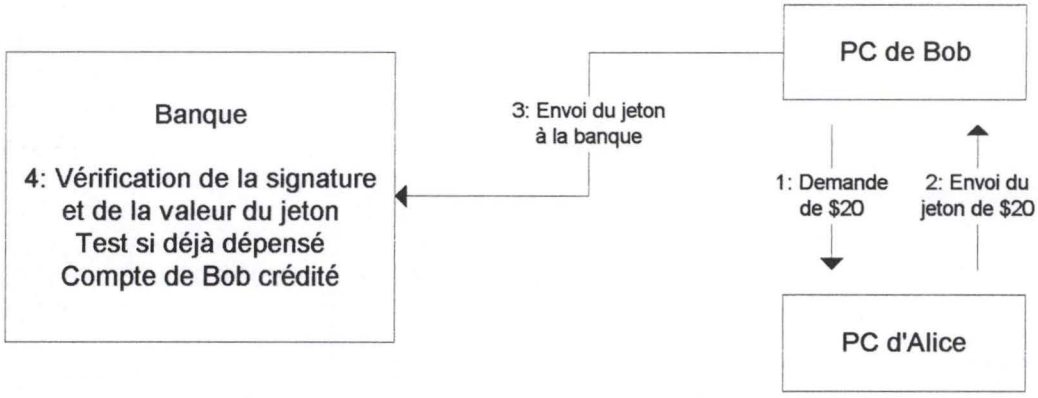


Figure 36: Transaction de paiement dans le système DigiCash. [GHOSH 98]

Plutôt que de voir son compte crédité, Bob peut conserver dans son porte-monnaie virtuel le jeton de $20 qu'il a reçu d'Alice. Bob doit cependant envoyer le jeton à sa banque pour authentifier le jeton et vérifier qu'il n'a pas encore été dépensé.

4. Chèque électronique

Ce moyen de paiement est fort peu utilisé et à notre connaissance uniquement disponible pour les consommateurs nord-américains. Peu d'informations sont disponibles à ce sujet. Nous le mentionnerons cependant car nous avons rencontré ce moyen de paiement lors de notre étude de cas.

Un chèque (en version 'papier') est à la base le message d'un consommateur demandant le transfert d'une certaine somme d'argent mentionnée de son compte au compte de quelqu'un d'autre. N'étant pas envoyé directement à la banque mais à la personne sensée recevoir les fonds, cette dernière doit présenter le chèque à la banque pour voir son compte crédité.

Un chèque électronique à toutes les caractéristiques d'un chèque papier. Il fonctionne comme un message destiné à la banque de l'acheteur et demandant de transférer des fonds. Et tout comme un chèque papier, ce message est donné (par transmission directe à travers un réseau ou par e-mail) au marchand qui endosse le chèque et le présente à la banque afin d'en obtenir l'argent.

Décrivons brièvement le système rencontré dans notre étude de cas. L'utilisateur voulant payer par chèque transmet au site marchand son numéro de compte, le numéro identifiant sa banque, ses coordonnées et celles de la banque, soient toutes les informations présentes sur un chèque traditionnel. Le système vérifie alors si les informations concordent auprès des banques. Si tel est le cas, il crée un fichier contenant une représentation graphique du chèque. Il ne reste plus au marchand qu'à aller télécharger son chèque, l'imprimer, l'endosser et le toucher auprès de sa banque.

Ce système peut être intéressant pour les personnes ne disposant pas de carte de crédit.

Nous avons voulu en savoir plus sur les procédures de sécurité utilisées afin de garantir la validité du chèque émis. Malheureusement le site Web d'InfoDial[33], société fournissant cette solution, est très peu documenté et nos e-mails sont tous restés sans réponse. N'ayant pas trouvé de société fournissant le même service, nos questions sont restées sans réponse.

5. Carte de débit

Pour terminer ce tour des différents moyens de paiement utilisables sur Internet et afin d'être aussi complet que possible, nous citerons une nouvelle initiative de Banksys rapportée par **[DATA 99]**. En effet, à partir d'octobre 1999, il sera possible de régler ses achats sur Internet au moyen de sa carte Bancontact/MisterCash. Banksys se flatte en effet de réaliser une première, à savoir le paiement sur Internet par carte de débit. Le code personnel PIN[34] activé sur la carte assurera la sécurisation de la transaction.

Dans un premier temps, les internautes ne pourront payer qu'auprès de commerçants belges, mais Banksys prépare l'internationalisation des paiements. Le lecteur de cartes sera lui disponible dès septembre.

Nous avons essayé d'obtenir de plus amples renseignements concernant ce mode de paiement auprès du porte-parole de Banksys. Malheureusement, ce dernier ne pouvait pas nous en dire plus.

---

[33] http://www.infodial.net/

[34] PIN: Personal Identification Number

6. Comparaison des différents modes de paiement

Nous ne disposons malheureusement pas d'assez d'informations pour pouvoir intégrer à notre comparaison le paiement par chèque électronique et celui par carte de débit. Nous nous limiterons donc aux cartes de crédit, aux porte-monnaie électroniques et aux porte-monnaie virtuels.

Nous avons choisi les points de comparaison suivants:

- Marché international: indique si le moyen de paiement est adapté pour des sites marchands ayant une clientèle internationale.
- Marché local: indique si le moyen de paiement est adapté pour des sites marchands ayant une clientèle nationale.
- Petites transactions: indique si le moyen de paiement est adapté aux transactions mettant en jeu de petits montants.
- Transactions importantes: indique si le moyen de paiement est adapté aux transactions mettant en jeu des montants importants.
- Sécurité client: indique s'il existe des solutions permettant l'utilisation de ce mode de paiement et qui garantit au client la protection de ses informations de paiement.
- Sécurité marchand: indique s'il existe des solutions permettant l'utilisation de ce mode de paiement et qui garantissent au marchand d'être payé.
- Coût client: indique si le coût d'utilisation du système est important pour le client.
- Coût marchand: indique si le coût d'exploitation est important pour le marchand.

Nous proposons la cote suivante:

- *: critère peu rempli
- **: critère moyennement rempli
- ***: critère rempli

Sur base de ce chapitre, nous pouvons alors établir le tableau suivant:

	Carte de crédit	Porte-monnaie électronique	Porte-monnaie virtuel
Marché international	***	*	*
Marché local	***	***	***
Petites transactions	**	***	***
Transactions importantes	***	*	*
Sécurité client	***	***	**
Sécurité marchand	**	***	**
Coût du client	***	**	***
Coût marchand	**	***	**

Tableau 7: Comparaison des moyens de paiement

Comme nous l'avons mentionné plus haut dans ce chapitre, les solutions de type porte-monnaie virtuel tendent à disparaître. On peut expliquer cela par le manque d'interopérabilité des différentes solutions.

Restent alors la carte de crédit et le porte-monnaie électronique.

La carte de crédit est très bien adaptée au marché tant national qu'international et les nouvelles solutions de type SET garantissent une sécurité maximale pour tous les acteurs en jeu. De plus, ce système ne demande pas d'investissement particulier à l'acheteur. Le seul petit défaut du système est la nécessité pour le vendeur de se connecter très régulièrement à l'organisme de crédit avec lequel il est lié afin d'autoriser et d'exécuter les ventes.

Les systèmes de porte-monnaie électronique intègrent des moyens de sécurité perfectionnés les rendant très sûrs. Ils sont également très bien adaptés aux marchés nationaux et aux transactions portant sur de petits montants (moins de 5000FB pour Proton). Le coût d'exploitation pour le marchand n'est pas très important puisqu'il lui suffit pour obtenir son argent de se connecter de temps en temps (minimum une fois par mois dans le cas de Proton) aux systèmes de l'institution financière avec laquelle il est lié. L'acheteur devra quant à lui acquérir un lecteur de carte à puce. Même si cela représente encore à l'heure actuelle un investissement, cela ne devrait plus durer. En effet, les claviers avec lecteur de carte intégré devraient inonder le marché.

La carte de crédit reste et restera à notre avis le principal moyen de paiement sur Internet. Les porte-monnaie électroniques, quant à eux, devraient prendre une certaine importance, sur les marchés nationaux uniquement, à moins que des efforts importants ne soient consentis pour rendre ces systèmes interopérables sur un plan international

Chapitre 4: Droit et commerce électronique

1. Introduction

L'apparition du commerce électronique soulève énormément de difficultés liées à son intégration dans la situation juridique d'aujourd'hui.

Dans le Code Civil, l'article 1108 reprend quatre conditions nécessaires à la validité d'une convention:

- *le consentement de la partie qui s'oblige*
- *sa capacité de contracter*
- *un objet certain qui forme la matière de l'engagement*
- *une cause licite dans l'obligation*

Mais dans le contexte du commerce électronique actuel, on peut s'interroger sur la rencontre des quatre conditions. Ce qui, par conséquent, pourrait remettre en cause la validité de l'engagement commercial.

Avec l'apparition du commerce électronique, et par conséquent l'immatérialité du contrat, c'est tout le régime de la preuve qui est remis en question.

Dans de telles conditions, une question est rapidement apparue:

"

Faut-il modifier profondément notre législation du droit de la preuve pour y faire entrer la réalité des ordinateurs et des technologies de la communication?

" (**[POULLET]**)

D'énormes efforts sont consentis pour faciliter la législation du commerce électronique sur le Web. Par la suite, nous verrons pourquoi aujourd'hui grâce aux techniques actuelles et à une nouvelle approche du droit, la tendance serait de répondre négativement à cette question.

Nous analyserons plus particulièrement la signature électronique, les Autorités de Certification et l'écrit électronique. Nous verrons également quelles sont les attitudes que les hommes de loi prennent ou sont prêts à suivre face aux nouvelles technologies.

2. La signature électronique et les Autorités de Certification

2.1. Position du problème

Suite au développement des réseaux et des communications qui y sont liées, il n'a pas fallu longtemps aux entreprises pour profiter d'une telle opportunité de faciliter la conclusion de contrats via le réseau. Ainsi, tant le secteur public que le secteur privé travaille dorénavant d'une manière plus rapide et efficace. On notera par ailleurs une réduction drastique de tous les documents manuscrits engendrant une diminution de l'espace d'archivage et de par leur aspect électronique, un accès plus rapide.

Tous les éléments sont donc réunis pour que se réalisent, sur les réseaux, une multitude d'opérations commerciales et pour que se nouent des liens obligataires. Et ce, en l'absence d'écrit papier et de la signature cristallisant l'accord intervenu entre les deux parties. De telles transactions se trouvent donc confrontées à certains obstacles juridiques.

En effet l'article 1315 du Code civil stipule:

"

Celui qui réclame l'exécution d'une obligation doit la prouver. Réciproquement, celui qui se prétend libéré doit justifier le paiement ou le fait qui a produit l'extinction de son obligation

"

Même si la preuve est libre et peut être exercée par toutes voies de droit comme, par exemple, le témoignage ou la présomption dans l'état actuel de droit, une forte valeur probatoire est accordée à l'écrit et la signature manuscrite. L'article 1323 en relève l'importance:

"

Celui auquel on oppose un acte sous seing privé est obligé d'avouer ou de désavouer formellement son écriture ou sa signature

"

L'article 1341 du Code civil pose en règle que:

"

Il doit être passé acte devant notaire ou sous signature privée, de toutes choses excédant une somme ou valeur de quinze mille francs,...

"

Pour une convention commerciale portant sur une somme supérieure à quinze mille francs, la preuve doit être rapportée par écrit et cette dernière n'aura de force probante que si elle est signée.

L'utilisation d'une solution électronique pour jouer le rôle de la signature et de l'écrit traditionnel a donc soulevé maintes questions qui demandent rapidement des réponses. La signature, l'écrit électronique et les Autorités de Certification semblent pouvoir fournir de bonnes solutions.

2.2. La signature électronique

2.2.1. Définition

En général, on considère la signature comme étant un graphisme personnel qui permet d'établir la présence physique de l'intervenant et par lequel la personne manifeste son consentement. (**[VEREYDEN 91]**)

La signature est appelée à remplir deux fonctions:

- Elle permet une authentification du signataire
- Elle indique l'approbation du signataire quant au contenu du document signé

2.2.2. La cryptographie et la signature

L'utilisation de la cryptographie[35] pour jouer le rôle de signature satisfait plus que parfaitement les caractéristiques qu'on en exige, à savoir: l'authentification, l'expression du consentement et l'efficacité.

Authentification de la signature

Si une paire de clés publique et privée est associée à un signataire connu, la signature digitale alloue le message signé au signataire aussi longtemps que la signature n'a pas été mise à mal par une perte, une divulgation, voire une corruption.

Expression du consentement

Pour assurer la sécurité de la transaction, le signataire a recours à la clé privée. En utilisant cette dernière, son propriétaire doit prendre conscience qu'il effectue un acte empreint de considérations légales.

Efficacité

L'utilisation de la cryptographie offre à la signature digitale toutes les fonctions requises et ce, avec un plus grand degré de certitude.

Dès lors que la signature digitale peut être assimilée à la signature manuscrite, on ne voit pas pourquoi elle ne pourrait pas endosser la force probatoire de cette dernière.

2.3. La signature électronique et l'adaptation du droit

2.3.1. Alternatives

Différentes alternatives s'offrent au législateur pour admettre la signature électronique . (**[ANTOINE 98]**, **[ICRI 97]**)

Suppression du régime de la preuve réglementée.

En libéralisant le régime de la preuve, le législateur ouvrirait les portes à toutes les transactions commerciales électroniques puisque qu'elles ne devraient plus être prouvées par un écrit signé. Tous les documents qui découlent de tels actes seraient alors admissibles.

Deux raisons fondamentales se posent en obstacle à une telle initiative. (**[LARRIEU 98]**)

---

[35] Pour de plus amples informations sur la cryptographie, voir le chapitre 2

Une telle solution bouleverserait le système juridique belge et mettrait ainsi à mal l'équilibre des intérêts que le régime de la preuve réglementée prétendait assumer.

D'autre part, cette solution n'enlèverait rien au pouvoir discrétionnaire du juge dans l'appréciation de la valeur probante du mode de preuve, sachant que la jurisprudence reste attachée à la conception formelle de la signature[36].

Élévation du seuil en deçà duquel la preuve est libre.

En rehaussant le plafond financier fixé par l'article 1341 du Code Civil, le législateur autoriserait des transactions commerciales sur un support électronique et donc sans preuve par écrit, portant sur une somme inférieure à la nouvelle limite fixée.

Une telle solution n'offre aucune réponse concrète au problème de la preuve, mais ne fait que le repousser d'une part en maintenant la suprématie de l'écrit papier signé et d'autre part, en n'offrant aucune valeur probante à la signature électronique.

Légitimation de la preuve électronique par le biais d'exceptions.

Il s'agit ici de légitimer la preuve électronique en étendant le champ d'application de l'article 1347 (commencement de preuve par écrit) ou 1348 (impossibilité de se procurer une preuve écrite) du Code civil. (**[FONTAINE 87]**, **[LECLERCQ 83]**, **[SYX 82]**,**[VERHEYDEN 91]**)

C'est toutefois la voie qui a été suivie par les législateurs français avec leur loi du 12 juillet 1980 et par les législateurs luxembourgeois avec leur loi du 22 décembre 1986.

De telles tentatives de légitimer la preuve électronique par le biais d'exceptions au principe de l'écrit signé se sont révélées néfastes. De telles solutions se révèlent limitées lorsque des lois spéciales réclament un écrit signé et, plus gravement, militent pour une acception trop large des preuves électroniques sans poser d'exigences de sécurité dans leur confection. (**[POULLET]**)

Adoption d'une définition plus fonctionnelle.

Comme nous l'avons déjà vu précédemment, l'utilisation de la cryptographie au travers de la signature et de l'écrit électronique permet entièrement d'assurer les fonctionnalités qui sont reconnues par la loi au papier et à la signature manuscrite. Dès lors, il conviendrait d'inscrire dans la loi une définition plus fonctionnelle qui ne soit pas restrictive aux techniques actuelles mais ouvertes aux évolutions du futur et s'attachant uniquement aux fonctions reconnues à la signature.

---

[36] Cass., 24 févr. et 3 nov. 1910, Pas., 1910, I, pp.241 et 475 ; Cass., 1 er mars 1917, Pas., 1917, I, p.118 ; Cass., 7janv. 1955, Pas., 1955, I, p.456 ; Cass., 2 oct. 1964, Pas., 1965, I, p.106

Une telle solution offre une réponse précise au problème de la preuve. En effet, elle met une fin à la suprématie du document papier et donne une valeur probante à la signature électronique.

2.3.2. Position du législateur belge

C'est cette dernière attitude qui a été poursuivie puisque le Conseil des ministres a adopté le 12 juin 1998 deux avant-projets de loi. Ils visent, entre autres, à modifier les règles du Code Civil afin qu'un document signé électroniquement ne puisse être rejeté d'office par le juge pour le seul motif qu'il se présente sous forme électronique. (**[GOBERT 98]**) Cette approche, technologiquement neutre, permet d'ouvrir la définition aux mécanismes actuels et futurs de signature électronique tout en excluant ceux qui n'offrent pas un niveau de sécurité au moins équivalent à la signature manuscrite.

Un des autres objectifs poursuivis par les avant-projets est de permettre à tous les secteurs d'activité de procéder à un archivage électronique tout en se réservant des moyens de preuve. En effet, "*est assimilé à un acte sous seing privé original l'écrit signé (manuscritement ou électroniquement) dont le maintien de l'intégrité du contenu est établi avec certitude*". (**[GOBERT 98]**)

Notons encore que des propositions de modifications de définition de la signature mûrissent actuellement. Nous retiendrons celle qui est offerte par Mireille Antoine et Didier Gobert dans **[ANTOINE 98]**:

"

Constitue une signature, outre la signature manuscrite, l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de ce dernier.

"

2.4. Les Autorités de Certification

2.4.1. Introduction

La signature digitale, basée sur la technique de cryptographie asymétrique et combinée à l'utilisation d'un certificat, permet de remplir trois fonctions importantes: d'une part, elle garantit l'identité de l'auteur d'un document signé digitalement et d'autre part, elle garantit l'intégrité de ce même document. Enfin, elle atteste la volonté du signataire de s'approprier le contenu de l'acte signé digitalement.

2.4.2. Définition et distinction

Du fondement de la signature digitale sur un système cryptographique asymétrique découle l'intervention de nouveaux acteurs et en particulier, des Autorités de Certification qui attestent de l'authenticité du contenu des informations publiées et publient, dans des registres ouverts, les clés publiques.

Dans un monde global où le réseau constitue la seule manière d'entrer en communication, la certification se définit comme une procédure par laquelle un tiers garantit la qualité spécifique d'une personne ou d'un produit. (**[COURET et alii 95]**)

Cependant, il convient de préciser d'emblée quelques concepts et de mettre en exergue les différences entre d'une part, Autorité de Certification et tiers de confiance (Trusted Third Parties) et d'autre part, Autorité de Certification et Autorité d'enregistrement. (**[ANTOINE 98]**)

Autorité de Certification et tiers de confiance

Lors de l'émission d'un certificat, un organisme devra garantir formellement le lien qui existe entre la personne et sa clé publique, il s'agit de l'Autorité de Certification.

Pour appliquer le chiffrement nécessaire à l'émission du certificat, il faut disposer d'une institution tierce qui conservera en toute sécurité une copie de la clé privée utilisée. C'est le tiers de confiance (Trusted Third Parties) qui s'en charge.

Autorité de Certification et Autorité d'enregistrement

Il convient ensuite de distinguer la fonction d'enregistrement de celle de certification. (**[TRUDEL 96]**)

Avant la certification, il convient de récolter l'ensemble des informations nécessaires à une telle attribution et ce, de manière fiable et sécurisée. Cette fonction peut être assumée par l'Autorité de Certification elle-même mais peut également être confiée à un organisme distinct appelé Autorité d'enregistrement.

Il conviendra ici, dès lors, de s'interroger quant à la répartition de responsabilité que pourrait encourir l'Autorité de Certification ou l'Autorité d'enregistrement.

Dans le cadre de ce travail, nous nous limiterons aux orientations actuelles données au régime juridique applicable aux Autorités de Certification.

2.4.3. Rôles de l'Autorité de Certification

Pouvant être assimilés à des notaires électroniques, les Autorités de Certification sont des tiers indépendants jouant plusieurs rôles, à savoir:

- Vérifier l'identité des titulaires de clés publiques
- Assurer la publicité la plus large des clés publiques
- Créer et délivrer des certificats, soit une structure de données signées digitalement qui fait le lien entre une personne et sa clé publique. Elle émet ainsi un certificat digital qui contient différentes informations relatives notamment à l'identité du titulaire du certificat, à sa clé publique et, bien entendu, à l'identité de l'Autorité elle-même. Notons encore que le certificat est réalisé par l'Autorité de Certification au moyen de sa clé privée, ce qui assure un degré de sécurité maximum.

Peuvent leur être encore assignés d'autres rôles comme par exemple, le stockage des messages échangés à des fins probatoires en cas de protestation, une fonction d'arbitrage entre parties en litige, l'horodatation de messages signés

digitallement, la vérification de signatures digitales et la confirmation de leur validité. (**[TRUDEL 96]**, **[CAPRIOLI 98]**)

2.4.4. Obligations des Autorités de Certification

La certification qui a pour ambition de rassurer l'internaute repose essentiellement sur la qualité des Autorités de Certification et des procédures de vérification.

Il est par essence obligatoire que les Autorités de Certification se munissent d'un système informatique fiable et assurent la confidentialité de la clé privée qu'elle utilise pour signer les certificats qu'elles produisent. L'Autorité devra se conformer aux prescriptions de la loi sur la protection de la vie privée mais aussi remplir une obligation de renseignement et de conseil. L'Autorité doit évidemment s'engager sur l'exactitude des informations figurant dans les certificats qu'elle émet. Outre leur exactitude, les informations devront être complètes mais aussi mises à jour.

L'Autorité de contrôle dispose d'un droit de suspension ou de révocation d'un certificat en cas de nécessité justifiée (par exemple, si le titulaire du certificat en compromet la fiabilité). La suspension, comme son nom l'indique, consiste en l'interruption, jusqu'à nouvel ordre, de l'usage d'un certificat. Quant à la révocation, elle entraînera le retrait du certificat sans effet rétroactif avant sa date d'expiration. Notons cependant que dans cette dernière hypothèse, elle devrait être précédée d'une décision de suspension. Ces deux alternatives peuvent aussi découler de l'initiative du titulaire du certificat.

La certification offre un avantage certain de par le fait qu'elle permet des sanctions faciles et efficaces puisque tant l'individu que l'entreprise craindront le retrait du certificat et la publicité qui s'attache à pareille circonstance.

2.4.5. Responsabilités des Autorités de Certification

Il faut aussi déterminer le degré de responsabilité de l'Autorité en cas de négligence dans la tenue des répertoires contenant les certificats et ce, afin d'alléger la charge de la preuve qui encoure à l'égard de l'utilisateur d'un certificat erroné.

Ainsi pourrait-on prévoir un régime de présomption de responsabilité à charge de l'Autorité de Certification. En cas d'identification erronée du titulaire du certificat, d'attribution par erreur d'une clé publique à une personne ou de certification d'une information incorrecte, l'Autorité de Certification serait présumée responsable du préjudice subi sauf si elle parvient à démontrer soit qu'elle s'est conformée aux obligations qui lui incombent, soit l'existence d'autres causes étrangères libératoires. (**[ONU 97]**)

2.4.6. Obligations des utilisateurs

L'utilisateur doit s'engager à fournir, de manière correcte et précise, toutes les informations qui sont utiles pour la délivrance d'un certificat.

La responsabilité de l'Autorité de Certification ne pourrait être mise en cause si les informations émises par le propriétaire du certificat s'avèrent fausses ou incorrectes. L'utilisateur doit aussi assurer la confidentialité de sa clé privée et, en

cas de doute, en avertir immédiatement l'Autorité de Certification pour que des mesures adéquates soient prises dans les plus brefs délais. Enfin, l'utilisateur doit s'engager à ne plus utiliser la clé privée liée à la clé publique certifiée par un certificat révoqué ou suspendu.

2.5. Les Autorités de Certification et l'adaptation du droit

2.5.1. Position du législateur belge

Au niveau belge, le Conseil des Ministres a adopté en première lecture, le 12 juin 1998, deux avant-projets de loi dont l'un est relatif à "l'activité d'Autorités de Certification agréées en vue de l'utilisation de signature digitales".[37] Ce dernier vise à mettre en place un régime juridique précis applicable aux Autorités de Certification qui désirent s'y soumettre.

Dans une des dispositions on retrouve clairement l'objectif qui est exprimé en ces termes:

"

La présente loi fixe les conditions générales d'agréation des Autorités de Certification... ainsi que les règles à respecter par ces dernières et les utilisateurs de certificats afin de renforcer la sécurité et la confiance dans l'utilisation de la signature digitale

"

Une Autorité de Certification est donc libre de demander ou non une agréation pour exercer ses activités de certification. Si elle désire se faire agréer, l'Autorité de Certification devra se soumettre aux conditions qui ont été prévues (indépendance, sécurité, garanties financières, interopérabilité) et, par conséquence à la loi ainsi qu'au régime clair de responsabilité y afférent.

On peut voir au moins trois bonnes raisons pour une Autorité de Certification de demander une agréation, et pour les utilisateurs de recourir à une Autorité de Certification agréée. (**[GOBERT 98]**) Premièrement, l'agréation constituera aux yeux du public une espèce de "label de confiance". Deuxièmement, une disposition de l'avant-projet établit un lien avec la nouvelle définition du Code civil en prévoyant qu'une signature digitale constitue une signature au sens de cette définition pour autant qu'elle soit réalisée sur base d'un certificat émis par une Autorité de Certification *agréée*. Finalement, on peut s'attendre à ce que de nombreuses lois particulières exigent que l'on passe par une Autorité de Certification *agréée* lorsque l'on utilise une signature digitale dans les relations avec l'administration et ce, en raison du niveau supérieur de sécurité.

---

[37] Ces deux avants projets de loi n'étaient pas encore publiés en novembre 1998

2.5.2. Principales Autorités de Certification

Les principales Autorités de Certification que nous avons recensées sont: ATT[38], BelSign[39], Entrust[40], GTE[41], IBM[42], InternetMCI[43], KeyWitness[44], Microsoft, Thawte[45] et Verisign.

2.6. L'écrit électronique

2.6.1. Définition

D'après M. Fontaine dans **[FONTAINE 87]**, trois conditions sont nécessaires pour qu'il y ait un écrit. Il faut qu'il s'agisse de l'expression d'un langage (mots et phrases) à travers des signes connus et traduisibles inscrits sur un support.

2.6.2. Valeur légales

Les qualités fonctionnelles qui sont propres à l'écrit, à savoir l'inaltérabilité, la lisibilité et la stabilité lui ont donné une forte valeur probatoire (**[MONTERO]**). Dans la mesure où un document électronique répond aux mêmes attentes, le statut d'écrit peut lui être conféré.

De par sa nature, en effet, le document électronique satisfait toutes les exigences. Sa dégradation est très lente, une suite de bits constitue un ensemble de signes connus et traduisibles rendant le document lisible; enfin les techniques renforcent, jour après jour, la carapace du document contre toute tentative de fraude.

2.7. L'écrit électronique et l'adaptation du droit

2.7.1. Position du législateur belge

L'article 1341 vise la signature et le législateur ne s'attarde nullement sur le concept de l'écrit.

Cependant, force est de constater que la reconnaissance d'une force probante à la signature électronique sous-entend également celle de l'écrit électronique.

---

[38] http://www.att.com/
[39] http://www.belsign.be/
[40] http://www.entrust.com/
[41] http://www.cybertrust.gte.com/
[42] http://internet.ibm.com/
[43] http://www.networkmci.com/
[44] http://www.keywitness.com/
[45] http://www.thawte.com/

3. Conclusion

La naissance du commerce électronique, comme nous l'avons vu, pose d'énormes problèmes en droit. Les nouvelles techniques actuelles permettent d'apporter nombres de solutions pour faciliter le travail des législateurs et offrir au commerce électronique un cadre favorable et juridiquement cohérent.

Après cette analyse, à la question posée dans l'introduction:

"

Faut-il modifier profondément notre législation du droit de la preuve pour y faire entrer la réalité des ordinateurs et des technologies de la communication?

" (**[POULLET]**)

nous pouvons constater que l'informatique ne requiert pas de révolution du droit. Elle nécessite une relecture du droit avec une approche plus fonctionnelle.

Chapitre 5: Marketing

1. Introduction

Les principaux objectifs d'un vendeur ont toujours été d'offrir des réponses aux deux questions suivantes:

- Comment attirer le client?
- Comment le fidéliser?

C'est à ces questions que nous allons tenter de répondre dans ce chapitre.

Dans la première partie, nous nous attacherons à analyser les moyens qui permettent de faire connaître le site aux clients potentiels. Nous avons consacré une attention toute particulière aux sites de recherche et à leur mode de fonctionnement puisqu'ils constituent le moyen le plus utilisé à ce jour par les internautes pour découvrir des sites. Une petite parenthèse traitera des bandeaux qui sont utilisés comme outils de promotion. Enfin, nous terminerons par quelques conseils supplémentaires permettant d'aider à promouvoir un site Web.

Dans la seconde partie, après avoir évoqué la nouvelle approche à adopter, nous énoncerons certaines règles à respecter pour augmenter les chances de garder un client.

2. Attirer l'attention

2.1. Position du problème

Comment un visiteur trouve-t-il un site Web? Cinq possibilités s'offrent à lui:

- Il tapera le nom de domaine de l'entreprise (http://www.entreprise.com) qu'il a probablement aperçu au travers d'un media de marketing.
- L'adresse lui a été communiquée par un ami.
- Il cliquera sur un lien qui pointe sur l'entreprise située sur un autre site Web.
- Il se laissera tenter par une bannière publicitaire que l'entreprise a achetée sur un autre site
- Enfin, dans la plus grande probabilité, il se connectera à un site de recherche. (**[STERNE 99]**)

2.2. Sites de recherche

2.2.1. Introduction

Vu l'importance des sites de recherche, il nous a semblé important de s'attarder quelque peu sur leur manière de fonctionner.

Après une définition de leur outil principal, à savoir le moteur de recherche, nous analyserons les principales techniques utilisées à ce jour. Elles nous permettront de terminer cette partie sur quelques conseils à suivre pour accentuer sensiblement les chances de se retrouver au top des sites de recherche.

2.2.2. Définition

Les moteurs de recherche sont des outils qui ont pour but de fournir une sorte d'indexation d'Internet, réseau assez chaotique. Ils permettent ainsi aux utilisateurs d'obtenir, en un temps record, les pages Web couvrant plus que probablement leur sujet d'intérêt. Ce dernier, introduit au moyen de mots-clefs par le requérant, sera usité pour choisir les sites les plus appropriés parmi les millions de sites Web dont les moteurs de recherche ont déjà pris connaissance.

Il existe deux catégories de moteurs de recherche: dans la première nous retrouvons des bases de données alimentées à l'aide de robots, quant à la deuxième, leur alimentation nécessite une intervention humaine. Dorénavant, nous utiliserons le terme d'*index* pour désigner la première catégorie et de *répertoire* pour désigner la seconde.

2.2.3. Index

Les index opèrent automatiquement. Ils utilisent des *software robots* qui visitent automatiquement les sites, les étudient et nourrissent ensuite à partir du résultat obtenu, leurs propres bases de données.

Ce type d'engin comprend trois éléments principaux:

- **Le spider,** aussi appelé crawler, visite une page Web, la lit et ensuite suit les liens contenus dans la page vers d'autres pages internes ou externes au site. Il revient visiter le site, à périodes déterminées, pour observer les changements.
- **L'index** ou le catalogue peut être assimilé à un immense livre contenant une copie de toutes les pages que le spider trouve. Si les pages Web sont modifiées, ce livre est remis à jour. Un certain délai peut parfois être observé entre la prise en compte des changements et la modification de l'index. Durant cette période, les modifications ne seront donc pas disponibles pour l'utilisateur.
- **Le moteur de recherche** lui-même, est un programme qui parcourt les millions de pages enregistrées dans l'index pour trouver celles qui correspondent à la recherche et les répertorie dans un ordre qu'il croit être le plus pertinent.

Techniques de recherche

Chaque index suit un ensemble de règles qui lui sont propres. On retrouve cependant deux méthodes principales pour guider la recherche. La première se base sur la position et la fréquence des mots-clefs sur une page Web. Quant à la deuxième, elle cherchera à déterminer le concept qui a voulu être exprimé par l'auteur et ainsi, ne s'attache plus simplement à ce qui a été écrit mais bien au sujet général qui est développé.

Fréquence et position des mots-clefs

C'est la technique la plus utilisée sur le Web. A moins que les auteurs de documents Web ne spécifient eux même les mots-clefs[46], c'est aux engins de recherche de les déterminer. Principalement, cela signifie qu'ils font ressortir et indexent les mots qui leur paraissent les plus significatifs.

Certains outils prêteront attention aux mots-clefs du haut de la page ou des premiers paragraphes du texte. Ils assument, en effet, que toute page pertinente pour l'objet de recherche contiendra le(s) mot(s)-clef(s) en son début. Ainsi, par exemple, Lycos[47] s'attaquera aux 20 premières lignes de texte et aux 100 mots qui reviennent le plus souvent. (**[DESIGN]**)

La fréquence sur la totalité d'un document constitue un autre facteur important pour déterminer si une page est appropriée ou non. Un moteur de recherche analysera le nombre de fois qu'un mot-clef apparaît par rapport aux autres mots de la page Web. Ceux repris plus fréquemment constituent souvent un indice quant à la pertinence de la page par rapport à un sujet donné.

A cet effet, Infoseek[48] utilise un système d'indexation sur la totalité de la page en reprenant tous les mots du texte à l'exception des articles et autres mots tels que: "a", "an", "the", "is", "or" et "www". Hotbot[49] travaille également de la même manière. Quant à AltaVista[50], il prétend indexer tous les mots, même les articles "a", "an" et "the". (**[DESIGN]**)

Enfin, il est aussi à signaler que d'autres outils de recherche différencient les majuscules des minuscules. AltaVista en est un exemple. (**[DESIGN]**)

Quoi qu'il en soit, de tels engins de recherche ne peuvent faire la différence entre des mots qui s'épellent de la même manière mais qui ont une signification différente (exemple: un bois dur, un examen dur, un disque dur,....). Il en résulte donc parfois des résultats très surprenants.

Les index ne peuvent également pas retourner des pages Web sur base des mots-clefs qui signifient la même chose mais qui n'ont pas été introduits dans la requête. Avec ce type de technique, une recherche effectuée sur les maladies du cœur ne retournera pas un document utilisant des mots comme "cardiaque" si le mot-clef employé est "maladie cœur".

Recherche basée sur un concept

A l'inverse des engins de recherche basés sur la recherche de mots-clefs, les systèmes conceptuels s'attachent plus à déterminer ce que l'auteur a cherché à

---

[46] Ce qui est possible en utilisant les balises META des dernières versions HTML, comme nous le verrons plus loin.

[47] http://www.lycos.com/

[48] http://www.infoseek.com/

[49] http://www.hotbot.com/

[50] http://www.altavista.com/

exprimer quittant, ainsi, une référence purement écrite. Dans le meilleur des cas, un tel moteur de recherche renverra des documents traitant du sujet de recherche, même si les mots dans le document ne s'accordent pas précisément à ceux introduits dans la requête.

Excite[51] est aujourd'hui le moteur de recherche général basé sur un tel principe. Pour ce faire, il utilise une approche numérique qui détermine le sujet d'un document en calculant la fréquence avec laquelle certains mots importants apparaissent. Quand plusieurs mots semblent proches d'un même concept, par analyse statistique, Excite déduit le sujet général du document.

Par exemple, le mot "cœur", utilisé dans un contexte médical sera souvent associé à des mots tels que "sang", "attaque", "artère", "poumon", "cholestérol", etc. Si le mot "cœur" apparaît dans un document contenant des mots tels que "fleur", "amour", "passion", "Valentin", etc., un contexte totalement différent sera établi et le moteur de recherche renverra la page pour un sujet de recherche beaucoup plus romantique.

Notons cependant que de tels engins fonctionnent mieux en théorie qu'en pratique. Cependant avec l'évolution de l'intelligence artificielle, ils sont promis à un bel avenir.

2.2.4. Les répertoires

Les répertoires, à l'inverse de l'index, nécessitent une intervention humaine pour constituer leurs catalogues. En effet, dans ce cas-ci, c'est dans une base de données composée de descriptions fournies par les concepteurs de sites Web ou par des éditeurs les ayant analysés que s'effectueront les recherches avec les mots-clefs de l'utilisateur.

Les changements effectués sur un site Web n'auront donc aucun effet sur les catalogues. Les astuces qui seront utilisées pour améliorer la position dans les index n'auront donc aucune influence ici.

Un des répertoires les plus connus à l'heure actuelle est *Yahoo!*[52].

2.2.5. Les engins de recherche hybrides

Les engins de recherche hybrides sont des index qui ont également associé à leurs bases de données un répertoire. AltaVista se trouve dans cette catégorie.

---

[51] http://www.excite.com/

[52] http://www.yahoo.com/

2.2.6. Tableau comparatif

Le site Web d'Abondance[53] nous propose un tableau comparant les caractéristiques et les fonctionnalités de quelques uns des index les plus connus.

	AltaVista	HotBot	Infoseek	Excite	Lycos
Date de lancement	Décembre 1995	Mai 1996	Janvier 1994	Octobre 1995	Juin 1995
Taille de l'index (millions de pages)	140	110	30	55	30
Délai de rafraîchissement de l'index	1 à 2 semaines	4 semaines	2 à 3 semaines	6 semaines	2 à 3 semaines
Nom du spider	Scooter	Slurp	SideWinder	Architext Spider	T-Rex
Recherche linguistique	Oui (25)	Oui (7)	Non	Non	Oui (15)
Recherche sur le titre	Oui	Oui	Oui	Non	Oui
Recherche sur le domaine	Oui	Oui	Non	Non	Non
Recherche d'URL	Oui	Non	Oui	Non	Oui
Recherche sur les adresses des liens	Oui	Oui	Oui	Non	Non

2.3. Les bandeaux

2.3.1. Définition

Il s'agit d'une publicité électronique, qui se présente sous forme rectangulaire et d'une dimension standard avoisinant, aujourd'hui, les 468 X 60 pixels. Le bandeau est dit actif puisqu'en cliquant sur ce dernier, l'internaute bascule sur le site de l'annonceur.

Selon les dernières études effectuées, le succès de la publicité au travers des bandeaux ou fameux *banners* est fortement remis en cause. Ainsi, on estime qu'en 1997 seulement 1% des internautes ayant vu le bandeau ont cliqué dessus. Des chiffres plus aggravants encore vont même jusqu'à atteindre 0,5% en septembre 1998 (**[VILLARS 99]**). Force est de constater donc que la publicité en ligne sous forme de bandeaux et, ce de manière non ciblée, ne marche pas.

Pour pallier ce problème, la société DoubleClick[54], située au Etats-Unis, utilise les techniques de personnalisation (voir infra) et se vante ainsi de fournir plusieurs millions de bannières publicitaires par jour, de manière ciblée.

Pour le lecteur intéressé, notons encore que le site Cybermedia[55] répertorie plus de 1000 bandeaux publicitaires belges.

---

[53] http://www.abondance.com/

[54] http://www.doubleclick.com/

Figure 37: Exemple de bandeaux

2.3.2. Rich Media

Il s'agit d'une technique de conception de bandeaux qui, au-delà des classiques assemblages de slogans et d'images, intègre en son sein du son, de l'image et une activité dépassant le simple clic de l'utilisateur.

Cette méthode pourrait donner un second souffle à l'utilisation des bandeaux. En effet, Wired Digital[56], sur un échantillon de 2400 visiteurs du site WebMonkey, a observé une attirance particulière des internautes vis-à-vis de trois annonceurs en ligne: l'assembleur technologique Novell[57], le fabricant de microprocesseurs Intel[58] et le libraire en ligne BarnesAndNoble[59]. Ces trois derniers utilisaient des bandeaux conçus en *Rich Media* et ont vu leur taux de *vu-clic* croître de 340%. (**[VILLARS 99]**)

Une telle technique semble donc intéressante mais, couvrira-t-elle les dépenses qui en sont conséquentes? Seul l'avenir pourra nous donner une réponse.

2.3.3. Les sites portails

Sous le terme de sites portails sont regroupés les sites au trafic relativement important comme, par exemple, les sites de recherche. Ils offrent un espace publicitaire sur leur site sous certaines conditions. Le vendeur pourra ainsi installer une vitrine sur le site portail qui touchera un pourcentage sur les ventes conclues grâce à lui.

---

[55] http://www.cybermedia.arcadis.be/
[56] http://www.wired.com/
[57] http://www.novell.com/
[58] http://www.intel.com/
[59] http://www.barnesandnoble.com/

On estime qu'en 2002, un cyber-marchand sur trois aura recours aux portails pour installer des vitrines et représenteront plus d'un milliard de francs belges de rentrées et cela uniquement dans les domaines de la vente de livres, de CD et de tickets d'avion. (**[INSIDE 98]**)

Il est donc important d'utiliser les programmes d'affiliation, tant en Belgique qu'au niveau européen.

2.3.4. Situation belge

Cinq régies se partagent le marché belge du Webvertising: AdNet[60], Publicast[61], BeWeb[62], IP Netvertising[63] et RMB Online[64]. D'autres sites se chargent aussi de placer des bandeaux sur leur propre espace électronique.

Pour 1998, le montant des investissements publicitaires en ligne pour les cinq régies citées s'élevait à 2,07 millions d'euros. Cependant, une campagne en ligne coûte chère comparée aux autres pays ou aux campagnes traditionnelles puisqu'elle atteint les 7500 euros. Les régies prennent en général une commission qui tourne aux alentours de 30 à 40%. (**[VILLARS 99]**) On peut se réjouir de la venue rapide de la concurrence, qui produira sans aucun doute une baisse de ces tarifs.

2.4. Quelques conseils

Suite à notre analyse, nous énumérons, ci-dessous, quelques conseils à suivre qui maximiseront les chances de retrouver son site en tête des moteurs de recherche.

Nous évoquerons, ensuite, certains conseils qui permettront de promouvoir le site de manière plus rapide.

- **Écrire un titre de page.** Il est souhaitable d'utiliser pour chaque page un titre descriptif de 5 à 8 mots avec un minimum d'articles. Il devra reprendre la meilleure combinaison des mots que les utilisateurs Web pourraient entrer dans leurs requêtes.
- **Utiliser les balises META.** Une balise META est une balise HTML permettant de décrire le contenu d'une page Web. Les mots insérés au milieu des balises META ne sont pas visibles pour le visiteur du site, mais pourront être utilisés par les moteurs de recherche pour identifier, indexer, et classifier le document. Il permet d'introduire des mots qui pourraient être utilisés dans la requête de l'internaute.

Une question intéressante est de savoir si les moteurs de recherche, avec l'utilisation de balise META, ne s'arrêteront pas qu'à ces dernières ou s'ils tiendront compte également de tout le texte de la page Web dans leurs bases de données.

---

[60] http://www.adnet.be/

[61] http://www.publicast.be/

[62] http://www.beweb.be/

[63] http://www.netvertising.be/

[64] http://www.online.rmb.be/

Chez Infoseek, tous les mots de la page seront inclus dans la recherche à l'exception des commentaires repris entre les balises <comment></comment>. (**[RICHMOND]**)

Deux balises META sont particulièrement utiles:

Description:

Il s'agit d'une ou de deux phrases qui reprennent en leur sein sur 200 à 250 caractères, les 20 plus importants mots-clefs. Elles devront être lisibles mais synthétiques avec, comme toujours, un minimum d'articles et autres mots non percutants.

Keyword:

Ici, il s'agit de reprendre les mots-clefs les plus importants incluant jusqu'à 1000 caractères. Puisque certains moteurs de recherche sont sensibles à la capitalisation, il n'est pas inutile d'utiliser à la fois des minuscules et des majuscules. Enfin, il est fortement déconseillé de reproduire plus de trois fois un même mot-clef au risque d'être éjecté de certains engins de recherche.

Exemple:

```
<HTML>
<HEAD>
        <TITLE>
        Best Buy Award Production High-speed Document Image Scanner
        </TITLE>

        <META NAME = "Keywords" CONTENT = " Scanner, High Speed
        document, Production scanner, High Speed Page Scanner document,
        Image, Imaging ">

        <META NAME = "Description" CONTENT = "High Speed Document
        Scanner vendor gets Best Buy Seal from Imaging and Document
        Solutions Magazine for the new VS-1266A high speed document
        image management scanner from VisionShape.">
</HEAD>
```

La plupart des sites de recherche utilisent les balises META pour indexer les pages. Il en est ainsi, par exemple, de Hotbot, Infoseek, Lycos et AltaVista. (**[DESIGN]**) Signalons cependant que tous les engins n'utilisent pas les balises META. Excite en est un exemple:

Our spider doesn't honor META tags. We believe our decision protects our users from unreliable information. (**[RICHMOND]**)

- **Soigner le premier paragraphe**. Certains spiders attachent énormément d'importance au premier paragraphe qui introduit en général le sujet abordé au sein de la page. Ils estiment, en effet, que l'auteur mettra en

avant les choses essentielles qui seront développées par la suite. La difficulté ici est de rendre le paragraphe autant agréable pour l'être humain qu'attractif pour le spider.

- **Se faire connaître des sites de recherche.** 80% des gens vont utiliser un des six sites les plus connus pour effectuer leur recherche: AltaVista, Excite, Infoseek, Lycos et WebCrawler[65] et Yahoo! [66]. Au niveau belge, la référence est AdValvas· Sur chaque site on retrouve un lien permettant d'ajouter son adresse Web. Pour *Yahoo!*, il s'agit de cliquer sur l'icône *How to suggest* a site et de se rendre au listing de sites de même catégorie que celui à inscrire.
- **Acheter des liens dans d'autres sites.** Chercher à obtenir des liens dans d'autres sites Web opportuns peut être intéressant. Il sera parfois même envisageable de payer un certain montant si le retour espéré en est supérieur.
- **Créer une signature e-mail.** L'utilisation d'une signature au bas de tout e-mail (les dimensions standards tournent autour de 6 lignes maximum et de 65 caractères) incluant l'adresse Web du site de l'entreprise et une raison pour visiter le site constitue un excellent moyen de promotion du site.
- **Les articles de presse.** Même s'il est de plus en plus difficile, aujourd'hui, de solliciter l'intérêt d'un journaliste pour la naissance d'un nouveau site, force est de reconnaître qu'un bon article de presse constituera un plus indéniable pour la promotion du site Web.
- **Imprimer son adresse Web partout.** Il est important, pour promouvoir le site, de mentionner son adresse sur tous les documents qu'ils soient publicitaires, commerciaux,... tout comme sur les entêtes de lettre, les enveloppes, les factures, etc. Il s'agit, en effet, d'une riche source de publicité sans frais.

3. Fidéliser le client

3.1. Une nouvelle approche

Pour les personnes surfant sur le World Wide Web, s'arrêter sur un site Web commercial, c'est en quelque sorte une version électronique d'une visite de l'entreprise. Tout comme le bâtiment d'une entreprise, tant l'aspect intérieur (outils de navigation, produits,...) qu'extérieur (design) auront une influence importante sur l'impression du visiteur et donc sur l'image que ce dernier retiendra de la firme.

Trois challenges principaux doivent, nous semble-t-il, être relevés par le Web designer:

- Offrir des outils de navigation de qualité
- Créer une interactivité suffisante
- Solliciter l'avis de ceux qui prennent le temps de visiter le site

---

[65] http://www.webcrawler.com/

[66] Ce site reste un des plus importants puisque son taux de visite mensuelle atteindrait les 80 millions par mois ([VILLARS 99])

Il est aujourd'hui bien trop facile de se perdre dans la multitude de dédales et de liens que les sites offrent. Structurer l'information que l'on met à la disposition du client est une condition requise pour ne pas le désœuvrer rapidement.

Un site Web n'est pas quelque chose que les gens lisent, c'est un endroit où ils interagissent, où ils exercent une activité. Le visiteur n'adopte pas la même attitude passive que celle qu'il adopte lors de la lecture d'un prospectus. Ici, il est amené à penser, effectuer des choix, étudier,... Bien guidé au travers de toutes ces activités, le client pourra avoir rapidement une bonne perspective de la société et de ses produits, engendrant de la sorte une plus grande satisfaction.

Internet, enfin, dans l'optique d'y effectuer un bon marketing, ne peut pas être considéré comme une immense poste, lieu de départ de tous les fascicules *toutes boîtes*. Non, Internet constitue un moyen révolutionnaire pour mieux connaître les clients et ainsi, mieux y adapter les lignes de produits.

3.2. Les règles

Les internautes auront tôt fait de zapper si le site offert ne répond pas à des critères essentiels de qualité concernant, comme nous l'avons déjà mentionné, la navigation, l'interactivité mais aussi le contenu et une présentation attrayante et ergonomique. Nous allons ici exprimer certaines attitudes à adopter pour offrir, au visiteur, toutes les raisons de revenir visiter le site.

3.2.1. Cibler le marché

Avant toute chose et plus particulièrement pour un site à caractère commercial, il faut faire une analyse du marché ciblé et des internautes potentiels qui seront amenés un jour à parcourir le site.

Dans le but de répondre aux attentes des clients, il est nécessaire de les connaître, ensuite de réagir en fonction des possibilités techniques disponibles.

3.2.2. HTML

Puisque le Web devient de plus en plus complexe et que les navigateurs prolifèrent, il est nécessaire aujourd'hui de produire un code HTML valide pour s'assurer d'une part, que l'information atteint la plus large audience possible et d'autre part, que le contenu est préservé.

3.2.3. Contenu et présentation

Le premier et le plus important élément dans la création d'un site Web est de définir un ensemble de principes mesurables pour tous les documents du Web. Ils ne sont pas rigides ou inflexibles. Mais un bon set de principes à suivre offre une base, une stabilité fondamentale pour la qualité du site[67]. Bien entendu, les standards peuvent (en fait, doivent) évoluer au cours du temps mais ils sont là pour offrir une certaine stabilité physique et temporelle au site. Le deuxième élément le plus important est de respecter ces standards.

[67] http://www.pantos.org/atw/35271.html

Une fois la clientèle visée bien cernée, il faut donc se concentrer sur le contenu et sa présentation.

Trois simples questions pourront aider le designer à définir globalement l'attitude à adopter pour la création du site une fois que le marché est ciblé: (**[STERNE 99]**)

- Que désire-t-on que les internautes trouvent?
- Où voulons-nous principalement les diriger?
- Et surtout, que désirons-nous leur faire faire?

Une fois les réponses obtenues, il faudra s'intéresser à la manière de présenter le contenu. On peut en quelque sorte l'assimiler à l'emballage du produit qui doit exercer une influence sur le client. Par exemple, des animations graphiques pour vendre des articles destinés aux jeunes donnera bien plus de résultats que s'il ne s'agissait de produits destinés à une population relativement âgée. Notons cependant que le temps de chargement étant proportionnel à la taille des animations, il sera nécessaire d'éviter de laisser le visiteur devant un écran se chargeant indéfiniment.

Les différents produits que l'entreprise désirent promouvoir sont aussi indicateurs quant au type d'ergonomie à appliquer au site. Par exemple, les sites consacrés à la promotion et la vente de jeux sont souvent beaucoup plus animés que des sites purement professionnels.

3.2.4. Structure et cohésion

L'ensemble des pages d'un site doit offrir au visiteur une structure constante. Comme dans la vie courante, le client aime avoir ses repères dans un magasin.

En visitant simplement deux pages, l'internaute doit être à même de pouvoir se faire une idée de la structure générale dominant le site. Elle doit être aussi intuitive que possible et, fournir ainsi, une adaptation rapide et efficace. L'usage de cadres (*frame*) est à cet effet très efficace. Il faut offrir au client, à chaque page, la possibilité de revenir facilement sur ses pas ou d'atteindre la Home Page.

Un autre aspect à considérer pour ne pas casser la structure d'un site est la qualité des liens. Il est important de s'assurer de l'exactitude des liens afin de ne pas rendre des pages orphelines. (**[PEREZ 99]**)

3.2.5. La Home Page

La Home Page, première fenêtre du site, revêt de par sa nature toute son importance. Vitrine du magasin, elle doit inciter l'internaute à y entrer, à parcourir le site.

Elle devra donc, en un clin d'œil, offrir au visiteur une structure compréhensible où il n'aura aucune peine à poursuivre de lui-même la navigation.

Des études ont démontré que l'être humain peut se souvenir simultanément de sept *objets* avec une variation de plus ou moins deux, selon les individus. Il faudra

donc veiller à limiter le nombre de liens mis à disposition dans les cadres de navigation Il faudra rester simple et suivre le principe du KISS (***K**eep **I**t **S**imple and **S**tupid*).

Il faudra également veiller à la présence sur la Home Page du logo de l'entreprise, et ce quelle que soit la manière utilisée.

3.2.6. Accessibilité

Nous entendons par accessibilité le temps nécessaire au chargement d'une page. Toutes les pages créées doivent offrir un téléchargement aussi rapide que possible. Il faut éviter de fatiguer l'internaute dans une attente infinie avant que n'apparaisse la page complète

3.2.7. Règles ergonomiques

Afin de fidéliser le client au site et de le pousser à revenir visiter les pages Web qui lui sont offertes, force est de reconnaître qu'il faut mettre à sa disposition un site cohérent dans sa structure mais également, et cela va de paire, dans l'ergonomie utilisée pour sa construction.

Un ensemble de règles est donc à respecter au niveau ergonomique.

Nous reprenons ici un ensemble de règles et de standards que nous avons repris sur base d'un corpus générique de règles ergonomiques standards validées sur le Web (**[BADOT 98]**).

- Un site Web doit contenir un titre percutant au sommet de chaque page.
- La longueur d'une page ne doit pas dépasser cinq à six écrans.
- Éviter les textes à la fois colorés et soulignés.
- Il doit exister au moins un lien dans chaque page.
- Essayer de conserver les couleurs de liens proposées par défaut.
- Encadrer d'une bordure colorée ou en trois dimensions les liens graphiques.
- Utiliser les balises appropriées pour spécifier la taille des graphiques.
- Proposer sur toutes les pages un lien vers la Home Page.
- Si la page est longue, utiliser des liens internes à la page pour naviguer à travers celle-ci.
- Le logo de l'entreprise doit être visible en haut de toute page du site.
- Une aide à la navigation doit être disponible dans tous les hauts de pages.
- Cette aide devrait être répétée en bas de page.
- Les bas de page devraient contenir l'adresse e-mail ou de contact de l'auteur de la page.
- Les bas de page devraient contenir la date de la dernière mise à jour de la page.
- En bas de page, utiliser des graphiques de petite taille.
- Si c'est approprié, ajouter une brève table des matières en haut de la page.
- Les graphiques présents dans une page doivent avoir un apport informationnel important.
- Lorsque cela peut s'avérer utile, fournir un lien vers une version texte de la page (*printer friendly*).

- Lors de l'utilisation de cartes sensibles (image contenant diverses zones cliquables), bien délimiter les régions cliquables.
- Essayer d'utiliser un dessin représentatif de la fonction associée à un lien graphique.
- Utiliser une miniature au lieu d'un lien textuel lorsque celui-ci conduit à une image.
- Le nombre d'éléments dans une aide à la navigation ne devrait pas dépasser la fourchette de 5 à 9 éléments.
- S'assurer que les liens soient discernables les uns par rapport aux autres.
- Éviter les animations inutiles

3.2.8. A ne pas oublier

La présence de certaines pages sur un site nous semble obligatoire dans un cadre commercial.

Ainsi, donner la possibilité à l'utilisateur d'accéder aux questions les plus fréquemment posées sur les produits et services de l'entreprise permettra à cette dernière de décharger son service commercial. L'utilisateur trouvera, en effet, avec une grande probabilité, les réponses aux questions qu'il pourrait avoir. De plus, une telle page mettra en exergue la connaissance, le savoir et le professionnalisme de l'entreprise.

Une page reprenant les questions relatives aux frais de livraison et d'emballage est également très importante dans le cas de sites proposant des produits tangibles.

Une page, voire mieux un bas de page, faisant référence à tous les renseignements utiles tels que adresses, numéros de téléphone, coordonnées des responsables,... est indispensable.

Enfin, pour les entreprises qui en ont la possibilité, une page qui permet de télécharger des versions d'essais de produits développés par la firme elle-même pourra offrir une bonne raison de visite de l'internaute certes, mais surtout mettra en évidence, de la meilleure manière qu'il soit, le savoir faire de la société.

3.3. Personnalisation

3.3.1. Position du problème

Internet est rapidement en train d'évoluer d'une simple base de données gérée dynamiquement vers un véritable moyen de transaction.

Même si le marché potentiel des clients devient de plus en plus massif, on s'oriente de plus en plus vers une démassification de l'offre. Tout ce que connaît une entreprise sur ses produits, son marché, ses services peut être appliqué aujourd'hui à une stratégie de business en ligne avec une nouvelle précision individualisée et ce, grâce à la personnalisation.

3.3.2. Définition

Par personnalisation, on entend l'ensemble des techniques utilisées pour fournir une offre ciblée au client; elle découle d'une analyse de ce dernier: ses habitudes, ses goûts, ses besoins, ses revenus,... Elle permet ainsi, par exemple, de reconnaître le client et lui diffuser des messages cohérents en égard à ses goûts et à son profil.

3.3.3. Personnalisation et vie privée

Pour parvenir à une personnalisation du site spécifique à l'internaute, des sites polymorphiques sont utilisés. Ils adaptent leur contenu, en temps réel, au profil détecté de l'utilisateur. Pour obtenir de telles prouesses, les cookies sont employés.

Un cookie est un ensemble d'informations persistantes qui est stocké par le navigateur dans un fichier particulier sur le disque dur de l'ordinateur du client et ce, sans que ce dernier n'en soit prévenu.

Chaque cookie contient un nom, une valeur, une date d'expiration (souvent très lointaine) et le nom du domaine auquel appartient l'ordinateur envoyant le cookie. Seul l'ensemble des ordinateurs, du même domaine, pourra par la suite accéder à ce cookie.

Par la suite donc, si la date d'expiration n'est pas dépassée et si le serveur appartient, comme nous l'avons déjà signalé plus haut, au même domaine (au niveau Domain Name Server) que le serveur ayant transmis la valeur initiale du cookie, le navigateur transmettra systématiquement le cookie lors de chaque connexion. Ce cookie va permettre au serveur d'identifier le client. En effet, le client aura pu fournir au serveur, lors de sa première visite, ses coordonnées. Le serveur aura alors stocké dans une base de données ces informations après les avoir associées à un nom et à une valeur de cookie. Le serveur pourra alors, par exemple, envoyer au client non pas une page standard mais bien une page personnalisée qui le salue par son nom et son prénom.

Cette fonctionnalité est abondamment utilisée par les sociétés de marketing direct afin de cibler les utilisateurs et leur offrir une page Web qui corresponde au mieux à leurs habitudes, goûts et centres d'intérêts.

Ce mécanisme technique permet au réseau de transformer l'ordinateur de l'internaute en une précieuse commère au service du réseau et de parvenir ainsi à cette inversion du paradigme où l'ordinateur client devient subrepticement le serveur des ordinateurs distants du réseau. (**[DINANT]**)

L'utilisation de cookies pose donc évidemment un important problème de respect de la vie privée du consommateur.

3.3.4. Quelques outils

Aujourd'hui, comme nous l'avons signalé précédemment, des logiciels traquent l'acheteur en ligne et analysent son comportement pour ensuite modifier l'offre en ligne.

Ils peuvent être regroupés en différentes familles de solution.

Il existe tout d'abord des outils de gestion des profils/utilisateurs tels que Engage Technology[68] ou Open Sesame[69]. Ce sont actuellement les outils les plus utilisés. Pour la grande majorité, ils reprennent des informations sur des formulaires que les acheteurs potentiels sont invités à compléter. Malheureusement ces derniers, trouvant cette pratique indiscrète et temporellement coûteuse, auront tendance à la négliger, voire même à la refuser. Leur efficacité peut donc fortement être remise en question.

Pour pallier ce problème, apparaissent de plus en plus, aujourd'hui, des plates-formes évoluées combinant des outils d'analyse du comportement de l'internaute et de personnalisation du contenu. Ces plates-formes surveillent le comportement de l'utilisateur, en font une analyse et sauvent leurs conclusions dans une base de données qui s'enrichit en permanence. L'outil dispose de plusieurs modèles qu'il confronte à l'utilisateur. Il peut ainsi personnaliser l'offre faite à un visiteur en proposant le modèle qui semblait susciter le plus d'intérêt (Netperceptions[70]).

D'autres outils surveilleront encore les accès au serveur. Ils observent les pages qui sont consultées et sont capables d'exploiter en ligne et hors ligne des statistiques de comportement et de fréquentation. Aria d'Andromedia[71], solution d'analyse d'activité, fait partie de tels outils.

D'autres solutions proposent quant à elles des système permettant un contenu personnalisable combinant des icônes, des photos, des blocs de texte, etc... (Story server de Vignette[72]).

Parmi les technologies les plus sophistiquées, certaines solutions émergent autour de réseaux neuronaux. Leur objectif est de percevoir, au travers de quelques clics du visiteur, son profil et d'y adapter la présentation de l'offre. De tels outils utilisent encore, à l'heure actuelle, des volumes de données gigantesques et restent qui plus est, très onéreux.(Portail in a Box d'Autonomy[73])

3.3.5. Conclusion

La personnalisation n'est plus, nous semble-t-il, une option mise à la disposition des entreprises. Il s'agit d'une pratique incontournable qu'il faut absolument inclure dans une stratégie Internet à long terme. Le commerce électronique trouve ici encore, toutes ses raisons pour s'imposer rapidement dans les habitudes de l'acheteur potentiel. Ne pas saisir une telle opportunité aura sans aucun doute, des conséquences néfastes sur le chiffre d'affaires des sociétés actuelles peu entreprenantes.

---

[68] http://www.engage.com/
[69] http://www.opensesame.net/
[70] http://www.netperceptions.com/
[71] http://www.andromedia.com/
[72] http://www.vignette.com/
[73] http://www.autonomy.com/

Nous nuancerons, cependant, notre enthousiasme en rappelant à nouveau les problèmes que de telles techniques soulèvent au niveau de la protection de la vie privée du consommateur.

4. Conclusion

La promotion d'un site Web relève d'une importance capitale mais elle n'est pas forcément simple. Comme nous l'avons vu, des techniques existent pour espérer retrouver un site indexé au sommet du résultat d'une recherche effectuée sur un site approprié. Les bandeaux, principalement ceux qui utilisent la technique du Rich Média offrent, eux aussi, un bon moyen de promotion et, surtout, quand ils se retrouvent sur des sites portails. D'autres petites astuces sont tout autant utiles pour organiser la promotion d'un site.

Une fois que l'internaute visite un site, il faut parvenir à le fidéliser. Nous avons montré un ensemble de règles autant techniques qu'ergonomiques pour y parvenir. Des outils, de plus en plus performants, naissent de nos jours pour fidéliser le client et lui offrir une personnalisation. Ils n'offrent cependant aucune solution quant au problème de la protection de la vie privée du consommateur et ne font d'ailleurs qu'accentuer les craintes des internautes.

Chapitre 6: Étude de cas

1. Introduction

Ce chapitre a pour intention de montrer au lecteur le travail pratique que nous avons effectué dans le cadre de notre mémoire.

Après une explication des motivations qui nous ont amenés à opter pour un tel travail et une brève présentation de l'entreprise VisionShape, nous aborderons les étapes que nous avons suivies tout au long de la construction du site. Nous chercherons également à mettre en évidence les améliorations que nous avons apportées au site de départ. Nous montrerons, au fil des différentes parties, pourquoi le nouveau site peut être considéré comme un site de qualité.

Enfin, dans la dernière partie de ce chapitre, nous décrirons et nous analyserons les outils de commerce électronique que nous avons utilisés.

A titre d'information, le temps que nous avons consacré à l'élaboration du site recouvre environ 300 heures de travail. Notons encore que notre tâche s'est limitée à la partie américaine du site qui représente cependant plus de 90% des pages constituant le site de VisionShape. Cette partie représente plus de 200 pages au format HTML.

Le site Web de VisionShape se trouve à l'adresse suivante: http://www.VisionShape.com/. La version du site telle que nous l'avons remise fin mai à VisionShape est quant à elle disponible sur le serveur Web de l'Institut d'Informatique à l'adresse suivante: http://www.info.fundp.ac.be/~bcoppens/VisionShape/. Notons cependant que les parties concernant le commerce électronique ne fonctionnent pas. En effet les outils nécessaires à ces parties se trouvent sur le serveur de l'hébergeur de VisionShape. Nous signalons également au lecteur que les liens des bas de page aidant à la navigation ne sont pas corrects. Ceci est dû au fait que l'architecture des répertoires de l'Institut d'Informatique est différente de celle du serveur de VisionShape. Mais que le lecteur se rassure: tous les liens présents sur le serveur de VisionShape sont quant à eux corrects.

Nos fichiers sont bien sûr disponibles sur le serveur de VisionShape. Il suffira au lecteur de se connecter à l'adresse suivante: http://www.VisionShape.com/new_Web/ pour tester les outils de commerce électronique et l'ensemble des liens d'aide à la navigation.

VisionShape met à jour actuellement son site Web en y intégrant nos fichiers. Cette intégration ne se fait pas toujours dans les règles de l'art. Ceci implique que la version de nos fichiers sur le serveur de l'Institut d'Informatique et celle sur le serveur de VisionShape ne correspondent pas toujours.

2. Motivation

Dans le cadre de la fin de nos études, nous avons été amenés à effectuer un travail qui constitue le point final de cinq années d'études.

Nous avons été principalement motivés par l'ambition de mettre notre connaissance concrètement au service d'une entreprise. En quelque sorte, nous cherchions à apporter une valeur réelle pour cette dernière dans le monde actuel.

Comme nous le montrerons par la suite, le site, dans sa structure, était chaotique, mais qui plus est, n'offrait que peu d'éléments attractifs pour fidéliser le client. Nous avons investi nos connaissances pour produire un site qui sera plus apte que le précédent à rencontrer les objectifs propres à un site commercial.

3. VisionShape

3.1. L'entreprise

VisionShape est une entreprise américaine née en 1978 et située à Los Angles. Depuis peu de temps, elle est également présente en Belgique avec le bureau qu'elle a ouvert à Louvain-la-Neuve.

VisionShape est une société essentiellement tournée vers la fabrication et le vente de scanners destinés au monde des entreprises. C'est en 1978 qu'elle développa son premier scanner, le CopiScan. En 1988, VisionShape chercha à offrir, également, un service de conseils et de consultance dans le domaine des scanners et du traitement de l'image. En 1992, VisionShape mis sur le marché son premier scanner à très grande vitesse destiné à des opérations de bureau. Aujourd'hui encore, VisionShape innove en introduisant le *Millennium Scanner* avec ses procédés avancés de traitement de l'image.

A côté des scanners, VisionShape commercialise également des logiciels de reconnaissance de caractères, des bibliothèques de fonctions graphiques, des éditeurs d'images, etc.

Les scanners développés par VisionShape ont déjà reçu de nombreux prix:

- **Best of AIIM 97** (décerné par *Imaging Magazine*)
- **Product of the Year 1997** (décerné par *Knowledge Management World*)
- **Best Buy** (décerné par *Imaging & Document Solutions*)
- **Four Stars (Excellent)** (décerné en 1998 par *Small Business Computing & Communications* dans la catégorie *High-speed document scanners*)

VisionShape s'est également vu décerner le **Best of AIIM 98** pour son *Tiffsurfer Internet Image Viewer*, plug-in permettant l'édition d'images au format Tiff dans un navigateur Internet. Le dernier né de l'entreprise, le *Millennium Scanner*, a quant à lui obtenu le **Best of AIIM 99** à Atlanta.

3.2. VisionShape et Internet

Depuis maintenant quelques années, VisionShape est présent sur Internet. Selon le directeur général de l'entreprise, Daniel Borrey, 75% de tous les nouveaux contacts et 50% des ventes ont pour origine le site Web de l'entreprise. La portion de commerce électronique, quant à elle, reste encore relativement faible.

Après avoir hébergé quelques pages dans un *Technical Mall* (TechExpo[74]), VisionShape a vite saisi l'importance de disposer de son propre site Web. L'entreprise pouvait ainsi mieux se faire connaître, se faire valoir et mettre une multitude d'informations à la disposition des internautes. Elle met d'ailleurs à disposition du visiteur des logiciels en libre essai pour permettre à l'acheteur potentiel une évaluation avant un achat définitif. Dans sa première année, le téléchargement engendra plus de 25000 demandes.

Enfin, VisionShape se tourna vers le commerce électronique pour avoir un retour financier. Après un essai de quelques mois, VisionShape s'est rendu compte que la vente en ligne de scanners ne marchait pas. Ceci s'explique sans doute par le fait que l'achat d'un scanner industriel demande un effort financier important et le client préfère encore aujourd'hui passer par le commercial de l'entreprise pour en faire l'acquisition.

La vente en ligne se limite depuis lors à celle du plug-in *Tiffsurfer Internet Image Viewer* ainsi qu'à des contrats de maintenance pour les scanners. La vente des logiciels de reconnaissance de caractères et autres bibliothèques graphiques devrait suivre sous peu.

4. Analyse de l'existant

4.1. Introduction

Nous allons dans un premier temps faire une description du site tel qu'il avait été créé par VisionShape. Ce point nous permettra de mettre en évidence les problèmes dont, à notre avis, souffrait ce site.

Signalons encore que VisionShape héberge ses pages chez InfoDial, société californienne. C'est également cette société qui lui fournit les fonctionnalités de commerce électronique.

4.2. Home Page

Le premier contact avec un site Web se faisant par la Home Page, c'est tout naturellement par cette page que nous avons commencé notre analyse du site de VisionShape.

[74] http://www.techexpo.com/

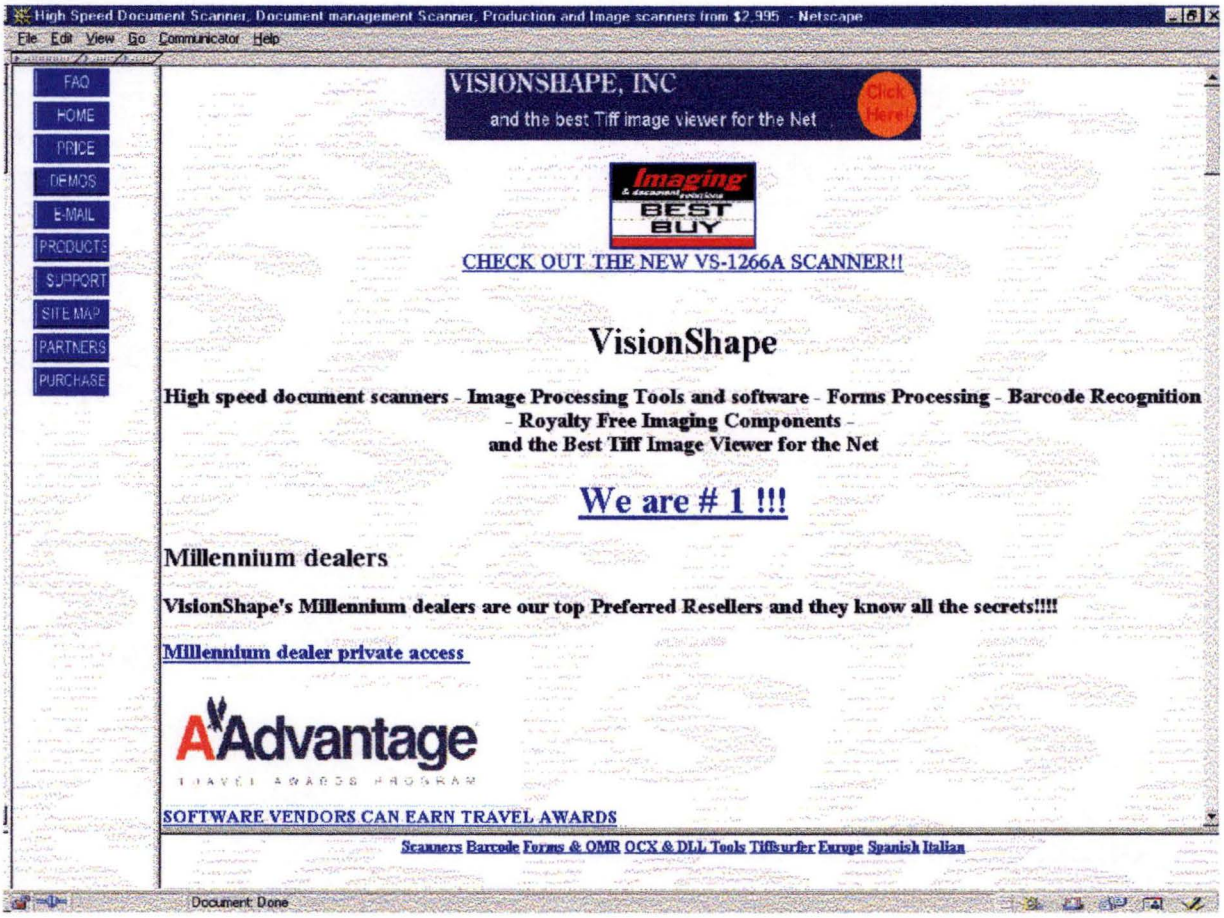


Figure 38: La Home Page de VisionShape

La Home Page du site de VisionShape est constituée de trois cadres: un cadre principal et deux cadres de navigation.

Cadre principal

La première chose qui frappe le visiteur que nous sommes est la longueur du cadre principale: une petite dizaine d'écrans. D'autres lacunes sont encore à signaler:

- Le logo de l'entreprise n'est pas visible de manière percutante. Il a été utilisé comme fond de page. Vu la couleur du logo et celle du fond de page, ce dernier ressort très peu.
- Une bannière située tout en haut du cadre invite le visiteur à cliquer dessus. Cependant le lien n'a pas été implémenté.
- La mise en page de la liste des produits située sous le nom de l'entreprise n'est pas cohérente.
- Le texte de la partie supérieure du cadre est centré. Pourquoi ne pas avoir respecté cette mise en page par la suite?

Si nous descendons plus bas dans le cadre principal, nous pouvons remarquer une inconsistance au niveau du choix des couleurs, souvent trop vives. La mise en page laisse aussi à désirer: le titre principal (*Table of Contents*) devrait être

centré et écrit dans un taille supérieure aux sous-titres (*Top Press Reviews, Technical Corner, ...*).

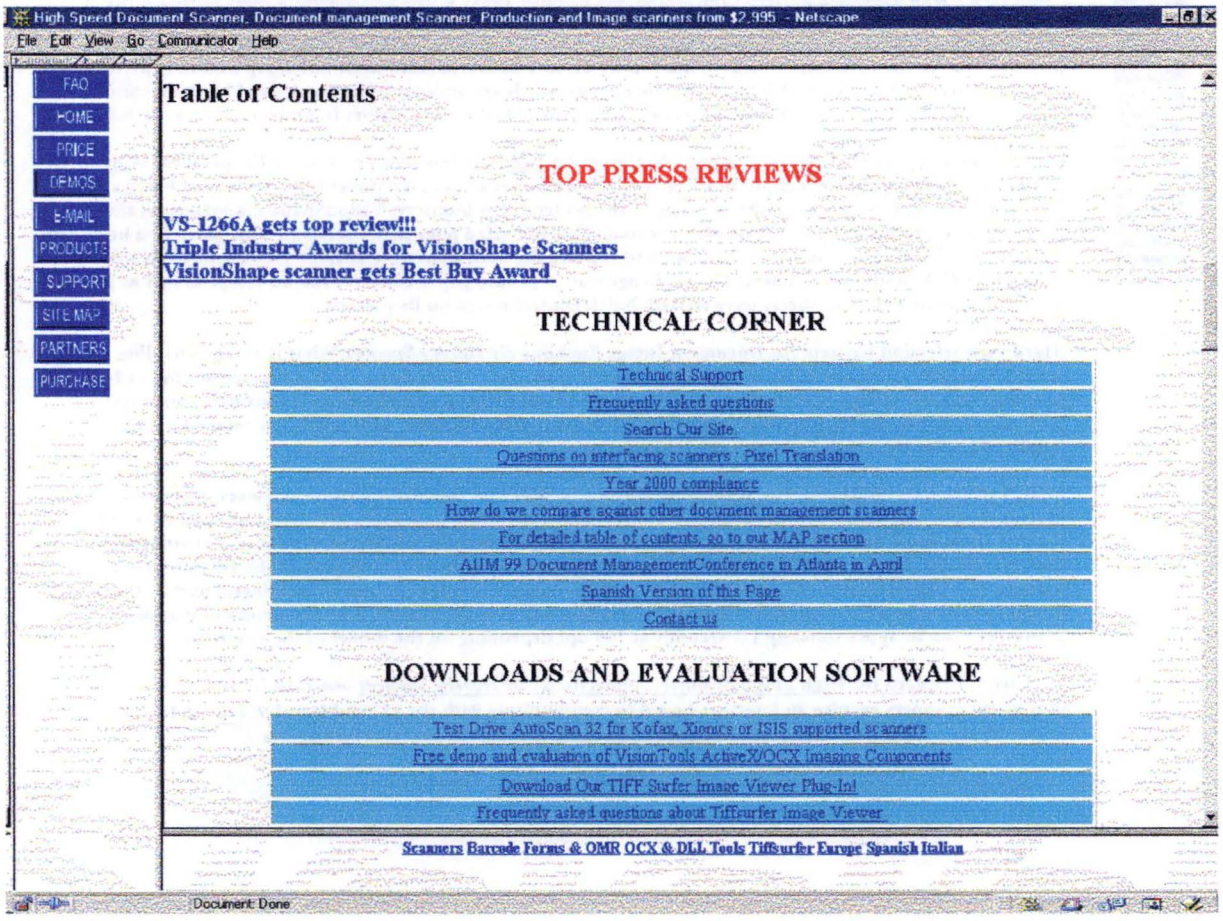


Figure 39: Home Page - milieu du cadre principal

Si nous descendons dans le bas du cadre principal, nous découvrons une présentation rapide des différents produits commercialisés par VisionShape. Le choix d'un tel emplacement ne nous paraît pas judicieux. En effet, ces présentations n'étant pas annoncées plus haut dans la page, les visiteurs risquent de ne pas descendre si bas. S'ils souhaitent avoir de l'information sur un produit, ils seront certainement plus tentés de se rendre dans la section consacrée aux produits. Remarquons aussi que la petite taille du caractère et le compactage de l'information ne rendent pas la lecture agréable.

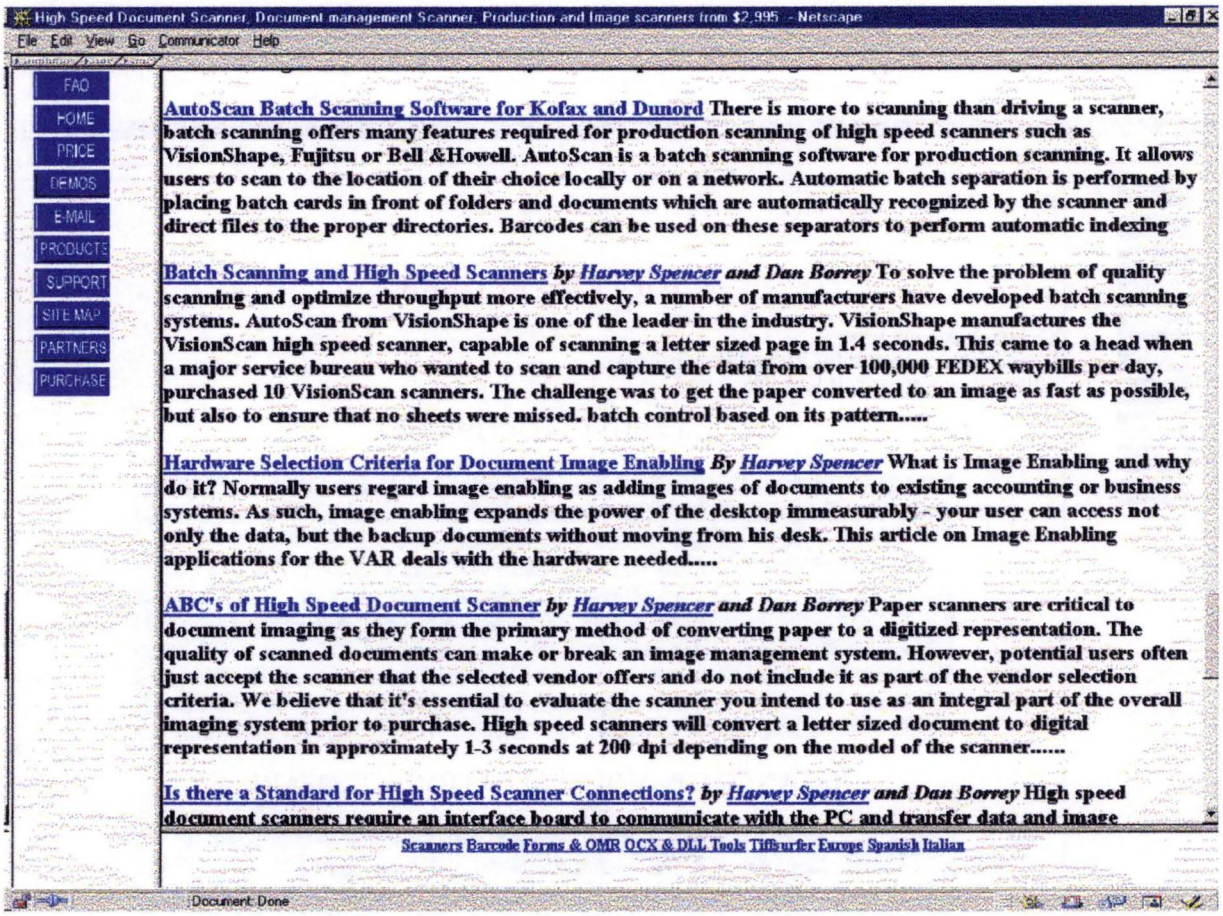


Figure 40: Home Page - bas du cadre principal

Cadres de navigation

La Home Page est constituée de deux cadres de navigation.

Le premier, situé à gauche du cadre principal, est constitué de boutons offrant des liens vers les différentes parties du site. On peut s'étonner de l'ordre dans lequel ces divers boutons ont été positionnés. En toute logique, le bouton 'Home' permettant au visiteur de retomber au cours de sa visite sur la Home Page aurait dû être placé en première position, voire en dernière position. Le bouton 'Price' aurait pu quant à lui se trouver sous le bouton 'Products'. Le bouton 'FAQ' (***F**requently **A**sked **Q**uestions*) aurait dû se trouver sous le bouton 'Support' ou ne pas exister. En effet, les FAQ peuvent être considérées comme un type de support. Le bouton 'Purchase' risque quant à lui de surprendre le visiteur. En effet, le cadre principal présente les scanners comme étant l'activité principale de VisionShape. Le visiteur pourrait donc croire que ce bouton lui permet d'acheter des scanners, ce qui n'est pas le cas!

On peut également s'interroger sur la taille et la disposition des boutons vu l'importance de ce cadre de navigation.

Enfin, le cadre de navigation inférieur offre des liens vers des sous catégories de produits et vers les pages européennes, espagnoles et italiennes du site. Il aurait sans doute été plus opportun d'offrir au visiteur les liens vers les pages étrangères dans l'autre cadre de navigation qui offrait toute la place nécessaire à ce choix.

4.3. Structure du site

Il est difficile lors d'une première visite du site d'en saisir la structure. Après avoir suivi quelques liens, le visiteur se sentira vite perdu et il se réjouira de trouver un bouton 'Home' lui permettant de revenir à son point de départ. Après plusieurs visite du site, l'internaute commence tout doucement à s'y retrouver, non pas que la structure du site se découvre mais plutôt parce qu'il commence à connaître le site et donc l'enchaînement des pages.

La structure du site est succinte: aucune séparation claire n'existe entre les différentes partie du site (produits, support, téléchargement,...). Des produits sont parfois présents dans deux sous catégories différentes de produits.

Ce manque de structure engendre une difficulté à maintenir ce site à jour. Cela se traduit, entre autres, par la présence de nombreux liens orphelins. De plus, en parcourant les répertoires où sont stockés les fichiers HTML de VisionShape, nous avons trouvé de nombreuses pages inaccessibles.

On remarquera le manque de structure à l'intérieur même des pages. La figure ci-dessous est extraite de la page présentant l'ensemble des scanners. Les liens vers les descriptifs de scanners, vers les software liés à ces derniers et vers d'autres pages telles que celles des comparaisons ou des articles de presse ne sont pas séparés.

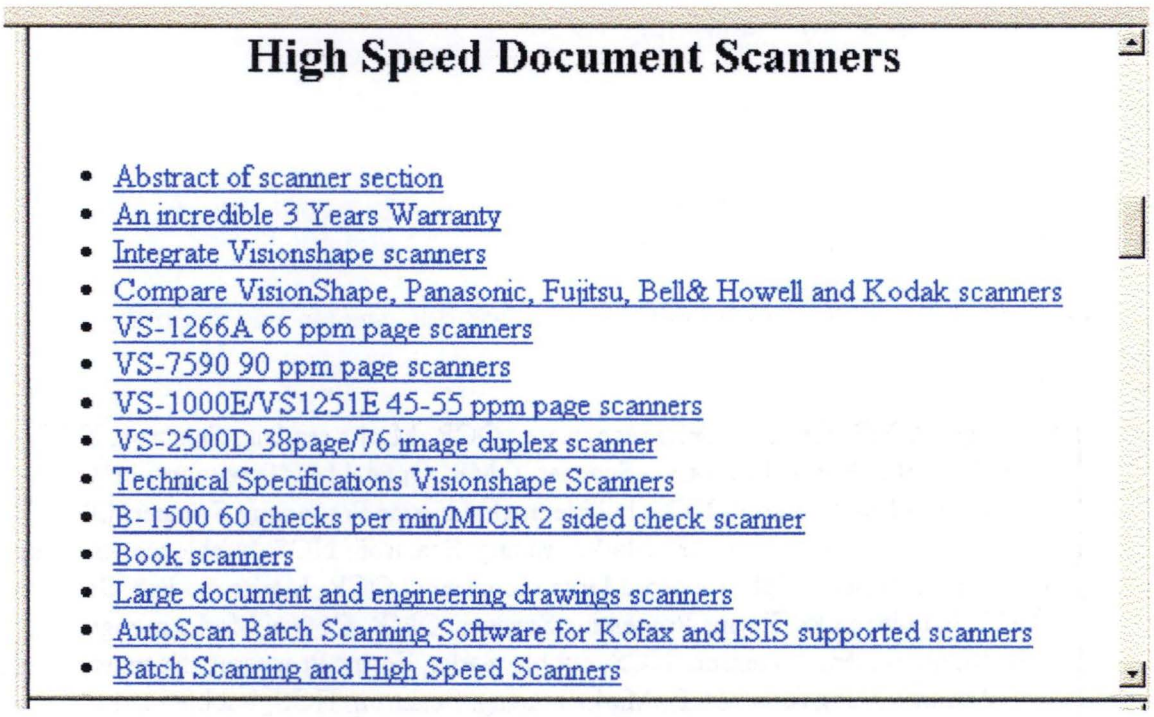


Figure 41: Extrait de la page générale consacrée aux scanners

4.4. Ergonomie

Les règles ergonomiques ne sont pas respectées. L'usage de couleurs, souvent très vives, est tout à fait aléatoire et a une forte tendance à fatiguer rapidement l'œil humain. L'exemple ci-dessous parle de lui-même. Il s'agit de la page

permettant de choisir sa destination parmi les différentes catégories de produits. Le lecteur remarquera aussi l'utilisation de deux orthographes différentes pour écrire le mot *toolkit*.

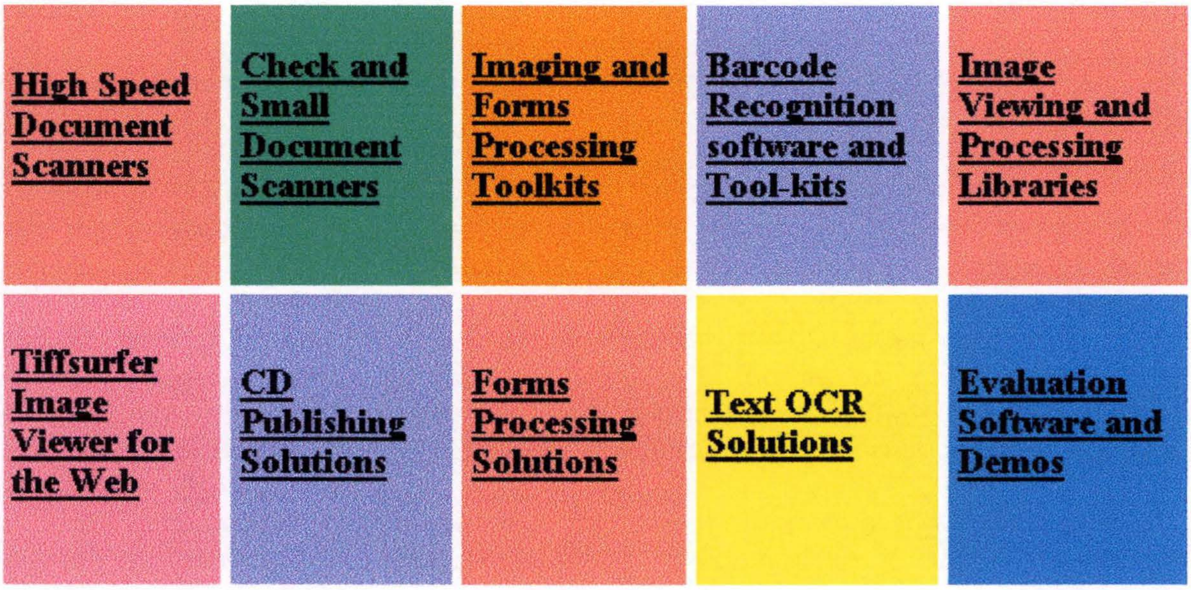


Figure 42: Cadre principal de la page relative aux produits

Lors de la création de ce site, aucun standard n'a été défini quant au choix de la police de caractère, de sa taille et de sa couleur. Les différentes figures illustrant les précédentes pages le démontrent.

Quant au logo de l'entreprise, il est parfois présent en haut de page, parfois en image de fond ou tout simplement absent.

La longueur des pages dépasse la plupart du temps les 5 à 6 écrans conseillés par les règles ergonomiques.

On rencontre également de temps en temps des bas de page dont on ne saisit pas l'utilité.

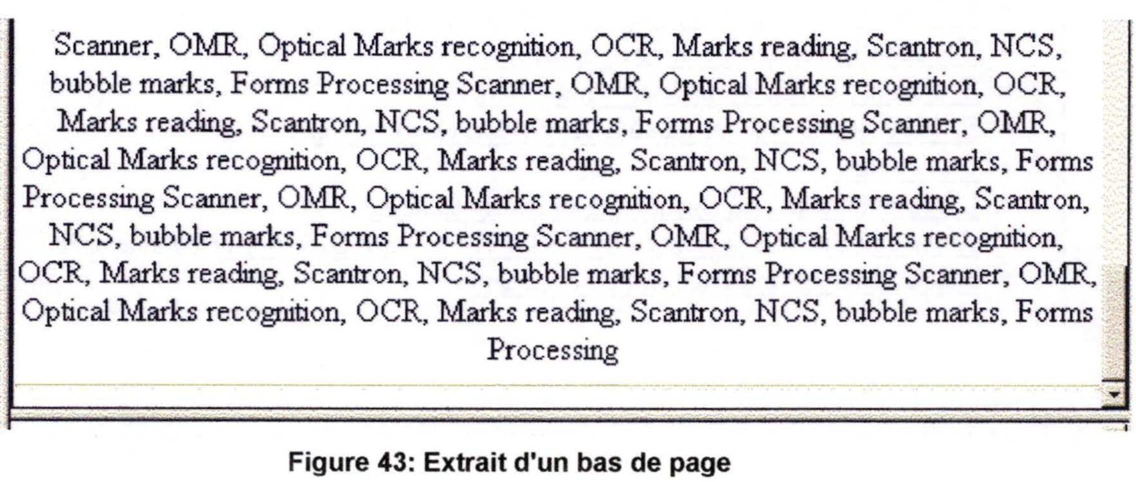

Scanner, OMR, Optical Marks recognition, OCR, Marks reading, Scantron, NCS, bubble marks, Forms Processing Scanner, OMR, Optical Marks recognition, OCR, Marks reading, Scantron, NCS, bubble marks, Forms Processing Scanner, OMR, Optical Marks recognition, OCR, Marks reading, Scantron, NCS, bubble marks, Forms Processing Scanner, OMR, Optical Marks recognition, OCR, Marks reading, Scantron, NCS, bubble marks, Forms Processing Scanner, OMR, Optical Marks recognition, OCR, Marks reading, Scantron, NCS, bubble marks, Forms Processing Scanner, OMR, Optical Marks recognition, OCR, Marks reading, Scantron, NCS, bubble marks, Forms Processing

Figure 43: Extrait d'un bas de page

Quant aux autres règles ergonomiques, elles sont pour la plupart d'entre elles plutôt bien respectées:

- Il existe au moins un lien par page.
- La couleur de lien par défaut est conservée.
- Présence à tout moment d'un lien vers la Home Page.
- Toutes les pages contiennent une adresse e-mail de contact, souvent située en bas de page.
- Toutes les pages contiennent un titre approprié.

4.5. Accessibilité

En ce qui concerne l'accessibilité, aucune remarque particulière n'est à faire. En effet, le temps de téléchargement des diverses pages est relativement court.

Notons encore qu'aucun plug-in n'est nécessaire pour visiter le site. Il ne contient pas non plus de scriptes, applets ou ActiveX, ce qui lui permet d'être compatible avec un maximum de navigateurs.

4.6. Code HTML

Le Webmaster n'ayant pas utilisé d'éditeur ou de correcteur de syntaxe pour la mise sur pied du site, ce dernier offre un code HTML non compatible avec les normes HTML 3.2 et suivantes.

Il contient en son sein des erreurs provoquant, par exemple, le genre d'imperfections visibles sur la figure ci-dessous.

Figure 44: Exemple d'imperfection causées par une mauvaise implémentation HTML

De plus, il nous était impossible d'ouvrir certaines pages avec l'éditeur que nous avons choisi par le suite pour réaliser notre travail. Il ne supportait pas, en effet, les fautes de codage commises.

5. Démarche et choix

5.1. Introduction

La reconstruction totale du site de VisionShape s'est imposée vu l'importance des problèmes rencontrés lors de notre première analyse.

Il est à remarquer que notre travail a porté sur la présentation et la structuration du site et non sur son contenu.

Notre travail a tout d'abord consisté à déterminer les clients potentiels et les produits vendus par VisionShape. Cette analyse nous a permis d'ébaucher la structure générale du site dans un premier temps et une structure détaillée dans un second temps.

Nous avons alors déterminé l'ensemble des standards typographiques et de mise en page que nous allions utiliser dans l'élaboration du site.

5.2. Détermination des clients potentiels et des produits de vente

Avant de commencer la construction du site Web à proprement parler, nous avons donc cherché à connaître les produits que l'entreprise commercialisait. Nous avons aussi tenté de définir le profil type du client potentiel.

- **Produits:** comme nous l'avons indiqué plus haut, après un essai malheureux, VisionShape ne compte plus vendre ses scanners par commerce électronique. Les produits vendus actuellement sur Internet se consistent en des produits intangibles: logiciels et contrats de maintenance.
- **Clients:** en ce qui concerne les clients, ils regroupent principalement des entreprises et non des particuliers. Les internautes potentiels se composent donc principalement de professionnels ayant des besoins précis dans le monde de l'édition ou du graphisme. Il ne faut donc plus les convaincre qu'ils ont un besoin, mais bien de satisfaire ce dernier chez VisionShape.

5.3. Contenu et présentation

Pour débuter, nous avons tenté de répondre aux trois questions suivantes:

- **Que désire-t-on que les internautes trouvent?** Il s'agit essentiellement d'informations concernant les produits et des réponses à leurs questions. L'internaute doit aussi avoir à sa disposition la possibilité de télécharger des versions d'essai des logiciels développés par l'entreprise.

- **Où voulons-nous principalement les diriger?** Notre intention est de diriger rapidement les internautes là où ils trouveront l'information recherchée et, bien entendu, vers la page d'achats en ligne.
- **Que désirons-nous leur faire faire?** Leur faire effectuer une visite plus intense du site (qui ne se restreint pas aux réponses aux questions éventuelles) et en ressortir avec une bonne appréhension de VisionShape.

Le site sur lequel nous avons travaillé est donc plus une source d'information qu'une source d'amusement. Pour procurer un sentiment de proximité, pour que le consommateur se sente un peu chez lui, nous avons donc opté pour un site assez simple offrant au client la possibilité d'obtenir les renseignements utiles en un temps restreint.

5.4. Structure générale

C'est sur base des réponses aux questions posées ci-dessus et après avoir défini la liste des sections les plus importantes au travers de l'analyse du site précédent, que nous avons cherché schématiquement à déterminer les relations entre les sujets pour exprimer le flux du site. Cette étape était nécessaire pour offrir une certaine cohérence au site, éviter la redondance et surtout, par la suite, les pages orphelines.

Au travers du site, ressortaient trois parties importantes qui seront sans doute la source de la présence du visiteur sur le site:

- L'intention d'acheter un produit de l'entreprise
- Le besoin d'un support
- La possibilité de télécharger des logiciels

Pour offrir au client un maximum de satisfaction, il nous a semblé utile de mettre à sa disposition une section *Press* que nous décrirons plus loin. Enfin, pour faciliter la navigation de l'internaute, nous avons mis à sa disposition une section *Site Map* reprenant la structure du site.

Nous avons donc opté pour la présence en permanence d'un cadre supérieur situé au-dessus du cadre principal et offrant un lien direct vers chacune de ces cinq parties. En son sein, se retrouvent intégrés le logo de la société et une possibilité d'accéder à une langue différente.

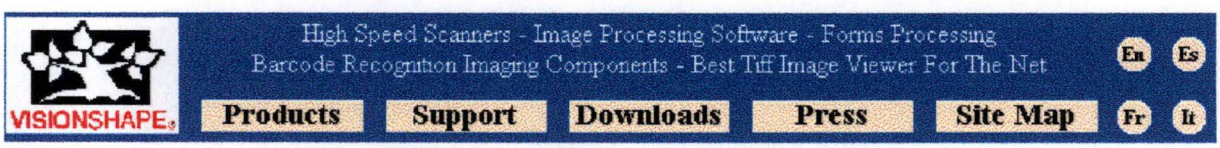


Figure 45: Cadre supérieur permanent

Enfin, dans le but d'améliorer la navigation nous avons intégré à chaque bas de page un bandeau reprenant des liens vers les différentes sections du site ainsi que les informations de copyright. On peut remarquer la présence à côté des liens menant vers les cinq sections présentées ci-dessus, des liens menant à des services auxiliaires que nous décrirons plus tard.

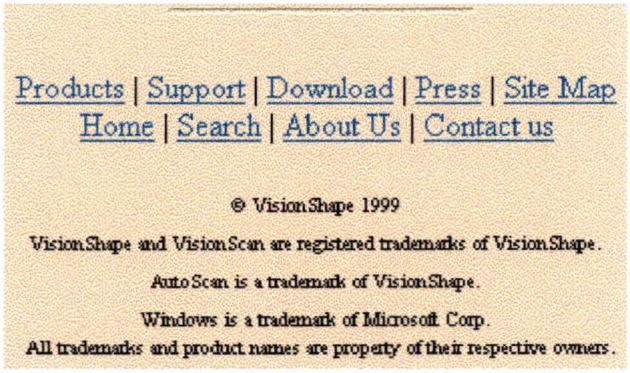


Figure 46: Copie d'écran du bas des pages

5.4.1. Home Page

Pour éclairer le lecteur, nous reprenons ci-dessous la Home Page qui met en évidence les propos que nous avons énoncés plus haut. Nous avons créé cette Home Page afin qu'elle offre en un clin d'œil une structure compréhensible où l'internaute aperçoit sans peine les principales parties du site. Le visiteur n'aura donc aucune peine à poursuivre de lui-même la navigation. S'y retrouve également le logo de l'entreprise ainsi que des liens vers les parties du site orientées commerce électronique que nous décrirons en détail dans la dernière partie de ce chapitre.

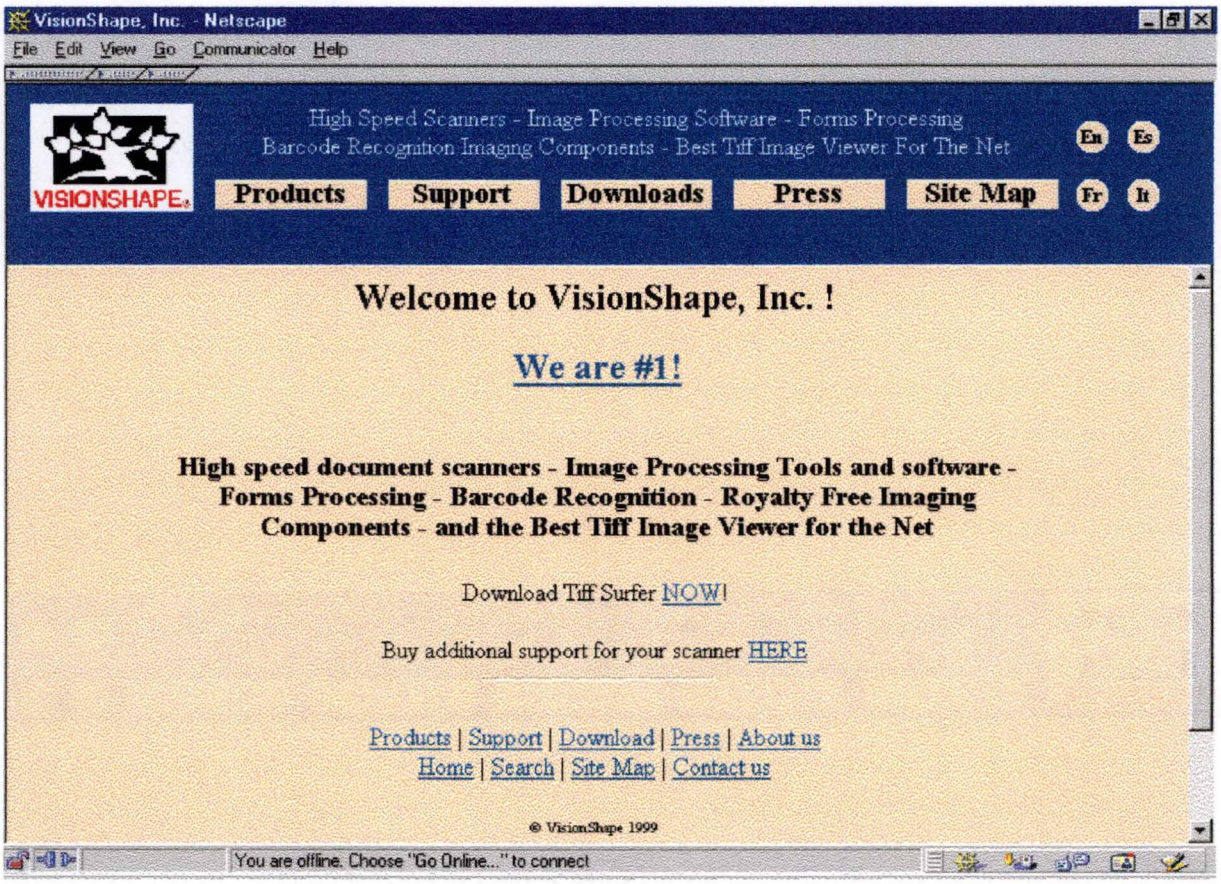


Figure 47: Home Page du site

5.4.2. Organigramme

Afin de faciliter la compréhension du lecteur nous avons inséré ici l'organigramme global du site qui sera entièrement détaillé dans les paragraphes qui suivent.

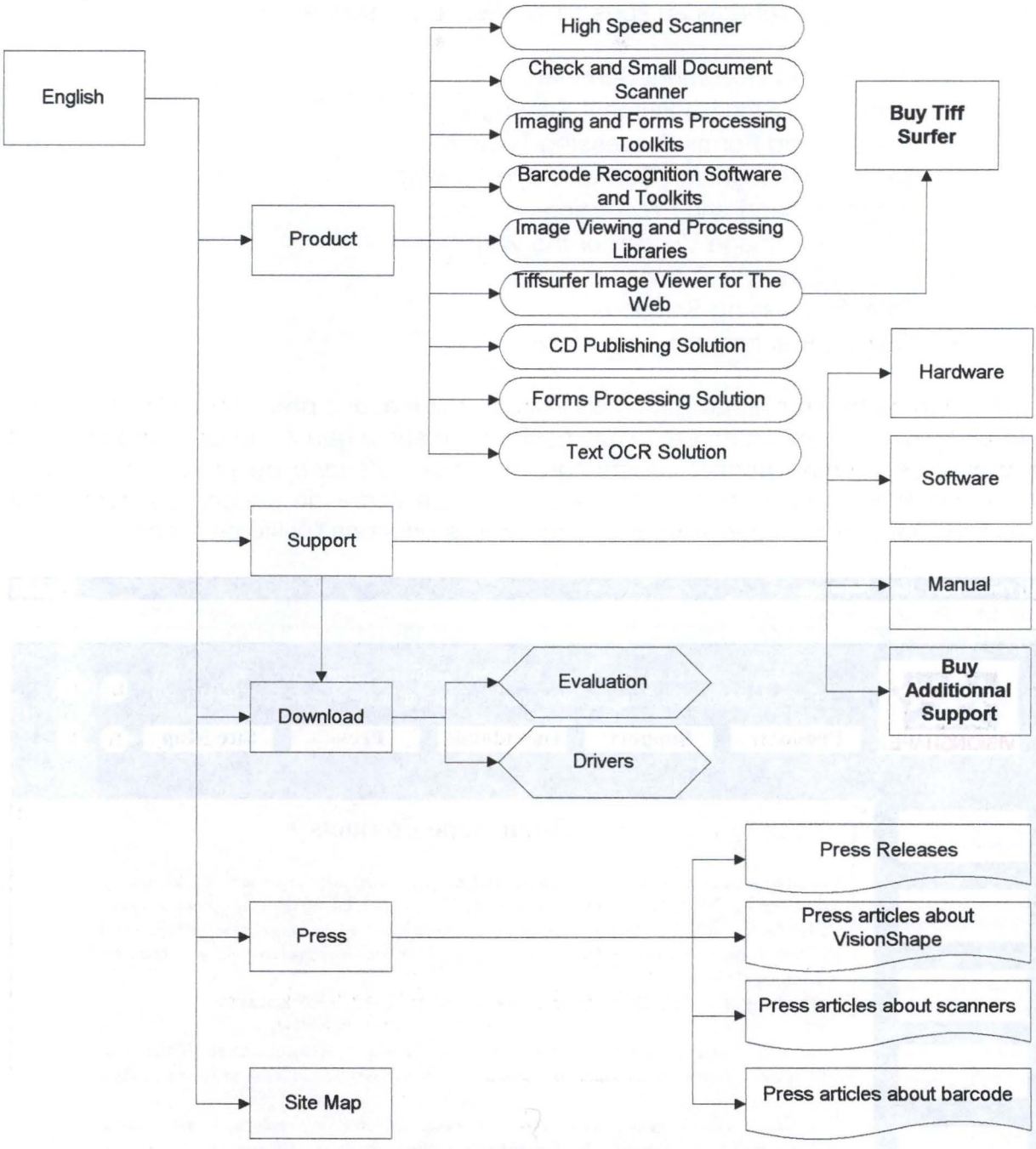


Figure 48: Structure du site

5.5. Structure détaillée

Comme la copie d'écran du bas de page nous l'a montré un peu plus haut, nous avons opté pour une structure à deux niveaux. Le premier reprend les cinq sections du cadre supérieur, quant au second niveau, il s'agit de services auxiliaires offerts aux visiteurs du site.

5.5.1. Premier niveau

Section Product

Le nombre de produits commercialisés par VisionShape étant assez important, ils ont été répartis en sous catégories. Elles sont au nombre de neuf:

- High Speed Document Scanners
- Check and Small Document Scanners
- Imaging and Forms Processing Tools Kits
- Barcode Recognition Software and Toolkits
- Image Viewing and Processing Librairies
- TiffSurfeer Image Viewer for the Web
- CD Publishing Solutions
- Form Processing Solutions
- Text OCR solution

Afin de faciliter la navigation du visiteur, nous avons présenté cette section en utilisant deux cadres: un cadre de navigation situé sur la gauche et un cadre principal à droite. Le premier permet de changer de sous catégorie de produit facilement, alors que le second contient l'information utile. Le cadre de gauche contient aussi des liens vers les services auxiliaires dont nous étudierons l'utilité plus loin.

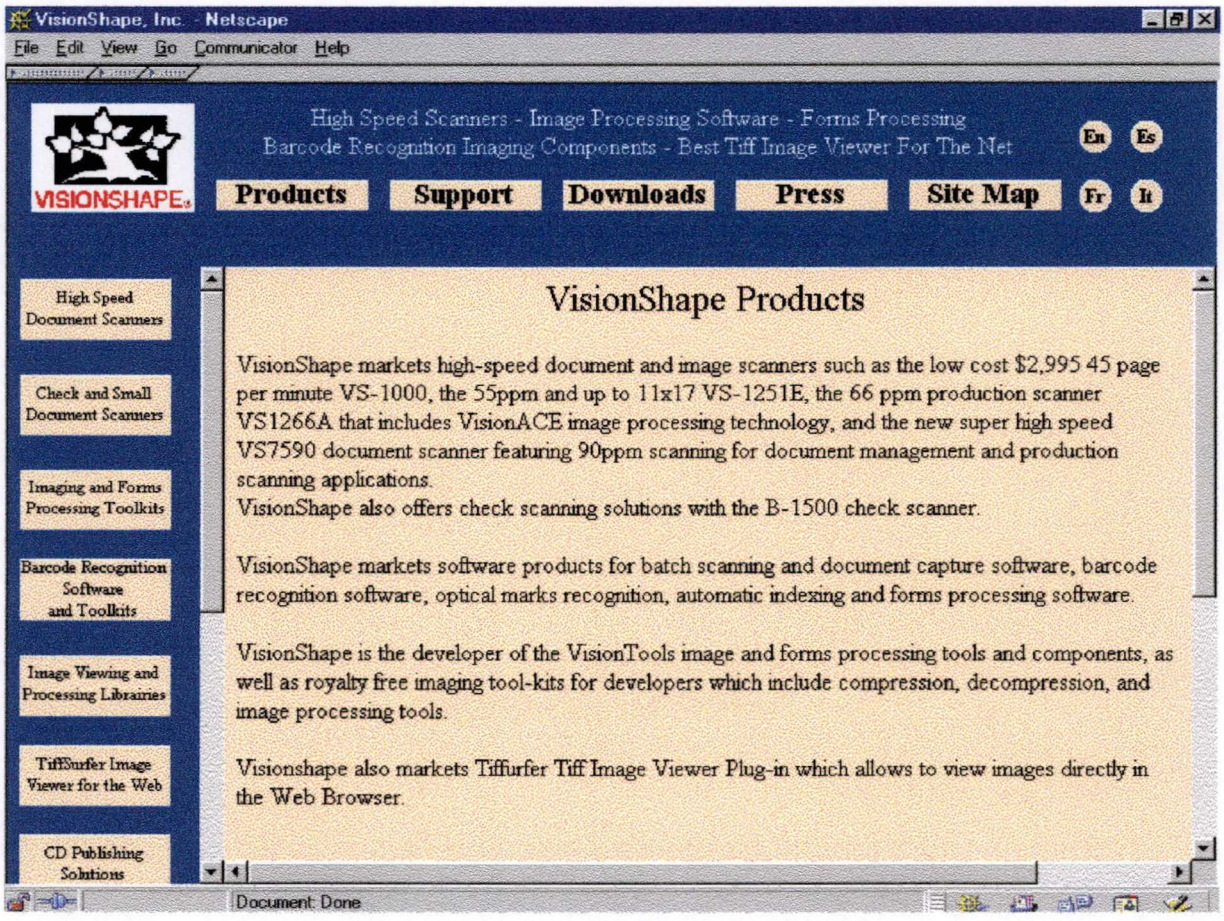


Figure 49: Page d'accueil de la section Product

Dans les pages présentant une sous catégorie de produits et lorsque cela était nécessaire, les liens vers les différentes pages qui la composent ont été regroupés suivant la nature des pages qu'ils visent. Ainsi, par exemple, pour la partie consacrée au *High Speed Document Scanners*, cinq sections ont été établies:

- Scanners: regroupe les liens menant aux pages décrivant les scanners.
- Software: regroupe les liens menant aux pages décrivant les logiciels liés aux scanners et commercialisés par VisionShape.
- Documents: il nous a paru judicieux de reprendre ici, entre autres, certains des documents que l'on rencontre dans la section Press (décrite plus loin) afin d'accélérer le parcours informationnel du visiteur.
- Warranty: lien menant à un document décrivant la garantie accompagnant l'achat d'un scanner. Ce document a été séparé des précédents afin de le mettre en évidence.
- Comparaison: lien menant à un document comparant les scanners de VisionShape avec ceux de la concurrence. Ici encore, le document a été séparé des précédents et ce pour la même raison que précédemment.

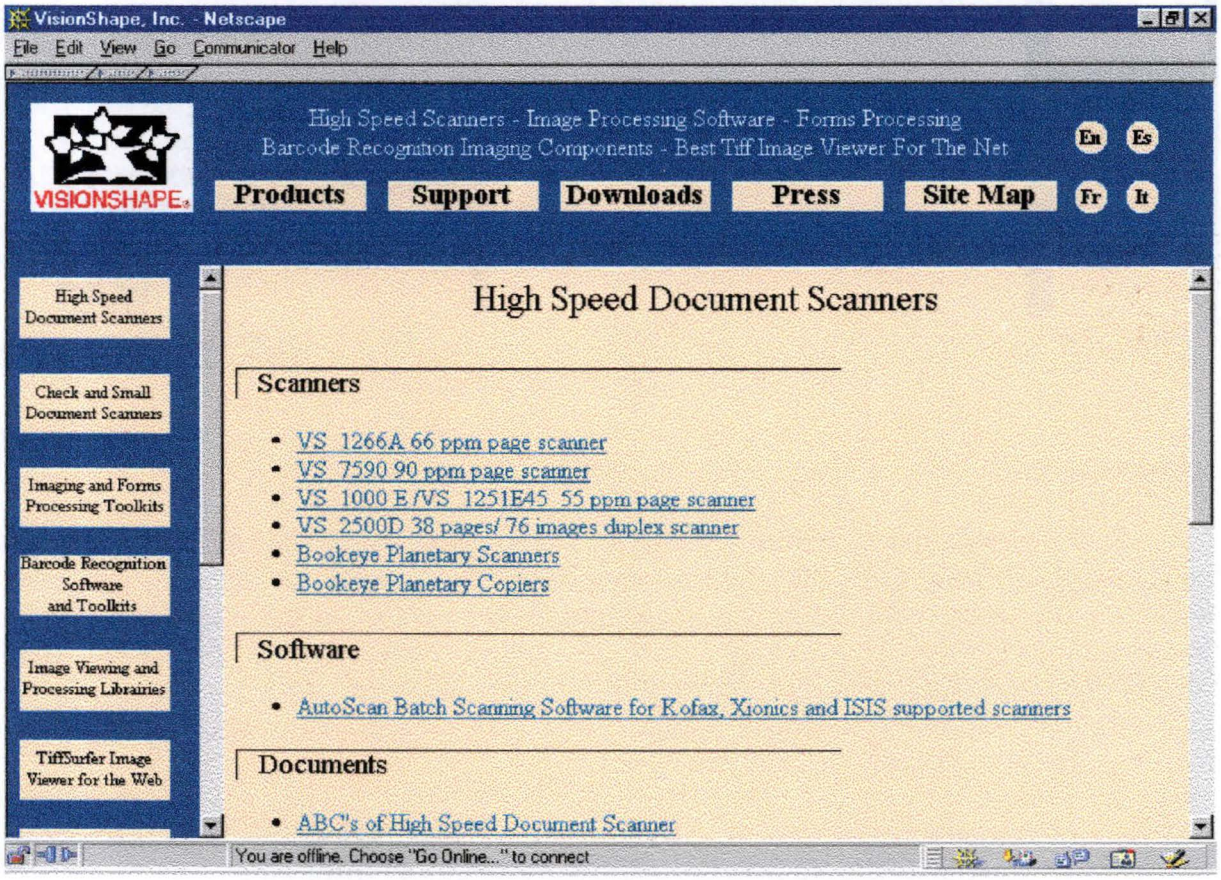


Figure 50: Page relative aux High Speed Document Scanner

Pour des raisons commerciales évidentes, dans les pages consacrées à un produit, nous donnons accès à un tableau reprenant les prix de vente des différents produits commercialisés par VisionShape et dans la mesure du possible à une illustration du produit. A chaque fois que cela était possible, nous avons également placé un lien vers un tableau comparatif des scanners de VisionShape à ceux offerts

par la concurrence. Enfin nous offrons la possibilité à l'internaute d'accéder aux spécifications techniques des appareils en vente.

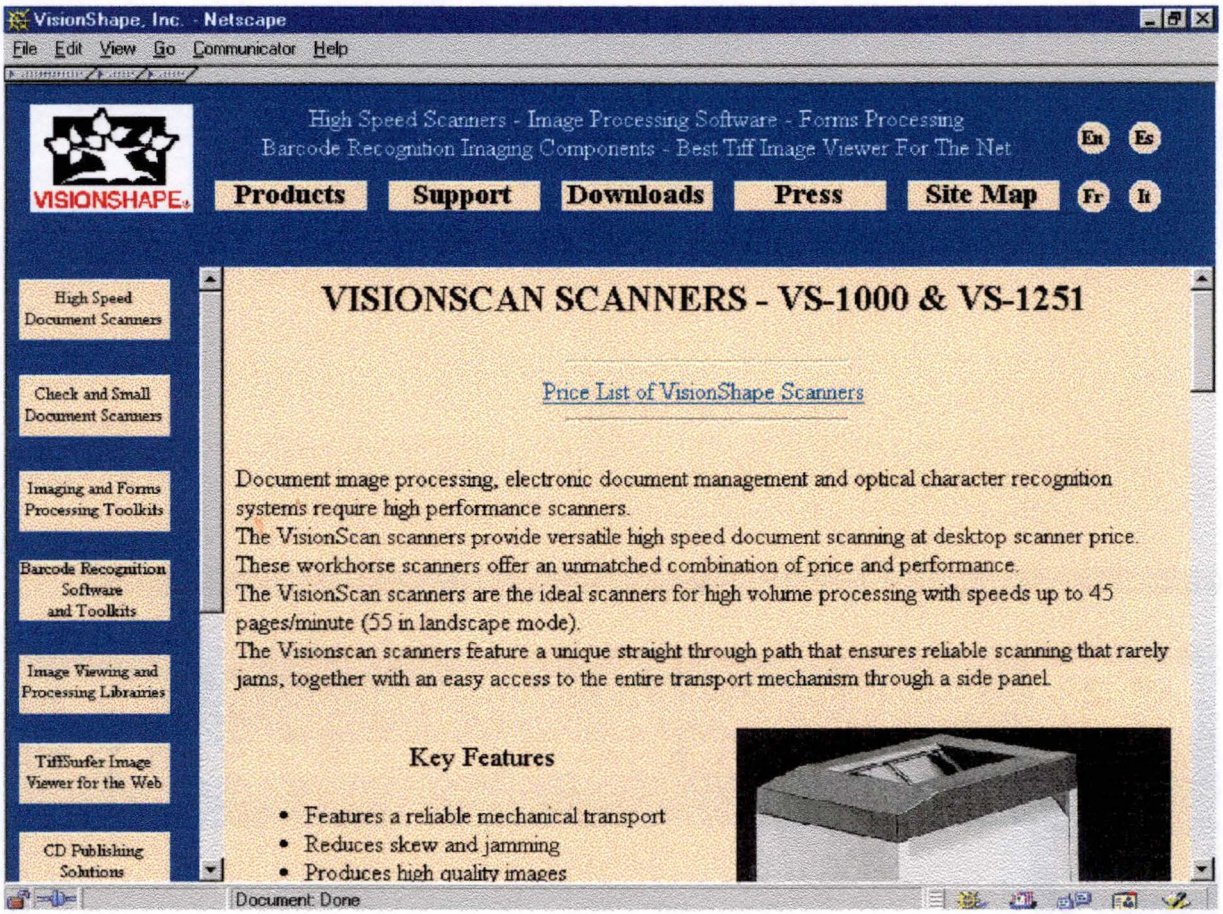


Figure 51: Page de présentation d'un scanner

Section Support

Dans cette section, comme son nom l'indique, nous avons rassemblé toutes les pages ayant pour but d'offrir d'une manière ou d'une autre au visiteur un support technique à propos des produits de VisionShape. On y retrouve entre autres tous les documents relatifs aux réponses aux questions fréquemment posées (FAQ, ***F**requently **A**sked **Q**uestions, **F**oire **A**ux **Q**uestions*). Les documents relatifs à l'utilisation des différents produits s'y retrouvent également. A nouveau, dans cette section, différentes catégories ont été définies:

- Hardware: reprend l'ensemble du support relatif aux scanners, comme par exemple les documents décrivant les procédures d'entretien.
- Software: reprend l'ensemble du support relatif aux logiciels commercialisés par VisionShape. On y retrouve entre autres un nombre important de FAQ.
- Manuals: permet au visiteur de télécharger les différents manuels d'utilisation édités par VisionShape.
- Buy Additional Support: ce lien mène à une page de commerce électronique permettant au visiteur d'acheter des contrats de maintenance supplémentaires pour ses scanners.

Puisque le support peut consister à télécharger la mise à jour des drivers pour les scanners, nous avons également ajouter, ici, un lien vers la section de téléchargement.

Si le visiteur ne trouve pas la réponse à ses questions il a également la possibilité de contacter VisionShape grâce au lien qui lui est fourni.

Ici aussi, nous avons opté pour une présentation en deux cadres: l'un de navigation à gauche et l'autre, principal, sur la droite.

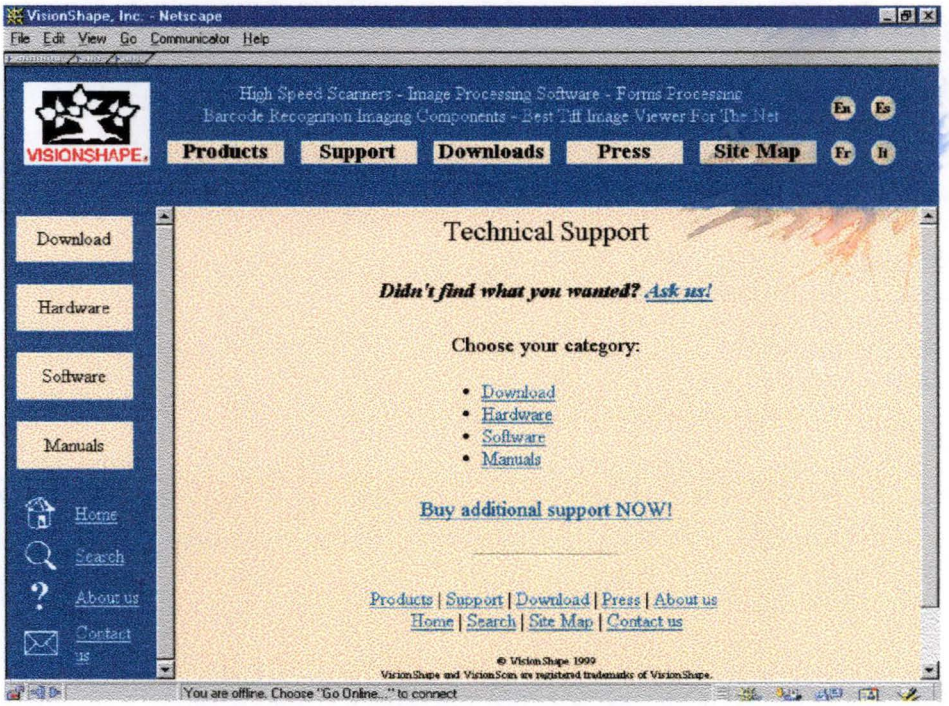


Figure 52: Page relative à la section support

Le lecteur pourrait être surpris à la vue de la figure ci-dessus de la redondance des liens vers les sections principales et vers les services auxiliaires du site. Cette redondance, conforme aux règles ergonomiques, permet de faciliter un maximum la navigation du visiteur à travers le site.

Section Download

Nous avons repris ici tous les produits téléchargeables en les classant d'après leur nature. Il s'agit aussi bien de drivers spécifiques aux scanners que de logiciels en version d'essai. Cette section est très importante étant donné que les utilisateurs du net sont toujours à l'affût de ce qui est gratuit.

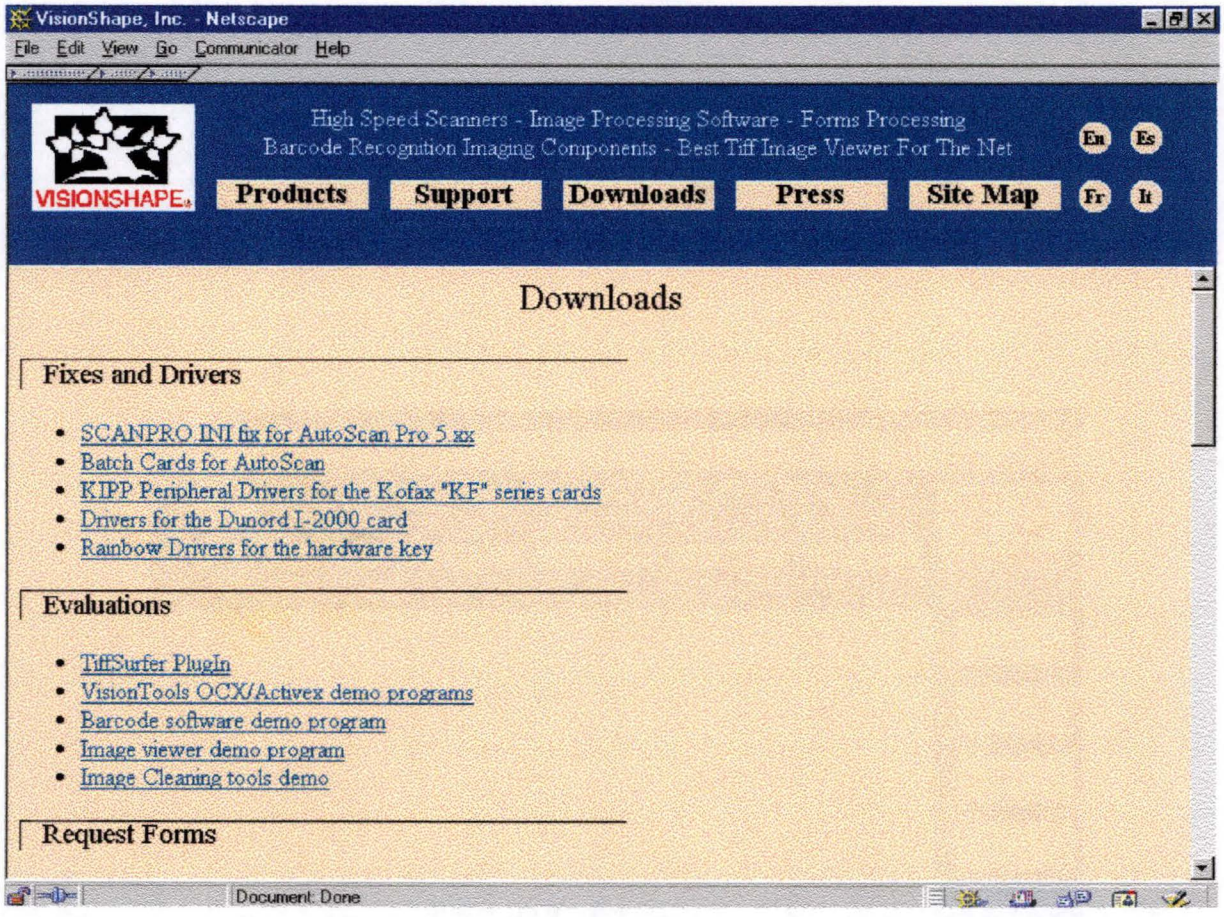


Figure 53: Page d'accueil de la section Download

Section Press

Cette section permet au visiteur de connaître rapidement la valeur de l'entreprise et des produits dont elle dispose. Les liens menant aux documents ont été rassemblés d'après leur nature. On y retrouve les annonces de nouveaux produits, l'ensemble des articles de presse parus sur VisionShape ainsi que ceux qu'elle a elle-même publiés.

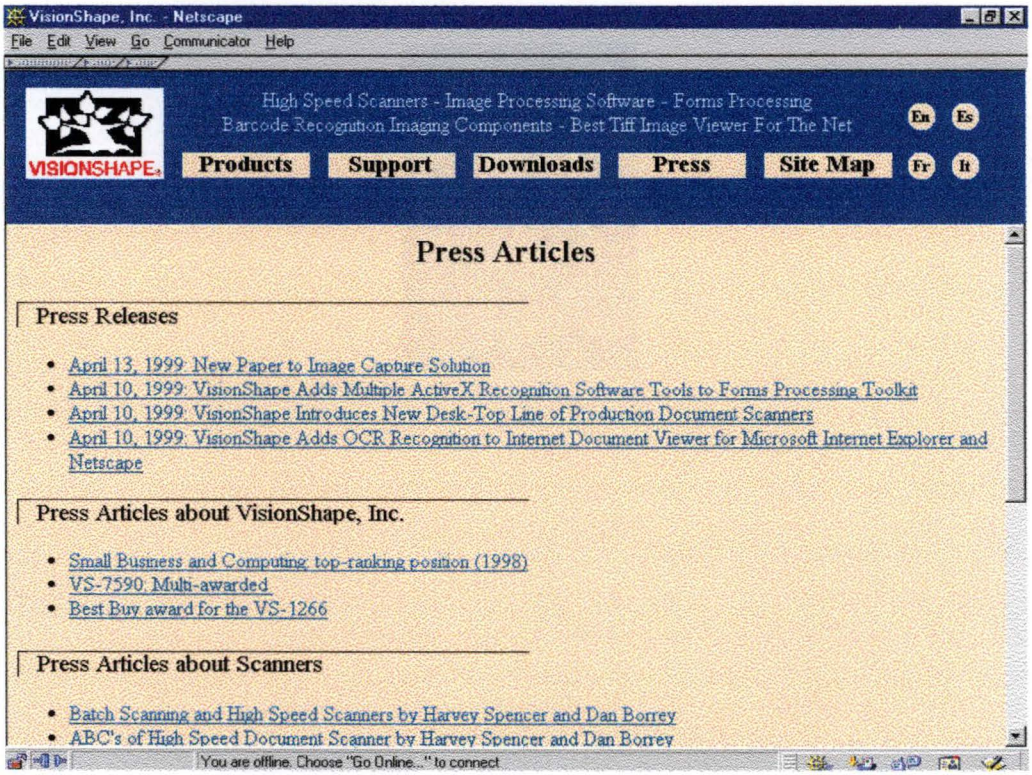


Figure 54: Page d'accueil de la section Press

Section Site Map

Quant à cette dernière section, elle devrait reprendre de manière schématique, la structure du site correspondant à l'organigramme présenté plus haut. Cette section n'a pas encore été réalisée. Elle le sera lorsque l'intégration entre le site de départ et celui que nous avons construit sera finalisée.

5.5.2. ***Deuxième niveau***

Ce niveau reprend les services auxiliaires utiles au visiteur.

- Un lien vers la Home Page permettant au visiteur de rapidement revenir a son point de départ.
- Un lien vers le moteur de recherche permettant à l'utilisateur d'effectuer une recherche sur l'ensemble des pages du site. Ce moteur est un outil mis à disposition par InfoDial, l'hébergeur de VisionShape. La base de données qu'il utilise n'est cependant pas à jour et fait toujours référence à l'ancien site. VisionShape demandera à InfoDial d'en réaliser la mise à jour en fin d'intégration.
- Un lien vers la page 'About us' décrivant VisionShape et donnant la liste de ses partenaires.
- Un lien vers la page 'Contact us' reprenant tous les moyens mis a disposition du visiteur pour contacter VisionShape

Rappelons encore la présence de liens vers les services auxiliaires dans les cadres de navigation des sections *Product* et *Support* pour faciliter au maximum la navigation du visiteur.

Figure 55: Liens vers les services auxiliaires dans les cadres de navigation

La version du site que nous avons rendue à VisionShape était présentée de façon légèrement différente: la section *Site Map* se trouvait dans les services auxiliaires, ce qui paraît plus logique, alors que le service *About us* était considéré comme une section de base puisqu'elle offrait un lien vers une description de VisionShape et la liste de ses partenaires. Les conséquences de ce changement de dernière minute souhaité par VisionShape n'ont pas pu être encore totalement réalisées faute de temps: les bas de page correspondent encore à la version que nous avions rendue.

5.6. Règles ergonomiques

Tout au long de l'élaboration du site, nous avons cherché à garder les mêmes standards typographiques (choix de la police, couleur des liens, ...) et de mise en page (taille et position des titres, propriétés des paragraphes, ...) pour offrir un site aussi agréable que possible. Nous avons, par exemple, opté pour des couleurs qui ne fatiguent pas le visiteur et qui correspondent aux couleurs utilisées par VisionShape dans ses documents écrits (publicité, manuels d'utilisation, etc.) à savoir les couleurs bleu marine et blanc.

Nous avons également essayé, dans la mesure du possible, de respecter l'ensemble des règles d'ergonomie présentées dans le chapitre 5 *Marketing* rappelées en partie ci-dessous:

- Une site Web doit contenir un titre percutant au sommet de chaque page. Les figures précédentes illustrent abondamment cette règle.
- La longueur d'une page ne doit pas dépasser cinq à six écrans. Cette règle nous a contraint à restructurer de nombreuse pages.
- Éviter les textes à la fois colorés et soulignés. Liens exceptés, aucun texte n'est souligné dans le site.
- Il doit exister au moins un lien dans chaque page. Cette règle est automatiquement validée par l'insertion dans chaque page du bas de page de navigation.
- Essayer de conserver les couleurs de lien proposées par défaut. Nous n'avons pas respecté cette règle ici. En effet, la couleur par défaut est le bleu clair et cette couleur se marie difficilement avec les autres couleurs présentes dans le site.
- Proposer sur toutes les pages un lien vers la Home Page. Cette règle est respectée grâce à l'utilisation des bas de pages.

- Si la page est longue, utiliser des liens internes à la page pour naviguer à travers celle-ci. La figure suivante illustre cette règle. En effet, dans une page FAQ, à côté de chaque question, se trouve une petite flèche permettant au visiteur d'accéder rapidement au haut de la page.
- Le logo de l'entreprise doit être visible en haut de toute page du site. Cette règle est validée par l'utilisation du cadre supérieur permanent contenant le logo.
- Une aide à la navigation doit être disponible dans tous les hauts de pages. L'utilisation du cadre supérieur permanent valide cette règle.
- Une aide à la navigation doit être répétée en bas de page. C'est bien le but recherché du bandeau de navigation inséré dans tous les bas de page.
- Si c'est approprié, ajouter une brève table des matières en haut de la page. Nous avons appliqué cette règle dans les pages de FAQ. L'ensemble des questions y sont rassemblée en tête de page.

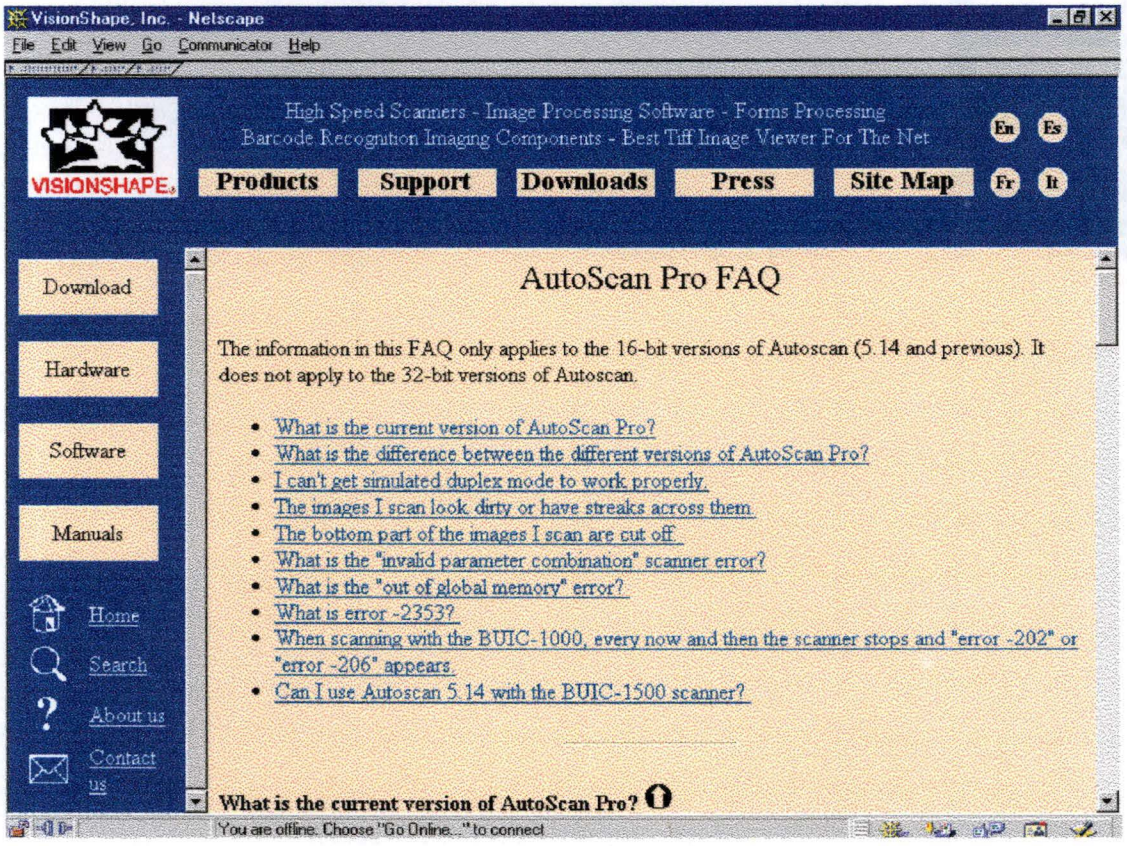


Figure 56: Page de FAQ

- Les graphiques présents dans une page doivent avoir un apport informationnel important. La figure ci-dessous illustre cette règle. La possibilité pour l'acheteur de voir le scanner lui permet, par exemple, d'évaluer l'espace nécessaire à l'intégration de ce dernier.

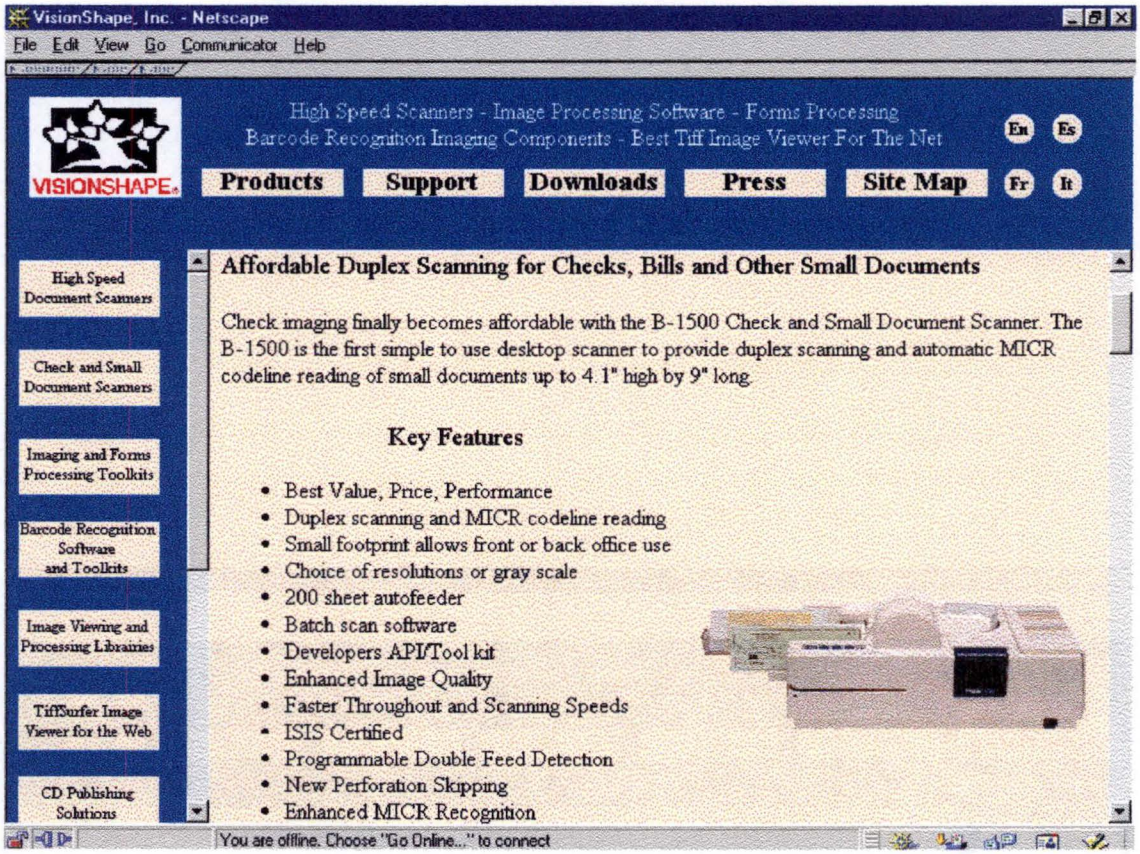


Figure 57: Utilité d'une illustration

- S'assurer que les liens soient discernables les uns par rapport aux autres. Nous avons pu facilement respecter cette règle.
- Éviter les animations inutiles: le site n'en contient aucune.

5.7. Accessibilité

Nous avons cherché à offrir un temps d'accès relativement rapide pour l'ensemble du site afin d'éviter à l'utilisateur de longs temps d'attente. A cet effet, les images téléchargées ne sont pas lourdes et le site ne contient pas d'animations qui se chargent indéfiniment.

Le chargement complet d'une page décrivant un scanner et reprenant la photo du produit analysé, prendra, par exemple, avec un modem doté d'une vitesse de transmission de 14.4kbps, en moyenne 18,3 secondes et une page texte (c'est à dire sans illustration) prendra, quant à elle, en moyenne 9.4 secondes[75].

Nous avons également éviter l'emploi de scriptes, d'applets ou de composants ActiveX, ce qui permettra à tous les utilisateurs et quelque soit leur configuration de profiter pleinement du site.

Enfin le site se prétend être compatible avec toutes les résolutions d'écran supérieures ou égales à 800 X 600.

[75] Calcul effectué par Doctor HTML, http://www2.imagiware.com/RxHTML/

5.8. Référencement

Le Webmaster a préféré assumer lui-même la tâche de référencement dans les différents index et répertoires. Il se chargera donc du remplissage des divers META et autres astuces utiles pour que son site soit facilement repéré par les moteurs de recherche.

Il signalera également aux sites de recherches que des modifications ont été apportées pour s'assurer du renouvellement des informations contenues dans les bases de données des différents sites de recherche.

6. Choix d'un éditeur HTML

La dernière étape avant la construction du site fut le choix d'un éditeur HTML.

Afin d'offrir une bonne qualité au niveau de la syntaxe et de faciliter notre travail, nous avons choisi d'utiliser un éditeur HTML WYSIWYG (***W**hat **Y**ou **S**ee **I**s **W**hat **Y**ou **G**et*).

HoTMetaL PRO 5.0 de SoftQuad[76] proposait toutes les exigences requises pour permettre un travail rapide, efficace, et correct au niveau syntaxique. HoTMetaL délivrait la facilité d'utilisation et le contrôle nécessaire pour créer un site Web.

HoTMetaL offre en effet un contrôle total sur le code HTML. Il met également à disposition des nouveaux outils spécifiques comme, par exemple, un remplissage automatique des balises, une coloration personnalisée de la syntaxe HTML, une liste d'éléments de référence à *glisser et déposer* pour une programmation rapide, etc. Notons également que les retraits automatiques ou personnalisables offerts par le produit permettent une structuration automatique du langage source et donc une meilleure lisibilité.

En son sein, HoTMetaL contient un outil de validation s'assurant à chaque modification de la validité de la syntaxe et de son adéquation avec les standards émis par le World Wide Web Consortium.

Hotmetal Pro 5.0 est capable de produire du code compatible HTML 2.0, 3.2 et 4.0. Nous avons opté pour la version proposée par défaut, à savoir la version 4.0.

L'assistant HTML permet de corriger les mauvaises codifications HTML importées d'autres applications et de créer des pages *browser-safe*.

Finalement, HoTMetaL est entièrement basé sur des standards. On peut ainsi créer de sites Web modernes et sophistiqués sans requérir à des extensions.

7. Outils de commerce électronique utilisés

Au niveau sécurité, le système proposé est un système de classe 3. L'entièreté des données formant la commande (produits achetés, informations personnelles et de paiement) sont chiffrées durant leur transmission grâce à SSL.

---

[76] http://www.softquad.com/

De par l'utilisation de SSL, l'entreprise a, bien entendu, dû se procurer un certificat auprès d'une Autorité de Certification. Dans notre cas, il s'agit d'un certificat obtenu auprès de VeriSign.

Étant de classe 3, ce système permet à l'entreprise d'avoir connaissance des détails des cartes de crédit.

Quant aux moyens de paiement, InfoDial permet l'utilisation de cartes de crédit ou de chèques électroniques. Il faut cependant remarquer que le paiement par carte de crédit constitue la majorité des paiements effectués.

7.1. Principe de fonctionnement

Le principe de base est celui du *Shopping Cart* ou caddie. L'utilisateur se promène sur le site et choisit au fur et à mesure les produits dont il a besoin. Il a, bien sûr, à tout moment, la possibilité de visualiser le contenu de son caddie et de retirer les produits qu'il ne souhaite plus acquérir. Une fois son choix fait, il peut alors régler ses achats par carte de crédit ou par chèque électronique. L'achat effectué, le client, tout comme le Webmaster du site, reçoit un e-mail reprenant le contenu de la commande ainsi que les informations personnelles de l'acheteur (nom, prénom, adresse de facturation, adresse de livraison, ...). S'en suit, quelques instants plus tard, un second e-mail, lui aussi envoyé aux deux parties, indiquant si le paiement a été accepté ou non.

Le travail des outils proposé par InfoDial s'arrête là. C'est alors au Webmaster de prendre les choses en main afin de faire parvenir au client les produits que ce dernier a demandés.

On peut schématiser le cycle d'achat par l'organigramme suivant:

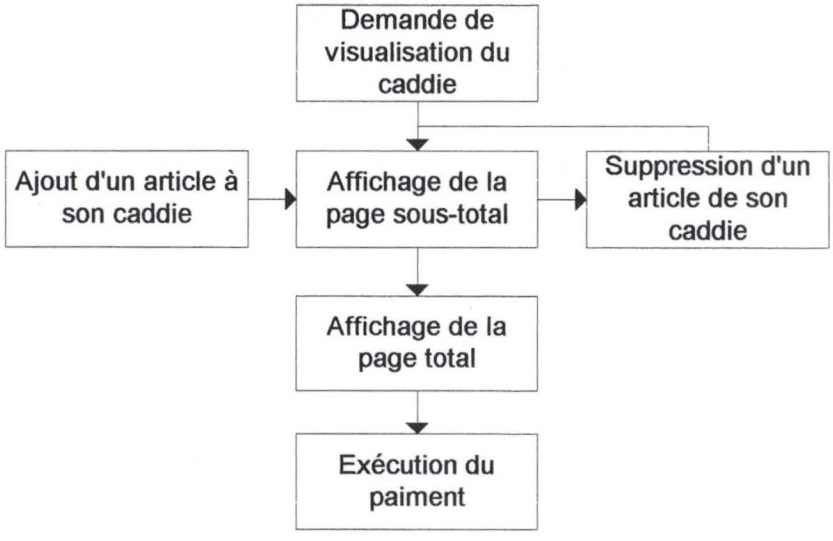


Figure 58: Cycle d'achat

7.2. Mise en œuvre

7.2.1. Mise en route

La documentation mise à disposition par InfoDial a un défaut important. En effet, les pages du support proposent une explication détaillée de chaque outil mais il manque un chapitre d'introduction qui expliquerait le fonctionnement général du système et l'interaction des outils entre eux. Par exemple, des shémas semblables à ceux ci-dessus et ci-dessous seraient les bienvenus. De plus, la structure du site présentant ce support n'est pas des plus agréable.

Enfin, les démos téléchargeables ne sont pas toujours en état de marche, ce qui ne facilite pas la tâche de compréhension.

Il s'en est donc suivi une perte de temps importante en début de travail puisque nous ne savions pas trop comment et par où commencer.

7.2.2. Principe de fonctionnement des outils

Les trois outils principaux sont: AddItem, ShowTotal et MoveMoney. Il s'agit de composants logiciels auxquels le concepteur du site peut faire appel. Ils s'enchaînent de la façon suivante:

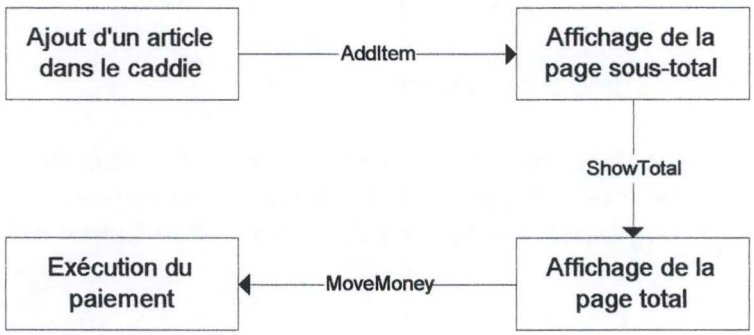


Figure 59: Enchaînement des outils

Les outils fonctionnent en utilisant des modèles. Chaque outil se sert des informations introduites dans le formulaire de la page en cours et d'un modèle pour générer la page suivante. Un modèle est un fichier HTML dans lequel on insère des balises propres aux outils. Lors de la génération de la page, ces dernières sont remplacées par de l'information.

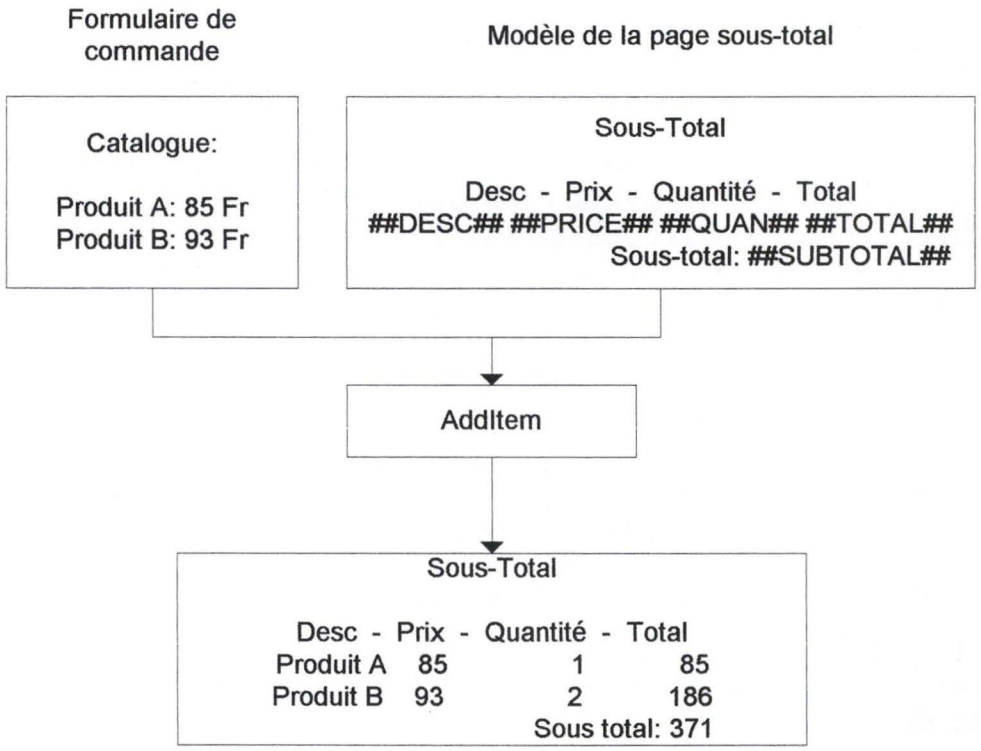


Figure 60: Principe des modèles

Prenons par exemple l'achat d'un produit.

Lorsque l'on ajoute ce produit à son caddie, on aboutit à la page sous-total. Cette dernière a été créée à partir d'un modèle dans lequel, par exemple, la balise ##DESC## a été remplacée par le nom du produit et la balise ##PRICE## par le prix de ce dernier.

L'outil connaît le nom et le prix du produit car lorsque l'utilisateur ajoute le produit à son caddie, c'est un formulaire de commande reprenant de telles informations qui est transmis à l'outil.

Enfin, pour visualiser l'état de son caddie sans devoir passer par l'ajout d'un article, l'outil SubTotal est utilisé.

Une fois ce travail réalisé, nous avons trouvé qu'il serait lourd de devoir retravailler les pages de type catalogue à chaque fois qu'un nouveau produit devait être ajouté.

Nous avons alors pris l'option de générer les pages du catalogue à partir d'une base de données. Cela permet au Webmaster de facilement gérer son site. En effet, en cas de changement de prix, par exemple, ou d'ajout d'un nouveau produit, il lui suffira, dorénavant de mettre simplement à jour la base de données.

InfoDial procure les outils nécessaires à la gestion de bases de données relationnelles. Ils supportent les fichiers de type Access, Excel, dBase, Paradox et FoxPro. Le Webmaster a souhaité l'utilisation d'une base de donnée de type Access.

Ces outils fonctionnent également en utilisant des modèles. La page générée reprend le modèle dans lequel elle remplace les balises propres aux outils par l'information qu'elle retire de la base de données.

7.3. Résultat

Ce point a pour seule vocation d'illustrer nos propos et de montrer au lecteur le résultat de ce travail sous forme de trois copies d'écran. La première représente une page du catalogue et la seconde illustre la page sous-total. La troisième est un extrait de la page total. Il est à remarquer que cette page demande à l'acheteur d'accepter explicitement les termes de la licence d'utilisation du logiciel qu'il compte acheter.

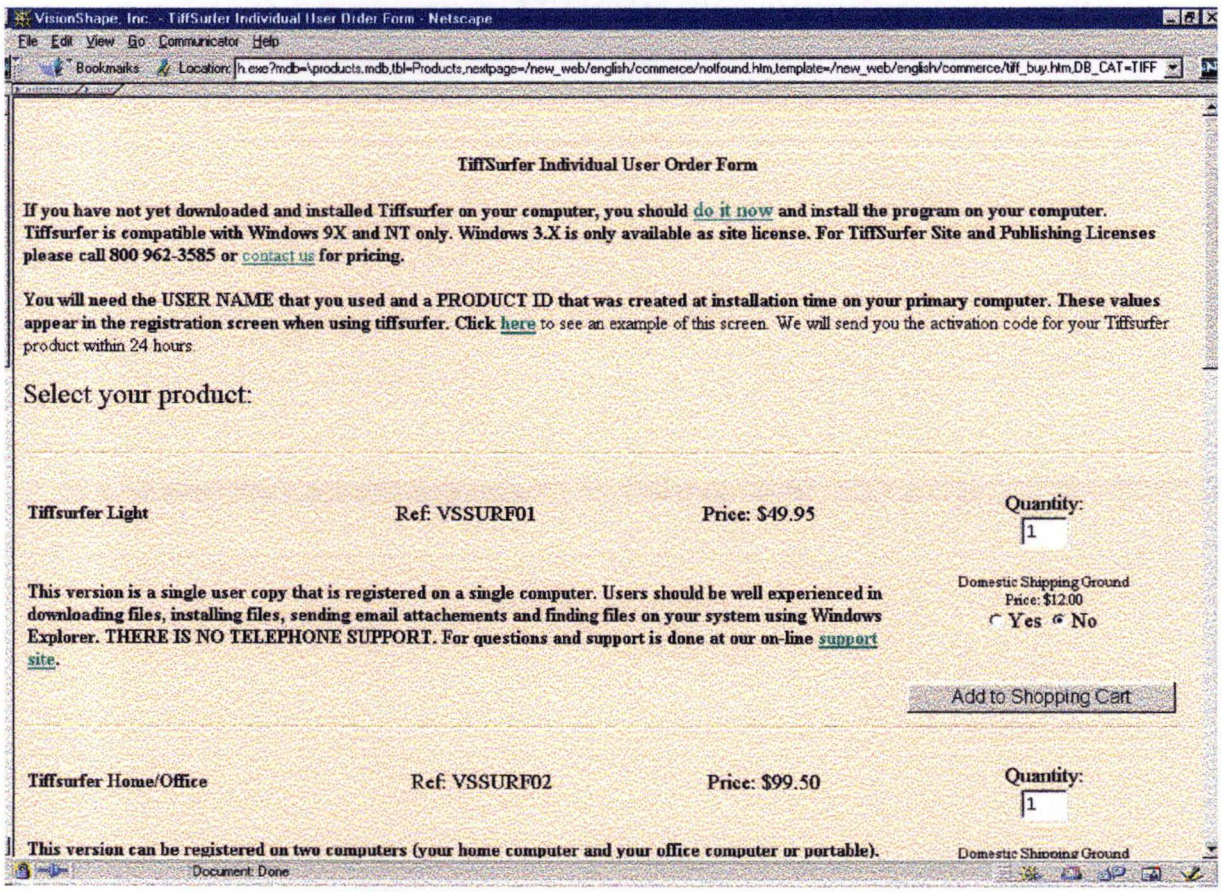


Figure 61: Extrait d'une page du catalogue

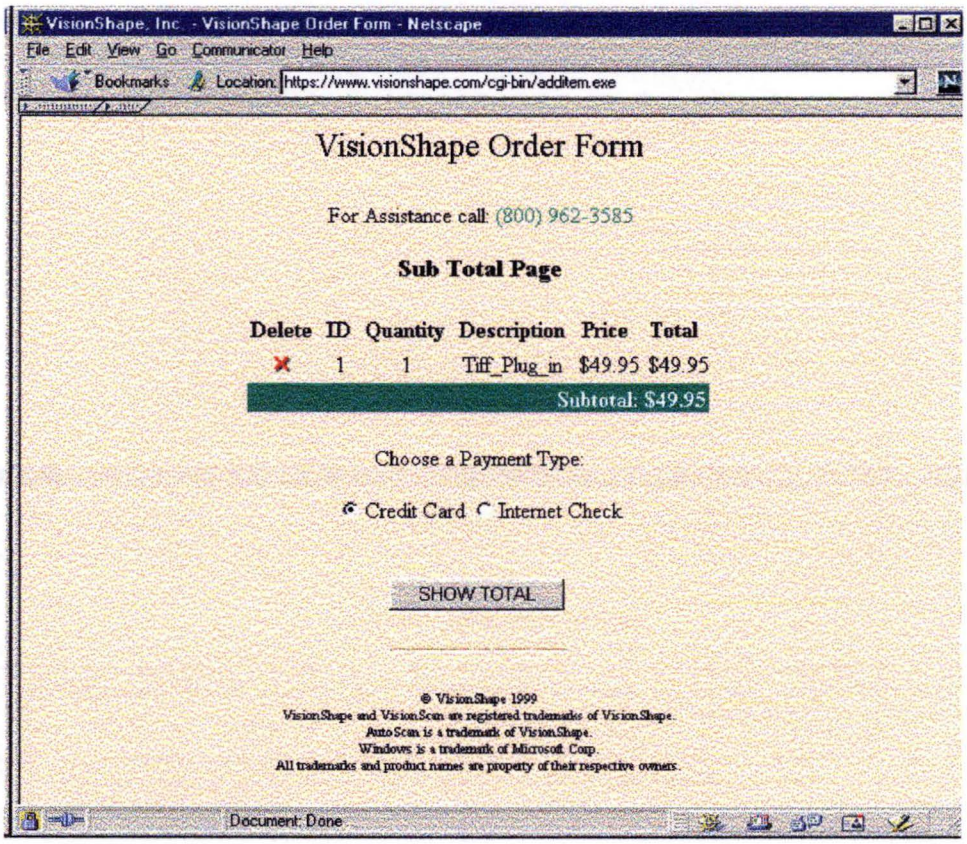


Figure 62: La page sous-total

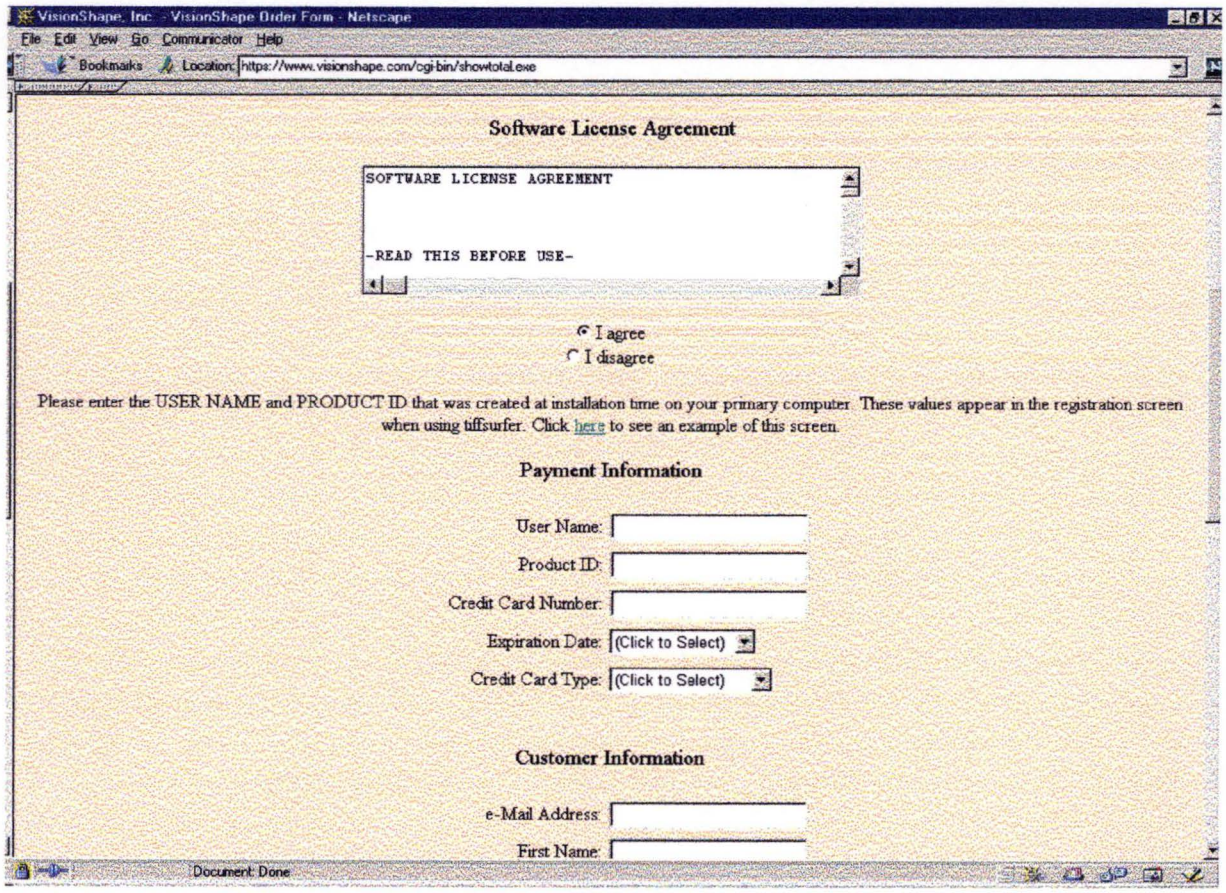


Figure 63: Extrait de la page total

7.4. Avantages de cette solution

Une fois que l'on a compris le système, celui-ci est très simple à utiliser. Il suffit au Webmaster d'insérer dans ses pages les balises faisant appel aux fonctionnalités de commerce électronique et de créer les modèles de page à partir desquels seront générées les pages vues par l'utilisateur.

De plus, cette solution ne nécessite pas de la part du Webmaster l'installation de logiciels ou de matériel. Tout est géré par InfoDial.

Enfin, ce système reste économique. En effet, l'hébergement de l'entièreté du site et l'accès aux fonctions de commerce électronique revient à moins de 4000FB par mois.

7.5. Défauts de cette solution

Un des défauts majeur de cette solution est le fait qu'il n'y ait pas moyen d'ajouter à son caddie plusieurs articles d'un simple clic. On pourrait, par exemple, imaginer un tableau reprenant un ensemble de produits frais. Il serait agréable de pouvoir, pour chaque produit, choisir la quantité souhaitée et ensuite, en un seul clic de souris, les ajouter à son caddie.

Les outils proposés s'arrêtant après que le paiement ait été effectué, il n'y pas moyen d'appliquer un tracking de la vente. Une mise à jour d'une base de données des stocks, une fois le produit envoyé à l'acheteur, s'avère difficile avec l'outil utilisé. Il serait, en effet, possible de le faire au moment de l'envoi de la commande et de toutes les informations de paiement. Cependant, en cas de refus du paiement il n'y a pas moyen d'annuler cette mise à jour.

Nous regrettons enfin qu'il ne soit pas possible de tester toutes les fonctionnalités de commerce électronique. On peut, bien sûr, entrer un numéro de carte de crédit non valide pour vérifier que la transaction est annulée. Malheureusement, le seul moyen de tester si une transaction a été acceptée, est d'utiliser une carte de crédit valable. Il est impossible, également, de tester les chèques électroniques. De plus, ce système n'était pas au point lors de nos tests. Nous avons effectué un achat avec des indications farfelues. Le Webmaster a, alors, reçu un e-mail le prévenant que la transaction avait été acceptée alors qu'il nous a été transmis, comme il se doit, un e-mail indiquant le contraire.

7.6. Évaluation

Nous estimons donc que les outils de commerce électronique proposés par InfoDial sont bien adaptés aux petites et moyennes entreprises disposant de peu de produits en catalogue et, tout spécialement, si ces derniers sont intangibles ou fabriqués à la demande, comme chez VisionShape. En effet, ce genre de produits ne nécessite pas ou une très faible tenue de stocks.

Le fait qu'InfoDial ne supporte pas des bases de données telle qu'Oracle confirme d'ailleurs notre sentiment: ses outils ne sont pas destiner à être utilisés par de grosses entreprises.

8. Conclusion

Malgré les connaissances apportées par les chapitres précédents et nos années d'étude, nous avons dû effectuer un travail par itérations.

Les chapitres précédents nous ont été d'une grande utilité pour structurer le site et le rendre plus convivial et attrayant. Il nous fut d'ailleurs très agréable de pouvoir mettre en application toutes les conclusions théoriques qui découlaient de notre analyse.

Le fait de mener un projet de bout à bout dans une limite de temps impartie nous a permis d'apprendre énormément tout en faisant parfois face à un stress jusque là encore inconnu.

Nous avons également été amené à nous familiariser avec quelques-uns des nombreux outils disponibles sur le marché pour l'élaboration d'un site Web et plus particulièrement de commerce électronique.

En clôture de ce chapitre, nous mettons à disposition du lecteur la lettre de remerciement que nous avons reçue de VisionShape pour le travail effectué.

VisionShape, Inc.

1941B East Miraloma Avenue
Placentia, CA 92870, USA
Tel. (714)792-3612
Fax (714) 792-3612

VisionShape Europe
Parc Scientifique Einstein
Avenue Albert Einstein
1348 Louvain La Neuve, BELGIUM
Tel. 3210 483514
Fax. 3210 483515

Internet: http://www.visionshape.com/
E-mail: sales@visionshape.com

June, 99

Attention Mrs. Xavier Hallard and Benoît Coppens

TO WHOM IT MAY CONCERN

This letter to thank you and congratulate you for the magnificent work accomplished in redesigning VisionShape Web site www.visionshape.com/new_web.

In particular I was impressed with the new implementation of the E-Commerce data base and forms. We are now a few days away from the full implementation of that site.

I am glad we could work together on this project and hope will have other opportunities in the future.

Dan Borrey
Sales Vice President

Chapitre 7: Vers un guide d'étapes

1. Introduction

Ce dernier chapitre offre en quelque sorte un résumé des questions à se poser lorsque l'on souhaite mettre sur pied un site Web de commerce électronique. Certaines réponses à ces questions ont été apportées dans les chapitres précédents.

Notre mémoire nous a permis de découvrir plusieurs facettes du commerce électronique (sécurité de la transmission, moyens de paiement, droit, marketing). D'autres facettes n'ont pu être couvertes, comme la sécurité des systèmes du marchand, la livraison, le service à la clientèle, ... Néanmoins elles seront couvertes dans les questions suivantes et ce, dans le but de rendre ce guide aussi utile que possible.

2. Se poser les bonnes questions

Nous avons classé les questions essentielles à se poser avant de se lancer dans la conception d'un site Web de commerce électronique en 18 catégories. Il est évident que cette liste de questions n'est pas exhaustive, mais nous pensons qu'elle reprend, cependant, les plus importantes.

C'est avec l'expérience acquise au cours de l'élaboration de notre mémoire et du site de VisionShape que nous avons établi ce classement et ces questions tout en s'appuyant sur **[GUIDE 98]**.

2.1. Évaluation de l'entreprise et opportunité du commerce électronique

Il est important avant toute chose, d'évaluer ce que peut apporter le commerce électronique à vos produits, à vos services, à votre entreprise et à vos clients.

- Quel est le type de votre entreprise: vente directe, détaillant, hébergeur Internet, etc.?
- Quels sont les produits que vous vendez?
- Disposez-vous déjà d'un site Web?
- Quel en est le nombre de visiteurs journaliers?
- Ce site remplit-il ses objectifs?
- Quel est le type de votre clientèle (sexe, revenus, éducation, enfants, etc.)
- Quel part de votre chiffre d'affaires projetez-vous de faire par voie de commerce électronique?
- Dans combien de temps pensez-vous faire des bénéfices grâce au commerce électronique?

2.2. Le produit

Il est nécessaire de vérifier si le produit que l'on veut vendre sur Internet, en principe, donc, à destination du monde entier, est autorisé à la vente dans tous les pays.

Dans le cas contraire, il faut mettre en place des moyens techniques qui n'autorisent la vente du produit et sa livraison que dans les pays permis. Il est indispensable de citer sur le site les pays autorisant la vente libre du produit.

- Pouvons-nous livrer nos produits partout dans le monde?
- Si ce n'est pas le cas, quels sont les moyens à mettre en place pour palier ce problème?

2.3. Stratégie: ressources internes et partenaires extérieures

Qui va concevoir le site? D'un côté, les ressources internes ont une bonne connaissance de l'entreprise, de l'autre, les partenaires extérieurs peuvent apporter une expérience technique et créative.

Une conception en interne impliquera, avant tout développement, un choix quant aux outils à utiliser. De nombreuses solutions sont disponibles sur le marché. Les évaluer n'est pas toujours chose aisée. La meilleure façon de procéder est probablement de visiter quelques réalisations pour chaque outil analysé et, dans la mesure du possible, d'interroger quelques utilisateurs.

Un site doit aussi évoluer afin de ne pas être rapidement obsolète. Il faut déterminer quelle stratégie l'entreprise adoptera pour tenir à jour le site.

- Disposons-nous du personnel compétent en interne?
- Disposons-nous en interne de suffisamment de personnel pour mener ce projet à bien?
- Allons-nous faire appel à des partenaires pour réaliser une partie ou tout le projet?
- En cas de développement mixte, qui supervisera les différentes parties et comment sera partagé le travail?
- Est-ce un membre ou une équipe propre à l'entreprise qui se chargera de la maintenance et de la mise à jour du site ou faudra-t-il faire appel à des ressources externes?

2.4. Caractéristiques et fonctionnalités du site

Déterminer les caractéristiques et fonctionnalités que l'on souhaite intégrer à son site de commerce électronique est un élément clé puisqu'elles seront à la base du développement du site.

- Quels services souhaitons-nous offrir au visiteur: catalogue interactif, personnalisation du site, ...?
- Sur quels éléments souhaitons-nous proposer un outil de recherche: mots-clefs, catégorie de produit, prix, marque, numéro du produit, ...?
- Souhaitons-nous intégrer un système de fidélisation?
- Proposerons-nous des logiciels en téléchargement?
- Quelles options devons-nous proposer lors de la finalisation de la commande (emballage cadeau, adresse de livraison et de facturation différente, ...)?
- Allons-nous proposer un site polyglotte?

2.5. Design du site

Avoir un design attrayant fait partie des éléments importants pour attirer et conserver un client. Ce point n'est donc pas à négliger.

- A quelle catégorie de personne est destiné notre site: enfants, adultes, professionnels, tout public, ...?
- Les outils de conception génèrent-ils du code HTML compatible avec les normes du World Wide Web Consortium?
- Les pages sont-elles écrites afin de se présenter de manière optimale aux robots de référencement?
- Disposons-nous déjà d'une charte graphique?
- Respectons-nous les règles ergonomiques?
- Comptons-nous utiliser des plug-in, scriptes ou applets pour dynamiser notre site?

2.6. Technologie

Il important de s'assurer que le site, une fois développé, sera flexible, modulaire et extensible afin qu'il puisse évoluer au fur et à mesure des évolutions technologiques.

Il est également important de déterminer comment sera intégré ce nouveau système avec ceux déjà en place dans l'entreprise.

- En quoi consiste l'existant (hardware, software, base de données, type des serveurs, ...)?
- Quels sont les systèmes existants que nous souhaitons intégrer au système de commerce électronique: base de données des commandes, des clients, des produits, systèmes de paiement, service à la clientèle, ...?
- Une base de données centralisée est-elle nécessaire?
- Avons-nous des préférences dans le choix des outils de commerce électronique?
- Développerons-nous certains outils ou utiliserons-nous des solutions existantes que nous paramètrerons nous-mêmes?

2.7. Marketing et promotion

Disposer d'un fantastique site de commerce électronique sans trafic n'est certainement pas une situation optimale. Un politique de marketing et de promotion est donc nécessaire afin de se faire connaître.

Cependant, une publicité sur Internet revêt un caractère international avec tous les problèmes que cela peut impliquer en termes de marques, de droits d'auteur, de légalité... Il faudra donc être attentif, par exemple, aux publicités touchant des produits sensibles comme les médicaments, les armes, l'alcool, etc.

Certaines techniques publicitaires pourraient également poser problème. Rappelons, à titre d'exemple, que la publicité comparative, quoique autorisée aux États-Unis, est interdite en Belgique.

- Le marketing et la promotion se feront-ils en interne ou en externe?
- Qui s'occupera de soumettre l'adresse du site aux différents moteurs de recherche?
- Comptons-nous faire de la publicité en ligne?
- Comptons-nous utiliser des listes d'e-mails dans des buts promotionnels?
- De quelle manière allons-nous générer du trafic sur notre site: moteurs de recherche, galeries marchandes, bannières, spots TV et radio, annonces dans la presse, ...?
- Quel budget comptons-nous investir dans le marketing et la promotion?
- Est-ce que la publicité offerte est juridiquement acceptable?

2.8. L'offre et le contrat

Le contrat qui lie le vendeur au consommateur doit être disponible sur le site. Il devra être écrit dans un langage compréhensible et reprendre toutes les conditions et aspects juridiques de la vente.

Il peut aussi être bon de définir une clause d'exonération de responsabilité en cas de rupture de stock.

Les *disclaimers*, terme anglais généralement employé pour désigner les exonérations de responsabilités, doivent apparaître sur le site et ce, de manière visible! Rappelons encore qu'elles doivent être écrites avec soin et que des exonérations totales de responsabilité n'auront aucune valeur juridique.

- Quel type de contrat allons-nous offrir au client?
- Est-il juridiquement valable, est-il compréhensible?
- Où allons-nous placer les termes du contrat sur le site pour qu'ils soient visibles?

2.9. Paiement

Le paiement constitue la concrétisation de l'achat. Il est donc important d'avoir une compréhension claire des processus qui se cachent derrière les différents systèmes de paiement disponibles.

- Quelles types de paiement en ligne permettrons-nous: carte de crédit, Proton, ...?
- Permettrons-nous l'utilisation d'autres types de paiement: virement, par contre remboursement à la livraison, par transmission des détails de la carte de crédit par téléphone ou fax, ...?
- Permettrons-nous l'utilisation de coupons de réduction?
- Allons-nous faire l'acquisition d'un serveur de paiement?
- Par quel moyen nous connecterons-nous à notre institution financière afin d'exécuter les paiements: ligne téléphonique, ligne louée, ...?

2.10. Sécurité

La sécurité est probablement un des points les plus importants pour les entreprises sur le Web. Il est donc vital de ne pas négliger cet aspect.

- Disposons-nous déjà d'une politique et de procédures de sécurité?
- Utiliserons-nous les standards SET, SSL?
- Avons-nous opéré une analyse des risques?
- Sommes-nous en mesure de comprendre ces risques et de pouvoir y faire face?
- Quelles sont les ressources que nous devons protéger: serveurs, fichiers, comptes, ...?

2.11. Fraude

Minimiser les fraudes est dans l'intérêt du marchand. Or certaines catégories de produits vendus sur Internet (divertissements adultes par exemple) sont plus exposées que d'autres. Il est donc important de déterminer si les produits vendus risquent ou non d'attirer les fraudeurs.

- Attendons-nous à avoir un taux de fraude élevé?
- Disposons-nous d'une politique en matière de fraude?
- Allons-nous accepter les commandes provenant des marchés extra européens?
- Quelle sera la valeur moyenne des commandes?

2.12. Traitement et exécution de la commande

Le traitement de la commande revêt, quant à lui, une importance capitale. Certains des aspects qui lui sont propres doivent donc être planifiés avec rigueur pour assurer, au maximum, la satisfaction du client.

De nombreuses entreprises de commerce électronique ne fabriquent pas elles-mêmes les articles qu'elles vendent. Si cela est possible, il faudra donc déterminer s'il est nécessaire d'intégrer leurs systèmes aux nôtres.

- Allons-nous utiliser un call center?
- Le traitement des commandes a-t-il lieu en interne ou en externe?
- Quelles sont les fonctionnalités que nous souhaitons intégrer au système de commande: confirmation de la commande, tracking de la commande,...?
- Quelle est la fréquence du traitement des commandes: à la réception, toutes les heures, une fois par jour, ...?
- De quelle manière les commandes sont-elles délivrées à nos fournisseurs: e-mail, fax, téléphone, EDI, ...?
- Disposons-nous de plusieurs fournisseurs?
- Disposons-nous de l'inventaire en temps réel de nos fournisseurs?
- Les commandes peuvent-elles contenir des produits provenant de différents fournisseurs?
- Les systèmes de nos fournisseurs et les nôtres sont-ils capables de communiquer entre eux?

2.13. Livraison

Les moyens de livraison sont de plus en plus sophistiqués et permettent, pour la plupart, le tracking sur Internet de l'envoi. Il est donc important de bien choisir les différents moyens de livraison mis à disposition de l'acheteur.

- Autorisons-nous les livraisons internationales?
- Nos fournisseurs nous avisent-ils du statut des livraisons qu'ils effectuent pour nous?
- Dans quels délais souhaitons-nous que nous/nos fournisseurs envoyons/oient les commandes: dans les 24h, dans les x jours, dans les x semaines, ...?
- Quels types de livraison proposerons nous: poste, FedEx, DHL, UPS, ...?

2.14. Service à la clientèle

Le service à la clientèle est crucial pour toute entreprise mais peut-être plus encore pour les entreprises opérant dans l'espace virtuel qu'est Internet.

- Disposons-nous déjà d'un service à la clientèle?
- Comptons-nous créer un service à la clientèle adapté au Web ou allons-nous utiliser le service à la clientèle existant?
- Allons-nous assurer nous-mêmes le service à la clientèle ou faire appel à un call center externe?
- Allons-nous conserver le profil et les commandes des utilisateurs?
- De quelle manière allons-nous informer un client du statut de sa commande: par téléphone, par e-mail, ...?
- Quelles sont les informations que nous fournirons au client: date d'envoi de la commande, numéro de la commande, statut de la commande...?
- Quelle sera la disponibilité du service à la clientèle: 7j/7, 24h/24, durant les heures de bureaux, ...?
- Souhaitons-nous disposer d'un service à la clientèle polyglotte?

2.15. Retours

Un client doit pouvoir, dans certaines conditions, retourner un produit qui ne lui convient pas. Il est donc important de mettre en place un système capable de gérer de façon efficace ce type de problème.

- Dans quels cas le client a-t-il le droit de retourner un produit et d'en exiger le remboursement?
- Dans quels cas rembourserons-nous aussi les frais de port?
- Le client devra-t-il nous avertir avant de nous retourner un produit?
- De quelle manière le client connaîtra-t-il le statut de son remboursement?

2.16. Respect de la vie privée

Le respect de la vie privée est un point clé pour les acheteurs en ligne. Définir une politique de respect de la vie privée compatible avec les lois en vigueur est important pour la réussite de l'entreprise.

- Disposons-nous déjà d'une politique en cette matière?
- De quelle manière mettrons-nous les visiteurs de notre site au courant de notre politique en matière de respect de la vie privée?

2.17. Comptabilité

Comprendre la façon dont l'entreprise va intégrer la comptabilité de son site de commerce électronique avec ses systèmes de comptabilité existants est un autre point important.

Dans le chiffre d'affaires de la société devra être intégré celui généré par le site Web soumis, lui aussi, à l'impôt des sociétés et à toutes ses obligations de preuve.

- Souhaitons-nous intégrer la comptabilité du site avec nos systèmes de comptabilité existants?
- Nos systèmes financiers et autres systèmes de reporting sont-ils compatibles avec la création d'un site de commerce électronique?
- Allons-nous devoir faire l'acquisition de nouveaux logiciels de comptabilité?

2.18. Analyse des résultats

L'analyse des résultats est le seul moyen de mesurer le succès d'un site de commerce électronique. Cette analyse permettra aussi à l'entreprise de cibler les éléments du site à améliorer.

- Quels systèmes allons-nous utiliser pour analyser le site?
- De quels types d'information souhaiterions-nous disposer: types de navigateurs utilisés par les visiteurs, type de clientèle (profession, revenus, ...), pages les plus/moins visitées, temps de visite moyen, ...?
- Comment allons-nous mesurer le succès de notre site de commerce électronique: nombre de visites, chiffre d'affaires réalisé, nombre de commandes, charge du serveur Web, ...?

Conclusion

Ce mémoire nous a permis de nous familiariser avec un domaine particulièrement à la mode: le commerce électronique. Nous nous sommes efforcés de donner au lecteur un aperçu aussi large que possible des problèmes qui surgissent aujourd'hui face à cette nouvelle approche du marché en les éclairant d'une bonne base théorique.

Le chapitre 1 nous a permis de situer l'environnement dans lequel le commerce électronique est appelé à évoluer principalement dans notre pays. La tendance à l'expansion du commerce électronique en Belgique se marque déjà, mais il reste encore du chemin à parcourir. Ce chapitre nous a également permis de constater la difficulté à obtenir des statistiques fiables sur le commerce électronique.

Dans le chapitre 2, nous avons exposé les techniques actuelles pour sécuriser la transmission de données. La technique la plus utilisée aujourd'hui est SSL. Cependant, les systèmes SET et C-SET pourraient accroître la sécurité tant du côté vendeur que du côté acheteur.

Le chapitre 3 a présenté les différentes techniques de paiement disponibles à l'heure actuelle sur Internet. Nous avons pu remarquer que la carte de crédit reste le moyen le plus utilisé, à côté des systèmes tels que les porte-monnaie électroniques et virtuels. De nouveaux moyens tels que les chèques électroniques et l'utilisation d'une carte de débit font leur apparition. Mais il est encore difficile, dans l'état actuel des informations prospectives disponibles, d'estimer s'ils sont promis à un bel avenir.

Nous avons traité, dans le chapitre 4, des problèmes juridiques que soulèvent l'apparition du commerce électronique. Nous avons également constaté qu'un cadre légal cohérent et favorable au commerce électronique pouvait être mis sur pied grâce aux techniques de chiffrement moyennant une nouvelle approche plus fonctionnelle du droit, ne nécessitant pas sa révolution.

Quant aux techniques propres au marketing, elle ont été développées dans le chapitre 5. Elles permettent non seulement d'attirer le client, mais aussi de fournir à l'internaute une offre de plus en plus ciblée. Nous nous sommes particulièrement intéressés aux techniques utilisées par les sites de recherche, de même qu'aux règles ergonomiques et enfin aux outils de personnalisation. Et nous n'avons pas manqué de remarquer les inquiétudes que soulèvent ces dernières quant au respect de la vie privée.

Le chapitre 6 abordait, quant à lui, la partie pratique de notre mémoire et cherchait à montrer au lecteur la démarche que nous avons suivie et les multiples améliorations que nous avons apporter au site Web de VisionShape. Ce travail constitua, pour nous, une occasion unique de mettre en pratique nos connaissances et de tester le résultat de nos réflexions. Nous estimions pouvoir, de la sorte, nous rendre utiles en aidant concrètement une entreprise sur le terrain et abordé, de cette façon, le milieu professionnel dans lequel nous serons amenés à évoluer prochainement.

Synthèse de notre travail, le chapitre 7 avait pour prétention de fournir au lecteur un guide qui lui sera d'une grande utilité s'il décide de se lancer dans le commerce électronique.

Nous avons consciemment cherché dans ce mémoire a être le plus pédagogique possible, de manière à offrir un support utile et nécessaire à toute personne intéressée par le commerce électronique, et ce, quelles que soient ses connaissances.

De notre réflexion et de notre expérience pratique, subsistent bien des questions. Parmi celles-ci, celles d'ordre juridique semblent laisser à l'informaticien le plus d'incertitudes. En effet, de par sa nature, le commerce électronique s'effectue dans un cadre international pauvre en réglementations appropriées pour gérer les transactions commerciales dans un environnement juridique adéquat. De plus, nous avons pu nous rendre compte de la difficulté que peut rencontrer un informaticien à se familiariser avec des articles juridiques souvent écrits de manière peu pédagogique. Même si l'on s'efforce, à l'heure actuelle, de traiter l'aspect légal des problèmes soulevés par le commerce électronique, force est de constater qu'il reste encore un long chemin à parcourir.

Comme nous l'avons déjà signalé, la personnalisation de sites Web offerte au client soulève nombre d'inquiétudes et d'incertitudes au niveau éthique. En effet, les techniques utilisées, souvent à l'insu de l'utilisateur, pourraient réduire à néant tous les efforts consentis pour fournir un environnement propice au respect de la vie privée. Ici aussi un travail important reste à faire pour informer l'internaute et lui permettre, en quelque sorte, de gérer facilement les informations qu'il désire, ou non, mettre à disposition du réseau.

Enfin, l'envers du décor, le miroir physique de ces multiples points de vente virtuels ne laisse pas non plus indifférent. Avec la mise en place d'une lourde logistique pour livrer les achats, dont le prix est souvent à charge du consommateur, il faut s'interroger sur le coût indirect que la communauté aura à payer. En effet, l'augmentation du trafic routier engendré par le commerce électronique et ses moyens de livraison rapide n'améliorera nullement les problèmes de pollution et de circulation de nos routes déjà encombrées. Il risquent au contraire d'accentuer leurs dégradations.

Nombreuses encore sont donc les questions qui conditionnent le développement du commerce électronique tant au niveau mondial qu'au niveau européen et belge en particulier. De plus, pour l'avoir côtoyé au États-Unis pendant quelques mois, nous pouvons sans aucun doute affirmer que l'engouement américain face au commerce électronique n'est pas encore au goût du jour en Europe. Mais les conditions suffisantes nous semblent réunies pour nous convaincre que, même s'il reste encore pas mal de travail à fournir, le commerce électronique a toutes les chances de devenir, dans un avenir proche, en Europe, *monnaie courante*.

Bibliographie

[ANTOINE 98]
ANTOINE Mireille, Gobert Didier, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des Autorités de Certification", Revue Générale de Droit Civil, n° 4, Septembre 1998, pp. 285 à 310

[BADOT 98]
BADOT P., DETEZ V., *Vers un corpus générique de règles ergonomiques validées pour la création de sites Web*, FUNDP, Namur, 1998

[BASLE 98]
Basle Committee on Banking Supervision, *Report on Risk Management for electronic banking and electronic money activities*, Basle, Mars 1998, p. 3

[CAPRIOLI 98]
CAPRIOLI E.A., "Sécurité et confiance dans le commerce électronique: signature numérique et autorités de certification", La semaine juridique, Éditions Générale, n° 14, Avril 1998

[COM 97]
Rapport COM (97) 157, *Une initiative européenne dans le domaine du commerce électronique*, Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, 15 Avril 1997

[COURET et alii 95]
Couret et alii, 1995, cité mais non référencé dans [POULLET]

[DATA 99]
DATANews, n° 22bis, 5 Juillet 1999, p. 7

[DESIGN]
http://www.designmaker.com/tools/tagmaster/metarank.htm

[DINANT]
DINANT Jean-Marc, "Les traitements invisibles sur Internet"

[ECONOMIST 98]
"Who will deal in dealerships?", The Economist; 14 Fevrier 1998

[FONTAINE 87]
FONTAINE M., "La preuve des actes juridiques et les techniques nouvelles", La preuve, Colloque UCL, 12 et 13 Mars1987

[FORRESTER]
Forrester Research in
http://www.forrester.com/ER/Research/Report/MarketOverview/0,1338,5673,FF.html

[FORRESTER 97a]
Forrester Research in "Cybersex", The Economist, 4 Janvier 1997

[FORRESTER 97b]
Forrester Research, "Report predicts strong grows in e-business", 1997

[GARTNER 98]
Gartner Consulting, *SET Comparative Performance Analysis*, Gartner Group, 2 Novembre 1998

[GHOSH 98]
GHOSH Anup K., *E-Commerce Security: Weak Links, Best Defenses*, John Wiley & Sons, 1998

[GOBERT 98]
GOBERT Didier, "Signature électronique et autorités de certification: la levée des obstacles au développement du commerce électronique", Revue Ubiquité, n° 1, FUNDP, Namur, Novembre 1998, p. 79 et s.

[GUIDE 98]
Visa, ClearCommerce, Shop.org, *The e-Guide*, 1998

[HUBIN 95]
HUBIN J, *La Sécurité Informatique*, Notes du cours "Sécurité et fiabilité des systèmes informatiques" du professeur RAMAEKERS J. mises à jour par GOSSENS P. en 1995.

[ICRI 97]
ICRI, *Les défis de la société de l'information et les missions de la Justice, Partie II: Le droit de la preuve face aux nouvelles technologies*, K.U.Leuven, Janvier 1997

[IDC 98]
Intrnational Data Corporation in Inside Internet, n° 19, Décembre 1998, p 48

[INSIDE 98]
Inside Internet; n° 19, Décembre 1998, pp 31 à 33

[KEHOE 98]
KEHOE Louise, "High Street in Hyper Space", Financial Times, 11 Avril 1998

[KOSIUR 97]
KOSIUR David, *Understanding Ellectronic Commerce*, Microsoft Press, 1997

[LARRIEU 98]
LARRIEU J., "Les moyens de preuve: pour ou contre l'identification des documents informatiques et des écrits sous seing privé", Cahier Lamy Droit de l'Informatique, H88, 1998, p. 9

[LECLERCQ 83]
LECLERCQ J.F., "Essai de solution d'une adaptation du régime des preuves en droit privé", Unité et diversité du droit privé, Bruxelles, ULB, 1983, p.350 et s.

[LIPS et al. 98]
LIPS Benoît, MAQUA Agnès, FOLON Jacques, VILLARS Dominique, ... *du numérique au multimédia*, Région Wallonne, Namur, 1998

[LORENTZ 98]
LORENTZ Francis, "Le commerce électronique, une révolution?"; Revue politique et parlementaire, Mai/Juin 1998

[MARGHERIO 98]
MARGHERIO Lynn, HENRY Dave, COOK Sandra, MONTES Sabrina, "The Emergency Digital Economy", US Department of Commerce, Washigton DC, Avril 1998

[MONTERO]
MONTERO Étienne, *Informatique et droit: le commerce électronique sur Internet*, Notes de cours provisoires, FUNDP, Namur, p. 11

[OCDE]
OCDE, http://www.oecd.org/dsti/sti/it/ec/

[OCDE 97]
OCDE; "Web casting and convergence: policy implication", 1997

[OCDE 99]
OCDE, "The Economic and Social Impact of Electronic Commere", Fevrier 1999

[OII 98]
Open Information Interchange, "OII guide to electronic payment", http://www2.echo.lu/oii/en/e-pay.html, Mars 1998

[ONU 97]
Guide pour l'incorporation dans le droit interne de la loi type de la Commission des Nations Unies pour le Droit Commercial International sur le commerce électronique, 12 Mars 1997, p.16.

[PETIT 98]
PETIT Ludmilla, DE VYLDER Alexandra, "Monnaie électronique et libertés individuelles: la carte Proton", Revue Ubiquité, n° 1, FUNDP, Namur, Novembre 1998, p. 29 et s.

[PEREZ 99]
PEREZ DE LEMA Mercedes, ESCALANTE Ana, PRAT Ainhoa, *Analyses des aspects et des outils automatiques de vérification qui confèrent de la qualité à un site World Wide Web*, FUNDP, Namur, 1999, p. 15

[POULLET]
POULLET Yves, "Quelques considérations sur le droit du cyberspace", FUNDP, chap. 1, p. 1 et s.

[RANDOLPH 98]
RANDOLPH, "Dell's Magic Formula", http://www.wired.com/, 28 Mai 1998

[RICHMOND]
RICHMOND Alan, "META Tagging for Search Engines", http://www.stars.com/Search/Meta/Tag.html

[SCHNEIER 96]
SCHNEIER Bruce, *Applied Cryptography*, John Wiley & Sons, 1996

[SET 97]
SET Secure Electronic Transaction Specification, Book 1: Business Description, Version 1.0, 31 Mai 1997

[STERNE 99]
STERNE Jim, *World Wide Web Marketing, Integrating the Web in Your Marketing Strategy*, second edition, Wiley Edition, 1999

[SYX 82]
SYX D., *Aspects juridiques du mouvement électronique de fonds*, K.B., 1982, p. 79

[TRUDEL 96]
TRUDEL P., PARISIEN S., *L'identification et la certification dans le commerce électronique*, Éditions Yvon Blais, Quebec 1996, p. 127 et s.

[VEREYDEN 91]
VEREYDEN-JEANMART N., "Droit de la preuve", Précis de la Faculté de Droit de l'Université Catholique de Louvain, Bruxelles, Larcier, 1991

[VILLARS 99]
VILLARS Dominique, "Des bandeaux controverses", Cyber Cahier de la Libre Belgique, 24 Juillet 1999, p. A