

Avril 2007



Performance.  
Everyday.

## Dossier n° 2 Le paiement en ligne

*Contact*

Hicham Abbad : 01 49 44 35 27 / [habbad@klb-group.com](mailto:habbad@klb-group.com)

[www.klb-group.com](http://www.klb-group.com)

Tél. : +33(0)1 49 44 35 00 • Fax : +33(0)1 49 44 35 01 • 2, rue Paul Cézanne F-93364 Neuilly-Plaisance Cedex  
Société anonyme au capital de 53 250 euros RCS Bobigny - N° SIRET 402 994 438 00032

# Sommaire

I. Qu'est ce qu'un service de paiement sécurisé en ligne ? .....	3
Le paiement en ligne .....	3
Le principe d'un paiement sécurisé.....	4
II. Le cryptage.....	4
SSL .....	4
Fonctionnement de SSL.....	4
Les certificats .....	6
III. Les systèmes préconisés par les banques .....	7
- SET .....	7
- La particularité française : le C-SET et le SET BO .....	7
IV. Les solutions de paiement en ligne disponibles en France : .....	8
V. La législation .....	8
La prédominance de la preuve écrite.....	8
L'avancée législative .....	9
La preuve et la signature électronique .....	9
VI. Les conséquences législatives sur le paiement en ligne .....	9
Le paiement par CB.....	9
Le paiement on line .....	9
VII. CONCLUSION .....	10

Dans le dossier précédent (E procurement), nous avons pu constater combien Internet pouvait modifier le travail des acheteurs. Les commandes en ligne apparaissent comme le meilleur moyen d'optimiser le processus d'achat. Les nouvelles technologies permettent alors de régler celles-ci par un moyen de paiement électronique qui diminue le coût de gestion des factures et qui s'inscrit totalement dans cette démarche d'optimisation du processus.

Pourtant, les entreprises comme les particuliers sont encore réticents à payer via Internet pour de multiples raisons :

- Tout d'abord au niveau législatif, la France a pris du retard : la loi pose problème quant à la légalité des documents échangés.
- Puis se pose la question légitime de la sécurité des transactions électroniques : Le Groupement d'Intérêt Economique des cartes bancaires (GIE) déclare que plus de 60% des fraudes se font sur Internet !
- Et bien sûr l'actualité qui étale l'impuissance du GIE face à un ingénieur qui pénètre le système que l'on croyait si protégé !

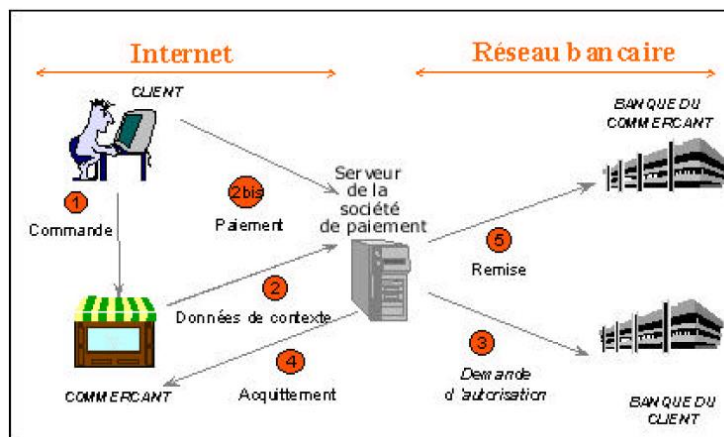
Peut-on alors faire confiance aux paiements en ligne alors que notre carte à puce donne des signes de faiblesse ? Quelles sont les méthodes pour sécuriser les transactions ? La législation s'adapte t'elle à l'évolution des techniques ?

Dans ce dossier, nous essayerons de vous donner un bref aperçu des acteurs du paiement en ligne, de leur moyen de sécurisation des transactions et des nouveautés juridiques françaises afin que vous puissiez évaluer par vous-même la fiabilité de ce nouveau moyen de paiement.

## I. Qu'est ce qu'un service de paiement sécurisé en ligne ?

### Le paiement en ligne

Actuellement sur le Web, le système de paiement le plus élémentaire consiste, pour un client, à fournir le numéro de sa carte de crédit avec sa date de validation au moment où il passe la commande. Pour que le système fonctionne, des sociétés de paiement en ligne s'inscrivent en interface entre vous et le fournisseur. Elles se chargent de vérifier le numéro de la carte, les listes d'opposition pour perte ou vol, l'obtention d'un numéro d'autorisation auprès du Centre d'autorisation Carte bancaire et de procéder à l'encaissement puis au crédit en compte de la transaction réalisée sur Internet.



**Ce service est payant. Plusieurs solutions sont proposées :**

- Un contrat de VAD (Vente à Distance) peut être signé avec la banque et la société de paiement en ligne se rémunère par un forfait par validation ou par une location mensuelle.
- Quand il n'y a pas de contrat VAD, la société de paiement se rémunère au pourcentage du CA généré sur le site.

Attention, toutes les sociétés de paiement en ligne ne fournissent pas les mêmes services. Certaines vérifient seulement la validité de la CB utilisée sans s'occuper de la transaction qui est à la charge du vendeur par son propre terminal de paiement (TPE). De même, en fonction du trafic généré sur le site, il est possible de négocier des tarifs plus adaptés.

## **Le principe d'un paiement sécurisé**

**En fait, pour sécuriser la transaction, la société doit assurer 4 principes :**

- La confidentialité : le contenu de votre transaction n'est accessible que par les deux parties concernées, l'acheteur et le vendeur.
- L'authentification : vous êtes sûr de l'identité du correspondant
- L'intégrité : aucune modification ne peut être faite pendant le transfert
- La non-répudiation : personne ne peut nier avoir participé à cette transaction.

La transaction doit donc être cryptée pour que la sécurité soit maximale.

## **II. Le cryptage**

### **SSL**

Aujourd'hui la solution la plus répandue pour sécuriser les transactions est le SSL (Secure Socket Layer, créée par Netscape).

Son succès s'explique par sa simplicité d'utilisation et par son intégration dans tous les navigateurs du marché.

SSL est un protocole de communication d'information qui permet d'assurer l'authentification, la confidentialité et l'intégrité des données échangées.

Les données à protéger sont constituées des informations concernant la CB et la transmission des données. Il utilise un moyen de cryptographie reconnu : l'algorithme à clé RSA.

SSL effectue la gestion des clés et l'authentification du serveur avant que les informations ne soient échangées.

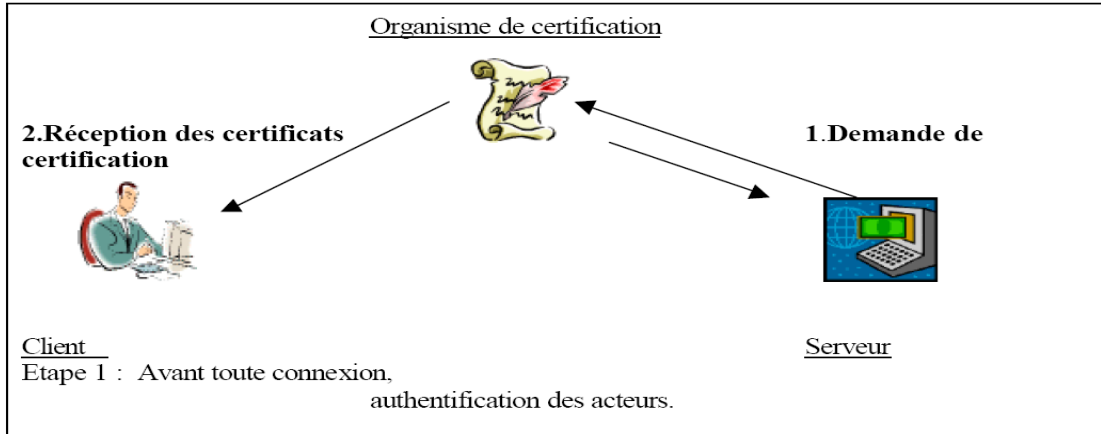
### **Fonctionnement de SSL**

**SSL fonctionne en trois étapes :**

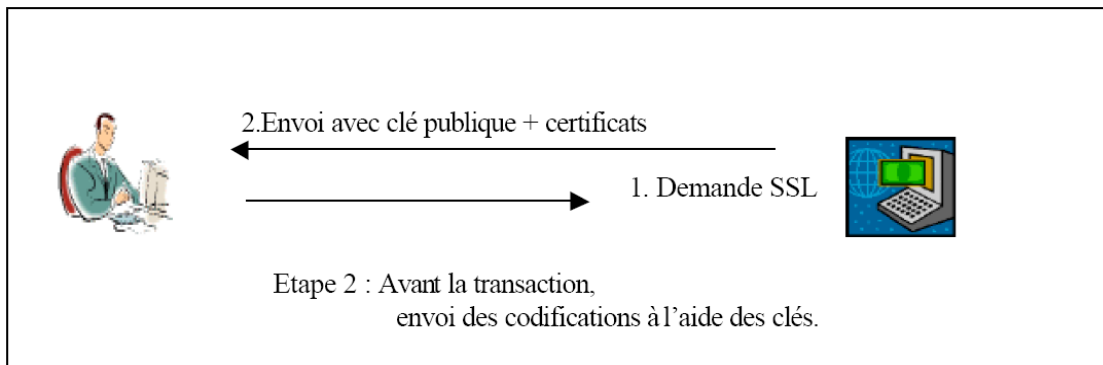
- 1- Authentification des acteurs à l'aide de certificats
- 2- Envoi des clés publiques. Une clé publique est une clé qui permet de coder un message. Il lui est associé une clé privée. Seul le propriétaire de la clé privée peut décoder le message codé avec la clé publique.
- 3- Envoi des informations codées.

Ces trois étapes sont décrites dans les schémas ci-dessous.

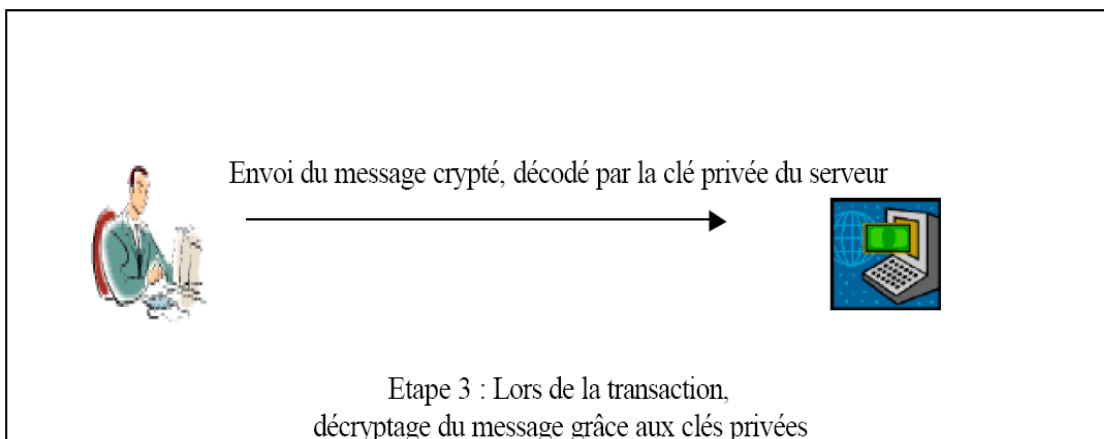
Schéma dans le cas où la société, seule, demande un certificat :



- a- Le serveur demande à être certifié par un organisme.
- b- Les navigateurs contiennent une liste d'organismes fiables.



Le serveur gère une paire de clés publiques/privées. Le logiciel client demande au logiciel serveur de lui fournir sa clé publique. Le certificat permet au logiciel du client de reconnaître de manière sûr l'identité du serveur.





Performance.  
Everyday.

Les informations du client sont aussitôt cryptées avec la clé publique du serveur et transmises au serveur. Le serveur décode le message avec sa clé privée. Il envoie ensuite au logiciel client une confirmation du bon déroulement de l'opération.

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

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

## Les certificats

Un certificat est un document électronique qui atteste qu'une clé publique est bien liée à une organisation ou à une personne. Il permet la vérification de la propriété d'une clé publique pour prévenir la contrefaçon de clés publiques. Un certificat contient généralement une clé publique, un nom ainsi que d'autres champs pour identifier le propriétaire, une date d'expiration, un numéro de série, le nom de l'organisation qui contresigne le certificat et la signature elle-même. Le format des certificats est défini par la norme X509.

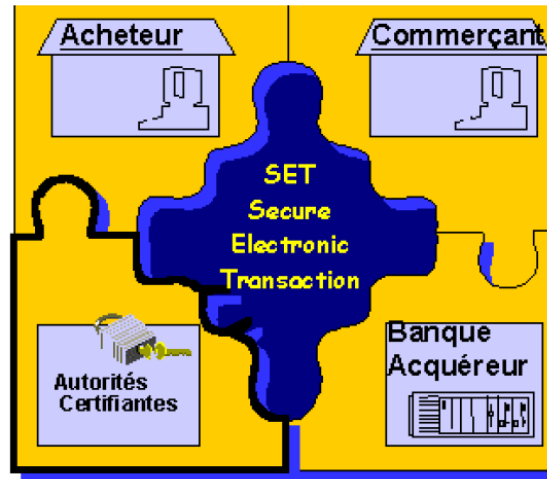
Le certificat doit être généré par un tiers de confiance. L'organisme certificateur donne la crédibilité au certificat.

Il existe deux types de certificats utilisés avec SSL : pour serveur et pour client. Un certificat coté client sert à identifier un utilisateur, il contiendra donc des informations sur cet utilisateur. Coté serveur, le certificat a pour but d'authentifier le serveur et l'organisme qui l'exploite. C'est ce type de certificat dont vous avez besoin pour mettre en place un serveur sécurisé HTTPS.

### III. Les systèmes préconisés par les banques

L'avantage du SSL est d'être un protocole indépendant, il peut donc s'inscrire dans d'autres protocoles plus élaborés. Les banques par exemple, l'utilisent à l'intérieur de leurs propres protocoles de sécurisation : le SET, le SET BO' et le C-SET.

#### - SET



SET est un ensemble de spécifications publiques promues par VISA, MASTERCARD, Microsoft, IBM, HP et Oracle. Le protocole SET permet de rendre les paiements sur les réseaux ouverts comme Internet et d'authentifier les acteurs tout en préservant la confidentialité des données.

A terme, pour les cartes à puce, le standard EMV (pour Eurocard, Mastercard, Visa) est appelé à définir la norme.

#### - La particularité française : le C-SET et le SET BO

Autour du projet standard SET gravitent en France deux projets concurrents, tenant compte de l'existant des cartes à puce françaises : SET BO' et C-SET.

Le GIE a donc mis en place les standards BO et C-SET en attendant un standard EMV, c'est à dire une carte à puce deuxième génération.

##### *LE BO'*

Le BO regroupe la Société Générale, la BNP, le crédit Lyonnais et VISA.

##### *C-SET*

Le consortium C-SET regroupe le Crédit Agricole, le Crédit Mutuel, les Banques Populaires, La Poste, Europav International. C-SET est la condition de sécurité posée par les établissements financiers pour offrir aux commerçants une garantie de paiement.

Cette solution présente un plus fort potentiel en Europe qu'aux USA où la carte à puce est inexistante (Allemagne 40 millions de carte, France 25, Pays Bas 10, Belgique 10).

## IV. Les solutions de paiement en ligne disponibles en France :

**Télécommerce (France Telecom)** <http://www.telecommerce.com> Télécommerce est une plate-forme prenant en charge tous les aspects d'une transaction commerciale sur un site (authentification, formulaire commande, paiement sécurisé,..). Abonnement + commissions sur les ventes.

**Payline** <http://www.payline.com> Payline assure le traitement des transactions cartes bancaires sur Internet. La saisie du numéro de carte s'effectue sur le site sécurisé de Experian. La facturation s'effectue à la transaction en fonction du volume de transaction.

**Cyber Card (Europay)** <http://www.cybercard.tm.fr> Europay qui regroupe des banques et des prestataires propose une solution de paiement en ligne basée sur la procédure C-SET (carte à puce + SET). L'expérimentation devait concerner 10 000 internautes en 1998.

**SIPS d'Atos** <http://galilee.sat.sligos.fr:sips.html> SIPS qui signifie Service Internet de Paiement Sécurisé est proposé par Atos résultat de la fusion de Sligos et d'Axime. SIPS assure un paiement sécurisé par cartes en francs et en devises ainsi que par le système Cybercash.

**CyberMut** [www.creditmutuel.fr](http://www.creditmutuel.fr) Le Terminal de Paiement Electronique (TPE) est un terminal dématérialisé conçu par le Crédit Mutuel. Ce TPE virtuel est basé sur la technologie de paiement sécurisé SSL.

**e-COMM** <http://www.e-comm.fr> E-COMM est un consortium d'entreprises crée en 1996 pour élaborer une nouvelle procédure de sécurisation des paiements par carte sur Internet. Le projet consiste à combiner l'utilisation d'une carte à puce avec le procédé SET. Le système nécessite donc un lecteur de carte connecté à l'ordinateur.

**MilliCent (Digital)** <http://www.millicent.digital.com> Millicent est une solution de micropaiement développée par Digital. Elle est destinée essentiellement à l'achat numérique en ligne (informations, livres en ligne, jeux, musique, etc...) et correspond à des montants allant de quelques cents à quelques dollars.

## V. La législation

### La prédominance de la preuve écrite

Le retard de la France sur l'utilisation d'Internet est dû en partie à une législation française peu adaptée à l'utilisation de l'information électronique.

En effet, le droit français se caractérisait, en matière civile, par la prédominance de la preuve littérale, c'est à dire par écrit, elle-même assimilée au support papier. Le Code Civil obligeait les deux parties à rédiger un écrit pour tout engagement supérieur à 5000F. Cette exigence a freiné l'utilisation des documents électroniques.

## L'avancée législative

Internet ne peut se développer que seulement si la loi reconnaît la valeur des documents électroniques. Il était donc nécessaire de légiférer sur une preuve qui ne serait plus écrite mais virtuelle.

Le gouvernement français a fait en mars 99 la proposition de loi n° 243 qui vise à reconnaître la valeur probatoire d'un message électronique s'il est identifiable par une signature électronique fiable et si la conservation durable du message, sous le contrôle du signataire, est assurée.

### La preuve et la signature électronique

Le projet de loi "Droit de la preuve et signature électronique" a été présenté en conseil des ministres en septembre 99 puis adopté devant l'assemblée et sera présenté au sénat en février 2000.

En voici un extrait validant la modification de la preuve :

" Art. 1316. - La preuve littérale ou par écrit résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission."

Cette loi, consistant à reconnaître la valeur juridique du document et de la signature électronique, sera donc promulguée dans les mois à venir. Elle modifierait la notion de preuve littérale pour la rendre indépendante du support utilisé.

## VI. Les conséquences législatives sur le paiement en ligne

### Le paiement par CB

Dans la vie courante, si un magasin vous prélève un montant par erreur via un échange carte bleue, vous devez apporter la preuve de l'erreur, ce qui est souvent très compliqué. Le paiement en ligne, lui, protège le client.

### Le paiement on line

En effet, la législation de ce type de paiement rentre dans le champ d'action de la VPC. Le peut toujours faire l'objet de la part du porteur de la carte d'une opposition (principe de répudiation de la transaction).

Si vous avez acheté sur Internet ou si quelqu'un a utilisé votre numéro de carte de façon frauduleuse, vous avez toujours la possibilité de refuser le paiement. Si vous vous apercevez d'une erreur plusieurs mois après le débit, et que vous estimez avoir été trompé, un simple appel à votre banque, et votre compte sera crédité du montant litigieux. Bien souvent quelques jours suffisent. C'est la règle !

## VII. CONCLUSION

Nous avons pu constater que la France, comme la plupart des pays Européens, se prépare à régler ses achats via Internet : la loi a été modifiée afin de rendre les documents électroniques légaux, des standards de sécurisation sont élaborés pour protéger les échanges et les utilisateurs restent protégés en cas de fraudes.

Pourtant, le système on line ne propose encore pas les caractéristiques rassurantes que l'on voudrait bien y trouver :

- Les acteurs apparaissent encore désorganisés : les standards de sécurisation ne sont pas unifiés.
- Le marché n'offre pas une stabilité suffisante pour que le monde de l'entreprise opte sans réticence : Kleline, par exemple, qui assurait le paiement en ligne de certaines grandes sociétés vient de fermer laissant ses clients finir leur contrat.
- Pour le moment, le volume des échanges est négligeable. En 98 le commerce électronique représentait en France 300 MF mais son développement rapide (5500 M\$ en Europe en 2000) suscite déjà l'engouement des pirates.

Avec le développement des sites d'achats sur Internet, le paiement on line apparaît comme un mode de paiement d'avenir mais, pour le moment, son utilisation est encore un peu prématurée pour les entreprises qui veulent de la fiabilité.

NM.