Solutions de paiement électronique

Antonin CHAZALET : Chazalet@imag.fr

M2PGI 04-05

Résumé :

Ce document traite du paiement électronique, c'est à dire des moyens mis en œuvre pour effectuer une transaction financière par le biais d'Internet. Ce type de transaction est, depuis plusieurs années, en forte augmentation. Cet essor est du aux faits, qu'un internaute possédant une carte bleue est un client potentiel, que les produits sont disponibles, à l'achat, 24h/24 et que les coûts associés aux produits sont réduits.

Néanmoins, de telles transactions, n'étaient pas, à leur mise en place, très bien perçues par le public. Or, de plus en plus, avec la démocratisation d'Internet, des systèmes de préservations des données dans la quasi-totalité des navigateurs Web et avec une « confiance collective », beaucoup de clients potentiels deviennent des clients effectifs.

Mots clés :

Paiement électronique, SSL, SET, sécurité, authentification, architecture de paiement électronique.

Table des matières :

1 Introduction

2 Partie 1 : Les solutions existantes

3 Partie 2 : Protocoles utilisés/utilisables

4 Conclusions et Perspectives

5 Bibliographie

1 Introduction :

Le paiement électronique est actuellement un type de transaction très bien implanté et utilisé par une majorité de personne ou entreprise ayant accès à Internet. Nous allons nous attacher à voir quelles solutions existent et surtout quelles solutions sont utilisées.

2 Partie 1 : Les solutions existantes :

Il existe six grandes sortes de solutions :

- La première est la transaction SSL sans intermédiaire.

Le marchand doit signer avec une banque un contrat de vente à distance (VAD) et il doit acquérir un terminal de paiement électronique (TPE). Il s'occupe du rapatriement des informations bancaires du client, qui sont stockées sur son serveur. Il doit saisir en mode manuel le montant à débiter sur le compte du client, via son TPE. Le marchand est autonome, il gère son propre site, mais en contre partie, il doit être fortement compétent en informatique. De plus il est le seul garant du bon déroulement du paiement. Enfin, il doit acheter un certificat SSL ou négocier celui d'un consortium.

- La seconde est la transaction SSL via un organisme bancaire.

Pour cela, le marchand doit sélectionner une solution bancaire et signer avec la banque un contrat de VAD avec location d'un TPE virtuel. La gestion des paiements se fait via l'extranet mis à disposition par la banque. Le marchand et le client sont en sécurité, l'organisme bancaire assure aux deux parties le bon déroulement du paiement. Le marchand n'a pas besoin d'acheter de certificat SSL.

- La troisième est la variante SSL sans intermédiaire.

Le marchand doit s'affilier à un serveur façade Web, il doit récupérer lui-même les coordonnées bancaires du client sur la base de donnée cryptée du serveur, il doit être formé à la récupération des informations de la base de donnée et il doit posséder un TPE. Par contre, il ne s'occupe ni du site, ni de la partie Web du paiement électronique. Mais il doit cependant entrer lui-même les coordonnées bancaires du client sur son TPE, pour effectuer le paiement proprement dit.

- La quatrième est la variante SSL Booking.

Ce système de transaction comporte des similitudes avec les systèmes de réservation. Le paiement effectif se fait lorsque le client passe chez le vendeur. Ce système est fonctionnel puisque le non respect du contrat par le client entraîne la transmission des coordonnées bancaires du serveur au marchand et ce dernier encaisse alors un dédommagement.

Ce système permet au client d'avoir une large offre, des prix très avantageux et un système de réservation rapide et disponible en permanence. Il permet aussi au marchand d'accroître sa visibilité, de plus l'« informatique » est délégué à l'entreprise hébergeante et le marchand est assuré de percevoir le paiement ou un dédommagement. Du point de vue du booker, il vend une technologie générique, il est intéressé aux transactions et il se positionne sur un nouveau marché prometteur (en effet, actuellement, un marchand ne cherche pas à se former à l'informatique, mais il cherche à pouvoir utiliser l'informatique comme moyen d'augmenter, à moindre coût et de manière significative, son chiffre d'affaire).

- La cinquième est la transaction par micro paiement.

Du point de vue du client : il faut qu'il crée d'un compte client dans une banque virtuelle (en ligne), qu'il l'alimente via virement et/ou carte bleue, qu'il effectue ses paiements via son compte en ligne grâce à un identifiant.

Du point de vue du vendeur, il faut qu'il crée un compte marchand dans une banque virtuelle (en ligne). Cette banque s'occupe des paiements, elle permet à ses clients de consulter leurs transactions en temps réel (latence ≤ 1 seconde), elle effectue automatiquement les virements du compte marchand en ligne au compte bancaire physique du marchand et elle prélève une commission de la forme $0,25 + 0,03 * \text{montant_achat}$ (en €).

- La sixième sorte est la transaction SET (Secure Electronic Transaction).

Cette transaction suit quatre grands principes, tout d'abord, le client et le marchand doivent avoir un certificat (délivré par une "autorité habilitée"), ensuite, le marchand ne voit aucune information de paiement, troisièmement, l'organisme de cartes de crédit ne voit aucune information relative à la commande et enfin la banque ne communique qu'avec l'organisme de cartes de crédit. D'un point de vue théorique, SET est la solution toute indiquée pour les e-paiements, malheureusement, il est relativement lourd à mettre en place, du fait des certificats à délivrer/posséder.

3 Partie 2 : Protocoles utilisés/utilisables :

Nous allons voir maintenant deux protocoles qui peuvent être utilisés pour le e-paiement. Ce sont les protocoles SSL et SET.

- Secure Socket Layer (SSL)

C'est un protocole général qui est destiné à sécuriser un échange client serveur (confidentialité, authentification). Il est utilisé dans plus de 95% des e-paiements. L'entreprise Netscape est à l'origine de ce protocole.

Ce protocole est un protocole d'échange de données, il assure la confidentialité des échanges entre 2 applications, ainsi que l'authentification des serveurs. Il est utilisé en particulier pour HTTP.

Il utilise RSA (clé publique) pour échanger des clés DES (secrètes), il ne fournit pas de garantie contre le déni, il authentifie un navigateur, non une personne. SSL comporte un protocole de négociation (choix clés) et un protocole d'échange (chiffré par DES). SSL est une couche entre au dessus HTTP et au dessous TCP/IP.

- Secure Electronic Transactions (SET)

C'est un protocole spécialisé pour les paiements : SET destiné à sécuriser les paiements par carte bancaire (confidentialité, authentification, intégrité, non déni). Ce protocole, malgré sa très bonne conception, est actuellement abandonné.

Les consortiums bancaires Visa et MasterCard ainsi que d'autres entreprises comme IBM, Microsoft et Netscape sont à l'origine de SET.

La spécification de SET est publique et gérée par un consortium.

Ce protocole a pour objectif d'assurer le paiement par carte bancaire sur l'Internet, avec garanties de confidentialité, intégrité de données, authentification du client et du fournisseur et non déni pour le client et le fournisseur.

4 Conclusions et Perspectives :

L'utilisation du e-paiement est toujours en plein boom, en l'espace de dix années, le flux monétaire échangé par ce moyen a été au moins multiplié par un facteur 300 (de 14M€ en 1994 à plusieurs milliards d'euros en 2004). Ce boom s'explique en grande partie par la démocratisation de l'accès à Internet et parce que les internautes ont confiance dans le système de e-paiement actuel (via SSL).

Qui plus est, la VAD et la VPC par Internet sont très appréciées des clients. Ces types de vente permettent l'anonymat, des tarifs très compétitifs et donc toujours plus bas, des comparaisons aisées, la possibilité de commander à toute heure du jour ou de la nuit, l'absence de déplacement et la livraison à domicile et le fait que ces types de vente soient très bien encadrés par la loi joue aussi un rôle important dans le succès du e-paiement. Les marchands, quant à eux, trouvent aussi leur compte dans la vente par Internet, en effet, ils n'ont plus besoin ni de locaux bien situés, ni de vendeurs, ce qui augmente d'autant plus leur bénéfice. Mais ils ont besoin de bien faire référencer leur E-Magasin et la gestion du stock et de la distribution prend une grande place dans l'organisation du E-Magasin.

A l'image de nos supermarchés, de amazon.com ou fnac.com, il paraît très probable que, dans les années à venir, nous voyons apparaître de plus en plus de E-Supermarchés.

5 Bibliographie :

- Sacha Krakowiac, Sécurité de systèmes répartis, cours,
<http://sardes.inrialpes.fr/people/krakowia/Enseignement/M2P-GI/Flips/10b-securite.pdf>
- TPE VIRTUEL : <http://www.paybox.com>
- <http://www.paiement-securise.org/boutique/catalog/paiement-securise.php>
- PAYPAL <http://www.paypal.com/fr>
- SSL <http://home.netscape.com/security/techbriefs/ssl.html>
- SET <http://www.setco.org>