Le cryptage SSL

La sécurité de Sogenactif repose sur l'utilisation du protocole de cryptage SSL (Secure Socket Layer).

Cette technologie, qui utilise une clé de cryptage à 128 bits, est le protocole le plus utilisé dans le monde (plus de 80% des sites marchands utilisent SSL).

Il est compatible avec la quasi-totalité des navigateurs.

Son rôle est basé pour l'essentiel sur :

- le scellement des informations relatives à la transaction entre votre site et votre client, sans que celui-ci ait à télécharger ou activer un logiciel supplémentaire

- le transport crypté du numéro de carte de votre client vers le serveur de paiement

- le stockage protégé des informations relatives à la transaction et au paiement sur le serveur de paiement Sogenactif

- une demande d'autorisation systématique avec blocage immédiat de la transaction émanant de toute carte inexistante, perdue ou volée, signalée par le porteur à sa banque

Sa mise en œuvre technique nécessite l'installation d'une interface applicative dite API (Application Program Interface), qui réalise les différentes fonctions de paiement ou d'interrogation au serveur Sogenactif :

- le téléchargement des API se fait directement en ligne à partir de votre extranet Sogenactif

- l’API doit être intégrée sur votre site marchand, par une personne ayant la maitrise de serveur http et de l'écriture de scripts CGI.

Le dispositif 3D Secure

Qu'est-ce que 3D Secure ?

3D Secure est un programme créé par les émetteurs internationaux Visa (Verified By Visa) et Mastercard (Mastercard Secure Code) afin de renforcer la sécurité des paiements en ligne. Il repose sur la mise en place d'un contrôle supplémentaire lors d’un achat en ligne : en complément des données bancaires, l’acheteur est invité à saisir une donnée personnelle permettant à sa banque de l’identifier et de valider l’opération.

Il ne s’agit pas d’une garantie de paiement mais d’un dispositif sécuritaire visant à réduire le risque d'impayé émis pour contestation du porteur.

Depuis le 1er octobre 2008, le programme 3D Secure est disponible pour les transactions françaises. Il s’applique donc aux porteurs français, détenteurs d’une carte «CB» ou «agréée CB», qui effectuent des achats sur un site marchand français.

Ce dispositif s'accompagne d'une évolution réglementaire appelée "liability shift" ou "transfert de responsabilité"; dont le principe est de faire supporter le risque d'impayé émis pour contestation du porteur à la banque de celui-ci et non plus au commerçant, si le porteur a validé son paiement en renseignant sa donnée personnelle, que sa banque a validé cette authentification et que le commerçant a respecté les mesures de sécurité énoncées dans les conditions générales de vente de son contrat Sogenactif.

Quel est le fonctionnement de 3D Secure ?

Les principales étapes d’une transaction 3D Secure :

1 - L’internaute effectue un achat sur un site Internet 3D Secure.

2 - Au moment du paiement, le MPI(1) installé sur le site du commerçant 3D Secure interroge, via les réseaux Visa et MasterCard, la banque de l’internaute.

3 - La banque de l’internaute demande à ce dernier de s’authentifier.

4 - L’internaute saisit les coordonnées de sa carte bancaire et une donnée personnelle (ex. date de naissance, Code Sécurité à usage unique).

5 - Après validation de cette saisie par l’internaute et accord de la banque de ce dernier, la banque de l’acheteur transmet un accord au commerçant pour poursuivre la procédure de paiement.

6 - Le commerçant transmet alors à la banque de l’acheteur une demande d’autorisation via la Société Générale et intègre ainsi le circuit classique de compensation bancaire.

(1) MPI : « Merchant-Plug-in ». Ce logiciel, indispensable pour la mise en place du programme 3D Secure, est installé par le prestataire technique de la solution Sogenactif, ATOS Worldline Worldline.

Quelles sont les méthodes d'authentification ?

Les méthodes d'authentification sont propres à chaque banque.

Depuis la fin 2010, sous l'impulsion de la Banque de France, toutes les banques françaises ont équipé leurs porteurs d'une méthode d'authentification forte. Si un porteur ne dispose pas de code d'authentification, il doit se rapprocher de sa banque.

Quels sont les avantages de ce dispositif ?

3D Secure présente de nombreux avantages, tant pour votre activité que pour vos clients :

- Pour votre site marchand : diminution de la fraude et des impayés ainsi que le transfert de responsabilité des impayés pour contestation de l'acheteur vers la banque de celui-ci.

- Pour vos clients : renforcement de la confiance dans le paiement en ligne par des méthodes d'authentifications renforcées, spécifiques à chaque banque.

Par ailleurs, il n'y a pas de surcoût à la mise en place de ce dispositif sur votre site marchand.

Quel est le périmètre de 3D Secure ?

Le programme 3D Secure ne concerne que les paiements à l'acte sur Internet effectués par une carte bancaire Visa ou MasterCard. Ne sont pas concernés, pour le moment, les paiements :

- récurrents,

- fractionnés (le premier paiement est 3D Secure),

- de vente à distance classique (téléphone, courrier…),

- créés directement par le commerçant sur un outil de back-office (création, duplication de transactions) puisque le porteur n'est pas présent.

A ce jour, le transfert de responsabilité ne concerne pas les cartes American Express, JCB, Franfinance, privatives, cartes commerciales hors zone euro des réseaux Visa et MasterCard (ex : cartes professionnelles et affaires).

Le programme PCI-DSS

Payment Card Industry -
Data Security System

Les banques sont soumises au programme PCI-DSS pour « Payment Card Industry – Data Security System » (Industrie des cartes de paiement - Système de sécurité des données), lancé par Visa et Mastercard en novembre 2004.

Ce programme établit des règles standards visant à assurer la sécurité des données des transactions sur Internet, pour tous les acteurs du commerce électronique.

Il vise à renforcer la sécurité des données des transactions sur Internet, notamment pour éviter les vols de fichiers comportant des numéros de carte.

Il établit des règles standards qui s'imposent à tous les acteurs du commerce électronique (par exemple : obligation de crypter les données conservées, interdiction de stocker le cryptogramme visuel…)

ATOS WORLDLINE est certifié « PCI-DSS compliant ». En souscrivant un contrat Sogenactif, vous bénéficiez de cette certification.

Les Aggregators

Dans le cadre de la réglementation MasterCard International, VISA International et Carte Bancaire relative au commerce sur Internet, il est interdit à toute société d'utiliser un contrat monétique de vente à distance souscrit auprès d'une banque Acquéreur (banque du commerçant) pour réaliser l'acquisition de transactions pour le compte de tiers.

Depuis juin 2005, les banques françaises ont l'obligation de mettre fin aux contrats commerçants utilisés pour des activités dites « Aggregators » - « Merchant Service Providers non conformes ».

En conséquence, tout commerçant qui souscrit l'offre Sogenactif s'engage « à accepter les Cartes "CB" et les cartes agréées "CB" pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle, auquel le porteur de ladite carte a effectivement et expressément consenti, et s'interdit de collecter des paiements dus à raison de ventes ou de prestations réalisées par d'autres commerçants ou prestataires avec leur propre clientèle ».