ALBERTA centreducyberfutur

# Technologies habilitantes pour la sécurité des transactions




Une initiative de :

LIAISONENTREPRISE
Le service d'information sur l'entrepreneuriat en Alberta

Financée par :

Diversification de l'économie de l'Ouest Canada
Western Economic Diversification Canada
Canada

# Technologies habilitantes pour la sécurité des transactions électroniques

Le terme « technologies habilitantes » désigne les programmes et les plates-formes qui servent à la construction des sites web de B2B (entreprise à entreprise) et de B2C (entreprise à consommateur). Même si beaucoup de gens d'affaires cherchent à se concentrer strictement sur l'aspect de leur entreprise qui concerne les ventes et les achats, et préfèrent laisser les aspects techniques aux spécialistes, il est quand même essentiel qu'ils comprennent clairement ces technologies habilitantes « sous-jacentes » pour mieux apprécier leur plein potentiel ainsi que leurs limites en matière d'affaires électroniques.  Ces technologies sont le chiffrement, le protocole SSL, le protocole SET ainsi que les cartes à puce.

## Le chiffrement

Le chiffrement est le processus qui consiste à rendre les données inintelligibles pour quiconque sauf leur destinataire.

Le chiffrement est le processus qui consiste à rendre les données inintelligibles pour quiconque sauf leur destinataire.

**Ce processus comporte quatre principaux éléments:**

**Authentification.**  Ce procédé permet aux clients d'être certains que les marchands à qui ils confient les renseignements sur leur carte de crédit sont réellement qui ils prétendent être. Le procédé peut également servir au marchand à vérifier que le client est le vrai propriétaire de la carte de crédit.

**Intégrité des données.** Ce procédé permet de s'assurer que le message n'a pas été modifié par un tiers durant la transmission

**Non-répudiation.** Cette fonction empêche les clients ou les marchands de nier qu'ils ont reçu ou émis un message donné.

**Confidentialité.** Cette fonction empêche les tiers de lire des messages interceptés. Les principaux éléments d'un système de chiffrement sont le texte ordinaire, les algorithmes cryptographiques, la clé et le cryptogramme. Le texte ordinaire est le message ou les données qui doivent faire l'objet du chiffrement. Un algorithme cryptographique est un ensemble mathématique de règles qui définissent comment

agencer le texte ordinaire à une clé. La clé est une suite de chiffres. Le cryptogramme est le message chiffré.

**Les deux principaux types de chiffrement utilisés aujourd'hui sont le chiffrement à clé secrète et le chiffrement à clé publique**

**Clé secrète.** Le chiffrement avec clé secrète entraîne l'utilisation d'une seule clé connue de l'expéditeur et du destinataire du message. Après avoir créé le message, l'expéditeur le chiffre avec sa clé et le communique au destinataire qui le déchiffre en utilisant une copie de la clé utilisée pour le chiffrement. Le chiffrement avec une clé secrète a ses limites, particulièrement en ce qui concerne la distribution des clés. Pour assurer la confidentialité, chaque expéditeur devrait fournir une différente clé à chaque destinataire avec lequel il entend communiquer; autrement chaque destinataire potentiel serait capable de lire tous les messages, qu'ils lui soient destinés ou non.
Cette méthode, si elle est relativement facile à gérer lorsque les parties ne sont pas nombreuses (par exemple expédier un courriel à un ami), n'est pas pratique pour le commerce électronique où il peut falloir communiquer avec des milliers de clients. Une autre limite du chiffrement avec une clé secrète est l'incapacité de cette méthode d'assurer la non-répudiation. Étant donné que les deux parties ont la même clé, l'une d'entre elles peut créer un message avec la clé secrète partagée et soutenir que le message a été émis par l'autre partie. S'il est utilisé seul, le chiffrement avec une clé secrète ne convient donc pas au commerce électronique. On utilise plutôt un système appelé chiffrement avec une clé publique.

Les certificats numériques constituent un des fondements des opérations électroniques protégées.

**Clé publique.** Le chiffrement avec une clé publique entraîne l'utilisation de deux clés : une que l'on peut utiliser pour chiffrer les messages (la clé publique); l'autre peut servir à chiffrer ou à déchiffrer les messages (la clé privée). On peut utiliser ces paires de clés de façons différentes : pour assurer la confidentialité ou l'authentification. Pour assurer la confidentialité, on chiffre le message avec la clé publique, car il ne pourra ainsi être déchiffré que par le détenteur de la clé privée. En ce qui concerne l'authentification, il faut chiffrer le message avec la clé privée. Lorsque le destinataire a déchiffré le message avec la clé publique, il est assuré que le message a bel et bien été émis par le détenteur de la clé privée. Étant donné qu'on peut mettre la clé publique à la disposition d'un grand nombre d'utilisateurs,

par exemple par l'intermédiaire d'un serveur ou d'une tierce partie, le chiffrement avec une clé publique ne présente pas les mêmes problèmes de distribution et de gestion que le système de la clé secrète.

Le système de la clé publique  a entre autres les désavantage d'être relativement lent. Par conséquent, lorsqu'il est utilisé à des fins d'authentification, il est préférable de ne pas chiffrer tout le message, particulièrement s'il est long. Pour contourner ce problème, on utilise la signature numérique. Les signatures numériques sont exécutées au moyen  d'un chiffrement avec une clé publique et servent à vérifier l'origine et le contenu d'un message. Le destinataire de la signature numérique peut être assuré que le message provient de l'expéditeur. D'ailleurs, étant donné que le fait de changer un seul caractère du message peut modifier le résumé du message de manière imprévisible, le destinataire peut être assuré que le message n'a pas été changé après la création du résumé.

On peut renforcer l'authentification en utilisant des certificats numériques, ce qui entraîne d'avoir recours à un tiers de confiance ou une société d'authentification (SA). Les détenteurs de clés publiques les soumettent à une SA accompagnées d'une preuve d'identité, et la SA appose sa signature numérique certifiant ainsi que la clé publique jointe au certificat appartient à la partie stipulée. Les certificats numériques constituent un des fondements des opérations électroniques protégées puisqu'ils permettent à toutes les parties d'une transaction de vérifier facilement et rapidement l'identité des autres participants.

## Protocole SSL – Protocole sécurisé de cryptage

Le protocole SSL de Netscape, actuellement la méthode la plus utilisée pour assurer la sécurité des opérations sur le web, est soutenu par la plupart des serveurs et des clients du web, y compris Navigator de Netcape et Internet Explorer de Microsoft. Le protocole SSL comporte plusieurs caractéristiques qui en font l'outil idéal pour les transactions de commerce électronique.

La confidentialité est garantie au moyen d'un chiffrement. Bien que l'information en transit puisse quand même être interceptée par un tiers, ce dernier sera incapable d'en prendre connaissance étant donné l'impossibilité d'accéder à la clé de chiffrement. Si un destinataire reçoit de l'information qui ne se déchiffre pas

Le protocole SET comporte également un autre avantage, soit que le marchand n'a pas accès aux numéros de cartes de crédit.

correctement, le destinataire saura que l'information a été modifiée en cours de transmission. L'authentification est effectuée au moyen de certificats numériques. Ceux-ci constituent un des fondements des opérations électroniques protégées puisqu'ils permettent à toutes les parties d'une transaction de vérifier facilement et rapidement l'identité des autres participants.

Essentiellement, le protocole SSL est une méthode de chiffrement avec une clé secrète accompagnée d'une méthode de chiffrement à clé publique authentifiée par l'utilisation des certificats. Si l'on utilise les deux méthodes de chiffrement, c'est à cause de la lenteur relative du chiffrement avec une clé publique comparativement au chiffrement avec une clé secrète. D'abord, le client et le serveur échangent des clés publiques, puis, le client génère une clé de chiffrement privée qui ne servira que pour cette transaction. C'est ce qu'on appelle une clé de session. Le client chiffre ensuite la clé de session avec la clé publique du serveur et la fait parvenir au serveur. Ensuite, pour le reste de la transaction, le client et le serveur peuvent utiliser la clé de session comme clé de chiffrement privée.

Une connexion SSL doit être initiée par le client (normalement un navigateur du web) qui demande qu'on lui envoie un document au moyen du protocole HTTPS plutôt qu'en utilisant le protocole normal HTTP.

Pour ce faire, il suffit tout simplement de remplacer le préfixe « http » par « https ». Examinons l'exemple http://serveur.domaine.com/index.html. Il s'agit d'une demande d'expédition d'un document par le protocole normal HTTP, tandis que les demandes du protocole SET précisent que le même document doit être envoyé au moyen du protocole https qui intègre le protocole SSL.

SET est le protocole d'opérations électroniques protégées mis au point par Visa et MasterCard, spécifiquement pour permettre des transactions sécurisées par cartes de crédit sur Internet. Il met à contribution les certificats numériques pour établir avec certitude l'identité des parties qui prennent part à un achat et chiffre les renseignements de carte de crédit avant de les expédier sur Internet.

À l'instar du protocole SSL, le protocole SET permet d'authentifier l'identité du marchant au moyen de certificats numériques. Toutefois, le protocole SET permet également au marchand de demander l'authentification de l'utilisateur au moyen de certificats numériques. Ainsi, il est plus difficile d'utiliser une carte de crédit volée. Le protocole SET comporte également un autre avantage, soit que le marchand n'a pas accès aux numéros de cartes de crédit, éliminant ainsi une autre source de fraude.

De nombreux projets pilotes utilisent le protocole SET, mais l'adoption générale de ce protocole s'est révélée plus lente que prévue. Cette lenteur s'explique surtout par l'acceptation croissante du SSL pour les opérations protégées par cartes de crédit ainsi que par la complexité et le coût du système SET.

Une transaction SET typique comporte l'échange de renseignements privés entre un client et un marchand (comme les articles commandés), et un autre échange d'information privée entre le client et la banque (comme le numéro de carte de crédit du client). Le protocole SET permet d'inclure les deux types d'information privée dans une seule transaction signée numériquement. L'information destinée à la banque est chiffrée à l'aide de la clé publique de la banque alors que l'information destinée au marchand est chiffrée à l'aide de la clé publique du marchand. Ainsi, le marchand n'a pas accès aux détails de la carte de crédit, ce qui élimine une source de fraude. En plus de ce chiffrement, les deux ensembles d'information sont signés numériquement. Enfin, les deux signatures sont combinées pour produite une seule signature qui ratifie l'ensemble de la transaction. Bien que le protocole SET ait un potentiel énorme, il n'est pas encore très utilisé.

## Les cartes à puce

Le potentiel d'utilisation des cartes à puce est énorme.

Bien quelles ressemblent en tous points à des cartes de crédit ou de débit normales, les cartes à puce possèdent au moins trois caractéristiques différentes : elles peuvent emmagasiner beaucoup plus de données, elles sont protégées par un mot de passe et elles comportent un microprocesseur intégré qui peut exécuter des fonctions comme le chiffrement.

Encore mal connues en Amérique du Nord, les cartes à puce sont loin d'être une nouvelle invention. En Europe, l'usage de ces cartes est très répandu pour les cartes de crédit, les cartes de paiement de téléphone et le paiement des péages sur les autoroutes. En France, le pays qui a le plus intégré l'utilisation de ce type de carte, on a commencé à les distribuer en 1967 et il y a maintenant quelque 25 millions de ces cartes en circulation. Toutefois, on prévoit que l'utilisation de ces cartes devrait augmenter rapidement à l'échelle mondiale au cours des prochaines années, avant tout en raison du phénomène Internet et de l'explosion du commerce électronique.

Le potentiel d'utilisation des cartes à puce est énorme, mais trois des fonctions de ces cartes sont particulièrement intéressantes pour ceux qui font du commerce électronique : leur capacité d'emmagasiner des clés de chiffrement, des porte-monnaie électroniques ainsi que la portabilité du profil de l'utilisateur.

## Emmagasinage des clés de chiffrement

Les cartes à puce constituent un moyen très sécuritaire de créer, d'emmagasiner et d'utiliser des clés privées. Dans la plupart des applications de base, on peut utiliser les cartes à puce pour emmagasiner des clés privées et des certificats numériques protégées par mot de passe. La sécurité peut être encore plus relevée à l'aide d'un microprocesseur intégré à la carte capable de générer des paires de clés publiques et privées et même d'effectuer le chiffrement. Les données qu'il faut déchiffrer ou qu'il faut ratifier à l'aide d'une signature numérique sont confiées à la carte pour que son microprocesseur exécute les fonctions et ensuite renvoie les données à l'ordinateur. Ainsi, la clé ne quitte jamais la carte et n'est pas vulnérable à une attaque d'un programme clandestin qui balayerait la mémoire de l'ordinateur pour y trouver des clés.

## Les porte-monnaie électroniques

Beaucoup d'applications qui existent aujourd'hui ont remplacé les transactions au comptant par des cartes à puce étant donné leur plus grand degré de sécurité que les cartes de crédit ordinaires. Bien que la plupart de ces systèmes (p. ex. Mondex, VisaCash, CLIP et Proton) aient été mis au point pour des applications de points de vente, il est probable que leur utilisation s'étendra bientôt au commerce électronique étant donné qu'elles constituent un moyen facile et sécuritaire de

traiter les transactions au comptant. Nombreux sont ceux qui prédisent que les lecteurs de carte à puce deviendront un élément normal des micro-ordinateurs.

## Portabilité du profil de l'utilisateur

Un des facteurs qui pourraient potentiellement réduire la croissance du commerce sur le web est l'accès restreint à Internet.

Un des facteurs qui pourraient potentiellement réduire la croissance du commerce sur le web est l'accès restreint à Internet.

Même si le nombre de domiciles et de bureaux qui ont accès à Internet croît sans cesse, Internet n'est toujours pas accessible pour tous, et même l'arrivée d'appareils d'accès économique (par exemple web TV) ne parviendra pas à régler complètement ce problème. En outre, même les personnes qui possèdent des ordinateurs branchés à Internet ne peuvent y accéder lorsqu'ils ne sont pas à la maison ou au bureau. Les cartes à puces pourraient constituer une solution à tout cela en fournissant un accès sécuritaire à des terminaux Internet publics ou à des téléphones à écran. L'information sur le profil personnel de l'utilisateur pourrait être emmagasiné dans la carte de manière à ce que l'apparence soit toujours la même, quel que soit l'appareil utilisé. Les microprocesseurs intégrés seraient en mesure de chiffrer tous les messages, éliminant du même coup tous les risques de sécurité.

## Contactez-nous

Le Centre du cyberfutur de l'Alberta, une initiative de *Liaison Entreprise*, est votre premier point de contact en Alberta pour tout renseignement concernant le cybercommerce. Nous offrons des conseils et des renseignements gratuits, impartiaux et faciles à comprendre sur le cybercommerce pour les petites et moyennes entreprises. Notre but est d'aider les entrepreneurs à prendre des décisions éclairées en vue de leur adaptation aux changements technologiques. Si vous avez des questions, une simple visite, un appel téléphonique ou un simple clic de la souris vous permettront d'y trouver réponse.

## Le Centre du cyberfutur de Liaison Entreprise

**Ligne d'information sur les affaires : 1 800 272-9675**

**Edmonton :** 10237, 104e Rue N.-O., bureau 100, Edmonton (Alberta) T5J 1B1
**Tél. :** 780 422-7722 **Téléc. :** 780 422-0055

**Calgary :** 639, 5e Avenue S.-O., bureau 250, Calgary (Alberta) T2P 0M9
**Tél. :** 403 221-7800 **Téléc. :** 403 221-7817

**Courriel :** info@cyberfutur.ca **Site Web :** www.cyberfutur.ca/alberta