Non confidentiel

Autorité de certification de l' ICP

FAQ : Sécurité du commerce électronique à l’ADRC

Section de l’ICP
Division des services de commerce électronique
Direction du commerce électronique

Date le 1er novembre 1999
Date Revised le 26 juin 2000
Version 2.0

Table des matières

1 Aperçu sur la sécurité

1.1 Quelles sont les incidences des services électroniques sur la protection de mes renseignements personnels?

Les questions relatives à la protection des renseignements personnels dans le cadre de la prestation électronique des services gouvernementaux sont d'une très grande importance. Ces questions comprennent la protection des informations au moment de leur transmission par voie électronique, le stockage des informations sensibles et le regroupement des renseignements personnels dans un référentiel central.

Les renseignements obtenus par voie électronique seront assujettis aux mêmes règles rigoureuses et aux mêmes mesures de protection que celles s'appliquant aux renseignements obtenus par les autres modes de transmission (*Loi sur la protection des renseignements personnels, Loi sur l'accès à l'information* et *Loi sur les archives*). Le projet de loi C-6, une fois adopté, régira le mode de partage des renseignements qui sera utilisé non seulement par les gouvernements, mais aussi par les entreprises privées. Ce projet de loi fera également en sorte d'inscrire dans la loi l'expression « signature numérique » comme autre équivalent de signature manuscrite.

Il existe un certain nombre de mécanismes pour assurer la protection des renseignements au cours de leur transmission par voie électronique. En règle générale, les besoins opérationnels déterminent le niveau de protection nécessaire.
Dans les pages qui suivent, nous traiterons de quelques-uns des moyens utilisés pour assurer la protection des renseignements ainsi transmis.

1.2 Que veut dire « sécurité des services électroniques »?

Pour assurer la sécurité des services électroniques, il faut satisfaire à cinq exigences, soit :

- **Authentification**: Capacité d'une personne, d'une organisation ou d'un dispositif de prouver son identité.
- **Autorisation:** Contrôle de l'accès à certains renseignements ou à certains privilèges, une fois l'identité établie.
- **Confidentialité:** Caractère secret des données ou des renseignements, et protection de ces données ou renseignements contre tout accès non autorisé (seules les personnes à qui ils sont destinés peuvent en prendre connaissance).
- **Intégrité:** Protection des données contre toute modification au cours de leur transfert ou une fois stockées.
- **Non-répudiation:** Protection contre les allégations fausses d'une partie qui, ayant participé à un transaction ou à une communication, refuse par la suite d'admettre que l'activité en question a eu lieu, qu'elle y a participé ou que le message a été transmis au moment où il l'a été (l'expéditeur du message ne peut pas prétendre qu'il n'en était pas l'auteur).

1.3 Quels mécanismes de sécurité l'ADRC utilisera-t-elle pour réduire les risques liés à l'échange électronique de renseignements?

Pour ses services offerts par voie électronique, l'ADRC utilisera différents mécanismes pour assurer la protection des renseignements et des systèmes, notamment:

- Protocole SSL (couche des sockets sécurisés)
  Protocole réseau qui chiffre les données de façon transparente sur les réseaux non protégés.
- Infrastructure à clé publique
  Fonction de sécurité fiable qui utilise des certificats numériques pour offrir un ensemble complet de services de sécurité.

Les transactions électroniques peuvent être protégées par divers moyens, selon le niveau de protection nécessaire. La décision doit tenir compte de la solution la plus appropriée pour régler le problème opérationnel ainsi que du niveau de protection requis.

1.4 Qu'est-ce qu'un secret partagé?

Un secret partagé est un renseignement qui n'est connu, idéalement, que de deux parties qui peuvent chacune s'attendre raisonnablement à ce que seule l'autre connaisse le renseignement en question. Le secret peut être un mot de passe ou un renseignement personnel, par exemple, un numéro d'assurance sociale ou le nom de fille de la mère. En règle générale, les secrets partagés comprennent plusieurs éléments d'information qui, ensemble, permettent de vérifier l'identité d'une personne. Les risques qu'une personne non autorisée connaisse tous les éléments d'information faisant partie du secret partagé sont faibles.

Par exemple, si une personne appelle l'ADRC pour se renseigner sur le montant d'impôt qu'elle doit payer, le préposé aux renseignements lui posera diverses questions auxquelles elle devra répondre correctement. Ces questions sont suffisamment personnelles pour que le préposé puisse s'assurer de façon raisonnable de l'identité de l'appelant. Si ce dernier ne peut pas répondre aux questions de façon satisfaisante, il ne pourra accéder à aucun renseignement sur le compte visé.

1.5 En quoi consistent les numéros d'identification personnels (NIP) et les mots de passe?

Les NIP sont des mots de passe numériques comprenant une série de chiffres que seul le détenteur de la carte connaît. On les utilise souvent pour vérifier l'identité des clients. Un exemple courant d'utilisation du NIP aux fins de sécurité est la carte bancaire qui permet au détenteur d'accéder à son compte à partir d'un guichet automatique, d'une machine de débit, etc. en composant le NIP associé à sa carte. Des mots de passe peuvent également être employés avec les données d'identification de l'utilisateur pour permettre au système de comparer, aux fins de vérification, les renseignements fournis par l'utilisateur et ceux stockés à son sujet.

Les codes d'accès au Web, qui sont les NIP particuliers à l'ADRC, sont utilisés avec d'autres renseignements personnels pour permettre à une personne d'accéder par voie électronique à certains renseignements sur Internet.

2 Notions de base sur la sécurité

2.1 En quoi consiste le chiffrement?

Le chiffrement est le processus qui consiste à coder des renseignements de nature délicate de façon à les rendre illisibles. Le déchiffrement est le processus inverse, soit la conversion des données illisibles à leur état initial.

Il existe deux principales méthodes de chiffrement, soit le chiffrement à une clé (symétrique) et le chiffrement à deux clés (asymétrique).

2.1.1 En quoi consiste le chiffrement symétrique (à une clé)?

Avec cette méthode, l'utilisateur se sert d'un seul élément d'information (appelé une clé) pour exécuter les processus de chiffrement et de déchiffrement. L'expéditeur se sert de la clé (qui est connue des deux parties) pour chiffrer les données au moyen d'un ensemble de règles appelé « algorithme». Le destinataire du message, qui connaît la clé et l'algorithme, exécute le processus inverse en se servant de la même clé pour ramener le message à son état initial. L'avantage de cette méthode tient au fait que les algorithmes de chiffrement symétrique sont, en règle générale, très rapides. L'inconvénient est de trouver un moyen pour que la clé ne soit connue que des deux parties concernées, sans risque d'interception par d'autres parties (en règle générale, l'algorithme utilisé constitue un renseignement public qui n'est pas protégé).

2.1.2 En quoi consiste le chiffrement asymétrique (à deux clés)?

Avec cette méthode, l'utilisateur se sert non pas d'une mais de deux clés, une publique et l'autre privée, pour exécuter les processus de chiffrement et de déchiffrement. Ces clés sont choisies minutieusement afin de s'assurer que le message chiffré à l'aide de la clé publique ne peut être déchiffré qu'avec la clé privée appropriée. Par exemple, l'expéditeur trouve la clé publique du destinataire (ce dernier peut même la lui envoyer par courriel puisqu'il s'agit d'un renseignement public) et s'en sert pour chiffrer le message. Le destinataire peut ensuite déchiffrer le message à l'aide de sa clé privée. L'avantage de cette méthode tient au fait qu'aucun renseignement sur la clé n'est transmis, éliminant ainsi presque tout risque d'interception par d'autres parties. Toutefois, cette méthode présente les inconvénients suivants : le nombre de paires de clés disponibles est limité (mais il y en a tout de même suffisamment pour permettre l'utilisation de ce processus), et les algorithmes de chiffrement asymétrique sont beaucoup plus lents.

2.2 Quelle est l'importance de la longueur de la clé?

La longueur de la clé est importante pour empêcher d'autres parties de trouver la clé utilisée pour chiffrer les données. Supposons qu'il existe un ordinateur pouvant vérifier un milliard de clés possibles à la seconde. En exécutant une vérification force brute (de zéro en montant) d'une clé de 40 bits (la longueur de la clé est exprimée sous forme binaire), cet ordinateur pourrait, en moyenne, trouver le résultat en 150 heures environ, soit un bit tous les 6 jours. La vérification d'une clé à 56 bits prendrait plus de temps : environ 10 008 000 heures, soit 417 000 jours ou 17 375 années. Et pour vérifier une clé de 128 bits, il faudrait $5{,}04 \times 10^{24}$ années. Des clés mieux protégées ne pourront donc être trouvées par un utilisateur malveillant qu'après beaucoup de temps. Toutefois le chiffrement et le déchiffrement des données prendront aussi plus de temps et de

ressources de la part des parties concernées.

2.3 Qu'est-ce que le hachage?

Le hachage est un fonction qui permet de traiter les données comme des entrées, peu importe leur longueur, et de produire un condensé ou un « hachis » (d'où le terme « hachage ») d'une longueur déterminée, habituellement 128 ou 160 bits. Ce condensé est utilisé pour représenter (et non remplacer) l'élément de données original. La fonction de hachage peut représenter de grandes quantités de données, à la condition qu'elles aient les propriétés suivantes:

- Cohérence
  Le même fichier d'entrée doit toujours produire le même résultat (soit le condensé).
- Imprévisibilité
  Pour un condensé particulier, il doit être pratiquement impossible d'inverser le processus de hachage et de produire le message original.
- Volatilité
  Cette propriété peut sembler être en contradiction avec la première, mais il est indispensable que la moindre modification du message d'entrée produise un condensé complètement différent. On réduit ainsi la possibilité que la modification d'un bit de données ne soit pas prise en compte par la fonction de hachage le même condensé.

Le tableau ci-dessous donne un exemple de condensé obtenu par hachage. Observez à quel point les messages d'entrée initiaux diffèrent des condensés obtenus. Notez également comment même une légère modification du message d'entrée produit un condensé très différent. Ces condensés ont été générés à l'aide de l'algorithme de chiffrement irréversible, défini par le National Institute of Standards and Technology des États-Unis (norme de fait de l'algorithme de hachage dans l'industrie informatique).

Message	**Condensé du message** (avec la base 16 pour représenter les bits)
Nous sommes le 1 novembre 1999	`8B9A1D92 CB9C4BDB 5EBF5F46 D462CBD6 E9467DB8`$_{16}$
Nous sommes le 2 novembre 1999	`F9FD7290 9CF45F2E C1F9005E 073ECC85 7BADB43B`$_{16}$

2.4 Qu'est-ce qu'une signature numérique? Comment la créer? Comment l'utiliser?

Une signature numérique est un moyen électronique permettant de valider l'intégrité et l'authenticité d'un élément de données déterminé. Par exemple, un utilisateur reçoit un document par voie électronique. Comment peut-il être assuré qu'un tiers n'a pas altéré le fichier? Même si le message a été chiffré, le destinataire doit avoir la certitude que le fichier n'a pas été modifié par un moyen quelconque. Cette assurance est particulièrement importante lorsqu'on utilise des applications de commerce électronique.

Pour créer une signature numérique, l'expéditeur traite le message à l'aide d'un algorithme de hachage. Il chiffre ensuite le condensé obtenu avec sa clé privée et l'envoie avec le message. Le destinataire reçoit le condensé chiffré et le déchiffre à l'aide de la clé publique de l'expéditeur. Puis, il applique au message original le même algorithme de hachage. Si les deux condensés sont identiques, le destinataire est assuré que le message n'a pas été altéré au cours de la transmission. Et comme le condensé correspondant a été obtenu à l'aide de la clé privée chiffrée de l'expéditeur, le destinataire est assuré que seul l'expéditeur peut être l'auteur du message.

3 Mise en oeuvre de mesures de sécurité

3.1 Comment fonctionne un secret partagé?

Lorsque deux parties entrent en communication, chacune pose des questions pour vérifier l'identité prétendue de l'autre partie. Par exemple, si une personne appelle l'ADRC pour se renseigner sur le montant d'impôt qu'elle doit payer, le préposé aux renseignements lui posera diverses questions auxquelles elle devra répondre correctement. Ces questions sont suffisamment personnelles pour que le préposé puisse s'assurer de façon raisonnable de l'identité prétendue de l'appelant. Si ce dernier ne peut pas répondre aux questions de façon satisfaisante, il ne pourra accéder à aucune information sur le compte concerné.

3.2 Qu'est-ce que le protocole SSL? Comment fonctionne-t-il?

Le protocole SSL (couche des sockets sécurisés) est un protocole de sécurité qui assure la protection des communications sur Internet. Ce protocole permet aux applications client-serveur de communiquer sans risque d'interception, d'altération ou de falsification des messages. C'est le service de sécurité le plus couramment utilisé sur Internet pour protéger les transactions effectuées au moyen d'un logiciel de navigation.

Au moment de l'établissement d'une connexion SSL, le client (le plus souvent un logiciel de navigation) et le serveur conviennent d'un algorithme cryptographique, puis choisissent une clé exclusive. Les deux machines choisissent l'algorithme le plus fiable et la clé la plus longue qu'elles sont en mesure de prendre en charge. Ce choix est important, car il est possible que certaines machines ne puissent pas prendre en charge un algorithme acceptable. Par conséquent, le chiffrement utilisé peut ne pas être aussi fiable que ce qu'exige la loi. La clé symétrique est établie sans être réellement transmise d'une machine à l'autre, de sorte qu'un intercepteur éventuel ne pourra la trouver dans aucun échange de données sur le réseau.

Une fois ces paramètres convenus, une voie de communication protégée est créée entre les deux machines. Toutes les données du client sont chiffrées et envoyées au serveur par cette voie protégée. Le serveur utilisant également cette voie pour répondre, il n'y a aucun risque d'interception des renseignements de nature délicate. La session terminée, la voie est supprimée de même que ses paramètres. Au moment de la communication suivante entre ces deux machines, le choix de l'algorithme et de clé fait l'objet d'une nouvelle négociation.

Comme pour la plupart des mécanismes de sécurité, plusieurs variantes du SSL sont disponibles. En règle générale, la version considérée la plus sûre de ce protocole est le chiffrement à 128 bits (la version 3 du SSL permet l'authentification du client au moyen de certificats numériques). Ce qu'il importe de retenir au sujet du protocole SSL, c'est qu'il permet de protéger la communication entre deux parties, mais pas nécessairement les fichiers ou dossiers joints. De plus, le niveau de sécurité assuré par le protocole SSL ne dépasse pas celui du lien le plus faible. Si un client utilise un chiffrement à 128 bits et que le logiciel de navigation appelle un site utilisant un chiffrement à 40 bits, c'est ce dernier qui sera utilisé pour chiffrer la session entre les deux parties.

3.3 Qu'est-ce que l'infrastructure à clé publique (ICP)? Comment fonctionne-t-elle?

ICP est un système informatique de gestion de clés permettant de créer, de mettre à jour et de transmettre en toute sécurité des clés de chiffrement et de signature numérique. L'ICP comprend quatre composantes principales:

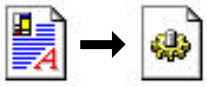
- Autorité de certification/Système de gestion de clés
  L'élément central de l'ICP est le système de gestion des clés. Il s'agit essentiellement d'une base de données protégée qui permet la création et la maintenance des clés.
- Service de répertoires publics
  Répertoires dont se servent les utilisateurs pour accéder aux certificats publics. C'est l'élément le plus utilisé dans une infrastructure de sécurité.
- Logiciel client
  Logiciel dont se servent les utilisateurs pour communiquer avec l'ICP. Il importe que le logiciel client soit suffisamment flexible pour servir à de nombreuses fins (soit protéger les fichiers, les dossiers, le courriel, les sessions en temps réel, etc.), tout en étant assez transparent pour que l'utilisation de produits de sécurité ne représente pas un fardeau pour les utilisateurs.
- Politiques et procédures
  Partie la plus importante de la mise en oeuvre d'une ICP. Pour que l'ICP fonctionne, des lignes directrices et des règles doivent être mises en place pour régir l'utilisation de la technologie. C'est l'aspect le plus difficile et le plus exigeant en temps de l'ICP, car les politiques et les procédures doivent être constamment mises à jour pour refléter l'utilisation prévue des ressources.

Le principal élément de l'ICP est une paire de certificats numériques, soit un certificat pour le chiffrement et le déchiffrement et un autre pour la signature et la vérification. Ces certificats contiennent des informations importantes, par exemple, qui a authentifié l'utilisateur, l'autorité qui a accordé le certificat, le nom du détenteur (dans le contexte de l'ICP, on parle de « nom distinctif ») et la période de validité (une date d'expiration est établie pour chaque certificat). La mise en oeuvre complète de l'ICP doit satisfaire aux cinq exigences de sécurité définies au début.

3.3.1 Comment l'ICP protège un message

Voici comment l'ICP protège un message

- Hachage du message
  Un condensé du message initial est créé.



- Chiffrement du condensé
  L'expéditeur chiffre ensuite le condensé au moyen de sa clé de signature privée. C'est la signature numérique de ce message.

- Chiffrement du message
  L'expéditeur génère ensuite une clé symétrique exclusive dont il se sert pour chiffrer le message. Cette clé n'est utilisée que pour la session en cours. Une nouvelle clé devra être générée pour les prochains messages.

- Protection de la clé symétrique
  Le traitement final consiste à protéger la clé symétrique au moyen de la clé de chiffrement public du destinataire. L'expéditeur doit extraire celle-ci du répertoire public du destinataire ou demander à ce dernier de la lui faire parvenir avant le traitement du message protégé.

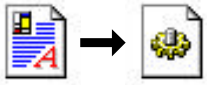
- Préparation du message
  Les données envoyées au destinataire ne ressemblent en rien au message original. L'envoi final comprend la signature numérique, le message chiffré, la clé chiffrée de la session, une copie de la clé de la signature numérique (le certificat public de vérification de l'expéditeur) et les algorithmes de hachage et de chiffrement qui ont été utilisés.

À cette étape, le message a été transmis au destinataire voulu et ce dernier exécute le processus inverse pour obtenir le message original et en vérifier l'authenticité.

- Détermination de la clé de chiffrement
  La clé symétrique de la session est déchiffrée au moyen de la clé privée de déchiffrement du destinataire.

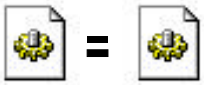
- Déchiffrement du message
  Le destinataire déchiffre le message au moyen de cette clé exclusive.

- Hachage du message
  Le destinataire produit ensuite un condensé (fonction de hachage) du message original, tout comme l'expéditeur l'avait fait.



- Déchiffrement du condensé reçu
  Le destinataire déchiffre ensuite le condensé reçu au moyen du certificat public de vérification joint au message.

- Comparaison des condensés
  La dernière étape consiste à s'assurer que le message n'a été altéré d'aucune façon. Pour ce, le destinataire compare les deux condensés. S'ils sont identiques, il a toutes les raisons de croire que le message n'a pas été altéré. Dans le cas contraire, l'utilisateur n'a aucune raison de croire en l'authenticité du message.



3.4 Quelles sont les principales différences entre l'ICP et le protocole SSL?

Il existe certaines différences entre ces deux niveaux de protection. Ils permettent tous deux de protéger l'information d'une session, mais de façon différente. L'ICP est plus difficile à mettre en oeuvre, mais elle permet, en bout de ligne, de disposer d'une infrastructure de sécurité plus utile et plus souple.

Le protocole SSL ne permet d'utiliser qu'une seule paire de clés pour assurer l'authenticité d'un message. Par exemple, l'expéditeur chiffre un message en utilisant la clé publique du destinataire et le signe en se servant de sa clé privée. Puis, le destinataire déchiffre le message à l'aide de sa clé privée et extrait la clé publique de l'expéditeur pour vérifier l'authenticité du message. Certes, l'utilisation d'une seule paire de clés simplifie le processus, mais les risques d'usurpation des clés sont beaucoup plus élevés. Un autre inconvénient est le manque de souplesse de l'architecture SSL, qui ne

peut être utilisée pour protéger les fichiers, les dossiers ou les messages de courrier électronique. Toutefois, elle peut être utilisée en combinaison avec d'autres types de mécanismes de sécurité, comme les secrets partagés, les NIP et les codes d'accès au Web.

Le choix du protocole SSL ou de l'ICP demeure essentiellement une décision opérationnelle reposant sur l'évaluation des besoins de l'organisation et sur les risques. Il est tout à fait possible qu'une organisation choisisse d'utiliser une combinaison de protocoles de sécurité pour les différents aspects de ses activités. Pour obtenir plus d'information sur le bon choix à faire, adressez-vous à votre agent de la sécurité TI.

4 Mise en œuvre de mesures de sécurité pour le commerce électronique

4.1 Pourquoi les entreprises canadiennes ou les Canadiens ont-ils besoin de certificats numériques?

Pour les entreprises ou les personnes qui effectuent fréquemment des transactions comportant des renseignements confidentiels ou délicats avec le gouvernement fédéral, l'utilisation de l'ICP a sa raison d'être. Elle leur permettrait notamment d'épargner temps et argent en leur évitant d'avoir à exécuter chaque fois la procédure d'authentification. Avec un certificat, les deux parties seraient assurées que l'identité de l'autre partie est authentique et n'auraient pas à entrer les données historiques nécessaires à l'authentification avant chaque transaction. Avec l'ICP, l'administration fédérale pourrait réaliser des économies si chaque programme de prestation de commerce et de services électroniques permettait de partager les coûts d'authentification de clients communs.

Actuellement, le gouvernement fédéral examine l'analyse de rentabilisation du déploiement à grande échelle de l'ICP. L'ADRC prête son concours à ce processus.

4.2 Qu'est-ce que l'ICP du gouvernement du Canada?

Il s'agit de l'infrastructure qui intègre les autres technologies (l'autorisation et l'authentification électroniques, les cartes à puce, etc.) en une solution transparente pour permettre la gestion sécuritaire de l'information ministérielle et du commerce électronique (à l'intérieur ou à l'extérieur de l'administration). L'ICP du gouvernement du Canada procure un processus uniforme de gestion et de certification des clés pour assurer la protection de la confidentialité et des signatures numériques dans toute l'administration fédérale. L'ICP permet à une organisation de gérer efficacement de gros volumes de signatures numériques.

Le Comité de gestion de la politique est un comité interministériel, présidé par le Secrétariat du Conseil du Trésor. Il sera responsable de l'approbation des politiques et des pratiques de délivrance de certificats utilisées par les autorités de certification. Certains ministères et organismes utilisent actuellement la technologie ICP et établissent des autorisations de certification pour les applications de commerce électronique et de sécurité.