SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUES AU GOUVERNEMENT DU QUÉBEC

FOIRE AUX QUESTIONS SUR L'INFRASTRUCTURE À CLÉ PUBLIQUE

RÉALISÉE LORS DU CHANTIER CADRE DE SÉCURITÉ
DE L'INFOROUTE GOUVERNEMENTALE

Secrétariat du Conseil du trésor

Sous-secrétariat aux marchés publics et aux technologies de l'information

Sous-secrétariat à l'inforoute et aux ressources informationnelles

Service des orientations et politiques de renouvellement

Version 1.6 PRÉ-PUBLICATION * 6 OCTOBRE 1997

PLAN DU DOCUMENT

LISTE DES QUESTIONS

1) Qu'entend-t-on par la sécurisation des échanges électroniques ?
2) Quels sont les principaux besoins en matière de sécurisation juridique et technique des échanges électroniques ?
3) Quels sont les principaux objectifs de la sécurisation juridique et technique ?
4) Quels sont les éléments juridiques à considérer ?
5) Quels sont les aspects techniques à considérer ?
6) Qu'est-ce que la cryptographie ?
7) Quels sont les deux types de cryptographie ?
8) Comment la cryptographie à clé publique peut-elle servir à signer un document électronique ?
9) Quel est le rôle de l'Infrastructure à clé publique (ICP) ?
10) Quels types d'organisation jouent le rôle d'ICP ?
11) En quoi l'ICP contribue-t-elle à la certification d'identité ?
12) Qu'est-ce qu'une Autorité de certification (AC) ?
13) Quel est le rôle d'une Autorité de certification ?
14) Quels sont les services habituellement offerts aux abonnés d'Autorité de certification ?
15) Qu'est-ce qu'un certificat d'identification ?
16) Ä quoi sert un certificat électronique d'identification ?
17) Que contient habituellement un certificat électronique d'identification ?
18) De quels critères doit-on tenir compte lors de l'évaluation d'une Autorité de certification (AC) ?

PRODUCTION, RÉDACTION, COLLABORATION, REMERCIEMENTS ET COMMENTAIRES

- **CADRE DE SÉCURITÉ DE L'INFOROUTE GOUVERNEMENTALE ***

FOIRE AUX QUESTIONS

1) Qu'entend-t-on par la « sécurisation des échanges électroniques » ?

Il s'agit d'assurer **en même temps** la sécurité juridique et la sécurité technique des échanges électroniques. Cette sécurisation est nécessaire afin d'établir un climat de confiance auprès des gens d'affaires et des consommateurs. Elle est essentielle au développement rapide et harmonieux des affaires électroniques sur les Inforoutes et à l'utilisation massive de la messagerie électronique dans la société.

Les échanges électroniques englobent la transmission de messages électroniques, la consultation de sites WEB, la réalisation de transactions électroniques, le transfert de fichiers et la transmission d'autres documents électroniques de nature administrative, commerciale ou technique. Ces échanges touchent par exemple aux échanges administratifs intra-organisationnels, aux documents utilisés dans le cadre d'achats de biens ou de services (commande, livraison, paiement, etc), aux télédéclarations à l'Administration par les entreprises (taxes, impôts, etc), ou encore, à la demande et à l'émission de licences et de permis. Au début des années 80, soit à l'aube de la télématique, on résumait ces différentes possibilités d'échanges électroniques par l'appellation « Information - Diffusion – Transaction ».

Le commerce électronique englobe à la fois les échanges commerciaux inter-organisationnels, de même que les échanges entre les entreprises (privées ou publiques) et les consommateurs. Le commerce électronique peut être réalisé à l'aide d'une vingtaine de technologies distinctes, dont la télécopie, la messagerie électronique, l'EDI, le télex et le WEB commercial. Ces technologies de l'information peuvent être utilisées de façon isolée (ex. : la télécopie), ou encore intégrées (ex. : code à barres + EDI).

2) Quels sont les principaux besoins en matière de sécurisation juridique et technique des échanges électroniques ?

Les organisations québécoises, tant gouvernementales que privées, souhaitent traiter un volume important de transactions d'affaires de façon fiable et automatique. Ces transactions doivent être effectuées dans des environnements informatiques à l'abri des menaces délibérées, tout en réduisant au strict minimum les risques d'erreurs et de défaillances.

Ces transactions sont effectuées dans un contexte juridique nouveau puisqu'elles sont dématérialisées; c'est-à-dire qu'elles ne constituent pas un document écrit sur support papier comme c'est le cas depuis des siècles.

En fait, l'utilisation d'un réseau distribué et ouvert, tel Internet, accroît le risque d'« accès non autorisé » (indiscrétion, modification des informations) et d'« attaques » (virus) des systèmes d'information branchés sur l'Inforoute. De même, le caractère « dématérialisé » des transactions accroît le risque qu'une personne transige sous une identité fictive, ou encore, usurpe l'identité d'une autre personne.

Les besoins de base en matière de sécurisation concernent donc la protection des renseignements confidentiels (personnels ou d'entreprises), la signature électronique des documents, la certification électronique d'identité des personnes et des dispositifs (ex. : sites WEB), le respect de la propriété intellectuelle et la sécurité des paiements.

Sur ce dernier point, citons simplement la sécurisation des messages de nature sensible», la protection des contenus diffusés sur les sites WEB et la protection des transactions administratives et commerciales.

3) Quels sont les principaux objectifs de la sécurisation juridique et technique ?
Cette sécurisation vise à assurer la disponibilité et le contrôle de l'accès aux systèmes informatiques, l'intégrité et la confidentialité des informations échangées, l'authentification de l'émetteur et du récepteur (chaque personne est bien celle qu'elle prétend être), ainsi que la non répudiation (soit la non contestation) par l'émetteur de cette information.

Il s'agit donc de conférer aux documents électroniques une valeur juridique (en terme de preuve) égale ou même supérieure aux documents papiers correspondants. Il ne faut pas perdre de vue que ces deux grandes catégories de support vont devoir coexister pour encore plusieurs années.

4) Quels sont les éléments juridiques à considérer ?
Il faut tout d'abord établir si l'on peut utiliser ou non un document électronique. C'est-à-dire s'assurer de la validité juridique de l'utiliser. En effet, la législation et la réglementation peuvent obliger dans certains cas un contenu spécifique (ex. : mention obligatoire), une forme particulière (ex. : constat d'infraction), un support particulier (ex. : formulaire à copies multiples, papier à en-tête, etc), ou un mode de livraison spécifique (ex. : huissier). Dans ces cas, l'utilisation de documents sous forme électronique peut s'avérer problématique.

Il faut ensuite établir si le document doit être signé ou non en vertu d'une obligation législative, contractuelle ou administrative. En effet, de nos jours, beaucoup de documents sont signés ou paraphés, sans qu'il n'y ait aucune obligation spécifique de le faire.

Il faudra également situer quelle est la valeur de preuve du document électronique en cas de litige. Signalons qu'en dépit d'une certaine « ouverture » du nouveau Code civil du Québec, quant à la valeur probante des documents électroniques, il n'existe encore aujourd'hui que peu ou pas de jurisprudence nous permettant de situer précisément l'interprétation possible de la nouvelle réalité électronique par les tribunaux, québécois ou étrangers. Il n'existe également aucune jurisprudence permettant de situer la force probante des documents électroniques, par rapport aux documents traditionnels sur support papier.

Finalement, l'on devra déterminer la durée de conservation (prescription légale) et la forme d'archivage électronique du document.

5) Quels sont les aspects techniques à considérer ?
Il existe déjà sur le marché toute une gamme de solutions permettant de réduire les risques inhérents aux nouveaux modes d'échanges électroniques. Ces diverses solutions visent par exemple l'enregistrement et le contrôle des accès aux systèmes informatiques, l'établissement de garde-barrière ("firewall") pour la protection de sites WEB, le chiffrement de confidentialité des contenus, la signature électronique des documents, l'horodatation (heure) des transactions, la journalisation des accès et des transactions ainsi que la certification électronique d'identité des personnes et des dispositifs.

Plusieurs des solutions les plus répandues actuellement utilisent des techniques de cryptographie.

6) Qu'est-ce que la cryptographie ?

La cryptographie est une discipline vieille de plusieurs siècles qui connaît actuellement un nouvel essor grâce à l'émergence de réseaux ouverts, tel Internet.

Cette discipline inclut les principes, moyens et méthodes de transformation des données visant à cacher le contenu d'un message ou d'une transaction, permettant ainsi l'échange sûr d'informations confidentielles.

Son principe de base est alors très simple. Un texte compréhensible est converti en texte inintelligible (chiffrement de confidentialité), en vue de sa transmission à une autre personne. Sur le poste de travail du destinataire, le texte chiffré est reconverti en format intelligible (déchiffrement) pour sa lecture ou son traitement. Il existe actuellement sur le marché plusieurs solutions technologiques de chiffrement, tel que Clipper/Capstone, Pretty Good Privacy (PGP), DES, Entrust, etc.

On utilise également la cryptographie pour assurer l'authentification (la personne est bien celle qu'elle prétend être), la non-répudiation (non-contestation du contenu par l'émetteur ou le destinataire du message) et l'intégrité de l'information grâce à un processus cryptographique spécial appelé signature numérique. Ce processus est décrit à la question 8.

7) Quels sont les deux types de cryptographie ?

La cryptographie dite « classique » (ou symétrique) repose sur l'utilisation d'une clé mathématique » qui sert au chiffrement et au déchiffrement des messages et autres documents. Ainsi, pour faire parvenir un message de façon sûre, il faut le chiffrer à l'aide d'une clé, puis faire parvenir au destinataire ladite clé de façon à ce que seul celui-ci puisse décoder le message. Ce type de cryptographie est appelée cryptographie symétrique.

Il existe un autre type de cryptographie appelé cette fois cryptographie asymétrique ou cryptographie à clé publique. Ce type de cryptographie utilise une paire de clés asymétriques (soit deux clés différentes mais complémentaires). La première demeure privée et secrète et n'est habituellement connue que par son détenteur (l'utilisateur ou abonné). L'autre est publique et figure habituellement dans un répertoire électronique de type X.500. Si l'on utilise la clé publique pour chiffrer un message, la clé privée permet alors de le déchiffrer. L'opération inverse (ou réversible) est également possible. Autrement dit, il suffit de chiffrer un message à l'aide d'une clé et le destinataire pourra ensuite utiliser l'autre clé pour le déchiffrer. Les répertoires de type X.500 permettent à vos correspondants (partenaires d'affaires, collègues de travail) de retrouver votre clé publique et chiffrer des messages que vous seul pourrez déchiffrer avec votre clé privée.

8) Comment la cryptographie à clé publique peut-elle servir à signer un document électronique ?

Comme nous l'avons vu, l'identité des personnes transigeant à distance revêt une importance particulière dans le monde du « Cyberespace », puisque la dématérialisation des transactions accroît le risque qu'une personne transige avec une organisation sous une identité fictive, ou encore, usurpe l'identité d'une autre personne.

La cryptographie à clé publique (ou cryptographie asymétrique) rend possible l'utilisation de la signature numérique. Ce type de signature électronique permet de corroborer l'origine d'un message grâce à un procédé technologique particulier.

Pour apposer une signature numérique dans un message électronique, on utilise une fonction mathématique qui produit un résumé du message. Le résumé ainsi obtenu est ensuite chiffré à l'aide de la clé privée de l'expéditeur. Le résultat, qui constitue la signature numérique, est alors annexé au message. Le destinataire du message peut ensuite s'assurer de l'origine du message, et de l'intégrité de son contenu, en déchiffrant la signature numérique au moyen de la clé publique de l'expéditeur, puis en comparant le résultat avec le résumé obtenu en appliquant la même fonction mathématique au message reçu. Quoique complexe à première vue, cette opération s'effectue habituellement par un simple « clic de souris ».

Comme nous l'avons vu, la signature numérique est une méthode de transformation des données qui assure l'authentification de l'émetteur, l'intégrité du contenu et la non-répudiation. C'est donc, d'une certaine manière, la transposition électronique d'une signature manuscrite, même si en fait elle ne ressemble pourtant en rien à une signature conventionnelle. En fait, il est largement reconnu par les spécialistes techniques que la signature numérique peut offrir un niveau de sécurité supérieur à la signature manuscrite.

La signature numérique peut être apposée dans n'importe quel document électronique (message de courrier électronique, logiciel, fichier de données, transfert électronique de fonds, etc.). Il existe plusieurs solutions technologiques de signature numérique, telles que Entrust, RSA B-Safe, etc.

Signalons que l'utilisation d'une Infrastructure à clé publique (ICP) peut contribuer à accroître le niveau de confiance en confirmant la validité des clés cryptographiques, l'identité du détenteur et le lien entre la paire de clés et ce détenteur.

9) Quel est le rôle de l'infrastructure à clé publique (ICP) ?

Essentiellement, une infrastructure à clé publique (ICP) contribue à l'authentification des détenteurs de clés en émettant des certificats confirmant la validité des clés et l'identité des détenteurs. Dans certains cas, l'ICP gère également la production et la distribution des paires de clés publiques et privées, quoique cette fonction peut parfois être assurée directement à partir de l'ordinateur de l'utilisateur. Enfin, l'ICP correspond également à un réseau organisé d'autorités de certification (AC).

10) Quels types d'organisation jouent le rôle d'ICP ?

Les ICP rencontrées jusqu'à maintenant proviennent essentiellement :

- d'organisations gouvernementales ;
- d'institutions financières et organismes de suivi du crédit ;
- du service national des postes ;
- de regroupements de professionnels (notaires, autres professionnels du droit, comptables, etc.) ;
- d'entreprises commerciales (firmes en télécommunication).

Au moment d'écrire ces lignes, quelques organisations québécoises et canadiennes ont déjà exprimé leur intention d'offrir dans les prochains mois des services de certification. Il s'agit entre autres du gouvernement du Canada, de la Société canadienne des Postes, de la Chambre des notaires du Québec (Notarius), de Verisign, d'Equifax et de Keywitness. D'autres ICP devraient également voir le jour prochainement.

11) En quoi l'ICP contribue-t-elle à la certification d'identité ?

Puisque les personnes qui participent à un échange électronique ne se voient pas -- elles ne se connaissent d'ailleurs peut-être même pas--, il est alors très important de prévoir un mécanisme formel de confirmation de leur identité. C'est ce que l'on appelle ici la certification électronique d'identification.

La certification, qu'elle soit électronique ou traditionnelle, se fait généralement par l'utilisation d'un tiers certificateur ou tiers de confiance. Ce tiers, tel un notaire, doit démontrer un degré de confiance acceptable pour la bonne marche des affaires.

Dans un document publié l'an dernier, la Chambre des notaires du Québec décrivait la certification comme étant :

> *un processus formel d'identification, partiel ou total, des parties entretenant des relations commerciales. Elle s'effectue généralement par le biais d'infrastructures technologiques et l'intervention d'une tierce partie impartiale et indépendante, soit l'autorité de certification, qui, par l'émission d'un certificat d'identification, garantit, à divers niveaux et suivant des normes pré-établies, l'identité des parties transigeant à distance. Elle sert à apporter la preuve formelle et objective, émanant d'une personne indépendante et impartiale de l'identité du signataire et à la lier au contenu d'un document électronique visant à manifester son consentement à un acte juridique.»*

Dans un contexte d'ICP, ce tiers de confiance, dont l'activité principale consiste à confirmer l'identité des personnes transigeant à distance, est donc l'Autorité de certification.

12) Qu'est-ce qu'une Autorité de certification (AC) ?

C'est une entité chargée d'établir et, par la suite, de garantir un lien formel entre une personne et une clé publique dans le cadre d'une ICP. Son rôle consiste à vérifier l'exactitude de l'information contenue dans le certificat électronique d'identification qu'elle émet, ainsi qu'à garantir, la validité de ce document face à un tiers. Elle exerce ces fonctions suivant un modèle hiérarchique qui permet la certification en chaîne par des autorités locales, régionales, sectorielles, nationales et internationales.

L'Autorité de certification est donc une composante essentielle de la structure de certification et de l'ICP.

13) Quel est le rôle d'une Autorité de certification (AC) ?

Habituellement, une Autorité de certification :

- confirme l'identité des personnes qui se servent de la signature numérique (évitant ainsi l'usurpation) ;
- émet des certificats signés numériquement avec sa propre clé privée (celle de l'AC), attestant ainsi du lien entre une clé publique et une entité (personne, dispositif) ;
- publicise sa propre clé publique ;

- fournit sur demande son propre certificat électronique d'identification, provenant d'une autorité de certification supérieure dans la hiérarchie de certification ;
- effectue de la certification croisée (reconnaissance mutuelle ou réciproque) avec les autres AC, afin d'assurer l'interopérabilité du processus de certification. Cette interopérabilité entre les Autorités de certification permet la certification d'identité de gens œuvrant chez d'autres employeurs, dans d'autres professions ou habitant même d'autres pays.

14) Quels sont les services habituellement offerts aux abonnés des Autorités de certification (AC) ?

Les services de base d'une Autorité de certification concernent :

- la gestion des clés de chiffrement ;
- la gestion des clés servant à la signature numérique ;
- la certification par l'émission des « certificats électroniques » ;
- la tenue à jour d'un répertoire des clés publiques ;
- la gestion des privilèges ;
- la gestion des supports de stockage de clés (ex. : carte à microprocesseur, disquette, carte PCMCIA, etc.) ;
- l'horodatation ;
- l'archivage de documents ;
- l'interopérabilité avec les autres AC ;
- l'émission des listes des certificats suspendus et révoqués.

15) Qu'est-ce qu'un certificat d'identification ?

L'utilisation de certificats dans notre société n'est pas un phénomène nouveau en soit. Qu'il suffise de penser au certificat d'immatriculation de véhicule automobile, au passeport, au permis de pêche et de chasse, etc.

L'on s'intéresse plus particulièrement dans le cadre de ce document au «certificat électronique d'identification du détenteur de clés cryptographiques».

Ce certificat atteste le lien entre une paire de clés asymétriques (privée-publique) et une entité. Cette entité peut être une personne, ou peut être même un dispositif, tel qu'un site WEB.

16) À quoi sert un certificat électronique d'identification ?

Le « certificat électronique d'identification » est un document émis électroniquement par une Autorité de certification, qui vise à lier une personne (ou un dispositif tel un site WEB) à une paire de clés asymétriques (privée - publique). Ce certificat porte la signature numérique de l'Autorité de certification qui l'a émis

Comme nous l'avons vu :

- les clés publiques sont distribuées sous la forme d'un certificat électronique ;
- ce certificat correspond à une identité électronique et lie une personne (ou encore un dispositif) à une clé publique ;
- ce certificat est signé numériquement par une autorité de certification.

17) Que contient habituellement un certificat électronique d'identification ?
Le contenu d'un certificat électronique d'identification est précisé dans la norme X.509 (version 3) de l'Union internationale des télécommunications (UIT) :

- numéro de série du certificat ;
- identifiant d'algorithme de signature utilisée par l'émetteur ;
- nom de l'émetteur du certificat ;
- période de validité ;
- nom du titulaire ;
- identifiant d'algorithme de clés publiques utilisés par le titulaire ;
- clé publique du titulaire ;
- de plus, un certificat de niveau 3 (toujours selon la norme de X.509 de l'Union internationale des Télécommunications) renfermera les détails de la politique de sécurité selon laquelle les clés sont émises.

18) De quels critères doit-on tenir compte lors de l'évaluation d'une Autorité de certification (AC) ?
Signalons tout d'abord :

- son mode de fonctionnement (son énoncé de pratiques de certification).

Cet énoncé précise entre autres (i) la méthode utilisée pour l'identification initiale des personnes (par ex. : Utilise-t-elle un fichier public d'identification, tel un registre d'État civil ?), (ii) la procédure formelle d'authentification et (iii) la méthode de révocation des certificats ;

- la fiabilité des méthodes d'identification, d'authentification et de certification utilisées (truc : procéder à une évaluation comparative du niveau de risque) ;
- la limite de sa responsabilité (truc : vérifier si l'AC n'exclu pas sa responsabilité pour son activité principale, soit la certification elle-même, dans le cadre de l'entente contractuelle qu'elle propose à l'abonné) ;
- la confirmation que l'AC détient bien une assurance responsabilité.

Une évaluation sérieuse doit aussi inclure notamment les critères suivants :

- le type ou l'origine de l'AC « privée, publique » ;
- le lieu de son siège social « ou sa principale place d'affaires » ;
- l'étendue géographique de son réseau « de distribution » ;
- sa base d'activité «s oit l'achalandage actuel et anticipé » ;
- la crédibilité actuelle de l'AC ;
- la compatibilité de ses services de tiers certificateurs par rapport à ses autres services ;
- la gamme et la qualité des services offerts ;
- la rapidité de livraison des services (délivrance des clés, émission des certificats, etc.) ;
- le niveau de sécurité du personnel de l'AC ;
- l'adhésion de l'AC à des « façons de faire communes » ou à des « pratiques recommandées » ;
- la reconnaissance de cette AC par les autres AC (reconnaissance réciproque) ;
- la fiabilité, tant juridique que technique, de sa solution technologique ;
- la facilité et la simplicité de la solution proposée, pour l'utilisateur ;
- la gestion des certificats ;
- la diffusion de listes des certificats suspendus et révoqués.

Foire aux questions sur l'infrastructure à clé publique

Document produit par :
la Direction de la coordination gouvernementale des technologies de l'information

Ce document a été rédigé par :
M. Yvan Lauzon
Secrétariat du Conseil du trésor (SCT)
Sous-secrétariat aux marchés publics et aux technologies de l'information

Avec l'aide des membres du Comité aviseur interministériel :
M. Michel Després
Secrétariat du Conseil du trésor
M. Claude Francoeur
Société de l'assurance automobile du Québec
Me François Lajeunesse
Secrétariat de l'autoroute de l'information
M. Ross Lamarre
Ministère du Revenu du Québec
M. Yvan Lauzon, coordonnateur du Comité
Secrétariat du Conseil du trésor
Me Michel Léonard
Ministère de la Justice du Québec
Me André Lord
Ministère du Revenu du Québec
M. Michel Marchand
Régie de l'assurance maladie du Québec
M. Raynald Perron
Secrétariat du Conseil du trésor
M. Bernard Plante
Secrétariat du Conseil du trésor
M. Michel Rosciszewski
Secrétariat de l'autoroute de l'information
M. Pierre P. Tremblay
Secrétariat du Conseil du trésor

Pour toute question ou commentaire :
M. Yvan Lauzon
Coordonnateur du Chantier
Cadre de sécurité de l'Inforoute gouvernementale
Téléphone : (514) 873-7237
Télécopieur : (514) 873-7749
Courrier électronique : Yvan.Lauzon@SCT1.gouv.qc.ca

*** REMERCIEMENTS ***

Remerciement à toutes les personnes qui ont contribué à la révision du présent document et plus particulièrement aux personnes suivantes qui l'ont commenté :

M. Pierre P. Tremblay, ingénieur, SCT-SG-DGT
Me Serge Parisien, avocat à la Faculté de Droit de l'Université de Montréal
Me Thierry Piette Coudol, avocat à la Cour de Paris & expert technique
M. Bernard Plante, ingénieur, SCT-SG-DGT
Mme Francine Thomas, directrice générale du Comité des responsables de l'informatique du secteur public (CRISP)