SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUES AU GOUVERNEMENT DU QUÉBEC

Document d'information sur l'infrastructure à clé publique élaboré 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
Direction de la coordination gouvernementale en technologies de l'information
Service des orientations et politiques de renouvellement

24 novembre 1997

TABLE DES MATIÈRES

RÉALISATION

Document publié par :
la Direction de la coordination gouvernementale en technologies de l'information

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

M^{e} François Lajeunesse
Secrétariat de l'autoroute de l'information

M. Ross Lamarre
Ministère du Revenu du Québec

Me Michel Léonard
Ministère de la Justice du Québec

M^{e} 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
Remarque

La forme générique du masculin a été utilisée dans ce document afin d'alléger le texte.

Pour toute question ou commentaire :

M. Yvan Lauzon
Coordonnateur
Comité aviseur interministériel
Cadre de sécurité de l'Inforoute gouvernementale
Secrétariat du Conseil du trésor
1410, rue Stanley, bureau 800
Montréal (Québec)
H3A 1P8
Téléphone : (514) 873-7237
Télécopieur : (514) 873-7749
Yvan.Lauzon@sctl.gouv.qc.ca

M. Michel Després
Directeur
Services des orientations et des politiques de renouvellement
Secrétariat du Conseil du trésor
875, Grande Allée Est, 4e étage
Québec (Québec)
G1R 5R8
Téléphone : (418) 528-6117
Télécopieur : (418) 646-3571
Michel.Despres@sct.gouv.qc.ca

Remerciements

Nos remerciements visent toutes les personnes qui ont contribué à la rédaction ou à la révision du présent document d'information.

Nos remerciements s'adressent plus particulièrement à Mme Sylvie Labrèche, M. Douglas Beeson et M. Richard Coveney, de l'Institut mondial du Commerce électronique, ainsi que Me Serge Parisien, du Centre de recherches en droit public de l'Université de Montréal.

AVANT PROPOS

Le développement des services électroniques accessibles à partir des Inforoutes s'effectue à une vitesse fulgurante depuis la fin de 1993. A tous les jours, de nouveaux services apparaissent avec des fonctions toujours plus poussées.

Toutefois, il semble bien que les transactions électroniques de nature commerciale ou administrative engageant l'Administration ne pourront se généraliser tant que l'on ne pourra garantir à la fois la sécurité juridique et la sécurité technique des transactions, et ce, à tous les intervenants impliqués, tels que : les utilisateurs (consommateurs, commerçants), les institutions financières et les organisations gouvernementales.

Cette sécurisation est essentielle afin d'assurer la confiance nécessaire au développement des activités commerciales sous forme électronique (courrier électronique, babillard électronique, formulaires EDI, site WEB.

En effet, l'identité des personnes transigeant à distance revêt une importance particulière dans le Cyberespace puisque la dématérialisation des transactions accroît le risque qu'une personne transige sous une identité fictive, ou encore, usurpe l'identité d'une autre personne. De même, l'utilisation de réseau distribué et ouvert, tel que l'Internet, accroît le risque d'accès non autorisé (indiscrétion, modification des informations) et d'« attaques » des systèmes gouvernementaux branchés sur l'Inforoute (ex. : virus). Dan un tel contexte, la signature électronique s'avère essentiel.

À ce jour, plusieurs pays (ex. : Allemagne) et près des trois-quarts des états américains (ex. : Utah, Floride) ont déjà légiféré pour définir quels moyens étaient juridiquement acceptables pour « signer » les documents électroniques, c'est-à-dire pour identifier les personnes et manifester leur consentement à un message ou une transaction électronique. De façon pratique, cette « signature électronique » peut-être réalisée à l'aide d'une paire de clés cryptographiques « asymétriques » (une clé privée et une clé publique). On parle alors de signature numérique.

Cette signature pourrait servir tant à l'interne (ex. : formulaire électronique, message électronique « sensible », application Intranet), qu'à l'externe (ex. : formulaire EDI, babillard électronique, commande électronique, application Extranet et Internet).

Il est donc important que le gouvernement du Québec se dote très bientôt d'une infrastructure adéquate pour être en mesure de fournir facilement, et à coût abordable, une « signature électronique » à ses employé(e)s.

Le gouvernement du Québec sera également appelé à participer au déploiement des moyens assurant la signature électronique et la certification électronique d'identité. auprès de ses partenaires d'affaire et ses diverses clientèles. Ces moyens contribueront à accroître la confiance dans les échanges électroniques impliquant l'Administration.

Plusieurs chantiers ont été lancés le premier mai 1997 afin de favoriser le développement harmonieux de l'Inforoute gouvernementale. Un de ces chantiers est le « Cadre de sécurité de l'Inforoute gouvernementale ».

Un comité aviseur interministériel a été mis sur pied dès le lancement de ce Chantier, ceci afin d'établir des orientations gouvernementales en matière de sécurisation des échanges électroniques et proposer un cadre de fonctionnement gouvernemental pour l'Infrastructure à clé publique. Formé d'une dizaine de personnes, juristes, technologues et administrateurs, ce comité a produit dans un délai extrêmement court une synthèse des enjeux, principes directeurs et orientations de base de la sécurisation des échanges électroniques au gouvernement du Québec. Ce document est disponible sur le site WEB du SCT.

Ces principes directeurs et orientations font l'objet d'une consultation gouvernementale élargie à l'automne 1997. Ils seront ensuite déposés en vue d'être adoptés officiellement par les autorités gouvernementales.

Des travaux plus détaillés, touchant aux aspects juridiques, organisationnels et techniques de l'ICP au gouvernement du Québec, sont actuellement en cours. Ceux-ci devraient conduire à la publication, en février 1998, de documents d'encadrement juridique technologique, et organisationnel de l'ICP gouvernemental, ainsi que « d'un Accord-type sur la certification croisée (reconnaissance mutuelle entre autorités de certification) », favorisant ainsi l'interopérabilité du processus de certification.

Le présent document d'information vise à donner au lecteur une vue d'ensemble de l'utilité de l'ICP et de ses composantes.

INTRODUCTION

L'utilisation des nouvelles technologies de l'information et des communications (NTIC) repose, pour la conduite des affaires, sur l'établissement d'un environnement sûr. La cryptographie à clé publique peut assurer un tel environnement sécuritaire pour l'échange de documents commerciaux, administratifs et techniques de nature sensible. Ces échanges impliquent généralement aussi bien les organisations publiques, que les entreprises privées et les individus.

À l'égard des gouvernements, l'OCDE déclarait d'ailleurs dans un document publié en mars 1997 :

« En tant que très grands clients et distributeurs de services publics, les gouvernements ont beaucoup à gagner de la mise en oeuvre des principes de l'administration électronique, qui évoluent de manière symbiotique avec le commerce électronique. Le commerce électronique s'inscrit dans une approche évolutive du commerce et de l'administration qui pourrait, à terme, entraîner l'application des technologies de l'information et de la communication à un très large éventail de processus de production et de distribution à l'échelle mondiale. »

Le Secrétariat du Conseil du trésor énonçait dans un document de novembre 1996 quelques-uns des grands principes dont il faut tenir compte dans le développement de l'Inforoute gouvernementale québécoise. Cette démarche était alors entreprise afin d'assurer l'efficacité de l'Administration publique, de maximiser les effets socio-économiques de son implication dans l'Inforoute sur les entreprises québécoises et d'améliorer du même coup les échanges entre l'Administration et la population.

« L'ensemble des citoyens doit avoir accès le plus tôt possible à cet outil de développement qu'est Internet, et ce, sans égard à leurs situations géographiques, sociales ou économiques. Les citoyens doivent également avoir des moyens pratiques, simples et peu coûteux de sécurisation des transactions d'affaires pour pouvoir transiger directement, tant avec les organisations gouvernementales, qu'avec les entreprises et les maisons d'enseignement. »

Comme on l'a vu, l'établissement avec certitude de l'identité des personnes ou des organisations revêt une importance particulière dans le développement de l'Inforoute gouvernementale.
D'ailleurs, un document récent produit à la demande du Secrétariat du Conseil du trésor en fait état :

« Les Autorités de certification, ou tiers certificateurs, représentent sans conteste l'un des sujets de l'heure en matière de commerce électronique. Le système de certification utilisé par ces tiers vise à renforcer la fiabilité et la sécurité des mécanismes de signature basés sur la cryptographie à clé publique. Le caractère transfrontière du commerce électronique et la nouveauté du sujet font que la notion d'autorité de certification ne peut valablement être abordée en vase clos. La Commission des Nations Unies pour le droit commercial international (CNUDCI), dans un Rapport du Groupe de travail sur le commerce électronique publié le 12 mars 1997, souligne l'importance des infrastructures de certification pour le développement harmonieux des transactions économiques par voie électronique. »

La globalisation des marchés et l'extraordinaire explosion de l'Internet font en sorte qu'il est facile d'acheter, vendre, échanger ou partager des biens et de l'information avec presque tout le monde, quasi n'importe où. Les membres de cette communauté virtuelle ne se connaissent peut-être pas. Dans ce contexte, comment deux parties, qui n'ont aucune autre relation entre elles, peuvent-elles se faire mutuellement confiance pour permettre l'échange d'argent ou d'information sur un réseau informatique ? La création d'une Infrastructure à clé publique (ICP) est une solution efficace à ce besoin d'identification dans un contexte de transaction à distance.

L'Infrastructure à clé publique (ICP) permet aux individus et aux organisations de communiquer et d'effectuer des transactions commerciales de façon sécuritaire sur des réseaux informatiques ouverts comme Internet, et ce, au niveau local, national ou mondial.

Ce système repose sur un ensemble de technologies, de normes et de politiques qui permettent d'assurer un environnement sécuritaire aux échanges électroniques sur les réseaux ouverts comme Internet.

1. Contexte des échanges électroniques sécurisés

Dans cette section nous traiterons du Commerce électronique, des téléprocédures, et des Administrations électroniques. Nous traiterons également des différents concepts et technologies associés à l'ICP, notamment, le chiffrement, la cryptographie asymétrique, ainsi que la signature électronique.

i) Le Commerce électronique se définit comme toute transaction dont le moyen de communication utilisé pour l'effectuer est électronique. Le Commerce électronique peut également être définit comme un ensemble de produits et de services qui permettent de réaliser des transactions et de partager de l'information essentielle à la relation d'affaire, en utilisant des réseaux électroniques et des systèmes informatiques. Le Commerce électronique peut se faire à l'aide d'une variété de technologies de l'information et de réseaux utilisées séparément ou de façon intégrée.

   Dans un environnement économique, le commerce électronique englobe ainsi la réalisation de transactions d'affaires ou commerciales sous forme électronique, associant tant les particuliers que les organisations privées et publiques, en vue de la production, la distribution et, le cas échéant, la vente de biens et services.

   Le Commerce électronique désigne également les effets de l'échange électronique de données commerciales sur les institutions et les processus législatifs, juridiques et réglementaires qui encadrent les activités commerciales. Ainsi, les échanges entre les administrations publiques, la population et les entreprises sont également assimilés à des activités de commerce électronique.

ii) Lorsqu'un échange électronique permet d'accomplir une procédure administrative, on parle alors de téléprocédure. En France, la COSIFORM (Commission pour la simplification des formalités) définit la téléprocédure comme suit :

   «... un ensemble organisé de modalités techniques d'échange de données structurées entre l'administration et les usagers, par lesquelles s'accomplissent les formalités déclaratives, ainsi que les relations contractuelles et commerciales, dans le respect des règles légalement ou réglementairement prévues. »

iii) En plus des téléprocédures, l'utilisation du courrier électronique, les processus d'information et les services interactifs avec les fournisseurs et la population sont des applications « électroniques » internes des administrations. En effet, les administrations électroniques sont définies comme étant des administrations publiques offrant leurs services ainsi que la diffusion d'information par des moyens électroniques.

   À titre d'exemple, le projet du G7 intitulé « Gouvernement en ligne » favorise l'utilisation des moyens électroniques plutôt que le papier.

iv) L'ICP repose sur l'utilisation de la cryptographie à clé publique. Cette dernière utilise le procédé de chiffrement qui est la « transformation cryptographique de données en vue de produire un texte chiffré ». Il s'agit donc d'une « opération qui consiste à transformer un texte clair en un texte codé à des fins de protection de l'information ». Cette transformation de données au moyen de la cryptographie pour rendre celle-ci inintelligibles (données chiffrées) permet d'en assurer la confidentialité. Dans un document récent, l'OCDE soulignait :

   « Sur le plan historique, le chiffrement a été utilisé pour un encodage de l'information afin de cacher des messages secrets aux parties non autorisées et, à ce titre, il a toujours joué un rôle important sur les plans de la sécurité militaire et nationale. Le chiffrement utilise un algorithme pour transformer les données de manière à les rendre inintelligibles pour quiconque ne possède pas la clé de chiffrement nécessaire pour les déchiffrer. La puissance de calcul accrue dont on dispose aujourd'hui permet d'utiliser des algorithmes mathématiques complexes pour le chiffrement des données. Le chiffrement soulève une question critique, relative à l'aspect peut-être le plus largement débattu et en même

temps le plus susceptible de conduire à de grandes disparités dans les réglementations nationales : il s'agit du conflit perçu entre l'utilisation privée du chiffrement à des fins de confidentialité et le souci exprimé par les gouvernements de voir cette utilisation limiter leur capacité de protéger la sûreté publique et la sécurité nationale. »

v) Le chiffrement s'effectue grâce à une clé de chiffrement. Celle-ci est le moyen de chiffrer un message pour le rendre inintelligible ou de le déchiffrer pour le rendre à nouveau intelligible. En théorie, on peut créer une clé à partir de n'importe quel symbole ou caractère. Mais en pratique, la cryptographie moderne, qui se fonde sur l'informatique, emploie des clés de chiffrement numérique. La clé elle-même est une longue série de chiffres. Par exemple, la clé utilisée par le logiciel Pretty Good Privacy (PGP) est un numéro à 1024 bits binaires, correspondant ainsi à un numéro à base décimale d'une longueur maximale de 309 chiffres.

vi) Lorsque le chiffrement et le déchiffrement utilisent une seule et même clé, la cryptographie est alors qualifiée de symétrique.

vii) À l'opposé, la cryptographie dite « asymétrique » emploie une clé pour le chiffrement et une autre clé complémentaire pour le déchiffrement. La cryptographie à clé publique fait appel à un système de cryptographie asymétrique qui consiste à rendre publique l'une des deux clés, soit la clé publique, tout en gardant confidentielle l'autre clé, soit la clé privée. Cette dernière sert à déchiffrer les documents reçus et rendre l'information lisible et compréhensible pour le destinataire. La clé privée permet également la signature numérique qui est décrite à l'annexe A.

viii) Le rôle d'une ICP est primordial puisqu'elle fait connaître la clé publique de ses abonnés et procède à l'émission de certificat électronique d'identité. En outre, elle assure un niveau élevé de confiance en offrant des services de confidentialité, de contrôle d'accès, d'intégrité, d'authentification et de non-répudiation des transactions.

2. Pourquoi une infrastructure à clé publique (ICP) ?

Le Commerce électronique entre les organisations existe depuis une trentaine d'années. Lors d'une transaction commerciale réalisée au moyen de l'EDI par exemple, une entente préalable a été signée par les partenaires d'affaires, en vue d'échanges récurrents. Dans le cas du commerce électronique sur le réseau Internet, puisque les parties ne sont pas en présence l'une de l'autre et ne se connaissent probablement pas d'ailleurs, il est crucial de développer des infrastructures, des politiques et des normes pour que les transactions électroniques puissent se faire de manière homogène et transparente à travers le monde entier.

Tout d'abord, la mise sur pied d'une ICP permet d'effectuer des échanges électroniques dans un environnement sécuritaire. En effet, puisque l'ICP repose sur le chiffrement des informations confidentielles, l'intégrité et l'authentification des messages échangés sont assurées.

Deuxièmement, grâce à l'utilisation de la signature numérique, le destinataire reçoit un document signé électroniquement. Ainsi, il obtient la confirmation de l'origine du message et de l'intégrité de l'information. Cela est possible en déchiffrant la signature à l'aide de la clé publique de l'expéditeur. La signature électronique, tout comme la signature manuscrite, a donc une fonction de non-répudiation, rendant possible l'utilisation en preuve de document reçu.

Une troisième utilité de l'ICP est la mise en confiance des parties par la certification électronique. Puisque les parties transigeant dans un environnement virtuel ne sont pas en présence l'une de l'autre, il est nécessaire qu'un tiers bénéficiant de la confiance des parties puisse confirmer à l'une et à l'autre que chacune est bel et bien celle qu'elle prétend être. Ce tiers de confiance, après vérification, attribue un certificat électronique personnalisé à chacune des parties. Le certificat est un document contenant diverses informations sur son « utilisateur », notamment sa clé publique.

En plus de favoriser le développement du commerce électronique, le gouvernement pourrait réaliser des avantages importants par la mise sur pied d'une ICP assurant les échanges administratifs sécurisés. Notamment, sur l'Inforoute, elle assurerait l'interopérabilité des applications de confidentialité et de commerce électronique entre les ministères, les partenaires commerciaux, les autres juridictions et les autres nations.

Les services offerts par un tiers de confiance permettraient d'abord de jeter les bases pour le développement à grande échelle de services de chiffrement des informations confidentielles de signature numérique de documents et de certification électronique d'identité. Ces services peuvent également toucher à l'horodation, éléments essentiels aux transactions électroniques. L'État bénéficierait également d'une architecture commune permettant l'établissement de normes et d'interfaces de programmation supportant un éventail de technologies de chiffrement et de signature numérique pour l'ensemble du gouvernement.

3. Les composantes de l'ICP

Tout comme dans un réseau de transport en commun ou dans un système de santé, une ICP dépend de plusieurs composantes pour fonctionner adéquatement. Certains éléments sont intangibles, tels les règles et principes de fonctionnement; d'autres sont des objets physiques, comme l'équipement et les logiciels informatiques. Cette section décrit les règles et les principes fondamentaux de l'ICP ainsi que leur fonctionnement en vue de l'échange sécuritaire d'information par voie électronique. Les précisions de la mise en oeuvre de ces principes seront abordés dans le chapitre 4.

Confiance entre les tiers

Un tiers de confiance est une entité reconnue pour sa capacité d'établir l'identité d'une personne. Le tiers de confiance agit donc en tant qu'intermédiaire et se porte garant de l'identité des autres parties. Tant que deux parties font confiance à un tiers, il peut exister une relation indirecte mais réelle de confiance entre deux étrangers. Voyons l'exemple suivant :

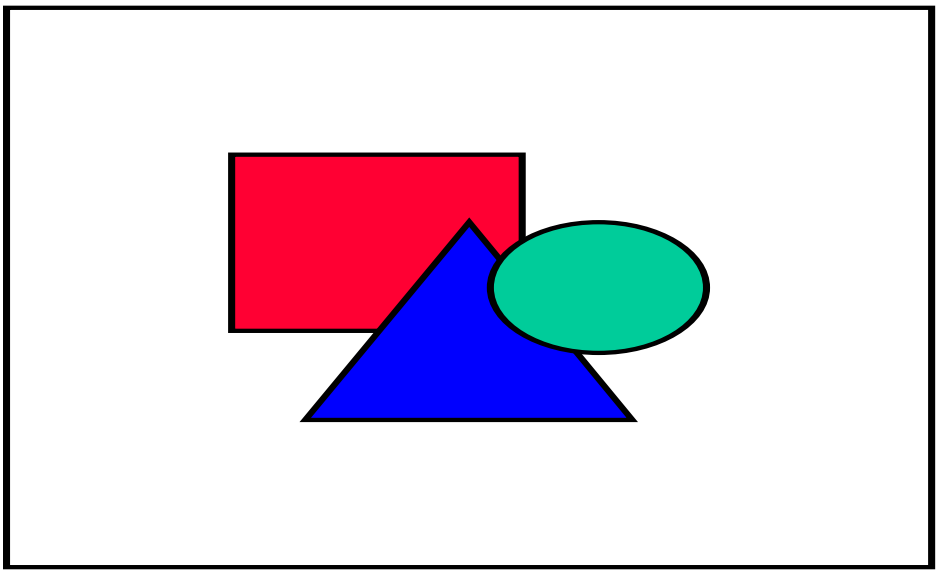

Figure 1- Confiance entre les tiers

Alice veut acheter un bien auprès de Bob, mais elle ne le connaît pas et rien ne lui permet d'avoir confiance en Bob pour effectuer la transaction en toute quiétude. Toutefois, Alice et Bob connaissent Charles et lui font tous deux confiance. Charles assure Alice que Bob est un marchand et qu'Alice est une cliente (Figure 1). Alice et Bob peuvent maintenant faire des affaires en toute confiance (ou du moins avec le même degré de confiance qu'ils ont en Charles).

Cette relation fondée sur la confiance est au coeur de l'ICP. Puisque l'ICP repose sur la cryptographie à clé publique pour les mécanismes de chiffrement et d'authentification, il doit y avoir un moyen permettant aux utilisateurs de savoir avec certitude qu'une clé publique donnée appartient bel et bien à la personne ou l'organisation pour laquelle elle a été émise. Une tierce partie de confiance permet aux utilisateurs d'avoir cette certitude. Au sein d'une ICP moderne, des agents de certification tiers appelés Autorités de certification (AC) jouent le rôle du tiers de confiance et sont chargés d'émettre les certificats électroniques aux utilisateurs.

Certificat

Par exemple, afin d'éviter de communiquer avec Charles chaque fois qu'elle veut faire de nouveaux achats, Alice peut demander à Charles de lui donner un document attestant de l'Identité électronique d'Alice. Bob en fait de même. Ensuite, lorsqu'Alice veut transiger avec Bob, elle n'a qu'à lui montrer la note de confiance de Charles et à examiner le document de Bob. Comme les deux documents sont signés par Charles, une relation de confiance quant à l'identité s'établit sans nouvelle intervention de la part de Charles.

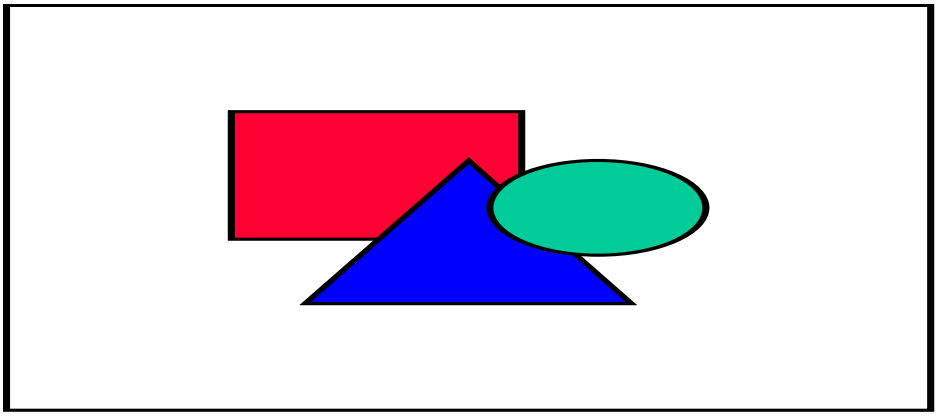

Figure 2- Échange de certificats

Dans le contexte d'une ICP, ces documents s'appellent des certificats. Un certificat est un document électronique qui garantit l'identité de la personne ou de l'organisation qui en est détentrice. Les certificats électroniques d'identité sont émis et vérifiés par des tiers de confiance qui fournissent ainsi un gage de confiance entre les participants d'une transaction électronique (Figure 2).

Concrètement, les certificats électroniques utilisés dans les ICP modernes contiennent de nombreux éléments importants d'information, comme le nom du détenteur et de l'émetteur, la clé publique du détenteur et la signature numérique de l'émetteur du certificat (tiers de confiance). Les renseignements sur l'identité du détenteur et de l'émetteur remplissent des fonctions évidentes pour l'établissement de la confiance. La clé publique du détenteur permet aux autres utilisateurs de communiquer de façon sécuritaire avec le détenteur du certificat. Finalement, l'application de la signature numérique de l'émetteur (le tiers de confiance) sur la totalité du certificat en assure l'authenticité et l'intégrité en faisant office de sceau.

Les certificats numériques sont habituellement émis dans le format normalisé X.509 (version 3) qu'on élaborera à la section technologique.

Autorité de certification

Une Autorité de certification, ou AC, est une personne ou une organisation responsable de l'émission de certificats électroniques aux utilisateurs d'une ICP. Selon les exemples déjà mentionnés Charles est une Autorité de certification. Tout comme les cliniques médicales locales constituent souvent le premier contact des patients avec le système de santé, les Autorités de certification se situent sur la ligne de front d'une ICP. Elles ont la responsabilité d'identifier un utilisateur, d'émettre et de signer les certificats prouvant l'identité de cet utilisateur.

À l'instar d'un hôpital qui ne peut soigner tous les malades d'une grande ville, une seule et même AC ne peut être responsable de gérer tous les utilisateurs d'une ICP. Ainsi, de petites AC peuvent chacune avoir la responsabilité d'un groupe local d'utilisateurs. Par ailleurs, chaque agence ou ministère de l'appareil

gouvernemental peut avoir sa propre AC pour s'occuper seulement de son personnel. De la même façon, une grande société peut avoir une ou plusieurs AC internes pour émettre des certificats aux employés de la compagnie. Des AC destinées au grand public peuvent aussi être mises sur pied, soit par des entreprises privées (comme VeriSign aux États-Unis), soit par des organisations gouvernementales ou paragouvernementales.

Certification réciproque ou croisée

L'utilisation des AC locales représentent des avantages indéniables : une plus grande flexibilité et une facilité d'accès. Cela soulève cependant une question importante : les utilisateurs certifiés par une AC locale pourront-ils communiquer avec les utilisateurs d'une autre AC ? Charles peut bien se porter garant de l'identification d'Alice et de Bob, mais il ne sait rien de Francine et d'Edgar, dont les certificats proviennent de Daniel. Par contre, Daniel connaît Francine mais ignore tout d'Alice.

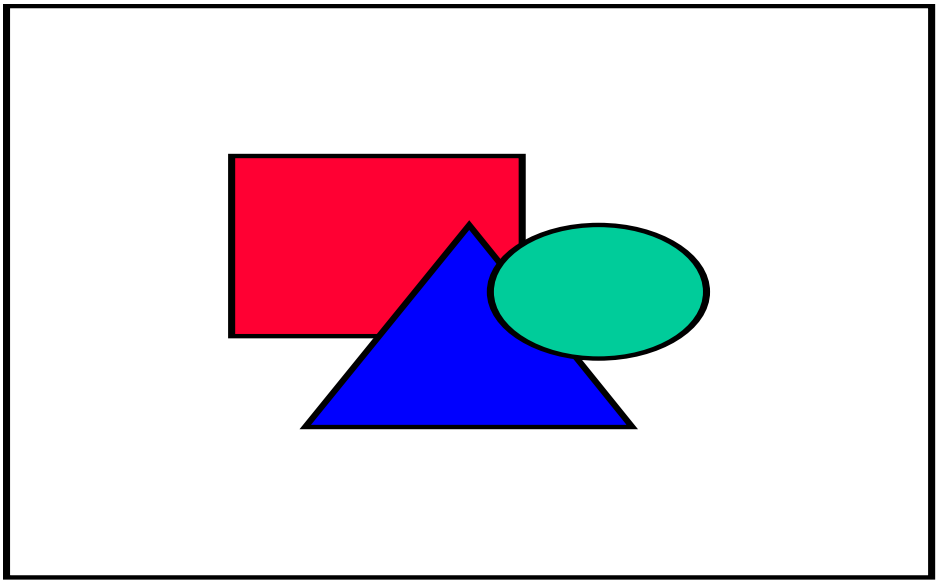

Figure 3- Certification réciproque

La solution à ce problème consiste à permettre à Charles de certifier Francine et vice versa. Cette pratique, appelée certification réciproque (ou croisée), permet à deux AC de se reconnaître l'une l'autre. Ce prolongement du concept de confiance permet aux utilisateurs d'une AC d'avoir implicitement confiance dans les utilisateurs de l'autre AC (Figure 3).

La certification réciproque est le fondement du prolongement du principe du tiers de confiance sur une grande échelle.
Hiérarchie de confiance

La certification réciproque entre deux AC est cependant insuffisante pour l'établissement d'une ICP nationale ou internationale. Le trop grand nombre d'AC locales rendrait peu pratique la réalisation d'ententes de réciprocité entre chacune. Par exemple, s'il y a 100 AC locales, chacune devrait gérer 99 ententes de certification mutuelle. Pire encore, chaque certificat émis par une AC devrait comprendre la signature des 100 AC de l'ICP.

On peut résoudre ce problème en considérant les AC locales comme les utilisateurs d'une AC d'un niveau supérieur. Cette dernière émet un certificat pour chacune de ses AC. L'AC locale inclut à son tour la signature numérique de son AC supérieur dans les certificats de ses utilisateurs. L'utilisateur peut ainsi vérifier le cheminement de la certification . « La structure qui en découle s'appelle ainsi une hiérarchie de

confiance ». Au sommet, on trouve une AC qui doit implicitement avoir la confiance de tous les utilisateurs de l'ICP (Figure 4).

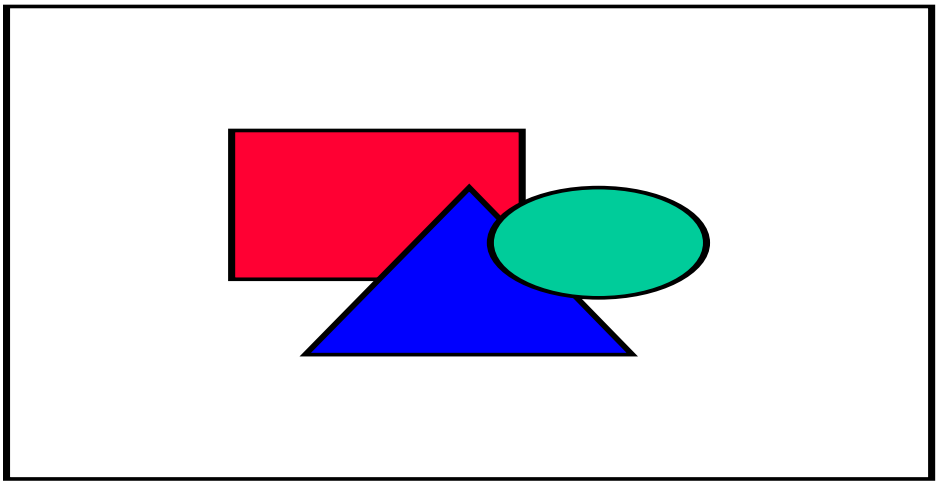

Figure 4- Hiérarchie de confiance

Sommaire sur les composantes de l'ICP

Comme on l'a vu, l'ICP est composée d'un ensemble de technologies, de normes et de politiques qui permettent d'assurer un environnement sécuritaire aux échanges électroniques sur les réseaux ouverts comme Internet.

L'ICP est un système qui permet aux individus et aux organisations de communiquer et d'effectuer des transactions commerciales de façon sécuritaire sur des réseaux informatiques ouverts comme Internet, et ce, au niveau local, national ou mondial.

Les utilisateurs se fient à un tiers de confiance, leur Autorité de certification locale, pour l'émission d'un certificat électronique signé qui inclut l'identité et la clé publique de l'utilisateur. En pratique, certaines AC peuvent être appuyées dans leurs tâches par des autorités locales d'enregistrement (ALE), lesquelles maintiennent un contact direct entre les utilisateurs lorsque l'AC est géographiquement éloignée. Les ALE ne peuvent pas émettre de certificat; elles peuvent par contre aider les gens à faire révoquer leur certificat, confirmer leur identité et distribuer les certificats de clé publique de leurs utilisateurs respectifs.

L'AC locale reçoit un certificat d'une AC d'un niveau supérieur; elle peut également conclure des ententes de réciprocité avec d'autres AC locales et d'autres niveaux. En retour, les AC intermédiaires peuvent être certifiées par des AC de plus haut niveau, dans une chaîne de confiance qui atteint finalement l'AC au sommet de l'infrastructure. L'ICP, en permettant des communications sécuritaires entre ses utilisateurs tout en offrant des moyens de prolonger la hiérarchie de confiance à l'extérieur des entreprises et des pays, fournit les fondations pour la transmission de communications sécuritaires à l'échelle de la planète.

4. Aspects technologiques de l'ICP

L'objectif d'une ICP consiste à permettre aux individus et aux organisations de transiger entre eux de façon sécuritaire. En pratique, l'ICP doit être capable de fonctionner correctement quels que soient les équipements ou logiciels informatiques utilisés. Une telle interopérabilité passe par l'adoption de normes, de protocole et de pratiques reconnues. L'annexe *B* présente quelques-unes des normes techniques rencontrées dans le cadre d'une ICP et décrit les certificats électroniques d'identité.

5. Émergence d'initiatives en matière d'ICP

Il existe actuellement, à travers le monde, plusieurs projets et initiatives en matière d'ICP. Certains sont des initiatives législatives, des avant-projets ou des textes de loi, alors que d'autres sont des projets pilotes ou opérationnels, des lignes directrices ou des cadres de travail.

La majorité des pays du G7, ainsi que des organisations internationales telles que la Commission des Nations Unies pour le droit commercial international (CNUDCI), la Chambre de commerce internationale (CCI), la Direction générale XIII de la Commission européenne et l'Organisation de coopération et de développement économique (OCDE) sont à mettre sur pied divers types de projets qui sont à des stades d'avancement différents. À ce jour, il n'existe qu'une seule infrastructure de certification entièrement opérationnelle, soit celle de la firme américaine VeriSign. Le phénomène de la mise en oeuvre d'ICP ne fait donc que débuter.

Pour sa part, le Canada dénombre plusieurs initiatives en émergence. Ces initiatives sont souvent embryonnaires et donnent lieu à une documentation publique parfois fragmentaire, voire inexistante. Or, sont présentés ici les projets et initiatives à propos desquels une documentation publique est disponible. Il s'agit des infrastructures de clés publiques du gouvernement fédéral, de la Société canadienne des postes et de la Chambre des notaires du Québec (Notarius).

Gouvernement du Québec

Plusieurs initiatives sont actuellement en cours au gouvernement du Québec touchant à la sécurisation des échanges électroniques sur les Inforoutes. Un portrait détaillé de la situation actuelle et des besoins en matière d'identification et de certification électronique des personnes et des dispositifs sont actuellement en cours de préparation au Secrétariat du Conseil du trésor et au Secrétariat de l'autoroute de l'information.

Ces initiatives seront présentées à la communauté gouvernementale au printemps 1998.

Gouvernement fédéral

En décembre 1995, le gouvernement fédéral a lancé un projet d'ICP dont le but est de faciliter le commerce électronique national et international et d'atteindre son objectif de recourir autant que possible aux transactions électroniques. L'ICP fédérale devrait fournir dès 1998 un processus uniforme de gestion des clés cryptographiques et de certification afin d'assurer, d'une part, la confidentialité des informations et, d'autre part, l'utilisation d'une signature numérique.

Actuellement, les ministères et les organismes fédéraux suivants participent au développement de cette ICP :

- Bureau du Conseil privé
- Centre de sécurité des télécommunications (CST-CSE) du gouvernement fédéral
- Citoyenneté et Immigration Canada
- Gendarmerie royale du Canada
- Ministère des Affaires étrangères et du Commerce international
- Ministère de la Défense nationale
- Postes Canada
- Revenu Canada
- Santé Canada
- Secrétariat du Conseil du trésor
- Travaux publics et Services gouvernementaux Canada

L'initiative de certification du gouvernement fédéral est chapeautée par l'Autorité de gestion de politiques

(AGP) qui est actuellement constituée d'un comité interdépartemental présidé par le Conseil du trésor. Les fonctions principales de l'AGP sont de voir au développement de politiques pour l'opération de l'ICP, et d'approuver les accords de certification croisée et de mise en correspondance de politiques avec les autres Autorités de certification hors de l'Administration fédérale.

Pour ce faire, l'ICP du gouvernement du Canada sera fondée sur la famille de produits logiciels de sécurité de la compagnie Entrust Technologies.

Le Comité de l'AGP travaille actuellement à l'élaboration des exigences de politique, de gestion et de l'infrastructure. Une première approche a été présentée en novembre 1996 dans le document Certificate Policy and Certification Practice Statement Framework. Le Comité travaille en collaboration avec le gouvernement fédéral américain dans le but ultime d'atteindre un cadre de travail commun et une compatibilité optimale en matière de politiques et d'énoncés de pratiques de certification.

Le Gouvernement du Canada a publié un Livre Blanc en mai 1997 dans lequel se trouve une présentation du cadre conceptuel et de la mise en oeuvre de cette ICP du gouvernement fédéral. Il a également publié, le 3 novembre 1997, une première version d'une politique de certificat. Cette politique définit pour quatre niveaux de confiance (rudimentaire, base, moyen, élevé), les certificats utilisés pour le chiffrement de confidentialité (4) et pour la signature numérique (4).

Société canadienne des postes

Dans le cadre d'un projet d'intégration des nouvelles technologies aux méthodes traditionnelles de transmission du courrier, Postes Canada travaille à la mise sur pied d'un service de distribution et de communications appelé pour l'instant Cases postales électroniques.

À la base de ce service se trouve le Répertoire national, une liste complète des individus résidant au Canada et leurs coordonnées respectives. Le service de distribution permettra aux destinataires de messages, dont les coordonnées seront répertoriées, de choisir le mode de communication par lequel ils voudront que les messages leur soient envoyés, soit par télécopieur, soit par courrier électronique ou traditionnel. Par ailleurs, le répertoire pourrait également contenir une zone dont l'accès serait restreint à Postes Canada, qui inclurait les champs d'intérêt des individus permettant ainsi le marketing ciblé.

Pour assurer la confidentialité de ces messages, Postes Canada développe actuellement une infrastructure de clé publique. Les utilisateurs génèrent leur paire de clés et procèdent à leur enregistrement auprès d'un maître de poste.

Les premiers essais pilotes sont planifiés pour la fin de 1997, début 1998. En plus du Répertoire national, Postes Canada souhaite offrir d'autres services à valeur ajoutée, notamment le timbrage électronique (horodation), l'archivage et le recouvrement de documents ainsi que la certification réciproque ou croisée.

En plus de participer au Comité de l'Autorité de gestion de politiques de l'ICP du gouvernement fédéral, Postes Canada entretiennent des relations avec l'Union postale universelle, le United States Postal Services et l'International Post Corporation. Cette coopération est fort souhaitable afin que les politiques ne divergent pas des décisions qui seront prises au sein de l'AGP fédérale.

Chambre des notaires du Québec

La Chambre des notaires du Québec a rendu public en avril 1996 le document Projet d'infrastructure de certification notariale. Ce projet est désormais géré par la corporation sans but lucratif Notarius, filiale de la Chambre des notaires.

Dans l'infrastructure à clé publique de Notarius, le Secrétaire de l'Ordre des notaires du Québec agit comme autorité de certification des notaires, rôle qu'il détient déjà dans l'environnement traditionnel du

papier. Ainsi, il certifie le statut légal et la signature officielle des notaires en exercice ainsi qu'aux fins de transactions internationales ou étrangères.

Une autorité supérieure de certification, le Centre de certification du Québec, est responsable de l'établissement des politiques et règles pour l'établissement, le contrôle et la vérification de niveaux inférieurs de certification au Québec et de la certification croisée avec d'autres autorités de certification. Le Centre est encadré par les normes de certification édictées par la Chambre des notaires du Québec dans le cadre de son contrôle de l'exercice de la profession par ses membres.

Ses fonctions sont d'assurer la gestion de la génération de clés cryptographiques et leur distribution. Dans le cadre de ce projet, le Centre de certification du Québec fournit un service de répertoire électronique selon la norme X.500 ainsi que des services d'horodation, d'archivage et d'arbitrage en cas de différends.

Quant aux notaires, ils utilisent leurs fonctions d'officier public, de conseiller juridique et de fiduciaire pour sécuriser les transactions juridiques.

La stratégie d'implantation de l'infrastructure de certification notariale se divise en trois phases : la mise en place de l'infrastructure, l'intégration aux transactions courantes et l'ouverture au commerce électronique.

La première phase, toujours en cours de réalisation, vise à brancher l'ensemble des notaires du Québec sur l'Inforoute notariale. En parallèle, la deuxième phase a pour but d'informatiser les échanges entre les notaires et leurs principaux partenaires d'affaires et d'intégrer l'EDI à leur pratique courante. La troisième phase est de rendre opérationnelle l'infrastructure de certification notariale auprès de la clientèle des notaires ainsi qu'au grand public.

Le choix d'une technologie particulière n'a pas encore été effectué mais on utilisera vraisemblablement Entrust.

Tout comme Postes Canada, le Centre de certification du Québec, proposé par Notarius, veillera à l'harmonisation de ses politiques avec les autres autorités de certification afin de faciliter le commerce électronique international.

Le début de l'implantation, soit l'émission de moyens de signature numérique aux notaires, est prévu pour le 5 décembre 1997.

6. Besoins de reconnaissance mutuelle des autorités de certification

Il est d'ores et déjà reconnu, par des organisations internationales et nationales, qu'un des principaux enjeux du Commerce électronique est la certification électronique d'identité des personnes. L'OCDE souligne d'ailleurs à cet effet :

« Le caractère transfrontière du commerce électronique et la nouveauté du sujet font que la notion d'autorité de certification ne peut valablement être abordée en vase clos.»

En matière de certification, l'enjeu le plus important est certes la reconnaissance mutuelle des Autorités de certification, aussi appelée certification croisée. Le rôle primordial de la certification a été décrit au chapitre 3.

Toutefois, rappelons que la certification est nécessaire pour s'assurer que les parties engagées lors d'une transaction sont bien celles qu'elles prétendent être, mais aussi qu'elles offrent le niveau de sécurité nécessaire pour mener à bien la transaction. Outre les normes techniques employées lors de la certification électronique, un cadre juridique doit être mis en place pour l'enregistrement des sociétés et des individus. Or, si les normes et politiques adoptées par l'autorité de certification d'une partie divergent de celles de l'autre, elles ne s'accorderont pas une reconnaissance mutuelle. Conséquemment, la transaction ne pourra s'effectuer et le commerce électronique ne pourra pas se déployer à grande échelle.

Dans un Rapport du Groupe de travail sur le commerce électronique publié en mars 1997, la Commission des Nations Unies pour le droit commercial international (CNUDCI) souligne l'importance des infrastructures de certification pour le développement harmonieux des transactions commerciales par voie électronique. Il fait état de l'obligation, pour une Autorité de certification supérieure, de reconnaître le certificat d'une Autorité de certification subordonnée en garantissant notamment l'exactitude des détails du certificat, de sa validité et son maintien en vigueur. Dans sa troisième version, la norme X.509 prévoit des extensions au certificat permettant à une AC ou à une ICP de limiter la reconnaissance à une AC en particulier ou à plusieurs.

Des efforts sont faits pour que la communauté internationale collabore à l'élaboration de politiques et de normes communes. À titre d'exemple, les organisations menant les quatre initiatives mentionnées au chapitre précédent reconnaissent l'importance de cet enjeu et travaillent de concert avec leurs pairs nationaux et internationaux et avec le secteur privé.

CONCLUSION

Les transactions électroniques commerciales ou administratives engageant l'Administration ne pourront se généraliser tant que l'on ne pourra garantir à la fois la sécurité juridique et la sécurité technique des transactions, et ce, à tous les intervenants impliqués.

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 sous une identité fictive, ou encore, usurpe l'identité d'une autre personne.

Il est donc très important que le gouvernement du Québec se dote très bientôt d'une infrastructure adéquate pour être en mesure de fournir facilement, et à coût abordable, une « signature électronique » à ses employé(e)s. Il devra également développer des façons de faire et des pratiques compatibles avec celles de ses partenaires d'affaires, tout en étant acceptables à ses diverses clientèles.

En fait, les moyens de sécurisation des transactions électroniques, comme l'ICP, devront être juridiquement acceptables, technologiquement réalisables, économiquement viables et facile à implanter dans les organisations gouvernementales.

ANNEXE A

Introduction à la cryptographie à clé publique

Dans un système cryptographique à clé publique, la réalisation des différentes fonctions d'identification suppose qu'une personne dispose de deux clés mathématiques complémentaires : une clé privée, dont le caractère secret doit effectivement être préservé, et une clé publique, qui peut être librement distribuée. La clé privée permet de signer le message. L'opération de décodage s'effectue, quant à elle, selon le principe de la complémentarité des clés: un message encodé avec une clé privée ne peut être décodé qu'avec sa clé publique complémentaire. L'exemple suivant illustre le fonctionnement de la signature numérique.

Alice désire envoyer à Bob un message informatisé signé de façon électronique. Après avoir écrit son message, Alice réalise un condensé de ce message (message digest) à l'aide d'une opération mathématique. Ce condensé digital est le résultat d'une fonction appelée fonction de hachage irréversible (« one way hash function » ou « message digest function »). Cette fonction permet de générer de, façon concise, une chaîne de données qui représente le message en question. Cette représentation est sécuritaire, très concise et permet de détecter tout changement apporté au message. En effet, il suffit au destinataire d'appliquer la fonction « hachage » au message reçu et de comparer le condensé ainsi obtenu avec celui transmis par l'émetteur. Toute différence entre les condensés signifie que le message a été modifié en cours de transmission.

Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l'aide de la clé privée d'Alice. Ce condensé encodé constitue la signature numérique. Alice envoie alors à Bob son message (en clair) accompagné de la signature numérique.

ANNEXE B

Normes de chiffrement

Les normes de chiffrement se divisent en trois catégories :

1. Algorithmes de hachage, lesquels produisent des résumés numériques des documents :
   - MD2
   - MD5
   - SHA-1

2. Algorithmes symétriques communs, lesquels emploient une seule et même clé pour le chiffrement et le déchiffrement :
   - DES (Data Encryption Standard)
   - Triple DES
   - CAST (Entrust Technologies)
   - RC2, RC4, RC5
   - IDEA

3. Algorithmes asymétriques, lesquels utilisent deux clés similaires mais différentes, l'une pour le chiffrement et l'autre pour le déchiffrement :
   - RSA
   - ElGamal
   - DSA
   - Certificats

   Pour être utilisables, les certificats d'une ICP particulière doivent être transmissibles et lisibles par d'autres ICP. Un format normalisé de certificat permet l'atteinte de cet objectif.

   Il existe plusieurs normes touchant le format des certificats numériques. La plus répandue est la norme X.509 (version 3), ou plus simplement X.509, laquelle contient les zones d'information suivantes :
   - version
   - numéro de série
   - ID de l'algorithme de la signature
   - nom de l'émetteur
   - période de validité
   - nom du détenteur
   - information sur la clé publique du détenteur
   - identificateur sujet unique
   - extensions
   - signature sur les champs précédents par l'Autorités de certification.

Services de répertoire

Les répertoires électroniques (ou annuaires électroniques) des réseaux informatiques agissent comme d'immenses carnets d'adresses. C'est grâce à ces répertoires électroniques qu'il est possible de retrouver les coordonnées d'une autre personne (par exemple son adresse de courrier électronique ou son numéro de téléphone). Dans le cadre d'une ICP, les annuaires contiennent également les certificats numériques. Ainsi, les répertoires électroniques rendent possible la transmission sécuritaire de documents à quiconque dont l'adresse est connue par l'ICP.

Il est primordial que les répertoires d'une ICP présentent leur information dans un format normalisé. Quoique plusieurs normes existent aujourd'hui, la communauté d'Internet semble se pencher vers la norme X.500. Cette norme prévoit l'existence d'une multitude de petits répertoires locaux dont chacun ne

gère qu'un sous-ensemble d'une ICP. Organisés selon une hiérarchie arborescente (un peu à la manière des AC), les répertoires X.500 permettent des recherches dans plusieurs des « branches » si une recherche locale ne permet pas de trouver la personne recherchée.

Les accès aux répertoires X.500 font également l'objet d'une norme, celle du Lightweight Directory Access Protocol (Protocole « léger » d'accès aux répertoires) ou LDAP.

Normes préliminaires pour Internet

Les travaux récents du Internet Engineering Task Force (IETF) ont mené à l'émergence de normes préliminaires pour une ICP pour Internet (PKIX).

Les normes proposées établissent les lignes directrices pour l'attribution, l'utilisation, la distribution et la gestion des certificats numériques dans le cadre d'une infrastructure fondée sur les réseaux ouverts comme Internet :

- Internet Public Key Infrastructure Part I: X.509 Certificates and CRL Profile
- Internet Public Key Infrastructure Part II: Operational Protocols
- Internet Public Key Infrastructure Part III: Certificate Management Protocols
- Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework

- Internet Public Key Infrastructure Part V: Time Stamp Protocols

ANNEXE C

Bibliographie

- Centre de la sécurité des télécommunications. Entrust_. Version 1.0. Gouvernement du Canada, août 1996.

- Centre de la sécurité des télécommunications. Infrastructure à clé publique du gouvernement du Canada - Livre blanc. Ottawa : Gouvernement du Canada, 21 mai 1997.

- Chokhani, S., et Ford, W. Internet Public Key Infrastructure: Part IV: Certificate Policy and Certification Practices Framework. (Internet Draft). PKIX Working Group, July 3, 1997, ftp://ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-01.txt.

- Clark, Tim. Everything you need to know about digital IDs, C|Net News.com, July 25, 1997, http://www.news.com:80/SpecialFeatures/0,5,12788,00.html (29-08-1997).

- Cobb, Stephen. Security Issues in Internet : NCSA White Paper on Internet Commerce. Version 2.0. National Computer Security Association, 1996, http://www.ncsa.com/library/inetsec2.html (06-08-1997)

- Csinger, Andrew. Little Sister beats Big Brother: Distributed grassroots certificate authorities for the Internet, EDI Forum, 10(2): 1997, pp. 79-81.

- Ford, Warwick. Standardizing information technology security, StandardView, 2(2): June 1994, pp. 64-71.

- Korzeniowski, Paul. With directory services, you're supposed to be able to find anything, anywhere. Do they work?, Byte, November 1995, http://www.byte.com/art/9511/sec5/art2.htm (06-08-1997).

- OCDE. L'OCDE adopte les lignes directrices régissant la politique de cryptographie. Communiqué de presse. Paris, 27 mars 1997, http://cs1-hq.oecd.org/dsti/iccp/crypto_f.html (05-08-1997).

- OCDE. Le commerce électronique : Opportunités et défis pour les gouvernements. OCDE (Science, Technologie et Industrie), 1997.

- OCDE. Sécurité, vie privée, chiffrement et droits de la propriété intellectuelle, mise à jour du 7 avril 1997, http://cs1-hq.oecd.org/dsti/iccp/legal/top-fr.html (05-08-1997).

- Parisien, Serge; Trudel, Pierre, et Wattiez-Larose, Véronique. L'état des infrastructures de clés publiques dans le monde. Centre de recherche en droit public (Faculté de droit, Université de Montréal), juin 1997.

- Parisien, Serge; Trudel, Pierre, et Wattiez-Larose, Véronique. Options relatives aux pratiques communes de certification au Québec. Centre de recherche en droit public (Faculté de droit, Université de Montréal), juin 1997.

- Pickering, Al. The security challenge and public key infrastructures on the Information highway, EDI Forum, 9(1): 1996, pp. 9-18.

- Secrétariat du Conseil du trésor. La sécurisation des échanges électroniques au gouvernement du Québec : Vers l'établissement de services communs adaptés aux inforoutes. Version 2.3. Gouvernement du Québec, novembre 1996.

- Société canadienne des Postes. Notes pour une présentation par Georges C. Clermont, président-directeur général, à la Graphic Communication Association, Congrès estival, Hôtel Royal York, Toronto, 31 juillet 1997, http://www.mailposte.ca/CPC2/corpc/speeches/gc970731f.html (29-08-1997)

- United Nations Commission on International Trade Law, Thirtieth session, Vienna, 12-30 May 1997. Report of the Working Group on Electronic Commerce on the Work of its Thirty-first Session. New York, 18-28 February 1997. A/CN.9/437, 12 March 1997, http://www.un.or.at/uncitral/sessions/unc/unc-30/acn9-437.htm (28-08-1997).

- United Nations Commission on International Trade Law (Working Group on Electronic Commerce), Thirty-first Session. New York, 18-28 February 1997. Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and related legal issues. A/CN.9/WG.IV/WP.71, 31 December 1996, http://www3.un.or.at/uncitral/sessions/wg_ec/wp-71.htm (28-08-1997).

- Wayner, Peter. Who Goes There? Before you can trust your business to the Internet, you must have reliable authentication, Byte, June 1997, http://www.byte.com/art/9706/sec5/art1.htm (06-08-1997).

ANNEXE D

Liste des acronymes

AC ..... Autorité de Certification

AGP ..... Autorité de gestion de politiques

CCI ..... Chambre de commerce internationale

CNUDCI ..... Commission des Nations Unies pour le droit commercial international

COSIFORM ..... Commission pour la simplification des formalités

EDI ..... Échange de documents informatisés

ICP ..... Infrastructure à clé publique

ITU-T ..... International Telecommunication Union- Telecommunication Standardization Sector

LDAP ..... Lightweight Directory Access Protocol

PGP ..... Pretty Good Privacy

SET ..... Secure Electronic Transaction

SSL ..... Secure Sockets Layer