SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUES AU GOUVERNEMENT DU QUÉBEC

Document de sensibilisation et d'information

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

20 OCTOBRE 1997

Préface

Introduction

1. Rappel de la situation gouvernementale

2. Contributions de l'inforoute à l'atteinte des défis gouvernementaux

3. Les échanges électroniques sur les inforoutes
    - 3.1 Les échanges d'information impliquant le gouvernement
    - 3.2 Le Commerce électronique sur les Inforoutes
    - 3.3 Les processus et fonctions d'affaires
    - 3.4 Les services transactionnels d'affaires

4. La sécurité des échanges électroniques gouvernementaux
    - 4.1 Typologie des échanges électroniques gouvernementaux
    - 4.2 Les exigences de base en matière de sécurité
    - 4.3 Les initiatives gouvernementales des dernières années
    - 4.4 Les fonctions de base de la sécurité
    - 4.5 Les mécanismes de sécurité

5. L'établissement de services communs
    - 5.1 Les besoins communs de sécurisation des échanges électroniques au gouvernement
    - 5.2 L'établissement de services communs adaptés aux Inforoutes

Conclusion

Annexes

A. Les technologies du Commerce électronique et les autres NTIC
B. Les particularités de l'EDI touchant à la sécurité
C. Les services de base de l'Internet
D. Les services commerciaux de l'Internet
E. Les risques et moyens de sécurisation des échanges électroniques
F. La carte à microprocesseur
G. La signature numérique et l'infrastructures à clé publique

Document produit par :
La Direction de la coordination gouvernementale en technologies de l'information (DCGTI).

Première édition :
La première édition de ce document de sensibilisation et d'information a été produite à l'automne 1996. Ce document a été rendu public pour la première fois le 24 mars 1997, sous le titre « Sécurisation des échanges électroniques au gouvernement du Québec : Vers l'établissement de services communs adaptés aux Inforoutes ».

Ce document a été rédigé par:
MM. Robert Cusson, Yvan Lauzon, René Lortie et Richard Parent
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

REMERCIEMENTS
Remerciements à toutes les personnes qui ont contribué à la révision du présent document et plus particulièrement aux personnes suivantes qui l'ont commenté :
M. Bernard Plante, Secrétariat du Conseil du trésor (SCT-SG-DGT)
M. François Lajeunesse, Secrétariat de l'autoroute de l'information
M. Paul-André Robitaille, Centre francophone de recherches sur l'informatisation des organisations (CEFRIO)
M^{me} Francine Thomas, Comité des responsables de l'informatique du secteur public (CRISP)
M. Pierre P. Tremblay, Secrétariat du Conseil du trésor (SCT-SG-DGT)

Pour toute question ou commentaire :
M. Yvan Lauzon
Téléphone : (514) 873-7237
Télécopieur : (514) 873-7749
Courriel : Yvan.Lauzon@SCT1.gouv.qc.ca

PRÉFACE

Les enjeux du développement de l'Inforoute gouvernementale (ou autoroute de l'information gouvernementale) sont importants afin d'assurer l'efficacité de l'Administration publique, maximiser les effets socio-économiques de son implication sur les entreprises québécoises et améliorer les échanges entre l'Administration et les citoyens.

En fait, la question n'est plus de savoir s'il faut encourager ou non le développement des différents types d'Inforoute au Québec (réseau Internet, câble, téléphonie numérique), mais plutôt quelles sont les actions concrètes à réaliser afin que l'ensemble des citoyens, des entreprises et des organisations gouvernementales passent rapidement de l'« ère papier » à celui de l'« ère des transactions électroniques ».

En effet, il ne fait nul doute que l'utilisation de l'Inforoute sera un facteur déterminant de développement économique des pays industrialisés dans les années à venir. L'ensemble des citoyens doit donc avoir accès le plus tôt possible à cet outil de développement, et ce, sans égard à leurs situations géographiques, sociales ou économiques. Les citoyens doivent également avoir à leur disposition 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.

En fait, 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.

Il semble bien que les transactions électroniques d'affaires impliquant l'Administration ne pourront se généraliser tant que l'on ne pourra garantir à la fois la sécurité technique et la sécurité juridique des transactions, et ce, à tous les intervenants impliqués, tel que: les utilisateurs (consommateurs, commerçants), les institutions financières et les organisations gouvernementales.

Sur le plan technique, il existe déjà sur le marché un bon nombre de solutions permettant de réduire les risques inhérents aux nouveaux modes d'échanges. Ces diverses solutions, en quête de déploiement, devront satisfaire des exigences juridiques précises, comme le démontrera notre document.

Nous espérons que ce document de sensibilisation, de vulgarisation et d'information apportera au lecteur un éclairage nouveau sur l'importante question de la sécurisation des échanges électroniques. Le gouvernement du Québec sera appelé très prochainement à faire des choix technologiques importants qui auront des retombées et des impacts majeurs sur le développement harmonieux du commerce électronique et des transactions d'affaires sécurisées au Québec.

Louis Lamothe
Directeur
Secrétariat du Conseil du trésor (SCT-SSMPTI-DCGTI)

INTRODUCTION

CONTEXTE

Les technologies du Commerce électronique regroupent plusieurs moyens de « faire des affaires » électroniquement, tel que l'échange de documents informatisés (EDI), la télécopie, la messagerie électronique, les babillards électroniques et la télématique d'affaires (une liste plus complète figure à l'annexe A).

Ces technologies ont connu une croissance phénoménale ces dix dernières années à cause des importants bénéfices qu'elles engendrent. Ces bénéfices découlent en grande partie de la vitesse des échanges d'information, de la saisie unique des informations (sauf pour la télécopie papier) et des possibilités d'intégration directe des informations aux applications informatiques de nos organisations.

Les Inforoutes connaissent également une croissance fulgurante depuis l'automne 1993 surtout à cause de la popularité des sites WEB (World Wide WWW) où l'information multimédia est à l'honneur. Ainsi les données, textes, images fixes ou animées, formulaires interactifs et liens dynamiques inter-sites se retrouvent alors intégrés.

Le Commerce électronique sur les Inforoutes est un sujet très populaire depuis 1994. Selon de nombreux spécialistes, ce type d'activité devrait générer à court, ou à moyen terme, un volume très important de transactions.

Cependant, ce type de Commerce électroniques sur les Inforoutes ne peut devenir une réalité tant que les opérations commerciales ne s'achèveront pas par des paiements. Il est en effet peu pratique d'utiliser un système télématique (tel Internet) pour commander des produits et un autre système manuel, (même un numéro téléphonique sans frais 1-800) pour compléter la transaction en effectuant le paiement. Les utilisateurs d'Internet veulent accéder à des services d'achat et des services de paiement qui sont accessibles simultanément et directement sur le WEB.

Des initiatives apparues ces derniers mois sur le WEB vont d'ailleurs dans ce sens. Elles ont pour nom CyberCash, DigiCash, Global OnLine et First Virtual. Ce dernier, par exemple, a réussi à rejoindre en moins de 14 mois, 150 000 acheteurs et 1 670 marchands en provenance de 148 pays. Certaines institutions d'ici, telle la Banque Nationale du Canada, ont déjà annoncé dès le printemps 1996 des systèmes de paiement sur le WEB (SécurNat). A la fin de 1996, près de 2,5 millions de personnes dans le monde avaient déjà commandé des biens et services à partir d'Internet, et ce, en dépit du peu de confiance en la sécurité de "bout en bout" de son architecture.

Du côté gouvernemental, en dépit d'un effort marqué de plusieurs organisations pour tirer profit des Inforoutes, très peu d'entre elles ont véritablement amorcé des transactions d'affaires sur le WEB.

DESCRIPTION DU DOCUMENT

Dans les deux premières parties de ce document nous présenterons un rappel de la situation gouvernementale en mettant en évidence le contexte difficile de fonctionnement des dernières années, et, nous situerons comment les Inforoutes peuvent contribuer à l'atteinte des importants défis de gestion auxquels nous faisons face actuellement.

Dans la troisième partie nous décrirons les principales fonctions d'affaires qui peuvent être réalisées électroniquement, alors que dans la quatrième nous élaborerons sur les propriétés (ou fonctions) de la sécurité des systèmes informatiques et des transactions d'affaires, ainsi que les mécanismes de sécurisation.

Nous compléterons le tout par une catégorisation des besoins de sécurisation des transactions d'affaires au gouvernement du Québec, ainsi qu'un plaidoyer en faveur de l'établissement de services communs de sécurisation; les besoins étant plutôt semblables d'une organisation à l'autre.

1. RAPPEL DE LA SITUATION GOUVERNEMENTALE

Il serait facile de s'alarmer à propos de la situation socio-économique du Québec à la seule lecture des nos grands quotidiens ou à l'écoute des bulletins de nouvelles télévisés. Pourtant le Québec dispose d'atouts majeurs. La « qualité de la vie » est appréciable, sa main-d'oeuvre est qualifiée et motivée, et qui plus est, le climat syndical est favorable au développement des affaires. Plus encore, le Québec d'aujourd'hui est une société de haute technologie plutôt bien « branchée ».

Le gouvernement du Québec, de son côté, fait face à des défis sans précédent. Sa main-d'œuvre a été plutôt vieillissante durant douze ans, compte tenu du très faible taux d'embauche. Heureusement, la situation s'est récemment amélioré à cause de la popularité des départs volontaires à la retraite). Sa marge budgétaire demeure toutefois très faible et ne peut plus assurer un accroissement réel des services nécessaires à une société en constante évolution.

2.CONTRIBUTIONS DE L'INFOROUTE À L'ATTEINTE DES DÉFIS GOUVERNEMENTAUX

Les Inforoutes ont connu une progression très rapide ces trois dernières années. Des projets ont été annoncés impliquant le câble (UBI), le réseau téléphonique numérisé (SIRIUS), ou encore, l'interfaçage des différents réseaux de télécommunication locaux, régionaux, nationaux ou internationaux (INTERNET).

Ainsi, Internet, qui fut autrefois réservé à des communautés spécifiques de chercheurs et d'universitaires, a connu un développement fulgurant ces dernières années grâce à l'arrivée des sites de types WEB où l'information multimédia (données, texte, son, image fixe, image animée) est à l'honneur.

Mais, de telles formes d'Inforoute font bien plus que de simplement « connecter » les gens en leur permettant de s'échanger des messages électroniques comme le ferait une simple messagerie. Ils offrent une gamme étendue de services de diffusion d'information, de communication et de transaction électronique, comme le démontre la « liste des services de base de l'Internet » retrouvée à l'annexe C.

En permettant des échanges très rapide d'information, ainsi que la réalisation de transactions entre des communautés restreintes ou plus étendues d'utilisateurs (à la limite toute la population d'une région, d'un pays ou du monde), ces Inforoutes sont en train de révolutionner la façon de "rendre les services" aux diverses clientèles.

Certes, nous avons connu des développements technologiques très intéressants ces dernières années, comme les guichets bancaires ou les codes à barres associés aux terminaux « point de vente ». Ces développements ont eu pour effet de diminuer considérablement la perte de temps liée aux files d'attente tout en diminuant les erreurs d'obtention des données.

D'ailleurs, certains problèmes de communication avec la clientèle, vécus depuis des décennies, sont en voie d'être résolus par les différentes formes d'Inforoute. Qu'il suffise de mentionner les files d'attente, les lignes téléphoniques constamment engorgées, les délais de réponse toujours trop longs pour le client. Rejoindre une clientèle grandissante, plus rapidement et plus efficacement, et ce, à meilleur coût représente certainement un objectif fort louable dans le contexte économique actuel marqué par une concurrence accrue.

L'impact de l'Inforoute sur notre quotidien est donc beaucoup plus important que la simple introduction d'une nouvelle technologie de l'information ou de la communication (NTIC). Certains auteurs parlent même d'une « révolution de la communication », plutôt que d'une simple « évolution », compte tenu de l'importance du changement pressentis. Courrier électronique « généralisé » , transactions d'affaires réalisées à distance, télémédecine, téléformation, téléavertissement etc. Les applications se comptent par centaines, voire des milliers. Annoncée et décrite par les médias depuis la fin des années '70, la véritable « société de l'information » est en train de naître chez nous.

Certaines communautés ont déjà atteint un niveau très élevé d'accès à l'Inforoute. C'est le cas de la région de la Baie de San Francisco avec 57% de gens « branchés », alors que ce taux serait de moins de 20% au Québec, comme dans la plupart des autres régions des pays industrialisés. Un tel niveau de « connexité » est intéressant car il réduit de façon appréciable les besoins de ressources requis pour la façon « traditionnelle » de rendre des services.

3. LES TRANSACTIONS ÉLECTRONIQUES SUR LES INFOROUTES

Après avoir dressé un portrait sommaire de la situation socio-économique du Québec et présenté l'apport probable des différentes formes d'Inforoute, nous allons maintenant traiter des transactions électroniques effectuées à l'aide de l'Inforoute.

3.1 Les échanges d'information impliquant le gouvernement

Les nouvelles technologies de l'information et de la communication (NTIC) permettent au moins trois formes d'échanges d'information soit :

- la communication interpersonnelle

(par exemple, le courrier électronique de type « un à un » , ou encore, de type « un à plusieurs » individus) ;

- la diffusion d'information

(par exemple, l'accès aux banques d'information) ;

- les transactions

(par exemples, les transactions commerciales, médicales, etc).

Ces nouvelles technologies de l'information offrent également des possibilités très intéressantes de divertissement, et ce, pour le plus grand plaisir des « jeunes et des moins jeunes ».

De leur côté, les organisations gouvernementales échangent des informations électroniques avec plusieurs clientèles formées de personnes physiques ou morales, dont :

- les autres organisations de notre gouvernement ;
- les autres organisations des autres gouvernements ;
- les organisations des réseaux (santé, éducation, municipalité) ;
- les organisations sans but lucratif (associations, ...) ;
- les entreprises (fournisseurs ou clients) ;
- les clientèles formées d'individus spécifique (bénéficiaires, détenteurs de permis, etc)
- et, finalement, l'ensemble ou une partie importante de la population (travailleur, électeur, ...).

Les flux transactionnels sont alors unidirectionnels ou bi-directionnels, selon les cas. Ces échanges informationnels peuvent être schématisés globalement comme suit :

Organisation gouvernementale → Usager
Organisation gouvernementale ← Usager
Organisation gouvernementale ↔ Usager

Ces informations peuvent être de différentes natures, comme le démontrent les exemples suivants :

Organisation gouvernementale → Usager

- la transmission d'avis public

(ex. : avis d'élection, avis de santé publique <vaccination...>)

- la diffusion de rapport annuel
- la publication d'autres ouvrages, brochures, dépliants, etc.
- l'émission de certificats (ex: Certificat d'étude)

Organisation gouvernementale ← Usager

- le remplissage de formulaires prescrits (ex. : recensement)

Organisation gouvernementale ↔ Usager

- la demande et la fourniture d'information
- l'accès à des banques d'information gouvernementales
- la demande et l'émission de permis

(ex: permis de conduire, immatriculation)

D'un point de vue juridique, les échanges électroniques peuvent être regroupés sous trois catégories, à savoir :

1. les échanges d'informations au cours desquels des renseignements, généralement nominatifs, sont transmis entre l'usager et une organisation gouvernementale (ex: consultation ou modification par un usager de son dossier personnel détenu par l'organisation gouvernementale) ;
2. les transactions commerciales visant l'achat ou la location de biens (comme l'achat d'un livre aux Publications du Québec) ;
3. les transactions accordant à l'usager l'attribution de privilèges ou de droits (comme la demande d'un permis de pêche ou de chasse).

Commerce électronique

La réalisation de transactions d'affaires ou commerciales, sous forme électronique, est désignée sous le nom générique de « Commerce électronique », depuis 1990. Une liste des principales technologies du Commerce électronique figure à l'annexe A.

D'un point de vue d'affaires, le Commerce électronique en milieu gouvernemental, comporte au moins trois volets :

- le volet « fiscal » : versement de taxes, impôts, droits, par les citoyens et entreprises au gouvernement ;
- le volet « bénéfices » : versement de pensions, allocations, subventions, remboursements à des citoyens et entreprises ;
- le volet « acquisitions » : achat de biens et services par le gouvernement auprès des entreprises.
- le volet « permis » : demande et attribution de droits ou privilèges.

3.2 LE COMMERCE ÉLECTRONIQUE SUR LES INFOROUTES

Les vocations actuelles des différentes formes d'Inforoute (Internet, câble, téléphonie numérique) ne représentent probablement pas encore un incitatif suffisant pour que la majorité des entreprises et des citoyens ressentent la nécessité de s'y brancher « coûte que coûte ». Celles-ci étant principalement limitée aux aspects culturels, récréatifs, éducatifs, ainsi qu'au courrier électronique.

Comme ce fut le cas en France avec l'introduction du système vidéotex Minitel, une foule considérable de services de langue française devront être mis sur pied rapidement afin que les utilisateurs y trouvent leur intérêt et demeurent « branchés ». (Voir les statistiques sur le Minitel à l'annexe A).

Pour exploiter le plein potentiel des Inforoutes et en arriver à une masse critique d'utilisateurs « branchés », il importe que l'ensemble des citoyens puissent effectuer des transactions commerciales à distance, et ce, de façon tout à fait sécuritaire.

Après avoir débuté dans des environnements passablement sécurisé comme celui de l'échange de documents informatisés (EDI) (voir annexe B), le Commerce électronique en est actuellement à ses premiers balbutiements sur l'Inforoute, tel Internet (voir l'annexe *D*).

Ceci peut s'expliquer en partie par le faible encadrement législatif ou réglementaire en matière de signature électronique, des lacunes existant en matière de certification de l'identité des parties transigeant à distance, du faible niveau de reconnaissance de la sécurité des différentes formes d'Inforoute par les gens d'affaires et du peu de confidentialité entourant les échanges commerciaux conclus sur l'Internet.

Plusieurs fournisseurs offrent déjà des solutions technologiques permettant la sécurisation technique des transactions, mais très peu d'entre eux sont en mesure d'assurer la sécurisation juridique des transactions et d'en déployer l'application à grande échelle. Par exemple, les systèmes de clés publiques, lorsqu'ils sont utilisés **sans** infrastructure de certification, ne fournissent pas tous les éléments de preuve nécessaires à la reconnaissance légale d'une transaction conclue à distance et n'éliminent pas le risque qu'un des contractants répudie la transaction en niant avoir été à l'origine de celle-ci.

En effet, le passage d'une « ère papier » à une « ère d'information électronique » ne change pas les relations juridiques qu'entretiennent les parties impliquées dans une transaction. Il transforme simplement le médium à travers lequel les personnes vont accéder ou échanger de l'information au cours des prochaines décennies.

La valeur juridique des transactions effectuées et conservées sur support informatique a été reconnue par les autorités gouvernementales québécoises dans le *Code civil du Québec*, mais elle exige un niveau de preuve que les solutions technologiques à elles seules ne peuvent rencontrer.

Les éléments et le niveau de preuve à fournir en cas de contestation d'une transaction électronique nécessitent à coup sûr un processus de certification permettant d'établir, le cas échéant, l'identité, et peut-être même la capacité, la qualité et les pouvoirs des parties transigeant à distance; ce qui constitue sans l'ombre d'un doute le confluent entre le droit et les nouvelles technologies de l'information.

Ceci est d'autant plus vrai dans le cas des réseaux électroniques dits « ouverts » à une large communauté d'utilisateurs tel qu'Internet, car ce type de réseaux est sans doute plus vulnérable et plus sujet aux attaques répétées, que dans le cas des réseaux « fermés », tels les réseaux de transfert de fonds SWIFT et INTERACT.

3.3 LES PROCESSUS ET FONCTIONS D'AFFAIRES

Les activités de nature commerciale trouvent leurs origines dès le début de la civilisation humaine et de la manifestation des premières formes de collectivités. Cependant les entreprises, comme on les connaît aujourd'hui, datent de la seconde moitié du XIX^{e} siècle.

Les **processus d'affaires**, quant à eux, sont relativement simples et peuvent s'énoncer comme suit :

- Création et mise en place d'une entreprise
- (publique ou privée)
- Gestion des ressources de l'organisation
  (humaines, financières, matérielles, informationnelles)

- Acquisition des biens & services
- Production de biens & services
- Vente de biens & services
- Livraison de biens ou prestation de services
- Paiement
- Déclaration aux Administrations ou aux compagnies de services publics

Ces processus d'affaires sont des phénomènes actifs organisés dans le temps. Il est possible d'énumérer pour chacun d'eux une série de **fonctions d'affaires**. Nous retrouvons par exemple « la gestion de l'encaisse et des placements » dans le processus de Gestion des ressources financières.

De même, nous retrouvons les composantes ou fonctions suivantes dans les processus d'Achat et de Paiement de biens ou de services :

- Offre de produits & services

(mise en disponibilité dans une vitrine ou un catalogue, recherche de client, publicité, promotion, ...)

- Demande de produits & services

(recherche de produits & services, recherche d'un fournisseur ou d'un partenaire potentiel, ...)

- Négociation et conclusion d'un accord ou acceptation des conditions générales de vente

- Commande unique, ou encore, commande ouverte
- (livraisons multiples réparties durant une période donnée)
- Demande de livraison des biens & ou prestation des services
- Livraison de biens ou prestation de services
- Paiement

3.4 LES SERVICES TRANSACTIONNELS D'AFFAIRES

Les principaux « services transactionnels », qui peuvent se retrouver sur les différentes formes d'Inforoute, peuvent être décrits sommairement comme suit:

AUTORISATION ÉLECTRONIQUE

(1) Manifestation, à l'aide d'un code ou autres composantes numériques, de sa volonté d'approuver un contenu et/ou d'autoriser un acte. **(2)** Mécanisme qui apporte la preuve de l'identité de celui qui le met en œuvre, il s'agit d'un mécanisme de « sceau informatique » qui permet de tenir lieu de signature lorsqu'il est appliqué à un document électronique par un utilisateur habilité à le faire.

Remarques : **(1)** Certains auteurs croient que la signature électronique correspond beaucoup plus à un sceau électronique qu'à une signature car on n'a en fait aucune certitude sur l'identité réelle de celui qui s'en sert. **(2)** Il est à noter également que plusieurs auteurs sont d'avis que la définition de la signature prévue au Code civil du Québec (art. 2827) est suffisamment large pour inclure les mécanismes électroniques qui rencontrent les exigences de cet article et qui permettent de remplir les fonctions d'une signature, à savoir identifier le signataire et manifester son adhésion au contenu du document signé. **(3)** La signature électronique, réalisée à l'aide de clé cryptographiques asymétriques, porte généralement le nom de « signature numérique ».

CATALOGUE ÉLECTRONIQUE
Consultation locale ou à distance d'un catalogue électronique présentant une description de produits et de services, souvent agrémentée d'une image.

CENTRE D'ACHAT ÉLECTRONIQUE
Disponibilité et accès à des descriptions de produits & services, ainsi que des fournisseurs, et ce, à partir d'un même service électronique. Les informations peuvent être gérées de façon distribuée (ex: plusieurs sites physiques), mais l'accès se fait toujours à partir d'un seul site dont l'interface avec l'utilisateur est normalisé pour en simplifier l'utilisation.

COMMANDE ÉLECTRONIQUE
L'utilisation de technologie, telle que l'audiotex, le courrier électronique public, le babillard électronique ou l'échange de documents informatisés (EDI), pour passer une commande à un fournisseur de biens ou de services.

CONSULTATION ÉLECTRONIQUE
Accès, local ou à distance, à des services d'informations électroniques tels que « revue de presse électronique », « journal électronique », « cote boursière », « autres informations financières », etc.

COURRIER ÉLECTRONIQUE
Utilisation de services de communication électronique, en direct ou en différé (via par exemple: une boîte postale électronique), pour l'envoi et la réception de message électronique.

DÉCLARATION ÉLECTRONIQUE (Télédéclaration)
Utilisation de technologies de l'information pour fournir des formulaires et autres informations demandées par les Administrations ou les entreprises de services publics (gaz, téléphone à domicile, hydro-électricité).

DÉTECTION A DISTANCE (Télédétection)
Utilisation de technologies de l'information pour effectuer la télédétection d'un objet (ex. : culture agricole, minerai, bateau en mer etc).

DIAGNOSTIC A DISTANCE (Télédiagnostic)
Utilisation de technologies de l'information pour témoigner de l'état actuel d'une personne (ex. : patient) ou d'un objet.

DIFFUSION D'INFORMATION ÉLECTRONIQUE
Utilisation d'application (ex. : babillard, banque d'informations) et de réseau de télécommunication (ex. : réseau par paquets X.25, Internet, Câblodistribution) pour la diffusion publique ou privée d'information.

PAIEMENT ÉLECTRONIQUE MINEUR
Paiement de petits montants fait par des individus ou des organisations, à l'aide de moyens électroniques (carte à puce, services électroniques, etc).

Remarque : D'un point de vue juridique, l'expression « paiement mineur » ou « petit paiement » pourrait se limiter au seuil maximal des litiges admissibles aux petites créances, soit moins de 3 000 $. D'un point de vue pratique, un petit montant pourrait correspondre à ce que les gens conservent habituellement dans leur porte-monnaie, soit moins de 50 ou 75 $.

PAIEMENT ÉLECTRONIQUE MAJEUR
Paiement de montants plus substantiels, fait le plus souvent par des organisations, à l'aide de moyens électroniques (réseau public à valeur ajouté (RVA), réseau privé, etc).

PUBLICITÉ ÉLECTRONIQUE
Diffusion électronique d'information publicitaire sur des produits et services.

PROMOTION ÉLECTRONIQUE
Promotion diffusée par moyens électroniques. (ex. : coupon rabais).

RÉPERTOIRE ÉLECTRONIQUE
Liste descriptive d'utilisateurs de service(s) électronique(s) présentant les coordonnées de cette personne (pages blanches), son organisation et sa structure (pages bleues), ses produits et services (pages jaunes) et l'index des documents et autres informations disponibles (pages vertes).

Remarque : Le répertoire peut être distribué, permettant par exemple l'accès à des sous-répertoires et la mise à jour individualisée de ces sous-répertoires.

SURVEILLANCE ÉLECTRONIQUE (Télésurveillance)
Activité de surveillance d'une maison, d'un lieu, de l'état d'une personne des phénomènes naturels, etc.

TRANSACTION FINANCIERE ÉLECTRONIQUE
Utilisation de technologies permettant de réaliser à domicile les services bancaires de base (virement entre comptes, paiement de factures, etc).

4. LA SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUES GOUVERNEMENTAUX

4.1 TYPOLOGIE DES ÉCHANGES ÉLECTRONIQUES GOUVERNEMENTAUX

Comme nous l'avons vu précédemment, chaque organisation gouvernementale et ses employé(e)s ont des besoins de communication diversifiés avec leur clientèle, avec d'autres employé(e)s de leur organisation, ou avec d'autres organisations.

Cette communication peut se partager entre deux classes, selon que des mesures de sécurité sont requises ou non :

i) la diffusion d'information gouvernementale

Ce cas pose peu de problème de sécurité puisqu'il s'agit habituellement d'information publique. L'intégrité peut avoir à être vérifiée pour s'assurer que ce qui est enregistré et/ou transporté n'a pas été modifié. De même, il y aurait lieu de s'assurer de la réalisation effective ou non des consultations et transmissions d'information, dans le cas où ces services seraient « payants », ceci afin d'éviter tout refus ultérieur de paiement (répudiation).

ii) les échanges personnalisés d'information ou des transactions d'affaires

Ces échanges personnalisés entre les employés du gouvernement ou avec un citoyen ou une entreprise, ainsi que les « transactions » (ces échanges qui ont une portée financière et/ou juridique) requièrent une gamme plus élaborée de garanties en plus de la vérification de l'intégrité du contenu :

- assurer la confidentialité de ce qui est enregistré ou transporté, par exemple quand un sous-ministre écrit à un autre sous-ministre, ou quand un hôpital ou un pharmacien adresse à la RAMQ un message contenant des renseignements personnels ;
- authentifier l'identité d'un utilisateur de l'Inforoute, si par exemple un citoyen veut avoir accès aux renseignements le concernant dans les banques d'information gouvernementale, ou pour toute transaction où il y a risque de fraude ;
- autoriser l'accès à des ressources informationnelles, par exemple si un employé veut avoir accès de chez lui aux ressources informationnelles contrôlées de son organisation ;
- autoriser l'accomplissement de transactions, selon les privilèges ou les pouvoirs d'un employé, par exemple acheter, payer, signer une entente ;
- assurer la non-répudiation de ce qui a été transmis grâce au mécanisme de signature électronique qui garantit l'intégrité du document en même temps que l'intention de responsabilité à l'égard du contenu et de sa signification en contexte.

La façon reconnue d'obtenir ces garanties dans le Cyberespace est de recourir à des mécanismes ou techniques de signature électronique, de chiffrement (codage secret des messages) et d'infrastructure à clés publiques (ICP), ou "Public Key Infrastructure" (PKI) en anglais, et ce, dans un cadre institutionnalisé et juridiquement reconnu d'autorité de certification.

4.2 LES EXIGENCES DE BASE EN MATIERE DE SÉCURITÉ

Objectifs de gestion touchant à la sécurité
Les organisations gouvernementales souhaitent pouvoir réaliser des transactions d'affaires de façon à pouvoir traiter, de façon automatique et fiable un volume important de transactions. Ces traitements doivent être effectués dans des environnements informatiques à l'abris des menaces délibérées, tout en réduisant au strict minimum les risques d'erreurs et de défaillances (voir liste complète à l'annexe E).

Ces échanges transactionnels se font le plus souvent en différé et ne nécessitent habituellement pas un traitement en temps réel. Les informations transmises sont généralement des données, des formulaires et autres textes, plus rarement des images ou des messages sonores. Les informations peuvent être volumineuses. Certaines sont confidentielles, elles sont alors codées chiffrées (codées) pour contrer les indiscrétions.

Besoins de base
Les besoins de base des organisations gouvernementales peuvent se résumer comme suit :

PROTECTION CONTRE LA FRAUDE & LA MALVEILLANCE
Ces besoins sont tout à fait semblables à n'importe quelle autre entreprise québécoise. Ils ne sont pas typiques au gouvernement.

PROTECTION DE LA CONFIDENTIALITÉ DES INFORMATIONS NOMINATIVES
Ex. : dossier « patient » <RAMQ, CSST, MSSS, établissements de santé>
dossier « étudiant » <MEQ>
dossier « de crédit » <MJQ>
dossier « judiciaire » <MJQ>
dossier « pensionné » <RRQ>
dossier « déclarations d'impôt » <MRQ>
dossier « détenteurs d'obligations » <MFQ>

PROTECTION DE LA CONFIDENTIALITÉ DES INFORMATIONS CORPORATIVES
Ex. : adresse personnelle des administrateurs des entreprises québécoises <IGIF>
revenus d'entreprises <MRQ>

RESPECT DES EXIGENCES JURIDIQUES, ARCHIVISTIQUES & D'AUDIT
Exigences à respecter
Pour respecter les objectifs de gestion énumérés ci-haut, il est nécessaire de s'assurer que les utilisateurs des systèmes sont des personnes habilitées, que les messages sont transmis dans les délais requis, que l'intégrité et la confidentialité sont suffisants.

Pour ce faire, il faut procéder tout d'abord à l'analyse des risques et conséquences informatiques, ainsi qu'à l'établissement de mesures de prévention et de protection touchant à :

- la prévention des accès non autorisés ;
- la sécurisation des messages ;
- la vérification des messages reçus ;
- au respect des exigences juridiques relatives à la capacité d'utiliser des documents électroniques à la place de documents « papiers », de la valeur probante en cas de mésentente et des prescriptions légales ;

- au respect des exigences d'Audit touchant à la capacité de reproduire au besoin le flux transactionnel et líordonnancement séquentiel des opérations, ceci par l'horodatation des échanges et la journalisation des transactions ;
- au respect des exigences archivistiques touchant au choix des informations ayant une valeur historique et aux conditions d'archivage électronique.

De façon plus précise, il faut être en mesure d'assurer :

- l'authentification de l'émetteur et du récepteur (personne ou dispositif) ;
- une attestation de livraison au destinataire ;
- une attestation de l'origine des informations émises ;
- la non répudiation (non contestation) par le récepteur ;
- la détection de l'altération de l'information échangée ;
- la confidentialité des échanges ;
- la conservation efficace des informations électroniques.

La portée d'une signature numérique

Comme on l'a vu précédemment, la signature numérique, lorsqu'elle est accompagnée d'un certificat de clé publique, assure l'intégrité du document en même temps qu'elle apporte une « certaine preuve » de l'identité de l'émetteur d'une communication.

Il importe de préciser dès à présent que le niveau de preuve requis peut varier selon qu'il s'agisse de transactions susceptibles d'être mise en preuve dans un contexte civil (où le niveau de preuve requis est la prépondérance des probabilités), ou dans un contexte pénal (ou la preuve doit être « hors de tout doute raisonnable »).

Niveau de sécurité

Il est possible de résumer les étapes de protection et de prévention à l'aide d'un modèle à 7 étapes (ou couches). Quoique discutable, comme c'est le cas pour n'importe quel autre modèle, un tel cadre offre l'avantage de permettre aux organisations gouvernementales de situer rapidement leur état d'avancement actuel :

(+ avancé)	7-Archivage électronique & Audit
	6-Certification
	5-Chiffrement des messages et transactions (si nécessaire)
	4-Signature électronique
	3-Protection des accès
	2-Sécurité physique
	1-Établissement de Politiques & Procédures de sécurité
	0-Évaluation objective de la situation (risques, menaces,
(de base)	menaces, conséquences, moyens de protection)

Il va s'en dire que le choix d'un niveau de protection adéquat découle de l'évaluation objective de la situation, du type d'information en cause et du contexte administratif et juridique.

Approche convergente

Nous avons voulu démontrer dans la présente section, le recoupement entre les dimensions informatiques, juridiques, audits et archivistiques. En fait, les différentes disciplines que sont la sécurité informatique, le droit, la comptabilité et l'archivistique visent toutes à s'assurer que les échanges d'information et transactions électroniques sont autant, sinon plus, sécuritaires que leurs équivalents « papiers ».

4.3 LES INITIATIVES GOUVERNEMENTALES DES DERNIERES ANNÉES

Comme nous l'avons, le gouvernement du Québec désire se tourner résolument vers l'utilisation des différentes formes d'Inforoute pour offrir aux citoyens du Québec les services auxquels ils s'attendent, pour assurer l'efficacité de son propre fonctionnement et aussi pour échanger avec les autres organisations « modernes » de la planète.

La sécurité des « réseaux ouverts »

Bien que reconnu universellement pour son efficacité, le recours aux réseaux « ouverts » de télécommunication ne va pas sans problème. En effet, l'information qui circule sur une voie publique -- donc accessible à tous -- n'est pas, à priori, à l'abri des risques d'indiscrétion, des risques d'altération ou de tout ce qui peut empêcher l'information d'arriver à destination.

La sécurisation des transactions commerciales, et la prestation de services réalisés par l'intermédiaire des réseaux publics, commande des solutions globales pour l'ensemble des organisations gouvernementales. La mise en place de « services communs » de sécurisation doit se faire en tenant compte des responsabilités des acteurs concernés tel que décrites dans la « directive de sécurité de l'Information électronique ».

La directive est très claire quant à la responsabilité de la sécurité de l'information détenue par chacun des ministères : Le ministère (ou l'organisme) est le premier responsable de ses actifs informationnels; il doit en gérer la sécurité, en assumer les coûts et collaborer à la réalisation de services communs. (Voir détails, à l'article 26 de la Directive).

D'autre part, le Secrétariat du Conseil du trésor, à titre d'expert et de conseiller doit identifier les besoins de services communs, déterminer les services communs pouvant être réalisés, de leur priorité et des modalités de réalisation. Enfin, il doit offrir des services communs ou en confier la charge à un ministère plus apte à le faire, ou encore à celui qui possède déjà le mandat de le faire. (Voir détails aux articles 20 à 24 et 30).

Le fait qu'un ministère puisse avoir recours à un service commun pour assurer la protection de son information ne diminue en rien sa responsabilité à l'égard de cette protection. Il lui faut donc s'assurer que ce service commun réponde effectivement à ses besoins. En pratique, cela veut dire que l'initiative peut venir du Secrétariat du Conseil du trésor, mais qu'il ne saurait mettre au point et proposer un service commun sans une participation active des ministères concernés.

Nécessité de l'identification

Toute communication est composée des quatre éléments suivants : un émetteur (expéditeur), un ou plusieurs récepteur<s> (ou destinataire<s>) et un canal (vecteur) qui porte le message et finalement le message lui-même (contenu).

Le canal peut garantir toute la sécurité voulue (CCITT X.800). Cependant, les mesures de sécurisation prévue dans les normes et autres documents techniques ne sont malheureusement pas appliquées par l'ensemble des intervenants.

On peut aisément comprendre que l'émetteur et le récepteur ne sauraient communiquer en toute sécurité sans avoir l'assurance que l'interlocuteur est effectivement celui qu'il prétend être. Dans une communication interpersonnelle on reconnaît son interlocuteur en le voyant, ou on reconnaît sa voix au téléphone, ou encore on reconnaît son écriture dans le cas d'une lettre.

Dans le type de communication qui nous concerne ici, ces moyens seraient impraticables et de toute façon nettement insuffisants. Il est donc primordial de mettre en place un moyen sûr de prouver l'authenticité de l'identité déclarée.

Une fois rassuré sur l'identité de l'interlocuteur, on doit rendre le message illisible à quiconque n'est pas le destinataire visé et faire en sorte que toutes tentatives de falsifier l'information du message ou relative au message soient détectées. Or les moyens utilisés pour atteindre ces fins s'appuient aussi sur une identification sûre non seulement des interlocuteurs mais également d'un intermédiaire (tiers) qui jouit de la confiance des deux premiers.

Comme on peut le constater, l'identification correcte des participants à la communication dans un réseau public « ouvert » constitue le fondement même de la sécurité des échanges.

4.4 LES FONCTIONS DE BASE DE LA SÉCURITÉ

Les principales fonctions (ou propriétés) de la sécurisation des échanges électroniques et des transactions d'affaires peuvent se résumer comme suit :

DISPONIBILITÉ
Accès possible, par les utilisateurs autorisés, aux systèmes informatiques et de télécommunication ainsi qu' aux informations qu'ils renferment.

INTÉGRITÉ
Information d'origine, non modifiée par une entité non-autorisée, et retrouvée au complet.

CONFIDENTIALITÉ
Protection de l'accès aux informations. Celles-ci n'étant accessibles qu'aux destinataire(s) autorisé(s). Protection des informations confidentielles de nature nominatives ou stratégiques.

AUTHENTIFICATION
La personne est bien celle qu'elle prétend être.

NON-RÉPUDIATION
Non contestation, par le récepteur d'un message, de l'intégrité ou la source d'un message.

4.5 LES MÉCANISMES DE SÉCURITÉ

Les mécanismes de sécurisation des échanges électroniques et transactions d'affaires peuvent se résumer comme suit :

ENREGISTREMENT
Inscription d'un utilisateur dans un annuaire électronique de type X.500 par exemple, auprès d'un fournisseur de services électroniques (inscription), ou encore, auprès d'une autorité d'enregistrement publique (ex. : IGIF), ou privée (Dun & Bradstreet).

CONTROLE DES ACCES
Processus permettant de limiter l'accès à des ressources protégées (matériels, transactions, applications, fichiers, bases de données, etc.) uniquement aux entités autorisées (personnes, matériels, applications, etc.).

SIGNATURE ÉLECTRONIQUE
Action consistant à adjoindre à un message, un élément appelé « signature » (code) permettant d'en garantir l'intégrité en même temps que l'authenticité de l'émetteur.

Remarque : Tel que signalé, la signature électronique est un terme générique qui englobe plusieurs procédés électroniques, dont la signature numérique qui est basée sur la cryptographie asymétrique.

SCELLEMENT
Action de l'expéditeur consistant à adjoindre à un message un élément appelé "enveloppe" scellée (ou sceau) afin d'en garantir l'intégrité. A la réception, le sceau est reconstitué par le destinataire puis comparé au sceau reçu. Si les deux sceaux ne sont pas identiques, cela indique qu'il y a eu altération du message, donc perte d'intégrité.

CHIFFREMENT
Action consistant à substituer à un message, ou à un ensemble d'informations que l'on souhaite protéger, un texte inintelligible par quiconque ne connaît pas la clé pour retrouver le texte d'origine. Son utilisation suppose un mode de distribution de clés.

Le chiffrement assure diverses fonctions : la confidentialité, l'intégrité (en permettant la détection de modifications des informations) et l'authentification (en protégeant le système contre les tentatives non-autorisées de connexion).

PARE-FEU (ou BASTION, « FIREWALL »)
Mécanisme logiciel ou matériel servant à se prémunir contre les accès non autorisés à des réseaux de télécommunications.

CERTIFICATION ÉLECTRONIQUE D'IDENTITÉ
Processus de validation applicable à un enregistrement (ex: certificat d'étude), à une capacité financière (ex: lettre de crédit bancaire), ou encore, à une transaction sécurisée (ex: certificat d'une autorité de certification). Cette vérification ainsi que l'émission du certificat correspondant s'exercent par une autorité (ou tiers) de certification. (Une description plus détaillée figure à la partie 5 de l'annexe E).

INFRASTRUCTURE A CLÉ PUBLIQUE (ICP)
L'infrastructure à clé publique (ICP) ou "Public Key Infrastructure ("PKI") est une infrastructure de certification électronique d'identité des personnes ou des dispositifs (ex: sites WEB).

L'annexe *E* renferme une liste beaucoup plus complète de mécanismes de sécurité. Nous invitons le lecteur à la consulter en se demandant quels mécanismes sont actuellement en place dans son organisation et lesquels devraient être implantés pour réaliser des transactions d'affaires sur les Inforoutes.

5. ÉTABLISSEMENT DE SERVICES COMMUNS DE SÉCURITÉ

5.1 LES BESOINS COMMUNS DE SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUES AU GOUVERNEMENT

Comme nous l'avons vu, les échanges informationnels les plus fréquents concernent:

- la diffusion d'information gouvernementale ;
- les échanges personnalisés d'information (ex. : courrier électronique) ;
- le transfert de fichiers d'applications ;
- l'échange de formulaires internes ;
- l'échange de formulaires normalisés (EDI) avec les partenaires d'affaires ;
- la réalisation d'autres transactions d'affaires.

Les échanges informationnels de types « échanges personnalisés » et « transactions d'affaires » requièrent une gamme plus élaborée de garanties :

- assurer la confidentialité ;
- assurer l'intégrité du contenu ;
- pouvoir authentifier l'émetteur ;
- autoriser l'accès extérieur aux employé(e)s à des ressources informationnelles corporatives ;
- autoriser l'accomplissement de transactions, selon les privilèges ou pouvoirs d'un employé (acheter, payer, signer une entente) ;
- assurer la non-répudiation de ce qui a été transmis grâce au mécanisme de signature électronique.

Ces garanties peuvent être obtenues par les mécanismes de sécurisation suivants:

- l'enregistrement ;
- le contrôle des accès ;
- la signature électronique ;
- le scellement ;
- le chiffrement ;
- l'établissement d'une infrastructure de clés publiques (ICP/PKI).

5.2 ÉTABLISSEMENT DE SERVICES COMMUNS

Contexte

Les mécanismes de sécurité énumérés à la section 5,1 doivent être disponibles à toutes les organisations gouvernementales. Ces organisations les utiliseront après une évaluation sérieuse de leurs besoins selon plusieurs facteurs dont le niveau de menaces et de risques, ainsi que le type d'information en cause.

Il est certain que les coûts devront être abordables, car l'expérience des dernières années démontrent que les gens ont des réticences à investir dans les outils de sécurisation technique ou juridique des transactions d'affaires.

Par exemple, près de la moitié (45 %) des entreprises québécoises utilisatrices de l'EDI ne disposent toujours pas d'Accord d'interchange EDI (entente juridique avec leurs partenaires d'affaires) (voir annexe B), et ce, en dépit des efforts de promotion des partenaires gouvernementaux et des associations d'utilisateurs (ex: Institut EDI du Québec). De même, très peu d'entreprises québécoises protègent leurs messages personnalisés et leurs transactions

d'affaires à l'aide de la technique du chiffrement. Ces réticences proviennent peut-être d'une insouciance, ou encore, d'une méconnaissance de la problématique et le fait que des solutions éprouvées soient déjà disponibles.

Comme nous l'avons vu, les organisations gouvernementales ont des besoins d'affaires similaires à ceux des entreprises privées. De même, les organisations gouvernementales ont des besoins de sécurité des échanges électroniques semblables à ceux des autres organisations de notre propre gouvernement, ou de celles d'autres gouvernements.

En fait, plusieurs organisations gouvernementales, para-gouvernementales ou péri-gouvernementales manipulent les mêmes types d'informations. Il n'est donc pas surprenant de constater la similitude des besoins.

La principale différence entre les secteurs public et privé concerne la confidentialité des « dossiers clients » . En effet, une seule fuite sur sept millions de dossiers peut avoir de fâcheuses conséquences politiques et juridiques.

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ainsi que la Loi sur la protection des renseignements personnels dans le secteur privé, prévoient toutes deux l'obligation pour les organisations, tant publiques que privées, d'assurer la confidentialité des renseignements personnels qu'ils détiennent.

D'autre part, il est important que les organisations gouvernementales adoptent des « façons de faire communes » pour assurer certaines fonctions comme l'authentification et l'autorisation (ex. : par la signature numérique) et la certification électronique d'identité, ceci, afin de faciliter l'acceptation juridique des nouveaux processus électroniques et de réduire les coûts unitaires.

Infrastructure
L'Infrastructure de « services communs » est composée de plusieurs couches distinctes ou niveaux de services. Par exemple, le modèle de services d'infrastructure du gouvernement du Canada est composé de 5 couches :

1) Transport (ex. : communication avec ou sans fil, services mobiles)
2) Réseau (ex. : commutation par paquets, répertoires électroniques)
3) Informatique distribuée (Dépôts électroniques, gestion des postes de travail)
4) Applications (EDI, formulaires électroniques, applications d'Internet)
5) Prestation de programme (guichet unique, centres d'appel)

Le modèle de services du gouvernement du Québec n'est pas encore arrêté officiellement. Cependant, voici quelques composantes qui devraient être mis en place à l'échelle gouvernementale afin d'améliorer la prestation de service aux employés de l'Administration, aux entreprises québécoises et aux citoyens :

Répertoires électroniques de type X.500

- Télémessagerie

(ex. : Services en cours de développement à la DGT (CT-SG)

- Sécurité des transactions d'affaires

(ex. : infrastructure d'autorisation et d'authentification électronique <AAE> ou <ICP> Infrastructure de clés publiques).
(ex: bastion de la DGSTI (Conseil du trésor)

- Ingénierie documentaire

(ex. : Définition type de documents (DTD) et stockage des documents électroniques en SGML, numérisation massive des documents papiers, dépôts électroniques des documents, indexation assistée des documents, interface normalisée aux formulaires électroniques, service de localisation de l'information électronique <GILS>, outils de navigation WEB et engins de recherche).

CONCLUSION

Il existe de nombreux moyens permettant d'assurer la sécurité des échanges électroniques « sensibles », comme les messages confidentiels et les transactions commerciales et d'affaires. Le choix des moyens à mettre en place dans nos organisations dépend de plusieurs facteurs dont le niveau de menaces et des risques, ainsi que le type d'information en cause.

Faute d'une solution « miracle », « unique » et « valable dans toutes les situations », il reste alors aux développeurs de systèmes, ainsi qu'aux intégrateurs de technologies, à élaborer des mécanismes complets, fiables et d'utilisation simple, rapide et économique pour les consommateurs.

Ces solutions « intégrées » devront certainement satisfaire les considérations juridiques entourant la signature et la preuve. **En fait, ces solutions devront être à la fois, juridiquement acceptable, techniquement faisable, organisationnellement déployable et économiquement viable**.

Ils devront également bénéficier de la confiance pleine et entière des utilisateurs, consommateurs, commerçants, institutions financières ainsi que des organisations gouvernementales. Cette confiance est une condition essentielle au succès du Commerce électronique et des échanges électroniques sécurisés sur les Inforoutes.

ANNEXES

ANNEXE A1
TECHNOLOGIES DU COMMERCE ÉLECTRONIQUE

Voici une liste des principales technologies identifiées, par la firme américaine Gartner Group et le ministère de la défense américaine (DOD), comme faisant partie du Commerce électronique :

- BABILLARD ÉLECTRONIQUE
- Service d'information en différé offert à une communauté locale ou régionale via l'utilisation du réseau téléphonique.
- BANQUE D'INFORMATION PARTAGÉE
  Accès aux banques d'information d'un partenaire d'affaire pour la gestion d'un processus d'affaire commun (par exemple, la gestion des stocks et l'approvisionnement).
- CODE A BARRES
  Utilisation de (code à barres) pour des activités de contrôle et d'inventaire des pièces.
- COURRIER ÉLECTRONIQUE
  Utilisation d'un service électronique public pour l'envoi de messages et de documents d'affaires.
- EDI
  Échange de plus de 300 types de formulaires normalisés entre des entreprises distinctes, pour leurs bénéfices mutuels. Ces messages touchent à toutes les fonctions des entreprises (finance, production...) et à la plupart des secteurs industriels (alimentation, douanes, santé,...).
- EDI FINANCIER
  Échange de formulaires normalisés EDI entre des entreprises et leurs Institutions financières, portant sur des transactions d'affaires et leur paiement.
- SERVEUR DE TÉLÉCOPIE
  Télécopie de formulaires, à la demande des utilisateurs, via le combiné téléphonique.
- TÉLÉCOPIE
  Transmission de l'image de documents d'affaires, via le téléphone.
- TRANSFERT ÉLECTRONIQUE DE FONDS
  Transfert d'argent entre institutions financières.

ANNEXE A2
NOUVELLES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Voici une liste sommaire d'autres nouvelles technologies de l'information et de la communication (NTIC) :

- AUDIOTEX
- Babillard vocal offrant un menu de messages ou des actions pré-déterminées que l'appelant peut sélectionner.
- BANQUE D'INFORMATION (Télématique Ascii)
  Accès payant à des banques d'information à caractère de diffusion publique, via l'utilisation d'un réseau de télécommunication (ex. : service Telnet, d'Internet).
- BORNE INTERACTIVE (Hyperborne)
  Terminaux d'accès public localisés dans des endroits publics tels des centres commerciaux, bureaux de poste, bibliothèques, etc.

- CARTE A MÉMOIRE
  Carte de la taille d'une carte de crédit contenant un micro-processeur ou puce. Cette puce permet l'exécution de programme assurant la réalisation de fonction de sécurisation des transactions.
- DISQUE OPTIQUE
  Utilisation de disque au laser pour la diffusion d'information sonore (CD-Audio), textuelle et image (CD-ROM), de film (vidéodisque), de cours de formation (CD-Interactif), ou encore, pour l'enregistrement permanent de documents administratifs (WORM) ou temporaire (disque réinscrivible).
- GESTION DE FLUX DE DOCUMENTS & DE TRAVAUX (WORKFLOW)
  Gestion des acheminements, des contrôles d'accès, des approbations (autorisations) et de l'archivage de documents à l'intérieur d'une organisation ou d'une communauté restreinte.
- IMAGERIE DOCUMENTAIRE
  Gestion de l'image des documents administratifs et d'autres documents spécifiques (plans, cartes, ...).
- TÉLÉMATIQUE
  Ensemble de services d'information incluant la communication bidirectionnelle (messagerie), la consultation de services d'information (banque d'information, téléformation, télésanté, etc) la réalisation de télétransactions d'affaires et de divertissement.
- TRAVAIL DE GROUPE (WORKGROUP)
  Deux individus, ou plus, partageant des fichiers et banques de données, généralement en temps réel (en direct).
- VIDÉOTEX
  Système de diffusion d'information sous forme textuelle ou graphique. Le Minitel utilisé en France est un bon exemple de système vidéotex. Contrairement à Internet, le Minitel n'offre pas le son, les images couleurs fixes ou animées ainsi que les liens hypertextes dynamiques.

ANNEXE B
PARTICULARITÉS DE L'EDI TOUCHANT A LA SÉCURITÉ

1- LA NORMALISATION

La normalisation de l'EDI touche à plusieurs facettes des échanges électroniques :

- Formulaires électroniques normalisés (ou messages)

  Le contenu des formulaires électroniques normalisés (appelés « messages » par les Nations Unies <EDIFACT/ONU>) est fixe et déterminé lors de la publication de la norme. Le contenu d'un message peut également être modifié à des périodes précises de l'année, soit en décembre pour la norme nationale américaine AINSI-X12, ou encore, en mars et septembre pour la norme internationale EDIFACT/ONU.

- Le vocabulaire normalisé des messages

  Les centaines des formulaires EDI appartenant à la norme AINSI-X12, ou à EDIFACT/ONU, sont composés d'un vocabulaire de base commun regroupant plus de sept mille (7 000) entités ou pièces. L'agencement d'une partie de ces entités forme chacun des formulaires normalisés ou messages.

- La syntaxe des échanges électroniques

  La syntaxe est également normalisée. Par exemple, la norme ISO 9735 décrit la syntaxe d'EDIFACT/ONU.

2- LE CADRE JURIDIQUE

Les utilisateurs EDI sont invités depuis plusieurs années par les associations d'utilisateurs (ex. : Institut EDI du Québec) et les gouvernements à conclure des ententes juridiques EDI (Trading Partner Agreement-TPA) avec leurs partenaires d'affaires. De telles ententes permettent de préciser le cadre juridique et technique dans lequel se feront les échanges, ce qui réduit ainsi les risques de mésententes et de conflits. Les enquêtes réalisées par EDI Group Canada, ou par le CEFRIO et l'Institut EDI du Québec, révèlent qu'à ce jour près de 55 % des utilisateurs de l'EDI au Québec, et ailleurs au Canada, auraient conclu de telles ententes. De tels contrats EDI ne règlent évidemment pas toutes les situations juridiques pouvant se présenter.

Quoique simple et pratique lorsque les partenaires sont en affaires depuis un certain temps déjà, la conclusion de telles ententes juridiques EDI est impensable dans un scénario d'EDI ouvert, c'est-à-dire là où les partenaires EDI ne se connaissent pas nécessairement.

C'est de cette réalité d'ouverture et de mondialisation de l'économie qu'ont émergé les « profils d'interchange EDI », que le juriste français Me Thierry Piette Coudol a fait connaître largement ces dernières années. En fait, il s'agit d'établir un modèle de règles de conduite et un référentiel (ou corpus) de conditions juridiques, auxquels les partenaires EDI adhéreront par simple mention de leur intention dans un message EDI.

En plus des « ententes EDI » et des « profils d'interchange EDI », certains états européens ont commencé à légiférer pour préciser le cadre juridique des échanges électroniques, favorisant ainsi sa diffusion rapide.

La Commission des Nations Unies pour le Droit du Commerce International (CNUDCI/UNCITRAL) a adopté un projet de loi cadre en mai 1996. Ce projet invite les états membres à adopter des lois qui stipuleraient clairement que les documents électroniques sont aussi valables que les documents « papiers » correspondants, si des conditions précises sont respectées. La loi-modèle de la CNUDCI n'aborde toutefois pas les questions relatives à la hiérarchie des preuves en cas de litige, des règles sur la responsabilité, les mesures de sécurité à adopter et la responsabilité des tiers (ex: réseau RVA).

3- LA SÉCURITÉ DES ÉCHANGES EDI

Des procédures précises de sécurité ont été élaborées pour délimiter les échanges EDI et réduire les mésententes et conflits. Ces procédures sont décrites dans le document X12.58 pour l'ANSI et dans plusieurs documents dans le cas d'EDIFACT/ONU. Ces procédures sont jugés très sûres et conservatrices, par les spécialistes de la sécurité informatique.

En fait, dans le « monde de EDI » on fait plus que de simplement sécuriser le contenu des messages. On en précise le contexte d'affaires, l'ordonnancement séquentiel des échanges de formulaires électroniques « business scénario », le contexte juridique et la réalisation technique.

ANNEXE C
SERVICES DE BASE DE L'INTERNET

Voici une liste sommaire des principaux services d'information sur les autoroutes de l'information :

- COURRIER ÉLECTRONIQUE PUBLIC

Envoi de message de texte libre (à structure non définie) via l'utilisation de boîte postale électronique. Internet permet de plus en plus de rejoindre les usagers des réseaux privés de messagerie.

- LISTE DE DISTRIBUTION (Groupe de discussion)

Envoi automatique de messages à tous les membres inscrits d'un groupe de distribution.

- NOUVELLES (News)

Accès à des messages et autres fichiers stockés dans des dossiers thématiques pour une période de 7 à 10 jours.

- ACCES EN MODE « FTP »

Accès à des fichiers stockés sur des ordinateurs éloignés à l'aide d'un protocole de transfert normalisé « file transfert protocol ».

- ACCES EN MODE « TELNET »

Accès en mode « session interactive », par l'exécution à distance d'une application. Par exemple, la consultation du catalogue de la Bibliothèque Nationale du Québec.

- ACCES EN MODE « GOPHER »

Accès à l'aide de menu à des informations structurées.

- ACCES EN MODE WEB (World Wide Web-WWW)

Accès à l'aide de « liens hypertextes » à des informations textuelles, sonores ou visuelles (images fixes ou animées).

- MOTEURS DE RECHERCHE

Il existent de nombreux outils de recherche tels Archie, Véronica, Wais, Yahoo, qui permettent la recherche par mots clés.

- NAVIGATEUR

Logiciel permettant de « naviguer » sur le WEB en passant facilement et rapidement d'un site à un autre.

- COMMANDE ÉLECTRONIQUE

Utilisation du WEB pour effectuer une commande à un fournisseur de biens ou de services.

- PAIEMENT ÉLECTRONIQUE

Paiement fait par des individus ou des organisations, à l'aide du WEB.

ANNEXE D
SERVICES COMMERCIAUX DE L'INTERNET

Depuis quelques années, il se développe des pratiques commerciales sur l'autoroute de l'information, partant de la simple offre de produits et services à travers une vitrine commerciale à la constitution de véritables Centres d'achat électronique. En fait, les entreprises peuvent vouloir se brancher sur l'autoroute de l'information pour différents motifs

1. Accéder à de l'information stratégique pour leur entreprise;
2. Diffuser des documents à leur clientèle et à leurs fournisseurs.
3. Établir une présence virtuelle auprès de millions de consommateurs disséminés aux quatre coins de la planète;
4. Établir un réseau virtuel d'affaires ne connaissant pas de limites temporelles, géographiques ou territoriales;

1- VITRINE

Le premier service auxquels les entreprises, tant privées que publiques, envisagent lorsqu'elles décident de s'engager du côté de l'Internet est la vitrine WEB.

En effet, la vitrine constitue en effet, tant dans le Cyberespace que dans le circuit traditionnel des affaires, une excellente façon de faire connaître ses produits & ses services de même que les orientations, le personnel et les valeurs de gestion de son organisation. La vitrine WEB peut donc être considérée comme le premier pas dans le commerce électronique sur Internet.

La vitrine WEB peut inclure, selon les cas, des fonctions de diffusion d'information, de catalogue électronique, de commande électronique et également de communication électronique pour permettre aux futurs acheteurs de demander plus d'information, et éventuellement, pour négocier des conditions particulières.

Il existe déjà de nombreux exemples de catalogues de produits disponibles sur Internet :

http:/www.amp.com
http:/www.hp.com
http:/www.part.net
http:/www.saqara.net

2- CENTRE D'ACHAT ÉLECTRONIQUE

Plusieurs Centres d'achats ou Supermarchés électroniques ont vu le jour ces trois dernières années. Que l'on pense à CommerceNet, Intermarket et The Branch Mall. Ces systèmes se veulent le point de rencontre entre l'offre et la demande. Des milliers d'acheteurs potentiels fréquentent régulièrement ce site de WEB en quête de « bonnes affaires ».

Les Centres d'achats électroniques peuvent permettre à un fournisseur de produits de vendre annuellement plusieurs centaines de milliers de dollars peut-être même des millions, par employé. Ce qui est de beaucoup supérieur à ce que permet les circuits actuels de distribution.

3- PAIEMENT SUR INTERNET

Il est acquis que le Commerce électronique sur les autoroutes de l'information devrait générer, à court ou à moyen terme, un volume gigantesque de transactions sur les Inforoutes. Cependant, ce type de commerce sur les Inforoutes ne peut devenir une réalité tant que les opérations commerciales ne s'achèveront pas par des paiements.

Il est en effet peu pratique d'utiliser un système télématique (tel Internet) pour commander des produits ou des services et un autre système manuel, (même un numéro téléphonique 1-800), pour compléter la transaction en effectuant le paiement. Les institutions financières offrent déjà le paiement électronique, souvent effectué à partir de systèmes privés de télécommunication tel Interact. Mais les utilisateurs d'Internet veulent accéder à des services de téléachat et de télépaiement accessibles simultanément et directement sur le Web.

Des initiatives apparues ces derniers mois sur le Web vont d'ailleurs dans ce sens. Elles ont pour nom CyberCash, DigiCash, Global OnLine et First Virtual. Ce dernier, par exemple, a réussi à rejoindre en moins de 14 mois, 150 000 acheteurs et 1 670 marchands en provenance de 148 pays. A ce jour 2,5 millions de personnes auraient déjà commandé des biens à partir d'Internet, et ce, en dépit du peu de confiance en la sécurité de "bout en bout" de son architecture.

Sur Internet, la question de l'authentification est double parce que l'acheteur et le vendeur ne sont pas en présence physique l'un de l'autre. Des services frauduleux pourraient alors proposer de fausses ventes pour empocher de vrais paiements. De plus, les informations confidentielles des cartes, comme le numéro de la carte bancaire et le code secret, peuvent être écoutés sur le réseau et reproduits pour provoquer de faux paiements. Le Code secret est un identifiant composé principalement de la fusion (ou concaténation) du numéro de série de la carte, du numéro de carte bancaire et de la date d'expiration de la carte. Le tout est codé par un algorithme de clés publiques de type RSA. Ce code est un bon moyen d'authentification. Mais il n'est pas une signature électronique, car il lui manque la garantie d'intégrité. Par opposition avec la signature électronique qui change selon le contenu du message, le code secret lui reste toujours identique.

Lorsque l'on aborde la sécurisation des informations sur les autoroutes de l'information, il ne faut pas perdre de vue qu'il existe deux grandes approches dans la protection des informations sur les autoroutes de l'information. On peut tenter de sécuriser l'ensemble du réseau de transmission (ce qui est impensable actuellement dans le cas des réseaux très ouverts tel INTERNET), ou encore, sécuriser ou « blinder » les messages eux-mêmes. Cette exemple vaut également pour les autoroutes automobiles où il est préférable de ne pas trop s'aventurer dans certaines régions reculées riches en brigands, sans y "sécuriser" au préalable son véhicule en s'assurant à tout le moins de son bon fonctionnement.

Services de paiement sur l'internet
Voici une liste des nouveaux modes de paiement disponible ou en développement sur l'Internet :

i. Nouveaux modes de paiement
« Monnaie électronique » : l'exemple de DIGICASH. Le client est crédité d'une somme d'argent en CyberBucks, stocké sur son disque dur, comme dans un porte-monnaie. Pour paiement de toute somme, l'acheteur prélève sur son crédit, disponible sur son disque dur et crédite le vendeur.

« Porte-monnaie électronique et carte bancaire » : l'exemple de « Global OnLine (GOL) » de France. C'est un service avec deux modes de fonctionnement. Les petites sommes sont gérées par un système de porte-monnaie électronique. Les sommes plus importantes sont payées par le système bancaire via le service GOL. Les messages de paiement de l'acheteur sont chiffrés (codés) et ne comprennent pas d'identifiant bancaire, mais l'identifiant GOL.

ii. Prolongement du système bancaire et de carte à puce

« Alliance du WEB et des cartes » : l'exemple FIRST DATA / NESTCAPE

Il s'agit de l'adaptation à Internet du paiement par Carte bancaire. Le site WEB du vendeur reçoit la transaction de paiement authentifiée par la carte bancaire de l'acheteur. La transaction générée par le navigateur Netscape a été préalablement chiffrée.

« L'adaptation de la carte bancaire à Internet » : l'exemple de VISA / MasterCard - EuroCard.

Le système consiste à « prolonger » les moyens existants. Ainsi le système des cartes à puce peut être adapté pour être employé plus efficacement sur le réseau (norme commune SET, Secure Electronic Transactions).

iii. Intermédiation avec le système bancaire

« Interface avec le système bancaire » : l'exemple de CYBERCASH.

Le client envoie une requête chiffrée (codée) au centre serveur CyberCash. Le centre serveur se connecte à la banque comme un « Terminal Point de Vente » (TPV) classique pour validation du paiement.

« Intermédiation avec le système bancaire » : l'exemple de FIRST VIRTUAL (F.V.).

Le vendeur adresse un message électronique au site WEB de First Virtual. Le serveur de F.V. interroge le client par courrier électronique sur la transaction de paiement : refus ou acceptation ? Si le paiement est accepté, le paiement est transmis à F.V. par le circuit bancaire traditionnel.

« Paiement dans la boutique virtuelle » : l'exemple de OPEN MARKET

Le service de Open Market (O.M.) est une véritable boutique électronique. Le client effectue son paiement chiffré au site WEB de O.M. à partir de son navigateur et de sa carte bancaire.

ANNEXE E
RISQUES INFORMATIQUES & MOYENS DE SÉCURISATION DES ÉCHANGES ÉLECTRONIQUES

1- RISQUES INFORMATIQUES

DÉFAILLANCE

- Défaillance totale d'un équipement (non disponibilité)
- Dysfonctionnement non détectable d'un équipement (possibilité de défaut d'intégrité involontaire)

ERREURS

- Saisie
- Traitement
- Sortie des résultats

MENACES DÉLIBÉRÉES

- Vol
- Virus
- Falsification (faux messages)
- Altération de message
- Duplication de message
- Suppression de message
- Perturbation de transmission
- Non-validité d'un bon message
- Signature d'un faux message

2- TYPES D'INTRUSION

- Usager effectuant une opération non autorisée
- Non usager (Espion industriel / « Hackers »)

3- MÉCANISMES DE SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUE

- CHIFFREMENT

Opération consistant à substituer à un message, ou à un ensemble d'information que l'on souhaite protéger, un texte inintelligible par quiconque ne connaît pas la clé pour retrouver le texte d'origine. Son utilisation suppose un mode de distribution de clés.

Le chiffrement assure diverses fonctions : la confidentialité, l'intégrité (en permettant la détection de modifications des informations) et l'authentification (en protégeant le système contre les tentatives non-autorisées de connexion).

Il existe plusieurs mécanismes de chiffrement tels que la cryptographie asymétrique (RSA), la cryptographie symétrique (DES), l'Escrow Encryption Standard (EES).

- AUTORISATION ÉLECTRONIQUE

(1) Action consistant à adjoindre à un message, un élément appelé « signature » numérique (code) permettant d'en garantir l'intégrité en même temps que l'authenticité de l'émetteur.
(2) Plusieurs moyens de différents niveaux de sécurité peuvent être utilisés pour l'identification & l'authentification :

i. Ce que l'on possède sur soi (jetons)
   (ex: carte magnétique, carte à mémoire)
   (clés asymétriques)
ii. Ce que l'on sais (ex: numéro d'utilisateur, mot de passe)
iii. Ce que l'on fais (ex: signature PEN OP)
iv. Ce que l'on est (ex: empreinte digitale, empreinte rétinienne)

- SCELLEMENT

Action de l'expéditeur consistant à adjoindre à un message un élément appelé « sceau » afin d'en garantir l'intégrité. A la réception, le sceau est reconstitué par le destinataire puis comparé au sceau reçu. Si les deux sceaux ne sont pas identiques, cela indique qu'il y a eu altération du message, donc perte d'intégrité.

- CONTROLE D'ACCES

Processus permettant de limiter l'accès à des ressources protégées (matériels, transactions, applications, fichiers, bases de données, etc.) uniquement aux entités autorisées (personnes, matériels, applications, etc.).

Identification : action permettant d'attribuer un identifiant à une entité (logique, matérielle, humaine).
Authentification : action permettant de vérifier ou de garantir l'identité d'une entité. Le contrôle d'accès utilise l'identité authentifiée pour accorder l'accès à une ressource en fonction de droits prédéterminés. Il peut enregistrer, sous forme de trace d'audit, et signaler toutes tentatives non autorisée d'accès. Il peut mettre en jeu des listes maintenues par des centres ou par l'entité accédé, des mots de passe, des jetons utilisés pour distribuer les droits d'accès, des certificats, des libellés indiquant la sensibilité des données. Le contrôle peut avoir lieu aux deux extrémités de la communication. Le « mot de passe » est une expression alphanumérique secrète, choisit par l'utilisateur, et qui est sujette à modification à intervalle régulier.
Échange d'authentification :

a) lorsque les entités homologues et les moyens de communication sont considérés comme sûrs, l'identification de l'entité homologue est suffisante et peut être obtenue par un mot de passe; celui-ci est efficace contre les erreurs mais pas contre la malveillance.

b) lorsque les entités se font mutuellement confiance, mais pas aux moyens de communication, il convient d'employer une combinaison de mots de passe et de chiffrement ou d'utiliser des moyens cryptographiques.

Gestion des droits d'accès : une fois l'identité établie (par l'authentification), il doit exister un mécanisme d'attribution des droits d'accès aux ressources (informations, traitements) en fonction de l'identité et d'autres critères fixes ou variables liés aux ressources ou à d'autres paramètres.

- GESTION DU ROUTAGE / ACQUITTEMENT

Routage : fonction permettant d'assurer l'orientation correcte d'un message vers son lieu de destination.
Acquittement : opération consistant à confirmer la réception d'un message, d'un texte, après en avoir vérifié la cohérence syntaxique (disposition des informations).

- GESTION DU ROUTAGE / REDEMANDE

Routage : fonction permettant d'assurer l'orientation correcte d'un message vers son lieu de destination.

Redemande : demande de répétition d'un message perdu ou inintelligible à l'arrivée.

- ACCUSÉ DE RÉCEPTION (SÉMANTIQUE)

Confirmation de la réception d'un message, d'un texte, accompagné, s'il y a lieu, d'une approbation du format, ou, du contenu après vérification sémantique.

- CONTROLE DE ROUTAGE

Les systèmes (extrémités) ou les réseaux peuvent être amenés à sélectionner une route plus sûre, après détection d'une attaque persistante ou pour tenir compte de la sensibilité des données.

Ceci peut être fait grâce à deux types de mécanismes:
Routage du type « toutes routes sauf »
Un certain nombre de routes ne devront pas être empruntées (routage adaptatif).
Routage par route obligatoire
Une ou plusieurs routes devront être empruntées obligatoirement. (Si l'on ne précise qu'une seule route, la défaillance de l'un des tronçons entraîne une impossibilité de transmission).

- CONTROLE & CORRECTION D'INTÉGRITÉ

Elle s'obtient par l'utilisation des codes de détection d'erreur, des codes de contrôle cryptographique et de la numérotation des unités de données par horodatation.

Horodatation : adjonction, par un tiers de confiance, à un message ou à une transaction, d'un élément permettant de garantir l'heure de l'émission, ou de la réception, ou encore un numéro de séquence du message (par rapport à l'émetteur, au destinataire, à l'opérateur, etc.).
Bourrage : Dans certains cas, l'accroissement du flux des informations entre deux entités peut être significatif pour un tiers. Pour s'en protéger, on effectue un « bourrage » de voie. La ligne sera constamment utilisée, entre deux émissions de messages utiles, avec des messages dépourvus de sens. Ces messages inutiles seront éliminés à l'arrivée. Ils devront être variables et non identifiables comme messages de « bourrage » par un ennemi. On utilisera pour cela un générateur de messages qui respectera la fréquence des lettres et des diagrammes de l'alphabet employé.
Séquencement : Ce mécanisme consiste à affecter un numéro d'ordre à chacun des messages.
Étiquettes de sécurité : Les ressources comprenant des éléments d'information peuvent avoir des étiquettes de sécurité qui leur sont associées, par exemple, pour indiquer un niveau de sensibilité. Il est souvent nécessaire d'acheminer l'étiquette de sécurité appropriée avec des données en transit. Une étiquette de sécurité peut être une donnée supplémentaire associée aux données transférées ou peut être implicite; elle peut, par exemple, être la conséquence de l'utilisation d'une clé spécifique pour chiffrer les données ou résulter du contexte des données telles que la source ou la route. Les étiquettes de sécurité explicites doivent être clairement identifiables afin de pouvoir être vérifiées de façon appropriée. En outre, elles doivent être liées d'une manière sûre aux données auxquelles elles sont associées.

D'autres mécanismes, qui ne sont pas des mécanismes "réseau" proprement dits, méritent également d'être soulignés.

Système de secours : En l'absence de système réparti susceptible de prendre immédiatement la relève d'un système défaillant, il est nécessaire de disposer d'un système de secours.

Certification de logiciels/Conception-réalisation : Le procédé de certification est fondé sur la classification de toutes les entités qui concourent à un résultat en fonction de la classification DIC des résultats.

Certification de logiciels / à posteriori : Le procédé de certification consiste à analyser dans des circonstances ou à une fréquence déterminée au moins la syntaxe de l'application (et si possible la sémantique stratégique).

Moyens de sauvegarde/Restauration : C'est un mécanisme de copie/recopie/substitution encadré par des procédures précises.

Niveau de sécurité offert par le système (matériel +système d'exploitation + réseau)/Livraison
Certification à partir de critères harmonisés du type « Assurance qualité ». Lorsque le système est composé de sous-systèmes, chacun d'eux doit faire l'objet d'une certification. L'ensemble doit être cohérent. La cohérence réside en particulier, et indépendamment de la qualité (certification) de chaque sous-système, sur l'agencement de ces sous-systèmes: choix de l'architecture, liaisons entre sous-systèmes (étanchéité), etc.

Niveau de sécurité offert par le système (matériel +système d'exploitation + réseau)Audit
Certification fondée sur la classification de toutes les entités qui concourent à un résultat, en fonction de la classification DIC (Disponibilité, Intégrité, Confidentialité) des résultats.

Surveillance du réseau : Ce mécanisme permet d'identifier les éventuels dysfonctionnements du réseau et les différents points qui ne seraient pas conformes au cahier des charges.

Journal d'audit de sécurité : Les journaux d'audit de sécurité fournissent un mécanisme de sécurité appréciable étant donné qu'ils permettent potentiellement de détecter et d'enquêter sur les violations de sécurité en permettant un audit de sécurité ultérieur. Un audit de sécurité est une étude indépendante et un examen des enregistrements et des activités de systèmes permettant de tester l'adéquation des contrôles, de s'assurer de la cohérence avec la politique établie et avec les procédures opérationnelles, d'aider à évaluer les dommages et de recommander des modifications dans les contrôles de la politique et les procédures. Un audit de sécurité nécessite l'enregistrement des informations relatives à la sécurité dans un journal d'audit de sécurité, ainsi que l'analyse et la production de rapports à partir des informations provenant d'un journal d'audit de sécurité. L'enregistrement est considéré comme un mécanisme de sécurité, il est donc décrit dans ce paragraphe. L'analyse et la production de rapports sont considérées comme une fonction de gestion de sécurité.

La collecte d'informations pour le journal d'audit de sécurité peut être adaptée à divers besoins en précisant le type d'événement à enregistrer (par exemple, violations apparentes de la sécurité ou exécution d'opérations réussies).

L'existence connue d'un journal d'audit de sécurité peut servir d'élément dissuasif pour certaines sources potentielles d'attaques de sécurité.

Les considérations liées à un journal d'audit de sécurité tiendront compte du type d'information qui pourra, en option, être enregistrée, des conditions sous lesquelles cette information devra être enregistrée et la définition syntaxique et sémantique à utiliser pour échanger des informations de journal d'audit de sécurité.

Sécurité du système privé : Mécanisme générique qui regroupe tous les mécanismes du système privé.

- PARE-FEU (ou Bastion, « firewall »)

  Mécanisme logiciel ou matériel servant à se prémunir contre les accès non autorisés à des réseaux de télécommunications.

4- NOTARISATION

La notarisation est l'enregistrement des éléments essentiels reliés à une transaction entre deux parties, par une tierce partie dite « de confiance ». La notarisation améliore la sécurité du système dans la mesure où elle assure aux entités, grâce à un tiers indépendant auquel les parties ont confiance, l'intégrité, l'origine, la date et la destination des données.

Depuis des centaines d'années cette fonction de notarisation est effectuée par des notaires dans les pays de droit latin. Ces officiers publics ont la responsabilité de s'assurer que les parties sont aptes à contracter et que la transaction est conforme aux façons de faire reconnues.

Comme le décrit bien un document récent de la Chambre des Notaires du Québec :
« La certification est 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 le lier au contenu d'un document électronique visant à manifester son consentement à un acte juridique.

L'autorité de certification est une entité chargée d'établir et, par la suite, de garantir un lien formel entre une personne et une paire de clés asymétriques dans une infrastructure de clés publiques. Son rôle consiste à vérifier, d'une part, l'exactitude de l'information contenue dans le certificat d'identification qu'elle émet et à garantir, d'autre part, la validité du certificat d'identification du signataire d'un document destiné 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.

Le certificat d'identification est un document électronique émis par une autorité de certification qui lie une personne à une paire de clés asymétriques, soit l'élément de base de la signature numérique, dans une infrastructure de sécurité à clés publiques utilisée dans un environnement ouvert, du type de l'autoroute de l'information. Le certificat d'identification porte la signature numérique de l'autorité de certification qui attribue à une personne une clé publique contenant certains éléments d'information relatifs à son identité qu'elle rend volontairement disponibles et une clé privée lui permettant de signer un document informatique qu'elle expédie ou de vérifier un document informatique qu'elle reçoit, en toute sécurité sur l'autoroute de l'information.

La fonction de régistraire de l'autorité de certification consiste essentiellement à gérer l'émission, la distribution, la diffusion et la révocation des certificats d'identité associant une personne à une signature électronique. Cette fonction de base englobe généralement la tenue d'un répertoire de type X-500 contenant tous les certificats d'identification émis au profit des parties désirant transiger à distance auquel on peut se référer, le cas échéant, pour vérifier la validité du certificat émis au profit d'un tiers.

La fonction de fiduciaire de l'autorité de certification englobe la conservation d'une copie de la paire de clés, soit la clé publique et la clé privé du détenteur d'un certificat d'identification, émise au profit d'une personne physique ou morale pour des fins de protection, de surveillance et de contrôle par un organisme responsable de la gestion d'un secteur d'activités donné ou pour se ménager une preuve émanant d'une tierce partie indépendante et impartiale en cas de litige pouvant survenir à l'occasion d'une transaction.

La fonction de tiers-certificateur de l'autorité de certification consiste essentiellement à certifier à divers degrés, suivant le niveau de certification requis, l'identité du signataire d'un document ou d'une partie à une transaction conclue à distance. Cette fonction peut également englober l'horodatation du cheminement critique d'une transaction ou d'un document produit, signé, échangé et conservé sur un support informatique. Enfin, dans un pays de tradition civiliste, la fonction de tiers-certificateur d'une autorité de certification peut aller jusqu'à garantir le contenu d'un message ou d'un document.

La certification de l'identité des parties à une transaction s'effectue normalement en chaîne à travers des autorités de certification locales, régionales, sectorielles, nationales et internationales, quand les parties à un acte juridique conclu à distance possèdent un certificat émis par une autorité de certification faisant partie de la même chaîne de certification.

La certification entrecroisée s'effectue sur la base d'ententes de réciprocité entre les autorités de certification d'un même niveau. Le notariat constitue un modèle de reconnaissance réciproque des processus de certification utilisés par les différentes organisations notariales chapeautant les autorités régionales et locales de certification, soit les chambres des notaires et les notaires, dans près de 110 pays de tradition notariale.

Procédés techniques ou personnes physiques ?
Tout comme dans un environnement contractuel conditionné par un support papier, les niveaux de certification requis sur les Inforoutes dépendent en grande partie des besoins du marché, du type de transaction ou de contrat, de la preuve à établir en cas de litige et des impératifs de stabilité économique et juridique ayant pu ou pouvant être établi par l'État.

En fait, la certification de l'identité des parties transigeant à distance peut, pour des transactions usuelles et récurrentes, s'effectuer par un procédé purement électronique mais nécessite parfois l'intervention d'une personne physique externe à la transaction, soit le tiers certificateur.

Il s'agit en fait d'évaluer le niveau de risques associés au type de transaction et les valeurs en jeu pour choisir le mécanisme d'autorisation approprié. Il se développe actuellement une foule de mécanismes d'autorisation électronique à travers le monde, particulièrement dans le contexte de l'Internet, mais peu d'entre eux impliquent l'intervention humaine dans le processus de certification et la majorité d'entre eux ne disposent pas d'assises légales en matière de certification d'identité » .

5- VALEUR PROBANTE DES MOYENS DE SÉCURISATION JURIDIQUE ET TECHNIQUE

Les moyens de vérifier et d'authentifier les documents « papiers » sont très variables actuellement dans le monde des affaires. Il pourrait en être de même dans le cas des documents électroniques où plusieurs niveaux de services d'identification des parties, de validation, d'authentification, de certification, d'audit et d'archivage pourraient être utilisés.

En fait, d'un point de vue juridique, ce n'est pas le papier lui même qui est apprécié, mais bien le processus d'affaire et les usages qui le sous-tendent. Aussi, tant d'un point de vue juridique que pratique, c'est la "façon de faire" qui est appréciée par le tribunal et pas simplement le moyen utilisé.

Ainsi en France, il est courant de régler une note de restaurant ou faire ses petits achats par chèque car l'émission d'un chèque sans provision est une faute grave, sujette à emprisonnement. Ce qui n'est pas le cas chez nous dans le quotidien. Alors très peu de gens d'ici accepteront vos chèques sans autres formalités (identification de la personne, vérification d'authenticité, provision suffisante, etc).

De même, lorsque deux personnes s'échangent de petites sommes (ex: moins de 100 $), l'argent liquide (billet au porteur payable par la Banque centrale) est habituellement le moyen le plus utilisé. Les chèques, notes de crédit, mandats bancaires, mandats postaux et autres moyens de paiement sont donc relativement peu utilisés chez nous pour de tels transferts.

Un autre exemple sur l'acceptabilité des « façons de faire » plutôt que du moyen technique concerne le cachet postal. Celui-ci est accepté depuis longtemps par nos tribunaux comme moyen de datation. Cette acceptation n'est pas tant reliée à la forme et la dimension du cachet lui-même, que par l'acceptation de l'autorité qui les apposent (Poste Canada) comme tiers certificateur. En effet ce tiers n'a aucun intérêt particulier à fournir une fausse information au tribunal, à la faveur de l'une des parties. Toutefois les tribunaux, d'ici ou d'ailleurs, n'accordent habituellement pas une valeur semblable au cachet des services de messagerie d'entreprise privée.

ANNEXE F
LA CARTE A MICROPROCESSEUR

Une vaste réflexion est en cours actuellement au gouvernement du Québec concernant l'introduction de la « carte à microprocesseur ».

Appelée également, « carte à puce », « carte à mémoire » ou **CAM**, ce type de technologie présente plusieurs avantages indéniables en ce qui concerne la sécurité informatique. En effet, par sa miniaturisation marquée, ses capacités de stockage d'information électronique et de traitement informatique directement sur la carte, la CAM est véritablement devenue une « carte maîtresse ».

D'un point de vue technologique, signalons simplement qu'il existe trois sortes de CAM, soit la « carte à mémoire simple » (ex: carte prépayée non rechargeable), la « carte à logique câblée » (ex: carte prépayée rechargeable) et la « carte à microprocesseur évoluée ».

De telles cartes pourraient servir pour différentes fonctions comme l'authentification électronique, l'autorisation électronique (signature électronique), la monnaie électronique et la constitution de "dossier client" sectoriel ou global. En fait, ces fonctions pourraient s'avérer très utiles dans une multitude d'applications typiques, ou non, d'un milieu gouvernemental.

Authentification électronique
La CAM pourrait servir par exemple d'outil de contrôle de base (sorte de jeton) pour l'accès à des systèmes informatisés sur micro-ordinateurs, mini ou maxi-ordinateurs, de même que des moyens de contrôle d'accès à certains immeubles gouvernementaux et appareils tels que photocopieurs. Dans de telles applications, la CAM aurait une utilité semblable, voire équivalente, à celle de la carte à piste magnétique.

Autorisation électronique (signature)
Les caractéristiques de la CAM s'avèrent plus avantageuses et pertinentes pour la fonction d'autorisation électronique. Citons par exemple l'autorisation des transactions électroniques et la « signature électronique » des actes juridiques et administratifs.

Monnaie électronique
Les compagnies de téléphonie ont débuté en 1995 la diffusion massive de CAM pour l'achat prépayé de services téléphoniques.

De même, les grands émetteurs de cartes bancaires et de cartes de crédit (Visa, Mastercard, American Express) ont manifesté au même moment leurs intentions de favoriser la CAM. Il y aurait actuellement plus de 3 milliards cartes à pistes magnétiques et 800 millions de CAM dans le monde. Soulignons la progression constante des cartes à piste et l'importante progression des CAM depuis 18 mois.

Constitution d'un « dossier client »
La CAM pourrait également servir de carte d'identité pour l'ensemble de la population (ex: carte de citoyenneté, carte d'assurance maladie), ou encore, pour des clientèles spécifiques des organisations gouvernementales (carte d'électeur, carte de patient des établissements de santé, carte d'assurance médicament, permis de conduire, etc.).

Vers une carte gouvernementale multiservices

Plusieurs intervenants souhaiteraient utiliser une seule carte gouvernementale pour l'ensemble des services gouvernementaux énumérés ci-haut. Quelques documents récents du Comité des responsables de l'informatique du secteur public (CRISP) vont d'ailleurs dans ce sens. Une telle carte multiservice devrait spécifier la liste des services disponibles, tout en identifiant les droits d'accès et les permissions d'ajout ou de modification des informations qu'elle contient.

ANNEXE G
LA SIGNATURE ÉLECTRONIQUE PAR CRYPTOGRAPHIE ASYMÉTRIQUE (ou SIGNATURE NUMÉRIQUE) & L'INFRASTRUCTURE A CLÉ PUBLIQUE

1- SIGNATURE ÉLECTRONIQUE & CRYPTOGRAPHIE ASYMÉTRIQUE

Qu'est-ce qu'une signature électronique ?
La forme la plus usuelle de signature électronique est basée sur la cryptographie asymétrique dite à clé publique. Ce système comporte deux clés différentes mais complémentaires : une clé publique et une clé secrète. Divers produits spécialisés, logiciels et appareils, permettent de générer ces paires de clés nécessaires pour le chiffrement (codage) et le déchiffrement (décodage) des messages.

Comment fonctionne un système cryptographique ?
Un système cryptographique à clé publique exige l'utilisation des deux clés mathématiques complémentaires pour accomplir les différentes fonctions d'identification, d'intégrité et de confidentialité. La clé secrète, dont le caractère secret doit effectivement être préservé, fait uniquement l'objet d'une utilisation personnelle. En revanche, la clé publique peut être librement distribuée ou même incluse dans un répertoire électronique de clés publiques. L'une ou l'autre de ces clés permet d'encoder un message afin de le rendre illisible et inaccessible.

L'opération de décodage s'effectue selon le principe de la complémentarité des clés. Un message encodé avec une clé secrète ne peut être décodé qu'avec sa clé publique complémentaire. Inversement, si le message est encodé avec la clé publique, seule la clé secrète complémentaire permettra de le décoder, ceci afin d'assurer à l'expéditeur la confidentialité de ses données transmises.

Les exemples suivants expliquent de manière sommaire des différentes fonctions d'un système à clé publique.

Les fonctions d'« Identification du signataire » et d'« Intégrité du message »
Annie désire envoyer à Bernard un message informatisé signé de façon électronique pour prouver qu'elle en est bien l'auteur. Après avoir écrit son message, Annie en réalise un condensé à l'aide d'une opération mathématique. Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l'aide de la clé secrète d'Annie. Ce condensé encodé constitue la signature électronique du message. Annie envoie alors à Bernard le message en clair (i.e. non-codé) accompagné de la signature électronique. Lorsque Bernard reçoit le message et la signature, il décode la signature électronique, afin de pouvoir de vérifier son authenticité, en effectuant une opération mathématique grâce à la clé publique complémentaire d'Annie. S'il parvient à décoder la signature, Bernard est assuré que celle-ci a préalablement été réalisée avec la clé secrète complémentaire d'Annie et peut donc conclure de manière certaine qu'elle est l'auteur du message. Cette opération mathématique permet, par ailleurs, de vérifier la corrélation entre le message et le condensé, ce qui établit que le message n'a subi aucune altération lors de sa transmission.

La fonction de « Confidentialité du message »
Annie désire envoyer à Bernard un message auquel lui seul aura accès. Pour ce faire, Annie encode son message en utilisant cette fois la clé publique de Bernard qu'elle s'est procurée dans un annuaire de clés publiques ou que Bernard lui a envoyé. Une fois encodées et donc illisibles, les données peuvent être transmises en toute sécurité. Seule la clé secrète

complémentaire de Bernard sera en mesure de décoder le message. Annie est donc certaine que Bernard sera la seule personne capable de lire le message.

Pour une sécurité maximale
D'autres procédures et technologies peuvent intervenir dans ces scénarios de base afin d'augmenter le niveau de sécurité des échanges. Par exemple, l'ensemble des clés nécessaires à l'encodage et au décodage des messages peut demeurer secret: il s'agit de la cryptographie symétrique dite à <<clés secrètes>>. D'autre part, les clés secrètes peuvent être conservées sur une carte à piste magnétique ou sur une carte à puce auxquelles on accède par un code numérique secret. Enfin, pour plus de sécurité, les clés peuvent aussi être générées, octroyées et contrôlées par un tiers indépendant.

2- INFRASTRUCTURES A CLÉ PUBLIQUE

Plusieurs pays (ex. : Allemagne) et états américains (ex. : Utah) ont légiféré ces derniers mois pour définir quels moyens étaient juridiquement acceptables pour « signé » les documents électroniques; c'est-à-dire pour identifier les personnes et manifester leur consentement à un message ou une transaction. De façon pratique, cette « signature électronique » est réalisée à l'aide de « clés cryptographiques asymétriques ».

Outre l'utilisation des clés elles même, toute une infrastructure doit être mise en place afin de réaliser les différentes fonctions de la certification (tel que l'émission d'un certificat électronique d'identité par exemple), et ce, par les divers intervenants impliqués dans le processus. La carte à micro-processeur (carte à mémoire, ou carte à puce) est également une technologie porteuse dans ce type de créneau.

Il est 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 chacun de ses employé(e)s. Cette signature pourrait servir tant à l'interne (ex. : formulaire électronique), qu'à l'externe (ex: formulaire EDI).

Le gouvernement du Canada, qui a déjà doté l'ensemble de son personnel d'une adresse électronique, prévoit accorder une signature numérique à plusieurs d'entre eux, d'ici la fin de 1998.

Les autres gouvernements provinciaux, les entreprises et la population en général se doteront sans doute eux aussi, dans les prochains mois ou les prochaines années selon le cas, d'un moyen ou l'autre d'« autorisation électronique » afin de pouvoir transiger électroniquement à distance, et ce, de façon sécuritaire.

Il est à noter que plusieurs initiatives d'« autorité de certification » sont actuellement en développement, tant à l'échelle nationale, régionale, qu'internationale. Ces initiatives émergent :

i. d'organisations gouvernementales (ex. : au gouvernement fédéral : Travaux publics et services gouvernementaux Canada (TPSGC), Communication security establishment group (CSE, Défense Canada) ;
ii. d'institutions financières ou d'organismes de vérification de crédit (du type de la firme « Equifax ») ;
iii. de regroupements de juristes (ex. : chambre des notaires, Union internationale du Notariat Latin) ;
iv. de sociétés des postes (ex. : Postes Canada, Union Postale Internationale) ;

v. d'entreprises de télécommunication (ex. : ATT) ;
vi. d'autres entreprises privées.

Avec l'émergence de toutes ces autorités de certification, il est évident qu'il faudra songer très bientôt à l'« Établissement de pratiques communes de certification ».

Une étude sur cette question devrait d'ailleurs être produite d'ici juin 1997 par le Centre de Recherches en Droit Public (CRDP) de l'Université de Montréal. Cette étude se veut être une contribution tangible au développement harmonieux et cohérent d'une infrastructure de certification électronique d'identité à la grandeur du Québec.