SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUES AU GOUVERNEMENT DU QUÉBEC

DOCUMENT DE RÉFLEXION SUR LES ENJEUX, PRINCIPES DIRECTEURS & ORIENTATIONS GOUVERNEMENTALES

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

SECRÉTARIAT DU CONSEIL DU TRÉSOR

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

Direction des la coordination gouvernementale en technologies de l'information

Service des orientations et politiques de renouvellement

20 OCTOBRE 1997

ENJEUX, PRINCIPES DIRECTEURS & ORIENTATIONS GOUVERNEMENTALES

PLAN DU DOCUMENT

a) Enjeux

b) Principes directeurs

c) Orientations gouvernementales

Comité de réalisation

ENJEUX

1. FACILITER LE PASSAGE DES PROCESSUS « PAPIERS » AUX PROCESSUS « ÉLECTRONIQUES », LORS DE LA RÉVISION DES PROCESSUS ET DES MODES DE PRESTATION DES SERVICES GOUVERNEMENTAUX, EN SÉCURISANT LES DIVERSES ÉTAPES DU NOUVEAU PROCESSUS

   (en systématisant par exemple les différentes étapes du processus de production des documents électroniques: rédaction, révision, distribution interne, autorisation, distribution externe, réception, récupération et archivage électronique, tout en précisant clairement les moyens de sécurisation appropriés pour chaque étape)

2. FAVORISER LES ÉCHANGES ÉLECTRONIQUES SÉCURISÉS DANS LE CADRE HABITUEL DES AFFAIRES, EN TENANT COMPTE DE LA CAPACITÉ DE RÉVISION DES PROCESSUS DE PRESTATION DES SERVICES GOUVERNEMENTAUX ET DE LEUR RENTABILITÉ

   (par des échanges confidentiels avec les fournisseurs, les diverses clientèles <entreprises, bénéficiaires, citoyens> et les autres gouvernements. Ces échanges sont sécurisés par des moyens de chiffrement, de signature électronique des documents et de certification électronique d'identification. Cette sécurisation des échanges vise à démontrer un degré de confiance acceptable pour la bonne marche des affaires sous forme électronique)

   (ex. d'applications à sécuriser : achat électronique, diffusion électronique d'information gouvernementale, paiement électronique, télédéclaration avec l'Administration, émission de licences et permis)

3. ASSURER LA SÉCURITÉ DES INFORMATIONS ET LE RESPECT DE LA VIE PRIVÉE

   (en assurant : la disponibilité des systèmes, le contrôle et la journalisation des accès, l'intégrité et la confidentialité des échanges, l'authentification de l'émetteur et du récepteur <lien personne-message>, et finalement, la non-répudiation par ceux-ci)

   (ex. d'information à protéger : renseignements personnels, messages de nature « sensible », transactions administratives, transactions commerciales)

4. PROTÉGER LA « VISIBILITÉ CORPORATIVE » GOUVERNEMENTALE

   (en développant des sites WEB évolués, attrayants et à jour, tout en évitant que le contenu de ces sites soit modifié ou que le trafic des utilisateurs y soit détourné)

5. FAVORISER UNE FAÇON DE FAIRE « COHÉRENTE » AU GOUVERNEMENT EN MATIÈRE DE SÉCURISATION DES ÉCHANGES ÉLECTRONIQUES, ET COMPATIBLE AVEC CELLE DE NOS FOURNISSEURS, DE NOS CLIENTELES ET DES AUTRES ADMINISTRATIONS

   (en adoptant des orientations et des politiques administratives précises sur l'identification, l'authentification, l'autorisation et la certification électroniques)

   (ex. : moyens d'identification et d'authentification des utilisateurs)

6. FAVORISER UNE OUVERTURE SUR LE MONDE EN ADHÉRANT À DES « FAÇONS DE FAIRE RECONNUES », À L'ÉCHELLE NATIONALE ET INTERNATIONALE, EN MATIÈRE DE SÉCURISATION DES ÉCHANGES ÉLECTRONIQUES, ET CE, TOUT EN RESPECTANT LA LÉGISLATION EN VIGUEUR

   (en favorisant, en autant que possible, l'adoption de normes, protocoles, directives et pratiques reconnues, sur le plan national et international)

7. PROMOUVOIR L'UTILISATION DE LA CRYPTOGRAPHIE, SANS METTRE INDÛMENT EN PÉRIL LA SÉCURITÉ PUBLIQUE, LE RESPECT DES LOIS ET LA SÉCURITÉ NATIONALE

8. FAIRE DU GOUVERNEMENT UN « UTILISATEUR MODÈLE » DES SOLUTIONS DE SÉCURISATION DES ÉCHANGES ÉLECTRONIQUES

   (en se dotant des moyens d'identification électronique, des sites WEB sécurisés et des services de Certification électronique d'identité)

9. SENSIBILISER ET RESPONSABILISER LA COMMUNAUTÉ GOUVERNEMENTALE À L'IMPORTANCE DE LA SÉCURISATION DES ÉCHANGES ÉLECTRONIQUES, DANS UN CONTEXTE DE RÉSEAUX OUVERTS TEL QU'INTERNET

   (en responsabilisant les gestionnaires quant à l'évaluation des menaces et des risques associés aux échanges électroniques avec l'extérieur)

PRINCIPES DIRECTEURS

1. LES SOLUTIONS DE SÉCURISATION MISES EN PLACE DOIVENT DÉMONTRER UN DEGRÉ DE CONFIANCE PROPICE AU COMMERCE ÉLECTRONIQUE ET AUX AUTRES ÉCHANGES ÉLECTRONIQUES

2. TOUTE SOLUTION DE SÉCURISATION DOIT ÊTRE A LA FOIS TECHNIQUEMENT RÉALISABLE, JURIDIQUEMENT ACCEPTABLE ET ÉCONOMIQUEMENT JUSTIFIABLE

3. LE CHOIX D'UNE SOLUTION DE SÉCURISATION DOIT ÊTRE FONDÉ SUR UNE ÉVALUATION SÉRIEUSE DES MENACES ET DES RISQUES JURIDIQUES, ADMINISTRATIFS, ÉCONOMIQUES ET POLITIQUES

   (ceci afin d'éviter une négligence flagrante, ou tout au contraire, la tentation d'obtenir des garanties supplémentaires aux processus traditionnels sur support papier, par un perfectionnisme technique exagéré, dont les conditions de mise en œuvre et le coût financier seraient tout à fait injustifiables)

4. LE CHOIX D'UNE SOLUTION DE SÉCURISATION DOIT ÉGALEMENT TENIR COMPTE DE SON INTEROPÉRABILITÉ, DE SA PORTABILITÉ ET DE SA MOBILITÉ

   (ceci par l'adhésion à des normes, protocoles et façons de faire reconnues à l'échelle gouvernementale, régionale, nationale et internationale)

ORIENTATIONS DE BASE

1. FAVORISER LA LIBRE CONCURRENCE DANS LE MARCHÉ DES SOLUTIONS DE SÉCURISATION

   (ceci afin de respecter les règles harmonisées d'acquisition gouvernementale)

2. ADOPTER DES RÈGLES STRICTES ET PRÉCISES SUR LES SERVICES ATTENDUS

   (ceci afin d'obtenir des solutions arrimées aux besoins réels et bénéficier des meilleurs prix)

3. ADOPTER DES MESURES HARMONISÉES, VOIRE NORMALISÉES À L'ÉCHELLE GOUVERNEMENTALE, EN CE QUI À TRAIT À LA CERTIFICATION DES PERSONNES ET DES DISPOSITIFS (ex. : Site WEB)

   (ceci pour des motifs d'ordre juridique, mais aussi d'harmonisation et de cohérence face aux partenaires et aux clientèles)

4. PROCÉDER SYSTÉMATIQUEMENT AU CHIFFREMENT DES MESSAGES « SENSIBLES » ET DES TRANSACTIONS CONTENANT DES INFORMATIONS CONFIDENTIELLES

   (ceci afin de protéger les actifs informationnels et d'assurer leurs confidentialités, lorsque requis par la loi ou les circonstances.

5. FAVORISER LA CRYPTOGRAPHIE À CLÉS PUBLIQUES POUR LE CHIFFREMENT DES INFORMATIONS ÉLECTRONIQUES CONFIDENTIELLES

   (ceci, toutefois, en tenant compte de divers critères comme la nature des informations à sécuriser, la fréquence et le volume des échanges, de même que le nombre de participants aux échanges)

6. AUTHENTIFIER LES DOCUMENTS ÉLECTRONIQUES, LORSQUE REQUIS, EN UTILISANT LA SIGNATURE NUMÉRIQUE

   (ceci afin d'assurer la valeur légale, financière, administrative et patrimoniale des documents électroniques)

7. FAVORISER LA CRYPTOGRAPHIE A CLÉS PUBLIQUES POUR SIGNER ÉLECTRONIQUEMENT LES MESSAGES DE NATURE « SENSIBLE » ET LES TRANSACTIONS IMPORTANTES

   (ceci, toutefois, en tenant compte de divers critères comme la nature des informations à sécuriser, la fréquence et le volume des échanges, de même que le nombre de participants à ces échanges)

8. UTILISER SYSTÉMATIQUEMENT L'INFRASTRUCTURE À CLÉS PUBLIQUES "ICP", POUR LA CERTIFICATION ÉLECTRONIQUE D'IDENTITÉ DES PERSONNES ET DES DISPOSITIFS

   (ceci afin d'éviter l'usurpation et pour obtenir à la fois une sécurisation juridique et technique)

9. ÉTABLIR UN CADRE LÉGISLATIF ET RÉGLEMENTAIRE OU UN CADRE ADMINISTRATIF VISANT À ENCADRER LES ACTIVITÉS DES TIERS CERTIFICATEURS (OU TIERS DE CONFIANCE) AU QUÉBEC

   (ceci afin de protéger l'intérêt public et les consommateurs. Ce cadre administratif doit au moins inclure : des « Lignes directrices », un « Cadre de politiques et pratiques de l'Autorité de Certification », ainsi que des « Règles de meilleures pratiques »)

--> **DANS LE CADRE DU DÉPLOIEMENT DE SERVICES DE CERTIFICATION ÉLECTRONIQUE D'IDENTITÉ DES PERSONNES ET DES DISPOSITIFS, DE TYPE « ICP » :**

10. UTILISER UNE STRUCTURE DE CERTIFICATION À DIFFÉRENTS NIVEAUX DE CONFIANCE

    (ceci dans un souci de rentabilité et de continuité par rapport aux façons de faire actuelle dans le monde des affaires où coexistent divers degrés ou niveaux de risques, de confiance et d'assurance)

11. S'ASSURER QU'UN CERTIFICAT DE NIVEAU 1, 2, 3, OU 4, DISPOSE DE LA MÊME VALEUR DE CONFIANCE POUR TOUTES LES ORGANISATIONS GOUVERNEMENTALES

    (ceci afin de favoriser la reconnaissance mutuelle <ou réciproque> des Autorités de certification « AC » entre elles et éviter ainsi une véritable « tour de babel électronique »)

12 PROCÉDER À UNE ÉVALUATION DES AUTORITÉS DE CERTIFICATION « AC » SELON UNE APPROCHE COMPARATIVE ET EN UTILISANT DES CRITÈRES PRÉCIS

   (ceci afin de tenir compte des niveaux réels de menaces et de risques et des besoins propres à l'organisation)

DOCUMENT DE RÉFLEXION SUR LES ENJEUX, PRINCIPES DIRECTEURS & ORIENTATIONS GOUVERNEMENTALES

Document produit par :
le Sous-secrétariat à l'inforoute et aux ressources informationnelles

Ce document a été rédigé par :
MM. Michel Després & Yvan Lauzon
Secrétariat du Conseil du trésor
Sous-secrétariat aux marchés publics et aux technologies de l'information
Sous-secrétariat à l'inforoute et aux ressources informationnelles

Avec l'aide des membres du Comité aviseur interministériel :
Claude Francoeur
Société de l'assurance automobile du Québec

Me François Lajeunesse
Secrétariat de l'autoroute de l'information

Ross Lamarre
Ministère du Revenu du Québec

Me Michel Léonard
Ministère de la Justice du Québec

Me André Lord
Ministère du Revenu du Québec

Michel Marchand
Régie de l'assurance maladie du Québec

Raynald Perron
Secrétariat du Conseil du trésor

Bernard Plante
Secrétariat du Conseil du trésor