AVIS DE PERTINENCE SUR LA SOLUTION INTÉRIMAIRE DE L'INFRASTRUCTURE À CLÉS PUBLIQUES GOUVERNEMENTALE DU SECRÉTARIAT DU CONSEIL DU TRÉSOR

Dossier 01 11 07

Août 2001

TABLE DES MATIÈRES

INTRODUCTION

Depuis quelques temps déjà, le passage de l'État couloir à l'État réseau prend forme. Ce désir s'est concrétisé dans diverses actions dont l'adoption de la *Loi sur l'administration publique* en mai 2000. Cette loi, comme nous le verrons plus à fond dans ce texte, enjoint le Conseil du trésor (CT) à offrir des infrastructures communes et à favoriser la mise en commun de ressources à ce qui est désigné comme l'administration gouvernementale. C'est dans ce contexte que le 27 mars 2001, le secrétaire du CT s'adressait à la Commission d'accès à l'information (Commission) afin d'obtenir son avis quant à la conformité d'un projet intérimaire d'une ICPG au regard des règles applicables en matière de protection des renseignements personnels. Précisons que l'avis de la Commission est requis par décision du CT du 27 février 2001.

E-IDENTITÉ ET TRANSACTIONS ÉLECTRONIQUES

Le Québec, comme plusieurs autres États, cherche à augmenter le degré de confiance de la population envers les réseaux électroniques dans le but précis de favoriser le développement du commerce électronique et de la prestation électronique de services gouvernementaux. Or, souvent, les réseaux offrent peu de garanties de sécurité et de confidentialité à leurs utilisateurs, d'où l'absence de confiance des citoyens à leur égard.

En effet, une étude de juin 1999 commandée par le Secrétariat du Conseil du trésor (SCT) portant sur la perception des Québécois dans un contexte de transactions et d'identification électroniques (Les Québécois face aux inforoutes, Sciencetech communications) illustre bien ce propos. Ce document explique qu'« *Internet est un réseau numérique où chaque clic laisse une trace; il est possible de savoir qui fait quoi* ». Les citoyens sont sensibles à ce type de faiblesse car l'étude nous apprend qu'« *un élément important de ce sondage est l'expression fortement affirmée par les deux tiers des internautes de pouvoir naviguer sur Internet de façon anonyme. Il peut y avoir dans cette volonté une préoccupation de respect de la vie privée et de protection contre les abus du télémarketing et autres formes de harcèlement électroniques* ». C'est sans compter que 60 % des internautes interrogés considèrent de façon générale leur vie privée plus à risque qu'il y a une dizaine d'années, que 58 % croient avoir assez d'informations pour savoir comment les nouvelles technologies peuvent affecter leur vie privée et que 71 % refusent de fournir des renseignements personnels sur Internet. Finalement, ce sont 92 % des personnes interrogées qui croient à l'importance de garanties pour protéger les renseignements personnels sur Internet.

Cette étude fait ressortir et confirme les attentes fondamentales des citoyens quant au respect de leur vie privée, même lorsqu'ils utilisent Internet. D'autre part, des entreprises et le gouvernement ont des besoins pressants à l'égard du développement du commerce électronique et de la prestation électronique de services. Mais, pour commercer, on veut « identifier ». Comme le souligne l'étude commandée par le SCT : « *L'identification d'une personne est à la base du*

commerce électronique. Dans un environnement virtuel où les interlocuteurs ne se voient pas, comment s'assurer que l'on contracte bien avec la personne qu'elle prétend être? À l'inverse, comment préserver l'anonymat? C'est un enjeu majeur. ».

Afin de permettre les transactions électroniques, le gouvernement du Québec veut se doter d'un mécanisme qu'il nomme ICPG. Ce type d'infrastructure est mis en place dans le but d'établir l'identité de personnes qui, ainsi connues, pourront transiger dans un environnement sécuritaire. La question de la e-identité est donc au coeur de l'implantation d'une telle mécanique.

M. Pierre Trudel du Centre de recherche en droit public de l'Université de Montréal (CRDP), dans un document intitulé « *Aspects juridiques des technologies de l'information, Avril 2001* » soutient que « *L'identification est une activité visant essentiellement à réduire ou gérer les risques inhérents à une transaction* ».

1- GÉNÉRALITÉS SUR LES ICP

Dans un contexte de réseaux électroniques, ceux qui désirent se reconnaître à distance, effectuer des transactions électroniques en sécurité et s'échanger de l'information sensible doivent recourir à des artifices comme l'ICP.

Une ICP est un mécanisme permettant d'associer avec un certain niveau d'assurance un document électronique à une personne physique. Elle permet par la gestion de clés et de certificats électroniques d'assurer l'intégrité, la confidentialité et l'authentification des échanges et l'irrévocabilité de l'attribution des documents à leurs auteurs.

Très sommairement, une ICP permet d'attribuer une clé de signature à une personne et une clé de chiffrement des informations. Lorsqu'une personne transige avec un détenteur de clés, il peut en vérifier l'existence et la validité auprès de l'entité qui a émis la clé.

QUE GARANTIT UNE ICP

- Garantie d'intégrité d'un document par le scellement de son contenu (technologie de l'empreinte numérique « hash fonction »);

- Garantie de provenance du document et garantie de contrôle d'accès au document par l'authentification de l'identité des personnes liées au document;

- Garantie de non-répudiation de l'information par un moyen d'attribution du document à une personne (technologie de signature numérique);

- Garantie de confidentialité de l'information par le chiffrement des données qui forment le contenu du document.

ICP ET RISQUES LIÉS À LA VIE PRIVÉE

L'ICP est un outil utilisable par quiconque choisit d'instaurer un service de distribution de passeports électroniques qui pourront être utilisés à des fins d'identification sur un réseau électronique. Ce passeport électronique, le certificat, est une structure mathématique qui assure la fiabilité de cette pièce d'identité électronique.

Les ICP traditionnelles permettent d'assurer la sécurité des transmissions, la confidentialité des informations lors d'une transmission et l'authentification de l'auteur d'un document dans un contexte de réseau ouvert et d'accès à distance. Si l'utilisation d'une ICP répond bien à des impératifs de sécurité, il ne faut pas conclure prématurément qu'elle suffit à assurer la protection de la vie privée, particulièrement celle des détenteurs de certificats. Sécurité et protection de la vie privée sont deux concepts différents.

Le respect de la protection des renseignements personnels et du droit à la vie privée déborde le simple concept de sécurisation des échanges. **L'utilisation d'ICP implique pour les individus et organisations une cueillette d'informations additionnelles et une surveillance de leurs actions.**

En effet, les certificats digitaux peuvent être suivis, tracés et aussi liés à d'autres informations détenues sur une personne de façon irréfutable. Il est dès lors possible de compiler de façon extrêmement précise des profils individuels en fonction de l'utilisation du certificat, par croisement de données ou par déduction mathématique et logique (situation financière, habitudes de vie, préférences, …). Ces risques sont inhérents à l'usage de cette technologie. Ce type de surveillance peut être exercé par toute partie à une transaction ou à une communication, mais aussi par des employés moins scrupuleux d'une de ces parties, des pirates, des agences d'espionnage, par toute organisation de certification électronique (certification croisée) et, en milieu de travail, par l'employeur.

Certes, l'instauration d'une ICP est une action vertueuse en soi, mais qu'il faut situer à la lumière de son environnement général; c'est seulement ainsi que nous pourrons juger de son innocuité ou de sa nocivité.

> *« The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable. »* — U.S. Privacy Protection Study Commission, 1977.

Des acteurs s'inquiètent de la pression que pourrait subir la population pour utiliser des outils de communication et de transactions dans le but de satisfaire des objectifs économiques et commerciaux, alors que ces systèmes, par leur fonctionnement même, peuvent devenir d'importants vecteurs de surveillance électronique.

> « *Unless drastic measures are taken, individuals will soon be forced to communicate and transact in what could be the most pervasive electronic surveillance system ever built.* » — Private Credentials, Dr Stefan Brand, 2000.

Les principaux risques liés à l'utilisation des certificats d'identité électroniques sont les suivants :

1- Le traçage (traceability) : Toutes les communications et transactions qu'effectue un individu peuvent être automatiquement tracées grâce à son certificat et lui sont attribuables, notamment lors de la vérification de la validité du certificat auprès de l'autorité de certification.

2- L'analyse de trafic : L'observation de l'information relative à une communication entre utilisateurs (i.e. absence/présence, fréquence, sens, séquence, type, volume, ..) est possible par quiconque « écoute » sur le réseau. Il est d'une relative facilité d'intercepter des renseignements sur les échanges. Des informations sur le certificat sont nécessairement communiquées d'un relais à l'autre durant la télé-communication. L'analyse de trafic est une des vulnérabilités inhérentes à la technologie de l'ICP et est documentée par l'Union internationale des télécommunications dans la norme internationale UIT-T X.509.

3- Les possibilités de couplage : Grâce aux certificats électroniques d'identité qu'un individu présente auprès des différents intervenants avec qui il transige ou communique, ceux-ci détiennent désormais un identifiant unique qui leur permet de coupler les informations qu'ils détiennent. La tendance qu'on peut observer actuellement consiste précisément à l'intégration des données pour des utilisations autres que les finalités initiales.

4- La non-répudiation : L'utilisation d'un certificat électronique rend non répudiable le geste posé. En conséquence, le détenteur du certificat est généralement responsable des utilisations non conformes faites avec cet outil. Le cas échéant, il devra démontrer qu'il a pris des mesures appropriées pour éviter la mauvaise utilisation de son certificat.

5- La discrimination et la perte de contrôle sur l'information : Un certificat peut contenir plusieurs renseignements personnels : nom, adresse, courriel, … La technologie de l'ICP exige, de par les normes qui la régissent, que cette information soit diffusée publiquement par l'entremise d'un répertoire. Ce fait implique une détention d'informations qui peuvent être consultées sans égard à la nécessité d'obtention de l'information, souvent sans limite de temps et sans contrôle sur les finalités initiales poursuivies. La conservation et la destruction des certificats périmés ou révoqués demeurent au choix du détenteur, soit l'autorité de certification. Certaines informations sont même conservées à perpétuité; à titre d'exemple, le Registre des Droits Personnels et Réels Mobiliers (RDPRM) conserve actuellement les clés et certificats sans limite de temps.

D'autre part, l'utilisation des certificats ouvre la porte à la particularisation des services offerts en fonction du contenu du certificat et/ou des profils d'utilisation d'un citoyen. Par exemple, une entreprise pourrait choisir d'offrir des services amoindris à une personne si elle détecte que celle-ci transige avec un concurrent ou en fonction de sa situation géographique.

6- L'usure des certificats : Plus un certificat est utilisé, plus il devient possible mathématiquement (par comparaison et déduction) de trouver les clés de signatures et de chiffrement de celui-ci.

7- La constitution nécessaire de fichiers d'identité accessibles sur les réseaux : La diffusion du répertoire de certificats implique l'obligation de rendre disponibles des renseignements personnels sur le détenteur d'un certificat en tout temps, à toute personne. Pourrait-on imaginer qu'on consigne une copie de notre passeport canadien qui serait disponible publiquement pour des fins de validation?

L'ICP traditionnelle est tributaire de l'existence de fichiers d'identification rendus publics. En principe, une autorité de certification ne détient de l'information que sur les personnes qu'elle certifie. Cependant, afin d'éviter la multiplication des certificats, deux ou plusieurs autorités peuvent s'entendre afin de reconnaître mutuellement les certificats de l'un et de l'autre; cette mécanique s'appelle la certification croisée et implique des échanges entre les acteurs. À long terme, la reconnaissance graduelle entre autorités de certification engendrera la constitution d'un véritable mégafichier planétaire d'identification sous la responsabilité d'un nombre limité d'acteurs privés et publics.

En conclusion, même si la technologie de l'ICP permet d'assurer par des mesures de sécurité la « valeur » d'un document électronique, celle-ci est toutefois beaucoup plus invasive pour la vie privée des utilisateurs qu'une pièce de papier équivalente. C'est pourquoi, il faut s'assurer que les choix technologiques et les dispositifs mis en place lors de l'implantation de l'ICPG minimisent les risques. C'est ce dont nous allons traiter dans les pages qui suivent en décrivant, dans un premier temps, la solution intérimaire de l'ICPG et son évolution vers une solution permanente. Dans un second temps, nous donnons une appréciation générale du projet d'ensemble puisqu'il s'imbrique à la solution intérimaire et, ensuite, une appréciation de la solution intérimaire proposée.

2- DESCRIPTION DE LA SOLUTION INTÉRIMAIRE DE L'ICPG

Le 29 juin 1999, la mise en place de l'ICPG était autorisée. Le Québec, à l'instar des autres États, veut augmenter le degré de confiance envers les réseaux pour favoriser le développement du commerce électronique et de la prestation électronique des services gouvernementaux.

L'objectif visé pour 2004 est de permettre l'utilisation d'un passeport d'identification de l'ICPG par l'ensemble des employés du gouvernement québécois dont les fonctions requièrent une interaction avec des données confidentielles ou la nécessité d'authentifier de leur identité ou celle de leurs interlocuteurs avec les clientèles disposant d'un passeport électronique équivalent.

Le CT entend débuter la dispensation de son service d'ICPG par une solution intérimaire qui pourra être utilisée par tous les employés de l'État et tous les employés des entreprises mandataires de l'État ou de ses clients. Les certificats d'identité délivrés à ces travailleurs leur serviront exclusivement dans l'exercice de leurs fonctions. La certification des autres entreprises et des citoyens est à l'étude et aucune solution ne nous a été soumise à ce jour.

La solution intérimaire présentée par le CT, c'est-à-dire celle qui sera utilisée jusqu'en octobre 2003, propose d'utiliser concurremment deux services de certification. Un premier service permettra aux employés de l'État d'obtenir des certificats d'identité auprès de la Direction générale des télécommunications (DGT) du Sous-secrétariat aux services gouvernementaux du SCT. La délivrance des clés et certificats aux fonctionnaires s'effectuera avec l'autorisation du supérieur immédiat de l'employé qui attestera de son identité. Les certificats délivrés seront de niveau 2. Le niveau d'un certificat est relié à divers facteurs comme la robustesse de l'algorithme de chiffrement employé, les processus d'émission et de remise des clés et la rigueur du processus d'identification d'une personne. Un second service de certification sera destiné aux employés des entreprises mandataires de l'État et aux fonctionnaires de qui on exigera un niveau de certification supérieur. Les certificats délivrés par ce second service seront de niveau 3. Afin de mettre en place ce service, le système actuellement en usage au MJQ pour les fins du RDPRM sera modifié pour permettre une certification élargie à cette nouvelle clientèle. Le MJQ administrerait ainsi un serveur accrédité de l'ICPG.

…VERS UNE SOLUTION PERMANENTE

Une solution permanente de l'ICPG est en voie de définition par le CT et offrira, à la date prévue du 7 octobre 2003, un service intégré de certification des employés de l'État et de ses mandataires en partenariat avec le SCT et le MJQ. Cette solution sera détaillée aux plans administratif, juridique et technologique et une étude des impacts sur les ressources humaines, matérielles, financières et informationnelles sera produite. On sait d'ores et déjà que, dans cette solution permanente de l'ICPG, le MJQ deviendra l'unique gestionnaire des clés et certificats et que la DGT se verra confier le rôle de gestionnaire des infrastructures opérationnelles.

La solution permanente devra être soumise pour approbation au CT au plus tard le 31 janvier 2002. Il faut souligner que le CT réfléchit présentement à une solution de certification d'identité destinée aux citoyens et aux entreprises. Dans ce cas, nous ne connaissons pas le degré d'avancement des travaux et l'arrimage avec l'ICPG.

2.1 LE STATUT JURIDIQUE DE L'ICPG

Le CT a le mandat de fournir aux ministères et organismes (M/O) de l'État les services communs gouvernementaux dont ils peuvent bénéficier, notamment des services informatiques et de télécommunications.

> « ***3****. Le ministre peut, en application du paragraphe 2 de l'article 2, fournir aux ministères, aux organismes publics dont le budget de fonctionnement est voté en tout ou en partie par l'Assemblée nationale et à tout autre organisme désigné par le gouvernement, des services notamment dans les secteurs suivants : acquisition de biens et services, reprographie, transport aérien dans le cadre de fonctions ou de missions gouvernementales, courrier et messagerie, fournitures et ameublement, informatique, entretien des équipements bureautiques, télécommunication, édition, publication, diffusion et commercialisation de documents, placement média, audiovisuel, publicité et expositions. Ces services peuvent être fournis à titre onéreux.* ». — *Loi sur les services gouvernementaux aux ministères et organismes publics* (L.R.Q. c. S-6.1).

De plus, la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale* attribue au CT le rôle de déterminer « *les infrastructures communes de sécurité à mettre en place dans l'administration gouvernementale, leurs composantes et les procédures et règles de gestion associées ainsi que les cas où leur utilisation est obligatoire en tout ou en partie* ».

La *Loi sur l'administration publique* (Projet de loi no 82 (2000, chapitre 8), adopté le 25 mai 2000, sanctionné le 30 mai 2000. — Les articles 24 à 27 seront en vigueur le 1er avril 2002) confie au CT le mandat de définir des règles pour assurer la sécurité des ressources informationnelles et prévoir des mesures pour permettre la mise en commun d'infrastructure ou de services et en déterminer les modalités de gestion.

> « ***64****. Le présent chapitre s'applique à l'Administration gouvernementale à l'exception des organismes autres que budgétaires dont le personnel n'est pas nommé suivant la Loi sur la fonction publique.*

> ***65**. Les ressources informationnelles de l'Administration gouvernementale sont gérées de façon à :*
> 1. *utiliser de façon optimale les possibilités des technologies de l'information et des communications comme moyen de gestion des ressources humaines, budgétaires et matérielles;*
> 2. *contribuer à l'atteinte des objectifs d'accessibilité et de simplification des services aux citoyens;*
> 3. *favoriser la concertation entre les ministères et organismes et le partage de leur expertise et de leurs ressources.*
>
> ***66**. Le Conseil du trésor peut, en matière de ressources informationnelles :*
> 1. *adopter des règles pour assurer la sécurité des ressources informationnelles, y compris la protection des renseignements personnels et des autres renseignements qui ont un caractère confidentiel;*
> 2. *prévoir des mesures pour assurer la cohérence gouvernementale, pour permettre la mise en commun d'infrastructures ou de services et en déterminer les modalités de gestion;*
> 3. *déterminer, après consultation des ministères et des organismes, les cas où un projet de développement doit être soumis à certaines conditions ou modalités d'autorisation.*
>
> *Les ministères et organismes gèrent leurs ressources informationnelles conformément au présent article.*

Rappelons que la Commission, dans ses commentaires sur le projet de loi sur l'administration publique, a émis la réserve suivante :

> « *Par ailleurs, la Commission rappelle que ces deux dispositions législatives ne doivent en aucune façon mettre de côté l'un des principes fondamentaux de la Loi sur l'accès, soit le cloisonnement de chacun des organismes publics aux fins de la gestion des renseignements personnels.* » *— 99 20 19*

Le CT a donc la responsabilité de mettre en œuvre les infrastructures communes comme celle qui nous est soumise pour avis.

2.2 LES LIENS JURIDIQUES ENTRE LES ACTEURS

Le CT est le maître d'œuvre de l'ICPG et les services d'infrastructures communes de sécurité sont habituellement fournis par les Services gouvernementaux dont fait partie la DGT. À cet égard, la directive sur la sécurité énonce :

> « *Une infrastructure commune de sécurité déterminée par le Conseil du trésor est fournie par le Secrétariat du Conseil du trésor (Services gouvernementaux). Cependant, le Conseil du trésor peut mandater tout autre ministère ou organisme pour qu'il fournisse une infrastructure commune.* »

La solution intérimaire développée par le CT implique un partenariat entre la DGT, le MJQ, les sous-traitants et les AVI.

Les rôles qui seront assignés à chacun des acteurs dans la solution intérimaire sont les suivants :

- Gestion des encadrements administratifs et techniques (GEAT) : CT;
- Gestion des clés et certificats (GCC) niveau 2 : DGT;
- GCC niveau 3 : MJQ;
- Gestionnaire des infrastructures opérationnelles (GIO) : DGT et MJQ (firme LGS) pour leur partie respective;
- Gestionnaire des utilisations (GU) : ministères et organismes clients de l'ICPG.

Dans la solution permanente, le MJQ devient l'unique gestionnaire de clés et certificats et la DGT, l'unique gestionnaire des infrastructures opérationnelles.

Les documents qui nous sont soumis indiquent que la nouvelle mission confiée au MJQ nécessitera des modifications législatives (*Loi sur le ministère de la Justice* (L.R.Q. c. M-19)) et réglementaires, notamment pour reconnaître sa nouvelle mission de gestionnaire des clés et des certificats et pour permettre, s'il y a lieu, la facturation des services. Nous concluons des informations reçues que pour la solution intérimaire, le MJQ est un mandataire du CT et qu'une entente entre ces deux organismes devra être signée en vertu de l'article 67.2 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. c. A-2.1). La décision du CT du 27 février 2001 confirme cet état de fait en décrivant la subordination du MJQ au CT par un mécanisme de reddition des comptes semestriels des travaux et des investissements.

Dans la mise en œuvre de son serveur de certification de l'ICPG, le MJQ réutilise une partie de son système actuellement dédié au RDPRM. La gestion, l'exploitation et l'évolution du RDPRM sont actuellement assumées par la firme LGS, et ce, jusqu'en 2003. La réalisation de la solution intérimaire amène donc l'attribution d'un nouveau contrat sans appel d'offres à LGS afin d'assurer la réalisation de l'ICPG et l'opération technique, car cette entreprise détient *« la connaissance de l'ensemble des systèmes qu'il faut séparer et qui est propriétaire des droits de propriété intellectuelle sur ces système* ». —Décision du CT du 27 février 2001, 195936.

Notons aussi que dans le projet actuel, les données et les équipements informationnels (serveurs, bases de données, répertoires…) utilisés pour le RDPRM ne pourraient servir pour l'ICPG. Les données des deux systèmes ne pourraient être intégrées. À cet effet, un projet d'architecture technologique pour l'ICP du RDPRM

(version 1.2 — 31 mai 2001) nous informe que : « *La base de données pour les clients du GCC doit être isolée des services du RDPRM. Un serveur ainsi que des postes utilisateurs sont nécessaires afin de répondre aux besoins du GCC. Cette base de données contiendra plusieurs données sur des clients ne concernant pas la ligne d'affaire du RDPRM. L'application du GRC et l'application du GCC ne doivent pas être installées sur le même serveur dans le cadre du développement et de la production.* ».

Les AVI agissant dans le cadre de la partie du RDPRM de la solution intérimaire seront agréés par le CT. Il est prévu d'agréer en premier lieu les notaires actuellement accrédités par le RDPRM. Le CT pense aussi agréer d'autres AVI mais ne sait pas encore qui ils seront. Lorsque ceux-ci seront identifiés, ils devront être dûment mandatés par le CT (art. 67.2 de la Loi sur l'accès) afin d'assumer ce rôle. L'entente devra préciser toutes les questions relatives à la protection des renseignements personnels qui seront recueillis, détenus, utilisés, communiqués et détruits.

2.3 LES NIVEAUX DE CERTIFICATION ET LA CATÉGORISATION DE L'INFORMATION

Les services de certification peuvent émettre divers niveaux de certificats. Le niveau du certificat indique le degré d'assurance offert par le certificat, notamment quant à la rigueur des règles de vérification d'identité appliquées.

Les documents reçus du CT précisent que les niveaux de certification seront définis par la catégorisation de l'information : « *La mise en place de l'ICPG suppose la catégorisation de l'information en fonction du niveau de sécurité à assurer.* ». La catégorisation de l'information est un projet du CT dont nous ne sommes pas saisis pour l'instant.

2.4 LES MÉCANISMES DE VÉRIFICATION D'IDENTITÉ

Dans la solution intérimaire, la DGT offrira aux employés de l'État des certificats de niveau 2 puisque l'identité sera certifiée par le supérieur immédiat qui entérinera la réquisition de certificat de l'employé.

Le MJQ offrira aux employés des entreprises mandataires et à certains employés de l'État, non déterminés à ce jour, des certificats de niveau 3. On entend être plus rigoureux dans la vérification de l'identité pour les employés des entreprises privées et certaines catégories d'employés de l'État. Ces certificats seront délivrés après une vérification d'identité auprès d'un tiers, soit l'AVI autorisé par le CT. Une directive en rédaction par le CT viendra définir la procédure de vérification d'identité et les AVI seront aussi identifiés ultérieurement. Les AVI procéderont, pour le compte du CT, à la vérification de l'identité dans le cadre d'une rencontre physique, ils assureront la conservation de la preuve de vérification d'identité et ils assisteront à la signature de la réquisition de service à l'ICPG.

Les certificats émis dans le cadre du RDPRM sont de niveau 3. Les mécanismes fixés par le RDPRM exigent que les personnes autorisées à procéder aux inscriptions et aux modifications de celui-ci soient rencontrées personnellement par un notaire afin de vérifier l'identité de cette personne. La Chambre des notaires a une entente verbale avec le MJQ pour que des notaires effectuent la vérification d'identité; ce rôle leur est confié par le règlement sur le RDPRM. **Actuellement**, la vérification d'identité s'effectue suivant une procédure émise par le RDPRM du MJQ, soit :

- par la présentation de deux pièces d'identité acceptables à partir d'une liste dont une comporte une photo et une signature;

- la rédaction d'un procès-verbal de vérification d'identité qui précise quelles pièces le notaire a reçues.

Les notaires, sur la recommandation de la Chambre des notaires, photocopient les pièces produites afin de conserver la preuve de vérification d'identité. Ils assimilent leur action de vérification d'identité à un acte professionnel qui découle de leur fonction d'officier public.

2.5 L'ADHÉSION À L'ICPG ET LA RESPONSABILISATION DES ABONNÉS

Le CT n'a pas encore déterminé lequel des partenaires recevra les demandes d'adhésion des services de l'ICPG. Un comité d'orientation a été formé et devra trancher cette question.

La procédure d'adhésion **actuellement** utilisée par la DGT consiste à compléter une réquisition d'ICP (contenant les renseignements sur l'employé abonné, l'autorisation du gestionnaire et les coordonnées du gestionnaire certifiant l'identité) et à signer une déclaration du demandeur à qui on impose une série d'engagements.

Ces engagements concernent l'utilisation des clés et certificats aux seules fins permises par le M/O, le respect des politiques de certificats, la protection des jetons d'initialisation (numéro de référence et code d'autorisation), la protection des clés privées délivrées et du mot de passe permettant l'utilisation des clés et l'obligation d'aviser le certificateur en cas de compromission des clés. L'abonné autorise, dans cette même déclaration, la divulgation de renseignements personnels inscrits à la section *identification du demandeur* et accepte que le service de certification conserve une copie de sa clé privée de chiffrement. Les renseignements contenus à la section d'identification sont : le nom, le prénom, le ministère ou l'organisme, le nom de l'immeuble, l'adresse, le numéro de téléphone, le numéro de télécopieur et l'adresse de courriel. Certains de ces renseignements seront inscrits dans le certificat électronique.

Le projet de directive dont nous avons reçu copie fournit quelques éléments supplémentaires sur les responsabilités qui incomberont aux employés abonnés. L'abonné devra :

- garantir l'exactitude de l'information et la validité des documents fournis pour son identification personnelle ainsi que celle de l'organisme qu'il représente (8.1.1.4.1);

- assurer la sécurité et la confidentialité de sa clé privée et de ses codes d'accès (8.1.1.4.2);

- utiliser lui-même sa clé privée ainsi que le mot de passe y donnant accès et prendre les précautions raisonnables pour en empêcher la modification, l'utilisation non autorisée, la divulgation, la perte ou le vol; si une clé privée est conservée chiffrée sur une disquette ou un autre support facilement transportable, ce support doit être conservé dans un lieu à accès contrôlé, lorsque non utilisé (5.2.1).

Au moment de la vérification d'identité, il est prévu qu'un « secret partagé » soit convenu afin de permettre la réémission, au besoin, des certificats et clés de signature sans procéder à nouveau à la vérification d'identité. Le secret partagé est connu du GCC, de l'abonné et, dans le cas du RDPRM, de l'AVI.

2.6 LE FONCTIONNEMENT DE L'ICPG

Le CT finalise actuellement une directive sur la gestion des clés et certificats qui viendra établir les modalités de fonctionnement de l'ICPG. Seront précisés dans cette directive notamment les éléments suivants :

- la procédure d'adhésion et de vérification d'identité;
- la procédure de génération, de délivrance, de renouvellement, de récupération et de révocation des clés et certificats;
- la protection des clés privées;
- la forme et le contenu des certificats et liste de certificats révoqués;
- les modalités de conservation et la détention physique;
- la validation des certificats;
- les communications de renseignements personnels générées par le processus;
- les mesures de sécurité physique, administratives et opérationnelles;
- l'encadrement et les mesures de sécurité du personnel exploitant l'ICPG;
- les procédures de vérification de la sécurité informatique;
- l'archivage des données;
- la cessation des opérations d'un GCC;
- les sanctions des actes non autorisés ou négligents;
- l'impartition des activités de l'ICPG.

2.7 L'UTILISATION DE L'ICPG

L'ICPG est une infrastructure commune qui permettra aux M/O de requérir des certificats d'identité électroniques pour leurs employés. En théorie, les M/O détermineront dans quelles circonstances et pour quelles applications les certificats

d'identité seront requis pour leur personnel. En pratique, cette modalité serait restreinte par une décision gouvernementale obligeant l'utilisation d'une infrastructure commune pour des circonstances données, notamment par l'obligation d'utiliser cette infrastructure en fonction de la catégorisation de l'information.

> « *L'ICPG servira pour garantir l'intégrité, l'authentification, la confidentialité, la non-répudiation et la signature électronique. Les applications qui bénéficieront en premier de l'ICPG sont la sécurisation du courriel électronique, des portables, des postes de travail, des communications avec les serveurs web, l'accès aux intranets et les circuits virtuels privés (VPN) sur l'Internet.* ». — DGT, 18 mai 2001.

Quant à la partie RDPRM de la solution intérimaire, il semble qu'on veuille mettre en place une ICP prioritairement pour les besoins de la Société de l'assurance automobile du Québec impliquant les concessionnaires automobiles (Architecture de système du GCC, MJQ, 4 juin 2001). D'autres ministères et organismes pourront faire appel à ce service de certification.

3- APPRÉCIATION DE LA SOLUTION PROPOSÉE

La description de la solution intérimaire nous force à constater que plusieurs éléments importants concernant les dispositifs pour la mise en place de cette solution restent à établir.

Il en est ainsi :

- de la finalisation de la directive sur la gestion des clés et des certificats ainsi que des politiques afférentes à l'infrastructure;
- d'une procédure de vérification d'identité;
- de la détermination définitive des AVI;
- de la détermination des employés de l'État (nombre et types) qui seront visés;
- de la détermination des responsabilités qui incombent aux employés visés.

Le SCT doit comprendre dans ce contexte que l'avis qu'il sollicite de la Commission sur la mise en place d'une solution intérimaire de l'ICPG est fait sous réserve de la prise de connaissance de l'ensemble des éléments nécessaires à la mise en place de cette infrastructure.

Le présent avis porte sur la pertinence de mettre en place la solution intérimaire telle que décrite dans les documents fournis par le CT. Aucune appréciation en matière de sécurité et de fiabilité n'a été portée sur la technologie utilisée, soit celle de l'entreprise Entrust. Le système en place pour l'administration du RDPRM n'a pas non plus été examiné.

Une première appréciation portera sur le projet d'ICPG du CT, une seconde appréciation portera sur les choix d'implantation de la solution intérimaire.

Toutefois, il nous apparaît important à cette étape de consultation de la Commission sur le projet de l'ICPG de faire état d'une préoccupation générale de la Commission qui a trait au choix du ou des gestionnaires des certificats d'identité, tant à l'égard de la solution temporaire que de la solution permanente.

La solution intérimaire vise principalement la certification des fonctionnaires. Dans la solution permanente, le MJQ sera l'unique gestionnaire des certificats d'identité de ces fonctionnaires. Celui-ci détiendra donc physiquement un fichier centralisé de renseignements personnels des employés de l'État. Ce fichier de renseignements personnels n'est pas nécessaire à l'accomplissement de la mission du MJQ.

Il en résulte une dissémination et une circulation de renseignements personnels qui apparaissent inutiles. C'est pourquoi nous invitons le CT à ce stade-ci à bien évaluer les risques pour la protection des renseignements personnels dans la détermination des partenariats lorsqu'il en découle une détention par une entité autre que celle qui gère de tels renseignements.

En effet, la centralisation des certificats et la constitution sous-jacente de mégafichiers représentent des risques très importants à la vie privée, lesquels doivent être évalués dans la mise en place d'une ICP.

3.1 APPRÉCIATION DU PROJET D'ICPG

LES UTILISATIONS DES CERTIFICATS D'IDENTITÉ DES EMPLOYÉS DE L'ÉTAT

Les certificats d'identité délivrés aux employés de l'État seront utilisés exclusivement par ceux-ci dans l'exercice de leurs fonctions. Ces certificats serviront à apposer leur signature numérique sur des documents électroniques.

Les employés de l'État qui agissent dans le cadre de leur travail n'engagent pas leur responsabilité individuelle dans les tâches qu'ils exercent pour leur employeur. Par contre, la signature d'un fonctionnaire est parfois requise, par exemple, lorsqu'il pose un acte juridique qui engage la responsabilité du ministre. Ces actes juridiques reproduits dans un monde électronique pourront vraisemblablement être signés électroniquement.

> « *[…] il faut garder à l'esprit que toutes les lois constitutives des ministères prévoient que tous les actes, documents ou écrits doivent être signés par le ministre, ou par d'autres personnes déterminées, afin d'être attribuables au ministre et d'engager le ministère.* » — Rapport final de recherches Sylvie Veillette pour le compte du Conseil du trésor — 31 mars 2000 — Souligné par les auteurs.

Les plans gouvernementaux de délégation des signatures déterminent précisément la fonction des personnes autorisées à engager le M/O par leur signature.

Utilisation des certificats pour des fins de la signature

L'ICPG propose d'émettre des certificats d'identité aux employés de l'État dont les fonctions impliquent une interaction avec des données confidentielles **ou** la nécessité d'authentifier leur identité aux fins d'apposer une signature électronique. Rappelons que l'ICPG attribuera des certificats d'identité et qu'habituellement une pièce d'identité n'est exigée que pour des fins d'identification et non de sécurisation.

Recommandation 1- Nous recommandons que les utilisations des certificats d'identité soient restreintes aux strictes circonstances où l'employé doit décliner son identité **et** apposer légalement sa signature.

Il nous semble que des choix moins invasifs de la vie privée doivent être offerts lorsqu'il s'agit par exemple d'échanger de façon sécurisée et confidentielle des courriels ou des documents sans qu'une signature ne soit essentielle. La nécessité

dans ces cas de la signature et par le fait même d'une identification poussée des personnes ne nous a pas été démontrée.

M. Pierre Trudel du CRDP rappelle qu'« *En matière de protection de renseignements personnels, le principe de retenue (limitation en matière de collecte) vient guider les gestionnaires confrontés au défi d'assurer un équilibre entre les besoins de certitude, de sécurité et les obligations d'assurer le respect de la vie privée des personnes. En partant du principe suivant lequel on ne doit recueillir que les informations dont on est en mesure de démontrer la nécessité, compte tenu de la transaction considérée, on s'assure que les informations personnelles ne seront collectées que pour une fin clairement identifiable et limitée.* ».

Type de certificat et sécurisation des transmissions

En outre, nous croyons que d'autres types de certificats pourraient être octroyés pour des fins de sécurisation. Plutôt que de voir le nom d'une personne associé de façon indélébile à tous les gestes posés dans le cadre de ses fonctions, l'utilisation par un employé de l'État d'un certificat de ministère ou d'organisme permettrait de sécuriser les échanges et de réduire la circulation inutile de renseignements personnels sur les réseaux.

> « ***47.*** *Un certificat peut servir à établir un ou plusieurs faits dont la confirmation de l'identité d'une personne, de l'identification d'une société, d'une association ou de l'État, de l'exactitude d'un identifiant d'un document ou d'un autre objet, de l'existence de certains attributs d'une personne, d'un document ou d'un autre objet ou encore du lien entre eux et un dispositif d'identification ou de localisation tangible ou logique…* ». — *Loi concernant le cadre juridique des technologies de l'information*, Projet de loi no 161 (2001, chapitre 32), adopté le 21 juin 200, sanctionné le 21 juin 2001, non en vigueur. — Souligné par les auteurs.

Recommandation 2- Nous recommandons au Conseil du trésor d'examiner la pertinence de l'octroi de certificats à un ministère ou à un organisme et au titulaire d'une fonction plutôt qu'à un individu.

Choix technologique

Dans le développement de l'ICPG comme dans celui de tous les projets gouvernementaux, le choix d'une technologie est déterminant, car celle-ci peut conditionner la capacité de protéger la vie privée des individus, la visibilité et la circulation des renseignements personnels sur les réseaux tout en assurant la sécurité des échanges et la signature des documents.

Recommandation 3- Nous recommandons au Conseil du trésor de rechercher des technologies qui permettent de réduire, voire d'éliminer la visibilité et la circulation des renseignements personnels sur les réseaux tout en assurant la sécurité des échanges et la signature des documents.

Risques associés au type de technologie

Par ailleurs, comme le type de technologie utilisée dans l'ICPG présente des risques inhérents en matière de protection de la vie privée, nous souhaitons que les adhérents à ce service soient informés des risques de l'utilisation de l'ICPG et des conséquences découlant des engagements qu'ils signent.

Recommandation 4 - Nous recommandons que les adhérents à l'ICPG soient informés des risques inhérents à l'utilisation de l'ICPG.

Utilisation en milieu de travail

Nous apportons une dernière distinction quant aux signatures et l'exercice du droit à la vie privée en milieu de travail. Lorsqu'un fonctionnaire appose sa signature sur un document en vertu d'un plan de délégation et qu'il engage ainsi son M/O, il agit dans l'exercice de ses fonctions et sa signature prend un caractère public. Par contre, lorsqu'un fonctionnaire appose sa signature dans l'administration de ses conditions de travail, par exemple, pour soumettre un permis d'absence, la situation est différente. L'utilisation d'une technologie ne devrait pas être imposée lorsqu'un fonctionnaire agit dans sa zone de vie privée au travail. Rappelons que le besoin de s'identifier s'accompagne habituellement du libre choix du moyen d'identification utilisé. L'utilisateur doit avoir le choix des moyens technologiques qu'il estime suffisamment sûrs pour assurer la protection de sa vie privée. Comme le prévoit la *Loi concernant le cadre juridique des technologies de l'information* (Projet de loi no 161 (2001, chapitre 32), non en vigueur.), nous estimons qu'un choix doit être offert aux employés dans l'apposition de leur signature dans leur zone de vie privée au travail.

> « ***29****. Nul ne peut exiger de quelqu'un qu'il se procure un support ou une technologie spécifique pour transmettre ou recevoir un document, à moins que cela ne soit expressément prévu par la loi ou par une convention.*
> *De même, nul n'est tenu d'accepter de recevoir un document sur un autre support que le papier ou au moyen d'une technologie dont il ne dispose pas.*
> *Lorsque quelqu'un demande d'obtenir un produit, un service ou de l'information au sujet de l'un d'eux et que celui-ci est*

> *disponible sur plusieurs supports, le choix du support lui appartient.* »

Le projet de *Directive sur la gestion des clés et des certificats au gouvernement du Québec* (version 4.0, 1er juin 2001, 48 pages) prévoit pour l'activation des clés privées la possibilité d'utiliser des données biométriques. À ce sujet, qu'il s'agisse de fonctionnaires ou non, la *Loi concernant le cadre juridique des technologies de l'information* (Projet de loi no 161 (2001, chapitre 32), non en vigueur.), édicte que :

> « ***43.*** *Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques…* ».

Recommandation 5 - Nous recommandons au Conseil du trésor de mettre en place les dispositifs nécessaires pour permettre aux employés d'exercer un choix dans l'apposition de leur signature pour des activités personnelles reliées à l'exercice de leur fonction (zone de vie privée au travail).

LA CONSTITUTION D'UN FICHIER D'IDENTITÉ DES DÉTENTEURS DE CERTIFICATS

La mise en place de l'ICPG implique la création et la publication d'un fichier central des certificats d'identité de tous ses adhérents de même qu'un fichier des certificats révoqués.

L'article 57 de la Loi sur l'accès consacre un caractère public à certains renseignements d'identité des fonctionnaires à des fins de transparence de l'administration de l'État. Nous constatons que certains des renseignements qui seront diffusés dans le répertoire de l'ICPG ont donc un caractère public. D'autres peuvent soulever des doutes quant à savoir si des modifications législatives devraient être apportées.

Rappelons qu'un des risques des modèles d'ICP est la diffusion obligatoire du bottin de certificats et sa conservation à durée indéfinie. De la transparence de l'administration gouvernementale à la diffusion grand public planétaire d'un répertoire des fonctionnaires détenteurs de certificats, nous avons quelques réserves sur le respect des finalités.

Recommandation 6 - Nous recommandons au Conseil du trésor de prendre les moyens nécessaires pour éviter une diffusion inappropriée des répertoires de l'ICPG.

LA CUEILLETTE DE RENSEIGNEMENTS PERSONNELS, LA CONSTITUTION DE PROFILS ET LA SURVEILLANCE

Des risques identifiés des ICP, nous avons soulevé le fait qu'elles peuvent permettre de suivre l'utilisation des certificats et ainsi de recueillir de l'information sur le comportement de leurs détenteurs (qui sont les interlocuteurs, la fréquence (heure et date), le volume, …). Nous croyons que dans l'établissement des dispositifs de mise en place de l'ICPG, le CT devrait prendre des mesures pour les minimiser.

Recommandation 7 - Nous recommandons au Conseil du trésor de :

- délimiter les utilisations des renseignements contenus aux certificats et les modalités de conservation et de destruction;
- ne recueillir aucune information relative à l'utilisation des certificats et clés[1];
- ne dresser aucun profil ou n'effectuer aucune analyse de comportement à partir des informations nécessaires à la gestion de cette infrastructure;
- ne pas ajouter aux risques inhérents à l'ICPG en créant de nouveaux attributs du système[2].

[1] D'ailleurs, ces informations ne sont pas recueillies par la DGT actuellement.

Ces engagements devraient être pris par tous les partenaires de l'ICPG.

Rappelons aussi que dans le respect du cloisonnement des M/O, les renseignements relatifs à l'utilisation des certificats d'un M/O ne pourraient être intégrés et utilisés de façon globale par l'ICPG. Enfin, nous croyons que la cueillette d'informations à des fins de contrôle administratif du travail de l'employé ne devrait, le cas échéant, qu'être exercée par le M/O et non centralement.

LE CONSENTEMENT DE L'EMPLOYÉ

Les certificats d'identité constituent des outils de travail pour les employés de l'État visés. L'octroi de certificats pourrait devenir obligatoire en fonction des tâches qui seront assignées à quelqu'un.

La nécessité d'un consentement aux fins de diffusion du contenu du certificat d'un fonctionnaire trouve son sens dans la finalité et dans l'échelle de diffusion, puisqu'il est question de renseignements à caractère public. Notons que, pour cette problématique, il y a une analogie à faire avec les rôles d'évaluation qui sont des renseignements à caractère public, mais dont la diffusion pour toutes fins ne pourrait être acceptable.

LES RESPONSABILITÉS DES ABONNÉS

Une série de responsabilités est imposée aux abonnés lors de la demande d'obtention d'un certificat quant à l'utilisation de sa signature, aux mesures de sécurité à prendre pour éviter la mauvaise utilisation et à la non-répudiation des actes qui seront signés avec ce certificat. Par exemple, le projet de demande d'abonnement à l'ICPG stipule à la *rubrique Respect des politiques de certificats* que : « *Le ministère ou l'organisme auquel je suis rattaché m'a informé de mes droits et de mes obligations découlant des directives sur la gestion des clés et de certificats au gouvernement du Québec, et je m'engage à les respecter.* Du même souffle, le projet de Politiques de certificats (V0.12 Mars 2001, 61 pages) présente, entre autres, les exigences suivantes :

« *8.1.1.4.1 Représentations L'abonné ou son représentant doit garantir l'exactitude de l'information et la validité des documents qu'il fournit au responsable de l'AC ou à ses représentants tant pour son identification personnelle que celle de l'organisme qu'il représente s'il y a lieu.*

---

[2] Par exemple, déterminer au préalable les intervenants qui pourront valider un certificat équivaudrait à dresser une liste des correspondants d'un employé... (v. p 18/99 Architecture fonctionnelle).

8.1.1.4.2 Protection de la clé privée et des codes d'accès de l'abonné L'abonné ou son représentant doit assurer la sécurité et la confidentialité de sa clé privée et de ses codes d'accès telle que décrite à la sous-section 5.2.

8.1.2 Responsabilités L'AC, le personnel de l'AC, les abonnés, les utilisateurs et les mandataires d'organismes sont responsables pour tous dommages et intérêts découlant du non-respect de leurs obligations respectives telles que prévues par la présente politique de certificats. »

Dans le cadre de l'ICPG, la conservation des clés et mot de passe est confiée à l'utilisateur et c'est cette protection qui garantit l'utilisation appropriée de la signature électronique. L'utilisateur s'engage à protéger ses clés privées, à protéger le mot de passe qui permet d'y accéder et « *à prendre toutes les dispositions nécessaires pour prévenir leur perte, leur divulgation, leur modification et empêcher qu'elles soient utilisées par toute autre personne* ». Il se voit donc imposer des « dispositions nécessaires » pour assurer la protection de ses outils de travail.

Recommandation 8 - Concernant les engagements reliés à la « sécurité », nous demandons au Conseil du trésor ainsi qu'aux ministères et organismes de fournir aux détenteurs de certificats un environnement de travail qui leur permet de respecter ces engagements.

LA CATÉGORISATION DE L'INFORMATION

Le CT fera, dans un avenir prochain, la promotion de la catégorisation de l'information. Cette catégorisation guidera les niveaux de certifications requis pour les communications de renseignements personnels. Ce projet permettrait d'harmoniser l'approche envers l'information avec celle ayant cours au gouvernement fédéral. Aucun document ne nous a été fourni concernant ce nouveau concept de catégorisation de l'information.

Recommandation 9 - Nous demandons que la Commission soit consultée sur le projet de catégorisation de l'information.

Nous questionnons la pertinence de baser les niveaux de certification sur la catégorisation de l'information. La Loi sur l'accès ne tient pas compte du degré de sensibilité des renseignements personnels. La catégorisation des renseignements en fonction de leur nature pourrait induire une banalisation non souhaitée de certains types de renseignements et ainsi offrir à ces renseignements une protection inadéquate. La confidentialité des renseignements personnels et les possibilités de communications de renseignements ne sont pas reliées à la nature de l'information elle-même, mais à un ensemble beaucoup plus complexe de règles.

> « *Il est insuffisant de mettre en place des mesures de sécurité si l'on ne prend pas la peine d'identifier les risques de se retrouver en contravention des lois.* » — *Pierre Trudel, CRDP, allocution Aspects juridiques des technologies de l'information, avril 2001.*

3.2 APPRÉCIATION DE LA SOLUTION INTÉRIMAIRE DE L'ICPG

LES LIENS JURIDIQUES ENTRE LES ACTEURS

Afin d'assurer le respect de la Loi sur l'accès en matière de gestion des renseignements personnels, le CT devra dûment mandater les partenaires du projet, les AVI et le MJQ pour assurer leur contribution au service d'ICPG.

Le CT étant le maître d'œuvre de l'ICPG, les fichiers issus de l'administration de l'ICPG sont détenus juridiquement par celui-ci. Le CT devra produire à la Commission les déclarations de fichiers de renseignements personnels nécessaires à l'administration de l'ICPG (les clés, certificats, les bottins de clés publiques, liste de révocation, les dossiers clients, les dossiers de vérification d'identité…).

Recommandation 10 - Nous demandons au Conseil du trésor de rédiger et de faire signer les ententes à intervenir entre les partenaires de l'ICPG avant sa mise en service afin de respecter la Loi sur l'accès.

L'ADHÉSION DES ENTREPRISES PRIVÉES À L'ICPG

La solution intérimaire prévoit l'adhésion des employés des mandataires de l'État et de ses clients à l'ICP gouvernemental. Les clients des mandataires n'ont pas été identifiés.

Recommandation 11 - Nous demandons au Conseil du trésor de démontrer à la Commission les assises légales qui lui permettent de colliger les données sur les mandataires d'autres entités gouvernementales et aux entreprises privées.

Les liens juridiques établis plus tôt démontrent bien l'assise légale permettant au CT d'offrir des services communs gouvernementaux aux M/O; il en est autrement pour les mandataires de l'État et les entreprises privées.

Il ne nous a pas été démontré sur quelle assise légale ni précisé dans quel contexte des entreprises privées peuvent utiliser des services gouvernementaux offerts par le CT. Rappelons qu'un principe fondamental de la Loi sur l'accès est de restreindre la cueillette de renseignements personnels et la constitution de fichiers de renseignements personnels aux seuls renseignements indispensables à la réalisation de la mission de l'organisme. Aussi, on ne nous a pas démontré, de par la mission du CT, en vertu de quelles dispositions il pouvait constituer un fichier de renseignements personnels sur les employés d'entreprises privées mandataires de l'État. Ces renseignements n'ont pas par ailleurs de caractère public. En référence à l'article 57 de la Loi sur l'accès, les employés des mandataires ne peuvent en aucun cas être considérés comme des membres du personnel d'un organisme public ou

comme des personnes qui bénéficient d'un avantage économique conféré par un organisme public.

L'IMPARTITION DU VOLET MJQ

La DGT est un fournisseur naturel de services de certification et on peut lire dans la décision du 29 juin 1999 (CT), annexe 4 :

> « *La fonction de certification des employés et dispositifs du gouvernement est confiée en priorité au Secrétariat du Conseil du Trésor (Services gouvernementaux), mais pourra, dans les cas où cela est justifié, être exercée par un autre responsable approuvé.* ».

Les justifications ayant mené au choix du MJQ comme gestionnaire des clés et certificats de façon permanente et de gestionnaire des infrastructures opérationnelles pour la période intérimaire semblent être des considérations financières et de récupération d'expertise.

Ce choix a comme impact, sur la protection des renseignements personnels, d'augmenter inutilement la circulation des renseignements personnels requis pour l'administration de l'ICPG.

Le choix du MJQ comme partenaire implique aussi un risque supplémentaire quant aux renseignements personnels puisque ceux-ci seront exploités par la firme LGS en exclusivité jusqu'en octobre 2003, date où le transfert des connaissances devrait permettre à des fonctionnaires d'assumer l'exploitation de l'infrastructure. Comme LGS détient l'expertise entière du RDPRM, un contrat sans appel d'offres devra lui être octroyé afin de mettre en œuvre la solution intérimaire de l'ICPG. Cette impartition dans la gestion des renseignements personnels nous inquiète particulièrement puisque ces renseignements personnels seront gérés et exploités par une firme privée dont l'État est captif.

Recommandation 12 - Nous demandons au Conseil du trésor de soumettre à la Commission le contrat à convenir avec LGS afin de constater comment l'État veillera de façon effective à la protection des renseignements personnels qu'il détient, comment il assurera le transfert d'expertise aux employés de l'État et quelles mesures de sécurité, de confidentialité et de discrétion sont exigées de la firme de sous-traitants.

LE CHOIX DES AVI ET LA VÉRIFICATION D'IDENTITÉ

Le choix des AVI autorisés par le CT ne nous a pas encore été soumis. Le CT devra nous démontrer que le recours éventuel à ce nouveau type de sous-traitance

respecte les principes de protection effective des renseignements personnels qui seront recueillis, conservés, communiqués, utilisés et détruits.

Recommandation 13 - Nous demandons au Conseil du trésor de prendre les dispositions afin qu'il n'y ait aucune prise de copie des pièces d'identité présentées aux AVI de même qu'aucune cueillette des informations contenues sur ces pièces.

De plus, la nécessité de l'identification par des tiers imposée à des employés d'entreprises privées ne nous a pas été démontrée. Comme l'entreprise engage sa responsabilité dans l'utilisation des certificats produits, nous questionnons la nécessité de s'identifier auprès d'un tiers. Si elles s'avéraient justifiées, ces exigences d'identification ne devraient pas imposer une rigueur plus grande qu'à l'embauche ou avoir pour effet de rehausser ces exigences à l'embauche.

En outre, la nécessité d'identification des employés de l'État par des tiers (niveau 3) serait sans réel besoin. Elle serait utilisée simplement parce qu'il n'y a pas de certification croisée entre la DGT et le RDPRM.

Recommandation 14 - Nous demandons au Conseil du trésor de démontrer à la Commission la nécessité d'identification par des tiers d'employés d'entreprises privées et d'employés de l'État.

LES MODALITÉS DE GESTION DE L'ICPG

Les modalités de mise en oeuvre n'ont pas été examinées puisque le projet de directive sur la gestion des clés et des certificats est encore en évolution.

Recommandation 15 - La Commission demande au Conseil du trésor de lui soumettre cette directive pour appréciation lorsqu'elle sera finalisée de même que tout autre document pertinent (politiques…).

L'examen de ces documents nous permettra alors de vérifier l'à-propos des différentes procédures prévues dans la gestion de l'infrastructure; à titre d'exemple, citons la vérification d'antécédents judiciaires des employés de l'autorité de certification.

CONCLUSION

La communication de renseignements personnels et la vérification d'identité est nécessaire et légitime dans de multiples circonstances. Dans un monde électronique, tous conviendront que ces actes demeurent aussi nécessaires et légitimes. Nous croyons toutefois que le contexte électronique ne doit pas devenir un prétexte pour recueillir des renseignements personnels ou d'identité qui ne sont

pas indispensables aux actes posés, mais simplement pour combler des lacunes de sécurité inhérentes aux outils utilisés.

Direction de l'analyse et de l'évaluation