La certification électronique comme mécanisme de confirmation d'identité (l'infrastructure à clés publiques gouvernementale)

Michel Cloutier*

Introduction

Une infrastructure à clés publiques (ICP) est un ensemble d'acteurs, de pratiques et de technologies dédié à la gestion de clés et certificats de chiffrement (passeport et visas électroniques) pour permettre à des personnes et à des dispositifs:

- de se reconnaître à distance;
- d'effectuer, en toute sécurité, des transactions électroniques;
- d'échanger de l'information de nature délicate.

Cette définition tend à s'imposer comme le standard pour décrire le concept dont traite le présent document. Elle met en lumière que la technologie n'est qu'une partie de l'ICP

> *The PKI is not only software or hardware. It is an infrastructure, that is, a combination of products, services, facilities, policies, procedures, agreements, and people that provides for and sustains secure interactions on open networks such as the Internet.*[1]

---

* LL.M. Coordonnateur gouvernemental de l'ICPQ.

1. Federal Public Key Infrastructure Steering Committee, Access With Trust, US Office of Management and Budget, 1998 (www.gits.gov), p. 5.

On peut dire également qu'une infrastructure à clés publiques comprend une clientèle, une structure organisationnelle, des processus administratifs, un encadrement juridique et une technologie. Elle se situe au confluent du droit, de l'économie, de l'administration et de la technologie. Dans la mise en place d'une infrastructure à clés publiques, il est généralement reconnu que les aspects technologiques ne représentent qu'une petite partie des efforts à consentir.

Le présent document présentera d'abord le contexte dans lequel se développent les ICP, décrira les processus à la base de son fonctionnement et présentera les orientations adoptées par le Conseil du trésor le 29 juin 1999.

Le contexte

La confiance: élément central du développement des échanges électroniques

Le développement de l'autoroute de l'information invite les organisations, tant privées que publiques, à rechercher de nouvelles façons de faire des affaires et de rendre des services à leurs clientèles. Elles trouvent de plus en plus dans le commerce électronique et la prestation électronique de services des moyens de mieux servir ces clientèles tout en améliorant l'efficacité de leurs propres processus de travail. Cette évolution se traduit par une augmentation importante du volume d'affaires sur les inforoutes. En 1997, l'ensemble du commerce électronique en Amérique du Nord représentait un volume de 600 millions de dollars; on s'attend à ce que ce type de transaction représente en 2002 quelques dizaines de milliards de dollars au Canada seulement. Considérant qu'Internet représente un marché mondial, on peut comprendre l'importance du développement de ces outils pour l'économie du Québec dont le voisin américain est le pays le plus branché de la planète.

Ce développement est toutefois conditionné par la confiance des utilisateurs en la sécurité des réseaux ouverts. Or, ces réseaux sont généralement perçus comme non-sécuritaires; cette perception se vérifie d'ailleurs dans la réalité par de multiples exemples d'usurpation d'identité, d'intrusions dans les systèmes, de détournements de trafic et d'altération du contenu de sites Internet.

Pour assurer cette confiance et permettre le passage harmonieux du papier à l'électronique, l'un des moyens privilégiés consiste à mettre en place une infrastructure à clés publiques (ICP) permettant d'assurer rapidement, et de façon systématique:

– le chiffrement des informations pour en assurer la confidentialité;

– le scellement des documents électroniques pour en garantir l'intégrité;

– la signature électronique des documents pour en authentifier l'expéditeur et assurer la non-répudiation de leur contenu;

– la certification de l'identité des parties participant à un échange électronique pour éviter l'usurpation d'identité ou le détournement du trafic des sites WEB.

Le contexte international

Le rôle des États dans la mise en œuvre des conditions nécessaires au développement du commerce électronique a été réaffirmé par l'OCDE à l'occasion de la conférence ministérielle tenue à Ottawa au début d'octobre 1998, notamment par la Déclaration sur l'authentification pour le commerce électronique mondial. La plupart des gouvernements des pays industrialisés, dont les États-Unis, le Canada et l'Union européenne, sont à mettre en place des infrastructures à clés publiques afin d'améliorer la sécurité du commerce électronique et de la prestation électronique de leurs services, en plus de favoriser l'efficacité de leurs processus de travail internes. Des projets d'ICP sont également en cours dans différentes régions du pays. Ainsi, l'Ontario a annoncé récemment la mise en œuvre d'un programme d'ICP visant à sécuriser les communications électroniques gouvernementales et, ultimement, à doter les onze millions de résidents de l'Ontario d'une signature numérique infalsifiable. D'autre part, la Colombie-Britannique complète actuellement les encadrements juridique et technique de sa future ICP alors que l'Alberta procède à une évaluation de ses besoins.

La situation au gouvernement du Québec

Le Québec, à l'instar des autres États, a besoin de développer la confiance en les réseaux en vue de favoriser le développement du commerce électronique et de la prestation électronique des services gouvernementaux. En effet, une étude réalisée en septembre 1998 démontre que les transactions électroniques du gouvernement avec les entreprises augmenteront de 92 % d'ici trois ans. Les transactions électroniques avec les citoyens et avec les réseaux augmenteront de 22 %[2]. La même étude établit à 288 millions le nombre de transactions électroniques du gouvernement du Québec en 2001.

---

2. MLLA & Associés, *Étude sur les besoins en authentification sur l'inforoute dans les services publics québécois,* Québec, septembre 1998.

L'établissement de la confiance constitue d'ailleurs l'un des axes principaux de la Politique québécoise de l'autoroute de l'information publiée le 27 avril 1998 sous le titre «Agir autrement». Afin de répondre à ce besoin, le gouvernement a précisé les éléments à mettre en place pour instaurer cette confiance:

> La confiance repose enfin sur la disponibilité des infrastructures technologiques et administratives permettant de sécuriser les transactions électroniques sur l'inforoute. À cet effet, plusieurs outils permettant d'assurer une protection appropriée, et même souvent supérieure aux processus actuels, existent déjà. Le gouvernement envisage plus particulièrement de rendre disponibles des infrastructures permettant de signer numériquement et, au besoin, de chiffrer les échanges électroniques [...].[3]

La Politique québécoise de l'autoroute de l'information reconnaît l'importance d'assurer à la fois la cohérence des actions entreprises pour répondre aux besoins internes du gouvernement et la mise en place d'un environnement électronique sécuritaire pour l'ensemble du Québec. Pour l'application de cette Politique, le ministre délégué à l'Autoroute de l'information et aux Services gouvernementaux s'est vu confier, le 15 décembre 1998, le mandat de proposer une politique québécoise de cryptographie et d'identification électronique et d'élaborer les cadres organisationnel et technique nécessaires à la mise en œuvre de cette politique dans l'Administration. De son côté, le ministère de la Justice poursuit son mandat visant à proposer les modifications législatives nécessaires[4] pour assurer la reconnaissance juridique des documents et des signatures électroniques. Dans le cadre de ces mandats, le Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles (SSIGRI) poursuit les travaux de développement des normes et processus de l'ICPG et les Services gouvernementaux ont mis en place un serveur de gestion des clés et des certificats.

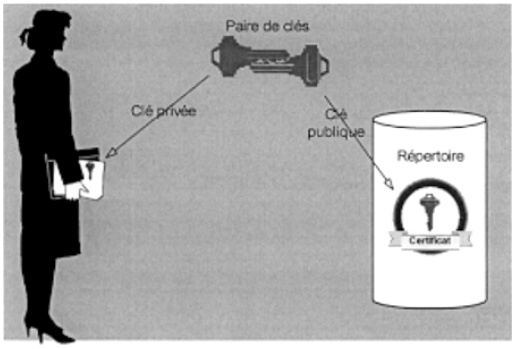
La mise en œuvre

L'ICP est basée sur la délivrance et l'utilisation de paires de clés de chiffrement. Chacune des clés d'une paire est complémentaire et permet de déchiffrer ce qui a été chiffré avec l'autre. L'une des deux

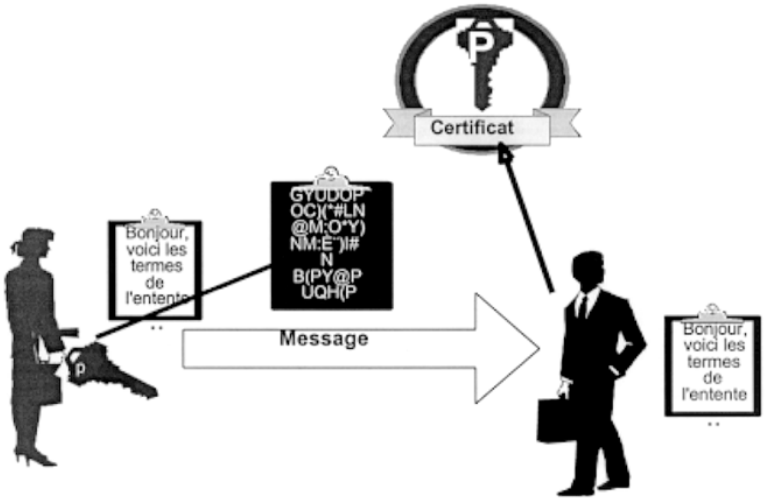
---

3. GOUVERNEMENT DU QUÉBEC, *Agir autrement*, La politique québécoise de l'autoroute de l'information, Québec, 1998, p. 21, www.mcc.gouv.qc.ca/cominfo/autorout/politique.pdf).
4. *Supra,* note 1, p. 61.

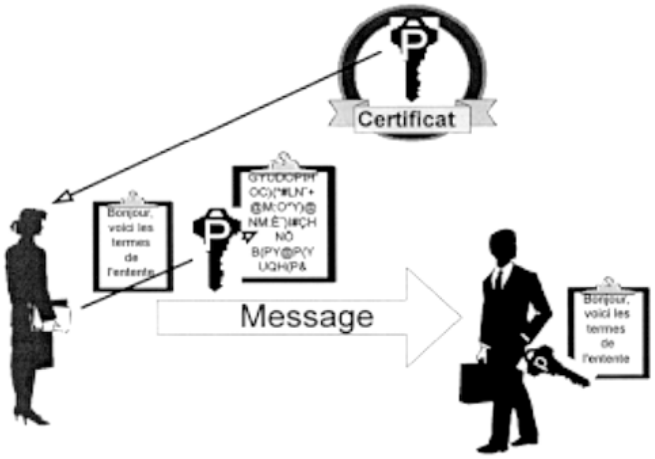
clés est rendue publique dans un répertoire (clé publique), l'autre est gardée secrète par son détenteur (clé privée).



En simplifiant considérablement le processus, on obtient les cas suivants: lorsqu'un message est chiffré par l'émetteur à l'aide de sa clé privée, toute personne qui reçoit le message peut le déchiffrer au moyen de la clé publique de celui-ci et établir de ce fait que lui seul a pu chiffrer ainsi le message, ce qui constitue la signature.



Par ailleurs, lorsque le même message a été chiffré par l'expéditeur avec la clé publique du destinataire, seul ce dernier peut le déchiffrer avec sa clé privée, assurant ainsi la confidentialité.



Pour permettre la récupération des clés servant au chiffrement sans rendre impossible la non-répudiation, on utilise deux paires de clés pour chaque usager: l'une sert à la signature, l'autre assure la confidentialité. Une copie de la clé privée de confidentialité est alors conservée, permettant ainsi à l'employeur d'avoir accès aux fichiers chiffrés par son employé dans le cadre de ses fonctions.

L'implantation d'une ICP est une opération impliquant des aspects technologiques, organisationnels et juridiques dans laquelle les questions organisationnelles et juridiques l'emportent largement sur les considérations technologiques (les spécialistes parlent de 80 % des efforts pour l'organisation et de 20 % pour la technologie).

Les fonctions à assumer

Cinq grandes fonctions opérationnelles doivent être effectuées dans le cadre d'une infrastructure à clés publiques:

- gestion de l'utilisation

Cette fonction consiste à autoriser l'attribution (délivrance, suspension et révocation) des certificats électroniques d'identité des clients et autres entités (ex.: Site WEB). Cette responsabilité découle du processus habituel de gestion des ressources et de délégation de pouvoirs.

- gestion des encadrements administratif et technique

Cette fonction consiste à assurer, par l'élaboration de politiques, de directives, de guides de fonctionnement et de normes techniques afférentes, de même que par l'accréditation des diverses composantes de l'ICPG, la cohérence requise pour en permettre le fonctionnement efficace ainsi que la reconnaissance réciproque et l'interconnexion avec d'autres services de certification externes autorisés par des ententes à cet effet.

- gestion de l'infrastructure opérationnelle

Cette fonction consiste, par délégation du responsable de la gestion des clés et des certificats, à assurer les activités techniques et opérationnelles supportant celui-ci, à voir à la sécurité des appareils et des logiciels utilisés par l'ICPG et à assurer le service technique à la clientèle. Le responsable de cette fonction développe, installe, opère et entretient les infrastructures matérielles et logicielles nécessaires pour supporter le GCC.

- gestion des clés et des certificats d'identification électronique et de chiffrement

Cette fonction consiste à assumer la responsabilité de la délivrance, suspension et révocation des clés et certificats et de toutes les activités opérationnelles du processus de certification dont, notamment, la signature des certificats (en tant que tiers certificateur), la gestion du répertoire concernant les certificats et la production des listes de certificats en vigueur, suspendus ou révoqués. Le responsable de cette fonction assure la mise en application des ententes avec les autorités de certification externes.

- vérification de l'identité et de l'enregistrement

Cette fonction vise l'exécution des tâches de vérification individuelle de l'identité des personnes, de leur enregistrement dans un répertoire pour fins de certification et les activités semblables dans le cadre de la révocation des certificats. Elle peut également consister à contrôler un dispositif, une application ou un processus (ex: Sites WEB). La fonction de vérification de l'identité et de l'enregistrement est au cœur du réseau de confiance que vise à établir l'ICPG, puisqu'elle assure un lien nécessaire entre une paire de clés et une personne.

Une répartition adéquate de ces fonctions et leur réalisation conforme à des normes et pratiques reconnues déterminera la valeur

des certificats délivrés dans le cadre de l'ICPG et, conséquemment, la confiance qui peut leur être accordée.

Le déploiement de l'ICPG

La délivrance de clés et de certificats à l'ensemble des acteurs impliqués dans les échanges et les transactions électroniques soulève non seulement des questions d'organisation interne, mais aussi et surtout des questions reliées à l'adhésion des utilisateurs. On distingue quatre types d'utilisateurs de l'ICPG, chacun présentant des caractéristiques particulières:

1. Les employés de l'État sont des usagers aux caractéristiques homogènes pour lesquels la mise en place d'une ICP est entièrement sous le contrôle du gouvernement[5].

2. Les mandataires et les partenaires du gouvernement sont plus ou moins étroitement intégrés aux processus d'affaires des ministères et des organismes concernés; ils sont en interface entre le citoyen et le gouvernement[6].

3. Les associations et les entreprises ont grandement intérêt au développement du commerce électronique et de la prestation électronique des services gouvernementaux, que ce soit pour s'acquitter de leurs obligations légales ou fiscales ou dans le but d'offrir des biens et services dans le cadre des marchés publics[7].

---

5. L'État est responsable de la certification de l'identité de ses employés dans le cadre de leur travail. Les processus mis en place doivent présenter un degré de sécurité compatible avec la valeur juridique attribuée aux actes de l'autorité publique. Par ailleurs, l'État-employeur se ménagera la possibilité d'accéder en tout temps aux documents produits par l'un de ses employés, même s'ils ont été chiffrés par lui pour fins de confidentialité; il faudra donc s'assurer de conserver une copie de la clé de confidentialité de chacun des employés. Les employés de l'État pourront utiliser l'ICPG par exemple pour assurer la confidentialité des renseignements nominatifs ou confidentiels.
6. Certains de ces groupes possèdent déjà une identification électronique qui leur est propre, d'autres ne sont pas encore organisés à ce chapitre. Ainsi, les notaires possèdent leur propre ICP, alors que d'autres n'ont pas développé une telle infrastructure. Par ailleurs, plusieurs mandataires ou partenaires ont des exigences de confidentialité qui ne permettraient pas à l'État de conserver une copie de leur clé privée de confidentialité. Cette catégorie de clientèle étant déjà en lien étroit avec le gouvernement, certains ministères et organismes ont déjà des projets qui pourraient avantageusement utiliser l'ICPG.
7. Si certaines grandes entreprises sont à mettre en place leur ICP, la plupart des PME ne disposent pas des ressources nécessaires pour le faire. Par ailleurs, nulle ne voudra être forcée d'utiliser une signature électronique différente pour traiter avec chacun des ministères et organismes avec lesquels elles échangent. Enfin,

4. Les citoyens sont particulièrement sensibles aux problématiques de respect de la vie privée et de protection des renseignements personnels[8].

Les problématiques reliées à chacun des types d'utilisateurs diffèrent les unes des autres. Dans la mise en œuvre de son infrastructure à clés publiques, l'État devra tenir compte de ces différences et développer des approches adaptées aux conditions particulières reliées à chacun.

Les niveaux de sécurité

La mise en place de l'ICPG implique une catégorisation de l'information en fonction de niveaux de sécurité à assurer. La mise en place d'une telle catégorisation des informations permettra d'établir des exigences de sécurité par niveaux et de déterminer dans quels cas l'utilisation de l'ICPG est requise ou simplement recommandée.

L'intervention du secteur privé

Le secteur privé peut être interpellé à trois titres par la mise en place de l'ICPG:

1. Comme fournisseur d'outils de cryptographie

Quelques entreprises vendent des logiciels de gestion de clés et de certificats ainsi que des logiciels permettant aux utilisateurs de chiffrer et de signer leurs documents. Pour assurer l'arrimage de ses

---

elles seront sans doute réticentes à laisser à l'État une copie de la clé privée leur servant à chiffrer leurs messages pour fins de confidentialité. La délivrance de clés et de certificats électroniques d'identité à ce type de clientèle pose la question de leur utilisation éventuelle dans des transactions privées et pourrait mettre en jeu la responsabilité de l'État pour d'éventuelles erreurs ou omissions.

8. La délivrance d'un certificat électronique d'identité aux citoyens constitue un instrument de protection de la vie privée et des renseignements personnels en ce qu'il assure la confidentialité et la provenance des transactions électroniques. L'établissement de l'identité des personnes physiques constitue toutefois une opération de grande envergure à laquelle peu d'États ont apporté une solution. Il apparaît évident que les citoyens seraient rébarbatifs à ce que l'État conserve une copie de leur clé de confidentialité.
L'identification des citoyens fait partie de la mission ou des opérations d'un certain nombre d'organismes publics, notamment le ministère des Relations avec les citoyens et de l'Immigration (Registre de l'état civil), la Régie de l'assurance-maladie du Québec (Carte-santé) et la Société de l'assurance automobile du Québec (permis de conduire).

systèmes au reste du monde, le gouvernement québécois utilisera les logiciels disponibles commercialement et reconnus au plan international dans le but de faciliter la reconnaissance mutuelle des certificats tant avec les autres gouvernements qu'avec le secteur privé.

2. Comme tiers de certification

Les tiers de certification sont chargés de certifier le lien entre une personne et une clé, permettant ainsi d'établir notamment l'origine d'un document. Ce nouveau métier, dont le leader est l'entreprise américaine Verisign, suscite un intérêt auprès de certains intermédiaires qui y voient un prolongement logique de leurs activités. Lors de la Commission parlementaire sur la question de la carte multiservices, les notaires ont indiqué aux parlementaires que leur fonction d'officier public et leur statut de délégataire de la puissance publique pour conférer l'authenticité à leurs actes les plaçaient en excellente position pour prétendre à cette fonction. Depuis ce temps, certaines institutions financières ont pris position dans ce marché ou développent un service de certification de haut niveau pour leurs clients.

3. Comme fournisseur de services-conseil

L'expertise dans le domaine est rare, les projets gouvernementaux pourront favoriser le développement d'une expertise de pointe dans ce domaine en pleine expansion à la faveur de la mise en place de l'ICPG, soit pour supporter le développement d'applications, soit pour gérer les infrastructures technologiques. Par exemple, les firmes Labcal Technologies, LGS et CGI et Bell, entreprises québécoises, ont développé une expertise reconnue par les gouvernements du Québec et du Canada. Des actions visant à l'exportation de cette expertise ont été entamées par certaines de ces firmes.

La cohérence de l'action gouvernementale

Le gouvernement ayant choisi de favoriser l'utilisation des inforoutes publiques comme moyen de délivrer les services gouvernementaux, les ministères doivent, pour assurer la sécurité des échanges et des transactions, se doter de moyens pour identifier leur clientèle. À l'heure actuelle, chaque projet est fondé exclusivement sur les besoins d'une application particulière dans le cadre du processus d'affaires spécifique que le ministère ou l'organisme concerné veut rendre accessible à distance.

Il peut ainsi se développer un ensemble de services particuliers utilisant la cryptographie à clés publiques qui risquent de faire en sorte que les clientèles du gouvernement du Québec se retrouvent en face d'une multitude de mécanismes isolés reproduisant le modèle de l'État-couloirs dans les applications gouvernementales de l'autoroute de l'information. Si ce morcellement devait prévaloir, il aurait pour effet de compliquer grandement les communications des entreprises et des citoyens avec l'État en les obligeant notamment à obtenir et détenir un passeport électronique spécifique à chaque ministère ou organisme, voire à chaque type de transaction avec un même ministère. Cela aurait également pour conséquence de multiplier, dans l'ensemble de l'appareil de l'État, les systèmes et les processus réalisant la même fonction: établir l'identité des employés et des clients du gouvernement afin de leur permettre d'échanger des documents et des informations par voie électronique.

Le gouvernement a intérêt à ce que les réseaux de la santé et de l'éducation de même que le monde municipal, qui transigent régulièrement avec lui, appliquent les mêmes normes et pratiques, facilitant ainsi l'interopérabilité des systèmes.

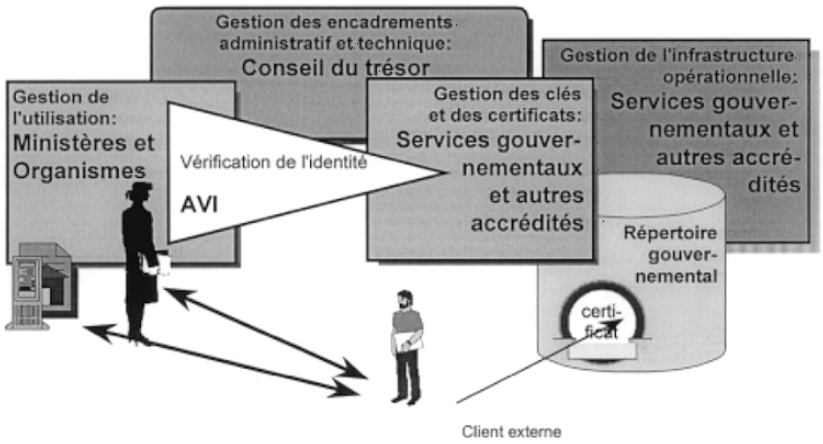
L'optimisation des ressources

Enfin, la mise en place de l'ICPG implique la disponibilité de ressources humaines et matérielles très spécialisées et un investissement important en ressources financières. Des coûts fixes importants sont générés par la mise en place de chaque serveur de gestion de clés et de certificats et par le développement de normes et pratiques régissant les opérations de chaque ICP. Une augmentation importante des coûts pourrait résulter d'un morcellement des structures en ce domaine. De plus, concernant les coûts variables, des économies d'échelle importantes peuvent résulter du regroupement des services et des acquisitions de logiciels.

Les orientations adoptées par le conseil du trésor

La mise en place de l'ICPG implique des enjeux socio-économiques, organisationnels, technologiques et juridiques qui ne trouvent pas encore tous des réponses satisfaisantes. Toutefois, pour assurer la cohérence et l'optimisation des ressources dans l'implantation de l'ICPG, des orientations de base ont été adoptées le 29 juin 1999. La décision du Conseil autorisait l'institution de l'Infrastructure à clés publiques gouvernementale et déterminait les rôles et fonctions des divers intervenants dans un modèle fonctionnel.

Le modèle fonctionnel de l'ICPG



Le modèle adopté confie chaque fonction à un intervenant distinct, suivant ses attributions administratives actuelles.

Ainsi:

- chaque ministère ou organisme assume la fonction de gestion de l'utilisation des clés et des certificats[9];

- la fonction de gestion des encadrements administratif et technique de l'ICPG est assurée par le Conseil du trésor qui exerce déjà ce rôle dans les autres secteurs de l'Administration[10];

---

9. Dans le contexte gouvernemental québécois, ces responsabilités appartiennent aux ministères et organismes. La fonction de gestion de l'utilisation implique que le responsable détermine les niveaux de confiance requis pour chacun des processus d'affaires concernés, les personnes qui auront accès à des clés ainsi que leurs obligations et privilèges. Cette fonction implique également la responsabilité d'adapter les processus d'affaires, les usages et les pratiques d'utilisation des certificats et de vérifier leur mise en application concrète dans l'organisme.
   Les ministères et organismes sont les responsables de la définition et de la mise en œuvre de leurs processus d'affaires; ils ont la responsabilité première de définir leurs besoins en matière d'échanges d'information par voie électronique et de déterminer les solutions de sécurité les plus appropriées. L'utilisation de l'ICPG dans ce cadre demeure leur responsabilité.
10. La fonction de gestion des encadrements administratif et technique s'apparente à celle de l'établissement des politiques de gestion qui s'appliquent à l'ensemble de la fonction publique. Comme, dans le cadre de l'ICPG, ces normes déterminent directement le degré de confiance que l'on peut accorder à un

- la fonction de gestion de l'infrastructure technologique, de même que la fonction de gestion des clés et certificats eux-mêmes, est confiée à des organisations accréditées par le Conseil du trésor;

---

certificat gouvernemental, il est essentiel que, parmi l'ensemble des ministères et organismes, ces politiques et pratiques soient les mêmes. Agir autrement signifierait qu'avant d'accepter le certificat d'un autre organisme, public ou privé, chacun des ministères et organismes doit procéder à la comparaison des politiques et pratiques et de la manière dont elles sont appliquées dans les faits. Comme la fonction de gestion des encadrements administratif et technique est un prolongement de celles assumées dans tous les autres secteurs de l'Administration par le Conseil du trésor et son Secrétariat, il apparaît naturel que ceux-ci assument cette fonction. Le Conseil du trésor aura donc un rôle fondamental à jouer, tant dans la coordination interne au gouvernement, que dans la coordination avec les entités externes: autres gouvernements ou secteur privé. Dans son rôle de Gestionnaire des encadrements administratif et technique, le Conseil du trésor assume, sous réserve des exigences de la loi en matière d'ententes internationales et intergouvernementales, la responsabilité de convenir d'ententes de reconnaissance réciproque avec des autorités de certification externes qu'il juge opportunes et qui s'imposent alors à l'ensemble de l'ICPG. Le Conseil du trésor assure aussi l'accréditation des intervenants, notamment les gestionnaires de l'utilisation, les gestionnaires des clés et des certificats, les gestionnaires de l'infrastructure opérationnelle et les AVI. Enfin, le Conseil du trésor détermine, notamment par une catégorisation de l'information par niveaux de sécurité, les cas où l'utilisation de l'ICPG est obligatoire. Agissant en tant que gestionnaire du cadre administratif et technique de l'ICPG, le Conseil du trésor exigera que, conformément à une directive gouvernementale:

1. soient délivrés toutes les clés numériques et tous les certificats de clés publiques dans le cadre de l'ICPG;
2. lors de l'inscription initiale, l'identité des détenteurs potentiels de clés et de certificats soit vérifiée;
3. le processus d'échange de clés et de certificats soit sécurisé et contrôlé;
4. le contenu et le format des certificats et des listes de révocation soient conformes aux normes techniques établies pour l'ICPG;
5. la conservation et la diffusion des certificats et des listes de certificats révoqués s'effectuent conformément aux normes techniques établies pour l'ICPG;
6. l'échange des clés, des certificats et des listes de révocation s'effectuent conformément aux normes techniques établies pour l'ICPG;
7. les aspects suivants fassent particulièrement l'objet d'une sécurité et d'un contrôle adéquats dans chacune des composantes de l'ICPG;

- l'environnement physique;
- le matériel technologique;
- les logiciels;
- les procédures administratives;
- la gestion du personnel.

Un comité consultatif assistera le Secrétariat du Conseil du trésor dans l'exercice des responsabilités d'appui à la gestion des encadrements administratif et technique; il sera formé de représentants des divers utilisateurs de l'ICPG:

– ministères et organismes du gouvernement;
– composantes des réseaux de la santé et de l'éducation, municipalités et sociétés d'État ayant adhéré à l'ICPG.

Par ailleurs, un comité de normalisation, formé de représentants des divers gestionnaires de clés et de certificats faisant partie de l'ICPG, sera chargé de

pour les employés et les dispositifs du gouvernement, la fonction de gestionnaire de clés et certificats est confiée en priorité aux Services gouvernementaux[11].

- la fonction de vérification de l'identité est confiée à des responsables accréditées par le Conseil du trésor; pour les employés de l'État, ceux-ci seront désignés par les ministères et organismes[12].

Conclusion

Avec les orientations adoptées par le Conseil du trésor, on peut s'attendre à ce que progressivement d'ici cinq ans, l'ensemble des employés de l'Administration québécoise dont les fonctions impliquent une interaction avec des données confidentielles ou la nécessité d'authentifier leur identité ou celle de leurs interlocuteurs devront disposer d'un passeport électronique pour voyager sur l'autoroute de l'information et être en mesure d'effectuer des échanges et des transactions sécurisées avec les clientèles disposant également d'un passeport électronique équivalent.

---

conseiller le Secrétariat du Conseil du trésor relativement aux normes et procédures qui seront applicables à l'ensemble de l'ICPG.

11. Le responsable de la fonction de gestion des clés et des certificats de confidentialité et de signature a pour mission de certifier, au nom des M/O et à l'intention des tiers, l'identité, la qualité et les pouvoirs des employés de l'État, de ses mandataires, partenaires, fournisseurs et clients. Il en est de même pour la certification des sites WEB et autres dispositifs que le gouvernement désire authentifier comme siens. Le responsable de cette fonction doit assurer, de façon toute particulière, la protection de la clé de signature des certificats et la conservation des clés de confidentialité. Ce sont la qualité, la fiabilité et la sécurité des processus opérationnels de gestion des clés et des certificats qui donnent aux clients les garanties suffisantes pour assurer la confiance à l'ensemble du processus d'authentification et de confidentialité.
12. La fonction de vérification de l'identité est essentiellement liée à la qualité et à la formation de la personne qui l'exerce. L'agent de vérification de l'identité (AVI) doit constater personnellement ce qu'il a pour fonction de vérifier et le certifier lui-même pour assurer l'authenticité de l'opération.
    Dans le cas des employés de l'État, les AVI seront:
    - désignés par les ministères et organismes;
    - formés par le responsable de la gestion des clés et des certificats;
    - accrédités par le Secrétariat du Conseil du trésor.

    Le nombre de personnes affectées à cette fonction dépendra essentiellement de la taille des organisations desservies, ainsi que de leur dispersion géographique.