AVIS DE LA COMMISSION D'ACCÈS À L'INFORMATION

SUR LE PROJET D'AUTHENTIFICATION

DES CITOYENS ET DES ENTREPRISES

DANS LE CADRE DU

GOUVERNEMENT ÉLECTRONIQUE

POUR LE

SECRÉTARIAT DU CONSEIL DU TRÉSOR

Dossier 04 00 51

Janvier 2004

MISE EN CONTEXTE

En mai 2000, le gouvernement du Québec adopte la *Loi sur l'administration publique*. Cette loi enjoint le Conseil du trésor à offrir des infrastructures communes et à favoriser la mise en commun de ressources à ce qui est désigné comme l'administration gouvernementale.

Le Québec, comme plusieurs pays du monde, cherche à favoriser le développement du commerce électronique et de la prestation électronique de services gouvernementaux. Mais, comme les réseaux électroniques offrent encore peu aujourd'hui de garantie quant à l'identité des utilisateurs, le gouvernement du Québec voulait se doter d'un mécanisme permettant d'établir l'identité des personnes qu'il nomme l'Infrastructure à clé publique gouvernementale (ICPG). Ce type d'infrastructure augmenterait le degré de confiance de la population et, ainsi, transigerait dans un environnement sécuritaire. Car, comme le souligne l'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) :

> « *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.* »

C'est dans ce contexte que le 27 mars 2001, le SCT s'adresse 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[1] au regard des règles applicables en matière de protection des renseignements personnels.

Le 21 août 2001, la Commission émet un avis relatif à la solution intérimaire de l'ICPG, lequel comprend quinze recommandations. Ces recommandations sont énumérées à l'annexe 1.

En automne 2001, le SCT soumet aux représentants de la Commission un plan d'action concernant le suivi des recommandations de cette dernière et propose de traiter certaines de ces recommandations dans le cadre de la définition de la solution administrative et technique de l'ICPG (SAT).

De novembre 2001 à la mi-mars 2002, diverses rencontres ont lieu entre des représentants de la Commission avec des représentants notamment du SCT, de la Direction générale des télécommunications (DGT) et du ministère de la Justice (MJQ).

[1] Dans sa phase intérimaire, l'ICPG vise à répondre aux besoins immédiats d'identification des employés, des applications et des dispositifs du gouvernement ainsi que de ses mandataires.

Durant cette période, la Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire est adoptée et la solution intérimaire démarre avec la Société de l'assurance automobile du Québec (SAAQ).

En octobre 2002, l'équipe du MJQ et du Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles (SSIGRI) dépose à la Commission la SAT préliminaire pour les services de certification de la solution cible. Cette solution cible transforme le projet initial d'ICPG puisqu'elle s'adresse aujourd'hui à toutes les catégories de clientèles desservies par les ministères et organismes : les entreprises, les mandataires, les employés de l'État et les citoyens. La Commission soulève par la suite au cours de l'automne une série d'interrogations en regard de cette nouvelle solution. En janvier 2003, les représentants de la Commission obtiennent des réponses du MJQ et du SCT à leurs questions.

En août 2003, le SCT demande à la Commission d'interrompre ses activités en regard de l'ICPG car la mise en place de la solution administrative et technique de l'ICPG (SAT) n'est plus envisagée à court terme, compte tenu notamment de l'importance des investissements requis et que de nouvelles orientations seraient éventuellement avancées.

C'est ainsi que le 17 décembre 2003, la Direction du soutien au déploiement de l'inforoute gouvernementale (DSDIG) du SSIGRI vient présenter à la Commission, le Service québécois d'authentification gouvernementale (SQAG)[2].

Le SQAG remplace la solution administrative et technique de l'ICPG. Il consiste à délivrer aux citoyens et aux entreprises[3] utilisant des services gouvernementaux par Internet un certificat numérique qui leur permettra de s'identifier en ligne.

Le SCT fait une demande pour obtenir un avis de la Commission le 20 janvier 2004.

PORTÉE DE L'AVIS

Le présent avis examine le fonctionnement et la conformité du SQAG aux exigences de la législation québécoise sur la protection des renseignements personnels en regard de la vérification de l'identité, la délivrance d'un certificat, l'inscription à un programme et corroboration d'identité, l'authentification des citoyens et des entreprises, la récupération d'un certificat et l'annulation et le renouvellement d'un certificat.

[2] La solution cible ou la SAT qui s'adressait aux employés de l'État, aux mandataires, aux entreprises et aux citoyens est remplacée par le SQAG qui s'adresse uniquement aux entreprises et citoyens. Par conséquent, la solution intérimaire de l'ICPG qui s'adresse aux employés de l'État et aux mandataires se poursuit.

[3] Tel que proposé dans le document sur les orientations et stratégie gouvernementale en matière d'authentification des citoyens et des entreprises, sont visées par le terme « entreprise » les sociétés, les associations et les personnes morales. Pour l'application des orientations proposées en matière d'identité préalable, la personne physique qui exploite une entreprise individuelle sous ses nom et prénom peut être considérée comme un citoyen plutôt que comme une entreprise.

Compte tenu des délais, notre examen ne porte que sur deux documents. Ces documents sont : « Orientations et stratégie gouvernementales en matière d'authentification des citoyens et des entreprises dans le cadre de la mise en place du gouvernement électronique » et « La conformité du SQAG aux exigences de la législation québécoise sur la protection des renseignements personnels ».

Il n'aborde d'aucune façon les fonctions de sécurité qui surviennent habituellement à la suite de l'authentification, notamment la fonction d'habilitation mise en place par ces derniers pour contrôler l'accès à leurs ressources ou pour donner des autorisations à leurs citoyens ou entreprises qui utiliseront les prestations électroniques de service.

DESCRIPTION DU FONCTIONNEMENT ACTUEL DE L'AUTHENTIFICATION DANS LES MINISTÈRES ET ORGANISMES

Plusieurs ministères et organismes offrent déjà des services en ligne aux citoyens du Québec. Certains des services qu'ils offrent nécessitent que le citoyen s'authentifie[4].

Par exemple, le ministère du Revenu authentifie ses utilisateurs à chacune de leur visite en leur demandant certaines informations ou secrets partagés, tels : le numéro d'assurance sociale (NAS), le montant inscrit à la ligne X de la dernière déclaration… Le MJQ identifie les clients du Registre des lobbyistes en leur délivrant un certificat d'identification numérique. Le ministère de l'Éducation identifie les étudiants qui accèdent à leur dossier en ligne en leur délivrant un mot de passe.

MISE EN PLACE D'UNE INFRASTRUCTURE COMMUNE - LE SQAG

Pour éviter que :

- chaque ministère et organisme mette en place sa propre infrastructure et ses propres processus d'authentification,
- le gouvernement multiplie les coûts de mise en œuvre et d'exploitation de ces infrastructures et de ces processus,
- les citoyens et les entreprises se retrouvent avec autant d'identifiants que de services auxquels ils veulent accéder sur Internet,

le SCT propose aux ministères, aux organismes, aux citoyens et aux entreprises une démarche concertée, le SQAG[5].

[4] L'authentification consiste à vérifier l'identité déclarée d'une personne de sorte que le ministère ou organisme a l'assurance que :
- les documents qu'il a reçus proviennent de l'émetteur déclaré ou de la personne identifiée,
- seules les personnes autorisées à recevoir des services y ont accès,
- les personnes ont accès aux renseignements personnels qui les concernent seulement.

[5] Le SQAG est né d'un projet de la Régie des rentes du Québec, qui a élaboré, avec la participation des membres du Forum des dirigeants des grands organismes (la Régie de l'assurance maladie du Québec, la Régie des rentes du Québec, la Société de l'assurance automobile du Québec, la Commission des normes

Dans les faits, le SCT fournirait aux citoyens et aux entreprises qui le désirent un identifiant qui sera reconnu par tous les ministères et organismes. Toutefois, chaque citoyen ou entreprise pourra, à son choix, détenir plusieurs certificats et pourra choisir quel certificat il utilisera dans un service particulier ou dans un ministère et organisme particulier.

DESCRIPTION DU FONCTIONNEMENT DU SQAG

Le SQAG comporte un ensemble de fonctions visant, d'abord, à attribuer un identifiant à chacun des citoyens et des entreprises du service, puis à permettre aux ministères et aux organismes de reconnaître cet identifiant.

L'attribution d'un identifiant gouvernemental SQAG aux citoyens et aux entreprises sera amorcée par une demande en ligne[6] lors de l'utilisation d'un premier service électronique transactionnel d'un ministère ou d'un organisme exigeant une identification. Une fois la connexion sécurisée établie, le ministère ou l'organisme invite le citoyen ou l'entreprise à répondre à certaines questions permettant de s'assurer que le citoyen ou l'entreprise est bien celui qu'il prétend être.

La fonction de vérification d'identité (FVI) sera assumée par certains ministères ou organismes désignés à cet effet. Elle sera faite en comparant les réponses fournies par les citoyens et les entreprises participants avec des informations déjà en possession de ceux qui effectuent la vérification. Les questions posées font référence à des informations connues du citoyen ou de l'entreprise et du ministère ou de l'organisme, on parle alors de secrets partagés. En général, pour atteindre le niveau de confiance moyen, un minimum de deux secrets partagés doivent être vérifiés. De plus, l'un de ces secrets doit avoir été préalablement transmis par la poste au citoyen ou par tout autre moyen qui sera évalué cas par cas lors de la désignation des ministères et organismes qui réaliseront la vérification d'identité.

Une fois la vérification d'identité effectuée avec succès, le ministère ou l'organisme ne transmet pas le nom ou une autre information au sujet du citoyen ou de l'entreprise, mais se limite à rediriger la session vers le fournisseur de certificats, le temps requis pour délivrer le certificat, à la suite duquel la session sera ramenée au ministère ou à l'organisme pour l'étape de l'inscription.

---

du travail, la Commission de la santé et de la sécurité du travail, la Commission administrative des régimes de retraite et d'assurances et la Société de la faune et des parcs du Québec) et du SCT, une étude de faisabilité concernant une solution d'authentification de clientèles grand public. Le SCT a, par la suite, réalisé des travaux complémentaires au cours de l'automne 2002. Le projet SQAG a ensuite été présenté au Comité stratégique des ressources informationnelles du gouvernement du Québec, qui a mandaté le SCT pour élaborer, en collaboration étroite avec certains ministères et organismes, une solution détaillée du SQAG.

[6] Une session est établie entre le poste du citoyen ou de l'entreprise et le serveur du ministère ou de l'organisme. À ce sujet, la connexion s'établissant entre le poste du citoyen ou de l'entreprise et le serveur du ministère ou de l'organisme est protégée par le protocole SSL (en général par un cryptage à 128 bits).

Un « applet » est alors téléchargé sur le poste du citoyen ou de l'entreprise, une fois que la session sécurisée par le protocole SSL a été établie entre le citoyen ou l'entreprise et le fournisseur de certificat. Cet « applet » contient les modules cryptographiques nécessaires à la création du profil de clés et à l'utilisation du certificat.

Le fournisseur demande ensuite au citoyen ou à l'entreprise de choisir un code d'usager et un mot de passe, lequel doit répondre à certaines caractéristiques de sécurité comme un nombre minimum de caractères. Le fournisseur demande ensuite au citoyen ou à l'entreprise de choisir des « secrets de récupération »[7]. Ces secrets sont nécessaires pour certaines opérations subséquentes sur le certificat délivré, notamment quand le citoyen ou l'entreprise oublie son mot de passe.

Une fois le choix effectué, le citoyen ou l'entreprise se voit délivrer un certificat comportant un code unique et non significatif, appelé « Meaningless But Unique Number ou MBUN », permettant de distinguer les certificats les uns des autres.

Lors de la délivrance du certificat, le citoyen ou l'entreprise accepte et signe, avec sa nouvelle clé, les conditions d'abonnement du fournisseur de certificats. L'entente d'abonnement comportera principalement un rappel des obligations du citoyen ou de l'entreprise à l'égard de son certificat[8].

Le fournisseur enregistre alors sur ses serveurs le code d'usager, le mot de passe (en format illisible - forme hachée), les secrets de récupération, le MBUN, le profil de clés et l'abonnement signé du citoyen. Par la suite, le fournisseur retourne le MBUN au ministère ou organisme qui a initié la demande de délivrance de certificat.

Une fois la vérification d'identité effectuée et le certificat délivré, le citoyen peut procéder à son inscription à l'un des services ou programmes offerts par le ministère ou organisme.

Cet identifiant SQAG ne contiendra pas de renseignements personnels à propos des citoyens et des entreprises. Il comportera plutôt un pseudonyme et prendra la forme d'un certificat à clé publique. La délivrance des certificats sera effectuée par un fournisseur désigné par le Conseil du trésor.

Dès que le certificat sera délivré, le ministère ou l'organisme procédera à l'inscription de chacun des citoyens et des entreprises participants au service électronique. Cette inscription implique la conservation d'un lien entre le certificat délivré MBUN et le numéro de dossier (identifiant administratif) sous lequel le citoyen ou l'entreprise est connu au sein du ministère ou de l'organisme. Le même certificat pourra être utilisé ensuite en vue de l'inscription à des services électroniques offerts par d'autres ministères ou organismes : le citoyen ou l'entreprise devra procéder à une inscription pour chaque service en ligne dont il voudra bénéficier.

[7] À titre d'exemple de secret de récupération demandé, notons le sport préféré, la couleur préférée, etc.

[8] À savoir qu'il ne doit en aucun cas divulguer son mot de passe, prêter son certificat ou l'utiliser pour d'autres fins que des transactions gouvernementales.

Ainsi, le citoyen ou l'entreprise qui se présente sur le portail d'un ministère ou organisme pour s'inscrire à un nouveau programme ou service doit, avant toute chose, activer son certificat. Pour ce faire, le ministère ou organisme redirige la session du citoyen ou de l'entreprise sur le site du fournisseur de certificats. Un « applet » est alors téléchargé sur le poste du citoyen ou de l'entreprise. Le fournisseur de certificats invite alors le citoyen à entrer son code d'usager et son mot de passe pour récupérer son profil de clés, dans lequel réside son certificat.

Une fois l'étape réussie, le certificat est déposé sur l'ordinateur du citoyen le temps de sa session sur le site du ministère ou organisme. La session du citoyen est par la même occasion redirigée sur le portail du ministère ou organisme qui a initié la demande d'activation du certificat.

Ce deuxième ministère ou organisme a alors accès au MBUN du citoyen ou de l'entreprise. Cependant, comme le certificat ne comporte pas d'information sur l'identité de son détenteur, le ministère ou organisme doit alors procéder à une corroboration d'identité en demandant au citoyen ou à l'entreprise des informations additionnelles qui sont comparées avec les données contenues dans leur base de données. Cette fonction sert à créer le lien entre un citoyen ou une entreprise détenteur d'un certificat et un dossier interne. Si le ministère ou organisme utilisateur est satisfait du résultat de la corroboration d'identité qu'il a réalisé, il procède à l'inscription, tel que décrit précédemment. Si le ministère ou organisme souhaite connaître le véritable nom du détenteur du certificat, il s'adresse donc aux services centraux pour connaître cette information.

Or, aucune information sur l'identité des détenteurs de certificats n'est conservée par les services centraux. La demande est donc acheminée par les services centraux au ministère ou organisme qui avait alors procédé à la vérification d'identité initiale. Ce dernier fournit au ministère ou organisme demandeur les trois premières lettres du nom et du prénom du citoyen ou de l'entreprise. Le ministère ou organisme utilisateur vérifie si le nom réel du détenteur du certificat est le même que celui qu'il a lui-même déterminé à la suite de la corroboration d'identité. Dans l'affirmative, il inscrit dans sa section de la banque des inscriptions un lien chiffré entre le MBUN et l'identifiant de programme (numéro de dossier).

Puisque le certificat ne comporte pas le numéro de dossier du citoyen ou de l'entreprise mais plutôt un pseudonyme, un ministère ou un organisme qui voudra inscrire un citoyen ou une entreprise à son service en ligne devra procéder de nouveau à une vérification d'identité afin d'établir le lien entre le certificat et le bon numéro de dossier.

Cependant, contrairement à la vérification d'identité initiale, qui doit être effectuée selon un niveau de confiance déterminé, le ministère ou l'organisme sera libre de choisir le niveau de la vérification qui sera effectuée pour inscrire un citoyen ou une entreprise à son service en ligne[9]. Cela offre la possibilité aux ministères et organismes de s'assurer

[9] Les canaux par lesquels le citoyen peut consommer des services nécessitent de mettre en place des mesures de protection selon différents niveaux de confiance. Les ministères et organismes sont responsables de déterminer à quels niveaux de confiance correspondent leurs processus d'affaires, en

eux-mêmes de l'identité du citoyen ou de l'entreprise, selon le niveau de confiance désiré par le ministère ou l'organisme concerné, avant d'établir le lien entre le certificat du citoyen ou de l'entreprise et le numéro de dossier interne.

Le SQAG est conçu afin de procurer une authentification de niveau de confiance moyen, celui qui est requis lorsqu'un ministère ou organisme doit s'assurer de l'identité du citoyen ou de l'entreprise avec un degré de certitude raisonnable pour offrir la prestation électronique de services.

Lorsque le citoyen ou l'entreprise accédera de nouveau aux services en ligne d'un ministère ou d'un organisme auxquels il se sera déjà inscrit, l'authentification sera effectuée en session sécurisée. Le citoyen ou l'entreprise n'aura alors qu'à présenter son certificat et à entrer son mot de passe, qui sera validé par le SQAG en vue de l'authentifier.

Pour ce faire, le ministère ou l'organisme redirigera la session du citoyen ou de l'entreprise sur le site du fournisseur de certificats qui l'invitera à entrer son code d'usager et son mot de passe afin que son profil de clés puisse être téléchargé sur son ordinateur le temps de la session au site du ministère ou de l'organisme. Si cette étape est réussie, la session est alors redirigée au ministère ou à l'organisme qui a initié la demande d'activation du certificat.

Assuré de la validité du certificat et de l'identité du citoyen, le ministère ou l'organisme effectuera une requête dans la banque des inscriptions afin de récupérer les données qui ont été déposées lors de l'inscription du citoyen ou de l'entreprise. Cette requête est basée sur le MBUN que le fournisseur de certificats a retourné au ministère ou à l'organisme et vise à vérifier que le citoyen ou l'entreprise est inscrit au programme.

Si le citoyen est inscrit, le ministère ou l'organisme déchiffre ce qu'il reçoit et récupère l'identifiant déposé lors de l'inscription. Si le citoyen n'est pas inscrit, le ministère ou l'organisme lui proposera la possibilité de s'inscrire.

Une fois l'authentification effectuée, le certificat validé et l'inscription vérifiée, le citoyen ou l'entreprise pourra accéder au programme offert par le ministère ou l'organisme.

Lorsque le citoyen ou l'entreprise veut accéder à un programme pour lequel il est inscrit, il doit activer son certificat. S'il ne se souvient plus de son mot de passe, il n'aurait qu'à cliquer alors sur l'option « J'ai oublié mon mot de passe » et entrer son code d'usager. Le système lui demanderait alors de saisir les secrets de récupération qu'il avait indiqués lors de la délivrance du certificat. S'il donne les bons secrets de récupération, le fournisseur de certificats l'invite à choisir un nouveau mot de passe, à la suite de quoi un nouveau certificat et profil de clés seront générés. Ils seront protégés par le nouveau mot de passe. Même si le citoyen ou l'entreprise a un nouveau certificat, cela ne veut pas dire pour autant qu'il devra refaire toutes les étapes suivant la délivrance d'un certificat. En effet, le

fonction d'une catégorisation de l'information et d'une analyse de risques. Les différents niveaux de confiance sont présentés à l'annexe 2.

nouveau certificat est associé au MBUN contenu dans le précédent certificat. Une fois qu'il a récupéré son certificat, sa session est redirigée sur le portail du ministère ou de l'organisme qui a initié la demande d'authentification et d'activation du certificat. Le citoyen peut alors accéder normalement au service. Par contre, s'il ne donne pas les bons secrets de récupération, le processus se termine et il doit recommencer tout le processus.

Enfin, le certificat peut être annulé pour différentes raisons :

- Il peut être annulé à la demande du citoyen en signant un formulaire, pourvu qu'il ait dûment été authentifié par le fournisseur de certificats et que le certificat soit valide. Par cette action, le citoyen ne pourra plus accéder aux programmes auxquels il est inscrit avec ce certificat. S'il désire utiliser de nouveau l'un de ces programmes, il devra recommencer le processus. Le citoyen sera informé des conséquences de l'annulation de son certificat.
- Le certificat peut être annulé par l'arrivée de son terme. En effet, conformément à l'article 48 de la *Loi concernant le cadre juridique des technologies de l'information*, lors de la délivrance d'un certificat, le fournisseur de certificat doit non seulement indiquer le début mais aussi la fin de la période de validité du certificat[10].
- Le certificat peut être annulé lorsque le fournisseur de certificats a des raisons de croire que celui-ci a été volé ou perdu ou que sa confidentialité est compromise conformément à l'article 58 de la *Loi concernant le cadre juridique des technologies de l'information*[11].
- Le fournisseur de certificats peut également décider d'annuler le certificat après une certaine période d'inaction par exemple.
- Le certificat peut être annulé à la demande d'un ministère ou organisme à la suite du décès du détenteur du certificat.

Le certificat qui sera utilisé pour le SQAG est semblable à celui actuellement utilisé pour l'ICPG.

Dans son « Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementale du Secrétariat du conseil du trésor » d'août 2001, la Commission mentionnait les principaux risques liés à l'utilisation des certificats d'identité électroniques de l'ICP.

[10] Toutefois, une pratique consiste à prévoir un renouvellement automatique des certificats, d'une part, pour permettre une continuité dans le processus et, d'autre part, pour éviter que le citoyen n'ait à recommencer les étapes relatives à la délivrance d'un certificat. Cette fonction de renouvellement automatique n'a lieu que lorsque certaines conditions sont rencontrées et sera mentionnée dans l'entente signée par le citoyen lors de la délivrance du certificat. Le citoyen sera aussi informé de la possibilité qu'il a d'annuler le certificat avant son terme.

[11] Dans ce cas, le ministère ou l'organisme responsable du SQAG doit en aviser le citoyen détenteur du certificat ainsi que les ministères et organismes qui utilisent ce certificat dans leurs relations avec le citoyen. Par ailleurs, il revient au fournisseur de certificats de procéder à la destruction du certificat et du MBUN associé.

Avec le SQAG, ces risques existent-ils toujours? Nous désirons rappeler ces risques qui avaient alors été identifiés dans cet avis.

L'ICP ET LES RISQUES RELIÉS À LA VIE PRIVÉE

***1- Le traçage** :*
Toutes les communications et transactions qu'effectue un individu peuvent être automatiquement tracées grâce à son certificat et lui être 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 télécommunication. 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… D'autre part, l'utilisation des certificats ouvre la porte à la particularisation des services offerts en fonction du contenu du certificat 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...

LE SQAG ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Dans un contexte où les ministères et les organismes sont détenteurs de fichiers comportant une multitude de données nominatives, il est primordial que ces derniers s'assurent que la mise en place du SQAG prendra en compte les risques énumérés précédemment.

Pour ce faire, le SQAG doit donc être conçu en respectant les critères suivants de protection des renseignements personnels :

- donner libre choix aux citoyens et aux entreprises,
- utiliser des pseudonymes,
- limiter la collecte des renseignements nominatifs,
- limiter la circulation de renseignements nominatifs,
- limiter la possibilité de couplage des données et d'utilisation à d'autres fins,
- limiter la possibilité de traçage de l'utilisation du certificat dans l'appareil gouvernemental.

Donner libre choix aux citoyens et aux entreprises

L'adhésion au SQAG sera volontaire pour les citoyens et les entreprises. Ces derniers pourront en effet opter pour les services au comptoir ou au téléphone plutôt que pour un mode de prestation électronique de services.

Cependant, s'ils retiennent le mode de prestation électronique de services, un ministère ou un organisme pourra, lorsque l'identification pour un service donné est requise, exiger la présentation d'un certificat SQAG pour compléter un échange électronique. Dans ce cas, les citoyens et les entreprises auront le choix du certificat qu'ils présenteront à leur interlocuteur et pourront ainsi détenir plusieurs certificats SQAG et choisir quel certificat ils utiliseront dans un service particulier ou dans un ministère ou un organisme particulier.

Par conséquent, la Commission comprend que le libre choix est donné aux citoyens et aux entreprises d'abord de participer ou non à la prestation électronique de services et s'ils retiennent le mode de prestation

électronique de services, ils auront le choix du certificat qu'ils présenteront à leur interlocuteur.

Utilisation de pseudonymes

La vérification de l'identité d'un citoyen ou d'une entreprise est d'abord effectuée par un ministère ou un organisme. En effet, lorsqu'un ministère ou un organisme a vérifié l'identité du citoyen ou de l'entreprise avec satisfaction, le ministère ou l'organisme déclenche alors un processus qui aboutit à la délivrance d'un certificat ne contenant pas de renseignements personnels mais comportant un pseudonyme ayant la forme d'un numéro non significatif « MBUN ».

Dès que le certificat est délivré, le ministère ou l'organisme procède à l'inscription du citoyen ou de l'entreprise au service électronique. Cette inscription implique la conservation d'un lien entre le certificat délivré (pseudonyme) et l'identité de ce citoyen ou de cette entreprise (par exemple le numéro de dossier de l'individu ou de l'entreprise ou tout autre code administratif) sous lequel ce dernier est connu au sein du ministère ou de l'organisme.

Puisque le certificat comporte un MBUN, un autre ministère ou organisme qui voudra inscrire un citoyen ou une entreprise à son service en ligne devra procéder à une corroboration d'identité afin d'établir le lien entre le certificat et le bon identifiant de programme. Cependant, le ministère ou organisme utilisateur sera libre de choisir le niveau de corroboration d'identité qui sera effectuée pour inscrire un citoyen ou une entreprise à son service en ligne.

Les services centraux du SQAG, opérés par la Direction générale des services informatiques gouvernementaux du SCT, gèrent les échanges entre les citoyens, les entreprises, le fournisseur de certificats, les ministères et organismes participants du SQAG et abritent la banque des inscriptions qui contiendra, en mode crypté, les inscriptions aux programmes et services de tous les ministères et organismes utilisateurs du SQAG.

Advenant qu'un ministère ou un organisme doit connaître le nom de la personne ou de l'entreprise détentrice d'un certificat en particulier, puisque le SQAG ne stocke pas cette information, il est prévu que la requête soit redirigée par le SQAG directement vers le ministère ou l'organisme qui avait procédé à la vérification d'identité initiale, lequel serait en mesure de fournir au ministère ou à l'organisme demandeur le nom du détenteur du certificat, et ce, tel que le prévoit l'article 48 de la *Loi concernant le cadre juridique des technologies de l'information.*

> *48. Un certificat peut être joint directement à un autre document utilisé pour effectuer une communication ou être accessible au moyen d'un répertoire lui-même accessible au public.*
>
> *Le certificat doit au moins comprendre les renseignements suivants :*

1º le nom distinctif du prestataire de services qui délivre le certificat ainsi que sa signature;

2º la référence à l'énoncé de politique du prestataire de services de certification, y compris ses pratiques, sur lequel s'appuient les garanties qu'offre le certificat qu'il délivre;

3º la version de certificat et le numéro de série du certificat;

4º le début et la fin de sa période de validité;

5º s'il s'agit d'un certificat confirmant l'identité d'une personne, l'identification d'une association, d'une société ou de l'État, leur nom distinctif ou, selon le cas, s'il s'agit d'un certificat confirmant l'exactitude de l'identifiant d'un objet, cet identifiant;

6º s'il s'agit d'un certificat d'attribut, la désignation de l'attribut dont le certificat confirme l'existence et, au besoin, l'identification de la personne, de l'association, de la société, de l'État ou de l'objet auquel il est lié.

Le nom distinctif d'une personne physique peut être un pseudonyme, mais le certificat doit alors indiquer qu'il s'agit d'un pseudonyme. Les services de certification sont tenus de communiquer le nom de la personne à qui correspond le pseudonyme à toute personne légalement autorisée à obtenir ce renseignement.

Par conséquent, la Commission comprend que le certificat SQAG contiendra un pseudonyme qui prendra la forme d'un numéro séquentiel non significatif, plutôt que le nom du citoyen ou d'une entreprise.

La Commission comprend également que ni le fournisseur de certificats ni les services centraux abritant le SQAG ne détiendront de base de données comportant le nom ou d'autres renseignements sur l'identité du citoyen ou de l'entreprise en question.

Limiter la collecte de renseignements nominatifs

La vérification de l'identité des citoyens et des entreprises du SQAG sera effectuée par la comparaison de renseignements sur ces citoyens et ces entreprises avec des données déjà en la possession des ministères et organismes. Cette manière de procéder permet de limiter au strict minimum la collecte de renseignements personnels.

Toutefois, en cas d'oubli de la part d'un citoyen ou d'une entreprise de son mot de passe, seules des informations dites des « secrets partagés » servant à la récupération de ce mot de passe seraient collectées[12]. Ces secrets sont conservés par le fournisseur sous forme

[12] À titre d'exemple d'information souvent recueilli, mentionnons le nom de la ville de naissance ou le passe-temps préféré.

hachée. Dans le cadre du SQAG, ces données seraient recueillies par le fournisseur de certificats qui ne connaît pas l'identité des détenteurs de certificats.

Advenant le cas où le fournisseur de certificats désigné par le Conseil du trésor soit de juridiction fédérale, tel le « Service epass, pour la délivrance du passeport électronique par l'Agence des douanes et du revenu du Canada », le SCT devrait s'assurer que les règles de droit en matière de protection des renseignements personnels soient maintenues.

Par conséquent, la Commission comprend que les seules données à caractère personnel recueillies par le SQAG sont des « secrets partagés », lesquels ne seront, à aucun moment, associés à l'identité des détenteurs de certificats.

Limiter la circulation de renseignements nominatifs

Les ministères et organismes demeurent les seuls détenteurs de renseignements personnels sur les citoyens. Ainsi, au moment de la vérification de l'identité d'un citoyen, les données saisies par l'individu seront comparées, chez le ministère ou l'organisme, avec celles qui sont dans ses bases de données à l'arrière-boutique.

De même, lors de l'inscription, le ministère ou l'organisme transmettra les données chiffrées aux services centraux du SQAG du SCT de manière à ce qu'il soit le seul à y accéder par la suite.

Le SQAG ne recueille donc pas de renseignements personnels pour la délivrance d'un certificat. Les renseignements personnels sont détenus par les ministères ou organismes dans leurs banques de données. Il n'y a pas de collecte supplémentaire de renseignements personnels. Le SQAG ne sait rien des rapports que les citoyens entretiennent avec les ministères et organismes, pas plus que les ministères et organismes entre eux ne savent les rapports qu'un citoyen ou une entreprise entretient avec un autre ministère ou un autre organisme.

Par conséquent, la Commission comprend qu'à aucun moment, des données nominatives sur un individu ne circuleront en clair dans le système SQAG.

Limiter la possibilité de couplage des données et d'utilisation à d'autres fins

Tel que cela a été mentionné précédemment, un citoyen ou une entreprise pourra détenir plus d'un certificat SQAG, donc autant de pseudonymes. Cette caractéristique, en plus de respecter le principe de libre choix du citoyen ou de l'entreprise, leur permet également de pouvoir segmenter l'usage du SQAG parmi les ministères et organismes selon leurs choix et leurs préférences. Ainsi, un citoyen ou une entreprise pourrait utiliser un certificat SQAG pour communiquer avec un ministère alors qu'il en utiliserait un deuxième

pour communiquer avec un organisme. Il pourrait aussi, à son choix, utiliser le même. Cette façon de procéder rendrait difficile un couplage de données à partir de cet identifiant.

Même si détenir plusieurs certificats pour un même citoyen ou une même entreprise permet de réduire les risques de couplage de données, cela ne les enraye pas complètement. C'est pourquoi l'identifiant SQAG ne doit pas venir se substituer aux numéros de dossiers ministériels à l'intérieur des programmes et des services.

Ainsi, il nous apparaît que les ministères et organismes doivent continuer d'identifier les citoyens et les entreprises à l'aide des numéros actuellement utilisés et faire le joint ou l'appariement entre ce numéro de dossier et l'identifiant SQAG lors de l'étape de l'inscription, tel que le SQAG le prévoit.

Le SQAG prévoit également que le lien entre le certificat et le numéro de dossier du ministère ou de l'organisme concerné sera fait à l'aide de procédés cryptographiques faisant en sorte que le ministère ou l'organisme n'aura pas à conserver dans ses banques de données le pseudonyme inscrit au certificat, empêchant donc toute possibilité de croisement de données à partir des certificats SQAG.

Par conséquent, la Commission comprend que le SQAG comporte un ensemble de mesures technologiques et administratives visant à faire en sorte que les ministères et les organismes ne puissent pas utiliser le pseudonyme inscrit au certificat pour des fins illicites de couplage de données ou pour toutes fins autres que celles prévues par le SQAG.

Recommandation 1

La Commission recommande que :

les ministères et les organismes utilisateurs du SQAG s'engagent contractuellement à ne pas utiliser le pseudonyme à d'autres fins que celles prévues par le SQAG.

Limiter la possibilité de traçage de l'utilisation du certificat dans l'appareil gouvernemental

Une autre préoccupation souvent associée à l'usage d'un identifiant commun concerne la possibilité de suivre le cheminement d'une personne dans les programmes et les services gouvernementaux. La possibilité de tracer le cheminement d'un citoyen ou d'une entreprise dans un ou plusieurs services est intimement reliée à l'obligation de conserver des journaux de transactions sur les activités d'un système. Ces journaux, générés automatiquement par les systèmes informatiques, servent notamment à trouver des erreurs ou

d'autres problèmes techniques, mais peuvent également servir à établir une preuve dans le cas d'une contestation judiciaire.

En effet, il pourrait être nécessaire de produire en preuve un ensemble de données servant à démontrer qu'un citoyen ou une entreprise est bel et bien à l'origine d'une transaction. Ces données pourraient également servir d'éléments de preuve dans le cadre d'une enquête relative à une usurpation d'identité.

Comme la vérification d'identité, la délivrance de certificats, l'inscription, l'authentification, etc. seront assumées par des entités distinctes, cette façon de faire permet ainsi de conserver des journaux de transactions dans des organisations distinctes et des systèmes différents, de sorte qu'il sera très difficile de tracer l'usage d'un certificat dans les services gouvernementaux.

Par exemple, les journaux de transactions associés à l'usage au jour le jour d'un certificat sont conservés par le fournisseur de certificats, lequel n'est pas en mesure de connaître l'identité des détenteurs de certificats SQAG, puisque les renseignements sur l'identité sont conservés par une autre entité, à moins que toutes les entités concernées soient de connivence.

De plus, des mesures administratives et contractuelles seront utilisées pour baliser l'usage et la sécurité des journaux de transactions.

Par conséquent, la Commission comprend que le SQAG comporte un ensemble de mesures technologiques et administratives faisant en sorte de limiter la possibilité de tracer l'usage d'un certificat dans l'appareil gouvernemental.

La Commission comprend également que le mode de fonctionnement du SQAG fait en sorte qu'il ne sera pas possible de savoir à quel moment ou à quelle fréquence un citoyen ou une entreprise en particulier visite un programme ou un service gouvernemental, à moins d'effectuer une enquête approfondie nécessitant la collaboration de toutes les entités concernées.

MESURES DE SÉCURITÉ

Les informations communiquées par le citoyen ou l'entreprise au ministère ou à l'organisme ou au fournisseur de certificats le sont dans le cadre d'une session sécurisée SSL, permettant de réduire les risques d'interception.

Les informations collectées par le fournisseur de certificats sont conservées dans un endroit sécuritaire et accessible aux seules personnes dûment autorisées. Il lui revient également de prendre des mesures de sécurité pour garantir l'intégrité des informations qu'il a en sa possession.

De plus, en séparant les fonctions de vérification d'identité et de délivrance des certificats entre deux entités distinctes, les risques de compilation et de collecte abusive d'information sont réduits.

Un lien entre un MBUN et un identifiant de programme est construit au moment de chaque inscription aux différents services électroniques. Afin d'assurer la sécurité de ce lien dans la banque des inscriptions hébergée par les services centraux, ce dernier doit être préalablement chiffré par le ministère ou l'organisme avec sa propre clé cryptographique et, de manière réciproque, déchiffré à chaque opération de lecture. Ces clés cryptographiques sont gardées secrètes par les ministères ou organismes concernés à l'intérieur de leur organisation. De cette façon, l'information déposée par chaque ministère ou organisme utilisateur demeure inaccessible à tous les autres ministères ou organismes ainsi qu'aux services centraux.

Le MBUN est enregistré en clair dans la banque centrale des inscriptions pour conserver le nom du ministère ou organisme qui a procédé à la FVI initiale.

Lors de la phase d'authentification et de validation du certificat, la communication du code d'usager et du mot de passe au fournisseur de certificats par le citoyen se fait dans le cadre d'une session sécurisée.

L'applet téléchargé sur le poste du citoyen ou de l'entreprise est désactivé à la fin de la session à la suite de l'action du citoyen ou à la suite d'une période d'inactivité. Dès lors, une fois la session terminée, toutes les informations sont effacées de la mémoire du poste du citoyen.

Des mesures de sécurité doivent également être mises en place à l'égard des banques de données du ministère ou l'organisme qui constituent un important gisement de renseignements personnels. Cette obligation n'est pas spécifique au processus SQAG, elle est requise par la loi.

Recommandation 2

La Commission recommande que :

le SCT s'assure que le fournisseur de certificats mette en place les mesures nécessaires pour éviter les bris de confidentialité et de sécurité et qu'il obtienne un engagement de ses employés à respecter des normes rigoureuses.

CONCLUSION

La Commission tient à souligner les efforts réalisés par le SCT ainsi que par plusieurs ministères et organismes pour définir une solution répondant aux exigences de la protection de la vie privée et des renseignements personnels. Cette solution est le SQAG.

En effet, l'architecture globale[13] du SQAG a été conçue notamment de manière à limiter la collecte et la détention de renseignements nominatifs sur les détenteurs de certificats.

Les ministères et organismes demeurent les principaux détenteurs de renseignements personnels sur les citoyens. Ils ne détiennent pas plus de renseignements personnels en raison du fait qu'ils ont décidé d'avoir recours au SQAG.

Quant au service de certification, il ne détient aucun renseignement personnel, sauf dans le cas où le citoyen décidait de son propre chef de choisir son propre nom comme code d'usager.

Le SQAG prend en considération les préoccupations que la Commission avait émises dans son avis « Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementale du Secrétariat du conseil du trésor » d'août 2001, à savoir :

1- Le traçage
2- L'analyse de trafic
3- Les possibilités de couplage
4- La non-répudiation
5- La discrimination et la perte de contrôle sur l'information
6- L'usure des certificats
7- La constitution nécessaire de fichiers d'identité accessibles sur les réseaux.

La Commission donne son accord pour la réalisation du SQAG et se réserve la possibilité de procéder à une vérification du projet implanté et à une analyse plus approfondie au niveau de l'architecture détaillée.

Par ailleurs, comme un cadre juridique doit être établi incessamment afin de :

- définir les responsabilités de chaque intervenant dans le processus de délivrance des identifiants SQAG,

- énoncer les modalités juridiques relatives à la délivrance et à l'annulation des certificats de même que les règles d'accès à l'information et de protection des renseignements personnels qui régiront le SQAG,

la Commission demande d'être consultée sur l'un des points énumérés précédemment dès que cela est réalisé ou disponible.

[13] Compte tenu des délais, la Commission ne se prononce qu'en regard de l'architecture globale qui lui a été présentée.

En raison de ce qui précède, la Commission demande au SCT de lui fournir, d'ici le 30 mars prochain, ses commentaires en regard des recommandations décrites précédemment. Les recommandations en question sont :

Recommandation 1

Les ministères et les organismes utilisateurs du SQAG s'engagent contractuellement à ne pas utiliser le pseudonyme à d'autres fins que celles prévues par le SQAG.

Recommandation 2

Le SCT s'assure que le fournisseur de certificats mette en place les mesures nécessaires pour éviter les bris de confidentialité et de sécurité et qu'il obtienne un engagement de ses employés à respecter des normes rigoureuses.

Annexe 1

Les quinze recommandations que la Commission a émises dans son avis relatif à la solution intérimaire de l'ICPG sont :

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

2- que le Conseil du trésor examine 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;

3- que le Conseil du trésor recherche 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;

4- que les adhérents à l'ICPG soient informés des risques inhérents à l'utilisation de l'ICPG;

5- que le Conseil du trésor mette 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);

6- que le Conseil du trésor prenne les moyens nécessaires pour éviter une diffusion inappropriée des répertoires de l'ICPG;

7- que le Conseil du trésor :
- délimite les utilisations des renseignements contenus aux certificats et les modalités de conservation et de destruction,
- ne recueille aucune information relative à l'utilisation des certificats et clés,
- ne dresse aucun profil ou n'effectue aucune analyse de comportement à partir des informations nécessaires à la gestion de cette infrastructure,
- n'ajoute rien aux risques inhérents à l'ICPG en créant de nouveaux attributs du système;

8- que le Conseil du trésor ainsi que les ministères et organismes fournissent aux détenteurs de certificats un environnement de travail qui leur permet de respecter les engagements reliés à la sécurité;

9- que la Commission soit consultée sur le projet de catégorisation de l'information;

10- que le Conseil du trésor rédige et fasse signer les ententes à intervenir entre les partenaires de l'ICPG avant sa mise en service afin de respecter la Loi sur l'accès;

11- que le Conseil du trésor démontre à la Commission les assises légales qui lui permettent de colliger les données sur les mandataires d'autres entités gouvernementales et aux entreprises privées;

12- que le Conseil du trésor soumette 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;

13- que le Conseil du trésor prenne 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;

14- que le Conseil du trésor démontre à la Commission la nécessité d'identification par des tiers d'employés d'entreprises privées et d'employés de l'État;

15- que le Conseil du trésor lui soumette la Directive sur la gestion des clés et des certificats pour appréciation lorsqu'elle sera finalisée de même que tout autre document pertinent.

Annexe 2

Synthèse des orientations gouvernementales par niveau de confiance pour l'authentification des citoyens dans le cadre de la mise en place du gouvernement électronique

Niveau de confiance	Mode de vérification d'identité préalable	Renseignements requis pour la vérification d'identité	Mesure d'authentification recommandée
Élevé	Sur place (en personne)	Deux pièces officielles dont une avec photo	Combinaison d'un dispositif physique transportable (jeton ou carte à puce) et d'un secret (mot de passe ou NIP); l'ajout d'un certificat de clé publique pourrait également renforcer l'authentification
Moyen	À distance	Au moins deux secrets partagés[14], dont une information ayant été envoyée par la poste à l'adresse géographique connue du citoyen[15]	Combinaison d'un certificat de clé publique d'identification et d'un secret (mot de passe ou NIP)
Bas	À distance	Renseignements facultatifs	Combinaison d'un code d'usager et d'un secret (mot de passe ou NIP)

[14] Il s'agit de renseignements connus uniquement du citoyen ou susceptibles d'être connus d'un nombre limité de personnes dans l'entourage du citoyen. À titre d'exemple, on peut penser à une information inscrite sur un rapport officiel soumis par le citoyen au ministère ou à l'organisme (par exemple, la ligne 220 de la déclaration de revenus).

[15] D'autres moyens pourraient être utilisés en remplacement de l'envoi postal. Par exemple, la transmission d'un code par téléphone ou par courriel à une adresse préalablement connue pourrait être utilisée pour effectuer une vérification d'identité à distance de niveau de confiance moyen. La validation à distance d'une information préalablement recueillie en personne peut également être utilisée : c'est le cas lorsque la vérification d'identité à distance est effectuée par la comparaison d'une signature manuscrite inscrite sur un formulaire avec un spécimen de signature préalablement recueilli et conservé de manière sécuritaire.

Synthèse des orientations gouvernementales par niveau de confiance pour l'authentification des entreprises dans le cadre de la mise en place du gouvernement électronique

Niveau de confiance	Mode de vérification d'identité préalable	Vérification de l'existence de l'entreprise	Identification du représentant	Vérification du lien entre le représentant et l'organisation	Mesure d'authentification recommandée
Élevé	Sur place (en personne)	Extrait du registre, documents constitutifs	Vérification d'identité de niveau élevé	Document attestant le lien	Combinaison d'un dispositif physique transportable (jeton ou carte à puce) et d'un secret (mot de passe ou NIP); l'ajout d'un certificat de clé publique pourrait également renforcer l'authentification
Moyen	À distance	Extrait du registre	Vérification d'identité de niveau moyen	Document attestant le lien[16]	Combinaison d'un certificat de clé publique d'identification et d'un secret (mot de passe ou NIP)
Bas	À distance	Extrait du registre	Vérification d'identité de niveau bas	Document attestant le lien	Combinaison d'un code d'usager et d'un secret (mot de passe ou NIP)

[16] Le vérificateur peut confirmer le lien du représentant avec l'organisation en communiquant avec le signataire. La vérification à distance peut exiger en plus la réception d'un document officiel attestant le lien.