Gouvernement en ligne

Authentification des citoyens et des entreprises dans le cadre du gouvernement électronique

Orientations et stratégie

Août 2004

Québec

Table des matières

1. Introduction

L'administration gouvernementale électronique résulte d'un mouvement de fond sur le plan international en vue de moderniser les services publics. Ce mouvement est en plein essor au Canada, aux États-Unis et en Europe, où l'on voit se multiplier les initiatives de services électroniques à la population et aux entreprises. Au Québec, le gouvernement insiste fermement sur la nécessité de mettre en place un gouvernement électronique, afin d'offrir des services de meilleure qualité aux citoyens et aux entreprises en tirant profit des technologies de l'information.

Déjà en l'an 2000, l'adoption de la Loi sur l'administration publique avait fortement stimulé les investissements dans les projets de prestation électronique de services. D'une part, les ministères et organismes ayant une mission horizontale, tels que le Conseil du trésor et son secrétariat, ont réalisé plusieurs travaux en vue d'encadrer l'évolution des services électroniques, de les coordonner et de doter l'appareil gouvernemental de bases de fonctionnement partagées et communes. D'autre part, un grand nombre de ministères et d'organismes ont réalisé des projets ou planifient des investissements visant à permettre aux citoyens et aux entreprises de traiter électroniquement avec le gouvernement.

Jusqu'à maintenant, des services de nature informationnelle rendus à des utilisateurs de façon anonyme ont été mis en œuvre, tels que la diffusion d'informations publiques, la consultation de registres publics avec paiement, la vente de publications gouvernementales et la promotion culturelle ou touristique. Par ailleurs, encore peu de services exigeant une connaissance de l'identité de l'interlocuteur sont actuellement offerts au grand public, citoyens comme entreprises. Or, les applications projetées, aussi bien par les gouvernements étrangers que par les ministères et organismes québécois, montrent les signes d'une évolution incontournable vers des services électroniques personnalisés, c'est-à-dire pour lesquels l'utilisateur devra être authentifié. Ces services permettront tantôt de s'inscrire à un programme gouvernemental, tantôt de produire une déclaration, tantôt de consulter un dossier personnel ou d'entreprise ou encore d'obtenir un document officiel émis par le gouvernement (permis, attestation, etc.). Pour ces services, l'interlocuteur devra être correctement identifié.

Dans le monde électronique, une personne établit son identité à l'aide d'un identifiant qui permet de la reconnaître à distance. La disponibilité d'un tel identifiant est une nécessité pour la mise en œuvre de services électroniques personnalisés. L'adoption d'une stratégie en matière d'authentification des

citoyens et des entreprises se révèle donc essentielle pour soutenir adéquatement l'évolution de la prestation électronique de services du gouvernement.

Selon le cadre gouvernemental de gestion des ressources informationnelles[1], le Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles (SSIGRI) du Secrétariat du Conseil du trésor (SCT) a pour rôle de conseiller le gouvernement sur la stratégie à adopter en matière de gestion des ressources informationnelles et de faire connaître aux ministères et organismes les orientations retenues par le gouvernement. Plus précisément, en ce qui concerne la sécurité de l'information et des échanges électroniques, il revient au SSIGRI de coordonner l'application de la sécurité en proposant au Conseil du trésor les orientations stratégiques concernant la prestation de services aux citoyens et aux entreprises.

Le présent document énonce les orientations et la stratégie retenues par le SCT en matière d'authentification des citoyens et des entreprises dans le cadre de la mise en œuvre du gouvernement électronique. Ces orientations visent à répondre aux besoins des ministères et organismes pour les services électroniques qui nécessiteront l'identification des utilisateurs.

[1] Voir *Cadre de gestion des ressources informationnelles en soutien à la modernisation de l'Administration publique*, Secrétariat du Conseil du trésor, janvier 2002.

2. Concepts

a) Vérification d'identité

La vérification d'identité permet d'établir l'identité d'une personne. Elle peut être effectuée à partir de caractéristiques, de connaissances ou d'objets qu'une personne présente ou possède.

La vérification d'identité préalable

Dans un contexte de prestation électronique de services, la vérification d'identité sera surtout effectuée préalablement à la délivrance d'un **identifiant** à un citoyen ou à une entreprise. Lorsqu'elle se fera sur place (c'est-à-dire en présence d'une personne), elle sera habituellement effectuée par la vérification de pièces d'identité officielles. Cependant, lorsqu'elle se fera à distance, la vérification d'identité préalable sera généralement effectuée par la comparaison d'une quantité plus ou moins grande de renseignements fournis par l'utilisateur avec des informations que les ministères et les organismes ont en leur possession. Elle pourra également se faire par la présentation de pièces d'identité électroniques officielles lorsque celles-ci seront disponibles.

La vérification d'identité subséquente (voir « Authentification »)

La vérification d'identité subséquente, également appelée **authentification**, survient à chaque fois qu'une personne utilise un **identifiant** pour établir son identité.

Dans le présent document, le terme « vérification d'identité » renvoie à la vérification d'identité préalable. Le terme « authentification » fait quant à lui référence à la vérification d'identité subséquente.

b) Identifiant

L'identifiant est une information généralement associée à une personne, connue de celle-ci (mémorisée) ou contenue sur un support logique ou sur un support transportable dont elle est la détentrice, et qui permet son identification.

Le type le plus courant d'identifiant utilisé dans un contexte d'échange électronique est le code d'usager.

Les identifiants sont souvent associés à des informations secrètes tels un mot de passe ou un numéro d'identification personnel (NIP), lesquels sont plutôt des **authentifiants**.

c) Authentifiant

L'authentifiant est une information confidentielle détenue par une personne, qui permet son **authentification**.

Le mot de passe et le NIP sont des authentifiants.

d) Authentification

L'authentification est un acte qui permet de vérifier l'identité déclarée d'une personne. Dans un contexte de prestation électronique de services, la fonction d'authentification permettra à un ministère ou à un organisme de s'assurer qu'il communique avec le bon citoyen ou le bon représentant d'organisation.

L'authentification permet ainsi de faire la preuve que l'on a bien affaire au propriétaire légitime de l'**identifiant** présenté; elle est généralement effectuée en vérifiant l'exactitude de l'**authentifiant** associé à cet **identifiant**.

e) Habilitation/contrôle d'accès (aussi appelés « autorisation »)

L'habilitation permet à un ministère ou à un organisme d'attribuer des droits d'accès, des autorisations et des privilèges à une personne ou à un objet.

Dans le contexte d'un service électronique, l'habilitation est effectuée à la suite de l'**authentification** et consiste la plupart du temps à vérifier si une personne possède le droit d'accéder à certaines ressources (des applications, des documents, etc.), les privilèges qu'elle détient sur ces ressources (ex. : lecture, écriture, modification, destruction) ou l'existence de certains attributs (ex. : employé, administrateur).

L'exemple suivant illustre l'interrelation entre ces concepts. Dans cet exemple, la vérification d'identité est effectuée en personne au comptoir d'un ministère ou d'un organisme : l'identifiant prend la forme d'une carte d'accès et l'authentifiant prend la forme d'un NIP.

1. L'utilisateur produit des renseignements permettant d'établir son identité.

2. Le ministère ou l'organisme procède à la **vérification d'identité** (vérification d'identité préalable).

3. Un **identifiant** est remis à l'utilisateur, qui doit alors choisir un NIP.

4. Afin d'accéder à un service, l'utilisateur décline son identité en utilisant son **identifiant**.

5. Afin de prouver qu'il est bien le détenteur légitime de l'**identifiant** présenté, l'utilisateur entre ensuite son NIP, qui sert d'**authentifiant**.

6. Le système d'authentification **authentifie** l'utilisateur en validant l'exactitude de l'**authentifiant** présenté (vérification d'identité subséquente).

7. Le système du ministère ou de l'organisme vérifie les **droits d'accès** et les **autorisations** de l'utilisateur.

8. L'utilisateur peut accéder au service en fonction des droits et des privilèges qui lui sont accordés par le ministère ou l'organisme.

3. Portée du document

Les orientations et la stratégie présentées dans le présent document concernent l'authentification des citoyens et des entreprises[2] dans leurs communications électroniques avec le gouvernement du Québec. Elles visent à offrir des recommandations quant aux mesures et aux processus d'authentification que les ministères et les organismes devront mettre en place dans le cadre du déploiement du gouvernement électronique.

Il est important de noter que les orientations énoncées relatives aux processus de vérification d'identité ne s'appliquent que lorsque l'utilisateur est déjà connu du ministère ou de l'organisme qui effectue la vérification d'identité. Ainsi, les orientations visent les cas où il est possible de comparer certains renseignements à propos de l'utilisateur avec des informations que les ministères et les organismes possèdent déjà.

Dans ce contexte, le présent document ne vise pas à offrir des recommandations quant à l'ensemble des vérifications requises pour inscrire un citoyen ou une entreprise à un programme gouvernemental qui nécessiterait la validation de certains renseignements précis, ces processus étant souvent prévus dans une loi ou un règlement particulier.

Par ailleurs, ce document ne traite pas des fonctions de sécurité qui surviennent habituellement à la suite de l'authentification, notamment la fonction d'habilitation que les ministères ou les organismes doivent mettre en place afin de contrôler l'accès à leurs ressources ou de donner des autorisations à leurs utilisateurs[3]. Ce document ne traite pas non plus de l'authentification des objets ou de la confirmation de l'exactitude de l'identifiant d'un document technologique au sens de la Loi concernant le cadre juridique des technologies de l'information.

Enfin, ces orientations ayant été élaborées dans une optique générale, il est possible que les recommandations formulées ne répondent pas à certains besoins spécifiques. Un ministère ou un organisme devra ainsi définir l'ensemble de ses besoins en fonction des risques prévisibles avant d'appliquer les mesures proposées dans le présent document, et pourra également déployer des mesures différentes dans un contexte particulier.

---

[2] Dans ce document, sont visées par le terme « entreprise » les sociétés, les associations et les personnes morales. Pour l'application des orientations proposées en matière de vérification 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.

4. Éléments d'encadrement de l'authentification

Cadre légal

Au regard du cadre légal, plusieurs lois québécoises comportent des dispositions dont les ministères et les organismes doivent tenir compte dans l'élaboration de systèmes d'authentification. Deux d'entre elles ont des incidences majeures sur les échanges d'information par voie électronique :

- la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);
- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1).

Loi concernant le cadre juridique des technologies de l'information (LCCJTI)

L'objet de la LCCJTI consiste à « assurer notamment la sécurité juridique des communications effectuées au moyen de documents, l'équivalence fonctionnelle des documents et leur valeur juridique, quels qu'en soient les supports, ainsi que l'interchangeabilité de ces derniers[4] ». La LCCJTI « vise également à assurer la concertation en vue d'harmoniser les systèmes, les normes et les standards techniques permettant la communication au moyen de documents technologiques[5] ».

Les orientations en matière d'authentification électronique doivent faire en sorte de faciliter l'application de cette loi par les ministères et organismes, en particulier les dispositions relatives à la nécessité d'établir un lien avec les personnes qui communiquent par l'intermédiaire de documents technologiques. De même, les ministères et les organismes qui mettent en place des systèmes d'authentification devront s'assurer de respecter le cadre légal mis en place par cette loi.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (en abrégé, Loi sur l'accès)

Cette loi a un important volet destiné à assurer une protection aux renseignements personnels détenus par l'administration publique et doit être prise en considération dans les orientations à définir. À cet

[3] Des travaux sont en cours au SCT afin de définir un modèle d'habilitation de la sécurité.
[4] Selon le premier paragraphe des notes explicatives au début du texte de la Loi.
[5] *Idem*.

égard, les principes de gestion applicables, à partir du moment où des renseignements personnels sont exigés et lorsque la Loi sur l'accès ne prévoit pas d'exception[6], sont les suivants :

- être en mesure de démontrer la nécessité des renseignements demandés;
- limiter la détention (et donc l'utilisation) des informations à la durée nécessaire et aux fins déterminées initialement;
- restreindre la communication des renseignements personnels à des tiers, sauf avec le consentement de la personne ou si la Loi le prévoit;
- s'assurer du maintien de la qualité des données personnelles;
- prendre les mesures de sécurité propres à assurer le caractère confidentiel des renseignements;
- avoir une gestion transparente des renseignements personnels, notamment offrir aux citoyens un droit d'accès à leur dossier et la possibilité de rectifier les renseignements inexacts ou incomplets;
- assumer la responsabilité du traitement des données.

Bien que ces critères soient généraux, il sera nécessaire d'en tenir compte dans l'établissement de tout système d'authentification destiné aux citoyens et aux entreprises.

Cadre administratif

En plus du cadre légal, il convient de mettre en relief les différentes initiatives gouvernementales des dernières années qui visent à encadrer la sécurité dans le contexte de la mise en place du gouvernement électronique.

Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale (en abrégé, Directive sur la sécurité)

La Directive sur la sécurité énonce les principes directeurs à respecter, nomme les intervenants concernés, détermine les responsabilités des ministères et organismes et prévoit l'instauration de mécanismes de coordination et de collaboration appropriés pour une gestion adéquate de la sécurité de l'information numérique et des échanges électroniques dans l'administration publique.

[6] Selon le *Guide sur la mise en place de mécanismes d'identification électroniques*, Pierre Trudel et France Abran, Centre de recherche en droit public, Université de Montréal, pour le ministère de la Culture et des Communications, avril 2001.

Dans ses principes directeurs, la Directive sur la sécurité indique les aspects sur lesquels doivent porter les mesures de sécurité, soit la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité (DICAI).

Guide de catégorisation

Le SCT a élaboré, en septembre 2003, un nouveau guide de catégorisation permettant de qualifier un processus d'affaires selon la valeur de ses attributs de disponibilité, d'intégrité et de confidentialité. Cette qualification permet de déterminer, pour chaque processus d'affaires, un niveau de risque auquel sont associées des mesures de sécurité.

Aspects architecturaux

L'architecture d'entreprise gouvernementale (AEG) définit un modèle général de la prestation électronique de services du gouvernement. Ce modèle s'inscrit dans les stratégies d'évolution du gouvernement en appui à la Loi sur l'administration publique. L'AEG prévoit, entre autres, un moyen d'identification électronique pour les citoyens et les entreprises aux fins de l'utilisation de services électroniques.

L'AEG décrit les volets affaires, information et application. Certains principes touchant la sécurité et la protection des renseignements personnels sont énoncés :

- la prestation des services se fait dans un environnement sécurisé;
- les renseignements nominatifs ou les informations confidentielles ne sont demandés à la clientèle que lorsqu'ils sont explicitement requis par le processus d'affaires actif;
- les échanges de renseignements nominatifs ou d'informations confidentielles nécessitent le consentement de la clientèle, sauf lorsque les lois les autorisent ou lorsque des ententes existent;
- les documents échangés entre l'État et la clientèle sont signés lorsque cela est requis;
- l'intégrité de l'information est maintenue tout au long de son cycle de vie, peu importe son support.

Hormis ces principes inspirés de la Loi sur l'accès et de la LCCJTI, l'AEG relaye la définition d'orientations plus spécifiques aux travaux de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN).

Dans cette dernière architecture, huit fonctions de sécurité sont définies, dont la fonction d'identification/authentification. Les règles architecturales générales associées à l'identification/ authentification indiquent notamment d'utiliser :

- un mécanisme d'authentification approprié au type d'activité ou d'échange d'information ainsi qu'à la valeur des communications;
- des méthodes d'authentification à multiples mécanismes.

Par ailleurs, l'AGSIN détermine trois niveaux de confiance (élevé, moyen et bas) permettant de classifier des options possibles pour des mécanismes d'identification et d'authentification.

Infrastructure à clés publiques gouvernementale (ICPG)

Le Conseil du trésor a décidé en juin 1999 de doter le gouvernement du Québec d'une infrastructure à clés publiques gouvernementale (ICPG). Cette infrastructure est un système de gestion de certificats qui permettent à des personnes de se reconnaître à distance et d'effectuer des transactions électroniques sécuritaires. Le système permet, entre autres, de confirmer l'identité des personnes ou des dispositifs agissant dans un environnement électronique.

Dans sa phase intérimaire, l'ICPG vise à répondre aux besoins immédiats d'identification des employés, applications et dispositifs du gouvernement ainsi que de ses mandataires. Il est prévu que cette phase intérimaire prendra fin lors du déploiement d'une seconde phase comportant une solution cible s'adressant à l'ensemble des personnes en relation avec l'État, soit les employés, les mandataires, les citoyens et les entreprises.

Afin de préparer le déploiement de la solution cible de l'ICPG et de permettre la délivrance de certificats aux citoyens et aux entreprises, plusieurs travaux ont été réalisés :

- *Définition des orientations stratégiques sur la certification*

  Le SCT définit actuellement des orientations stratégiques concernant les services de certification gouvernementaux cibles qui visent à mettre à jour les orientations déjà adoptées en 1999. Ces orientations stratégiques permettront de mieux définir les responsabilités des ministères et organismes dans la mise en œuvre de l'ICPG, notamment dans leur utilisation des certificats.

- *Solution administrative et technique de l'ICPG*

Le ministère de la Justice et le SCT ont reçu, en février 2001, le mandat de définir une solution administrative et technique pour offrir un service de certification destiné aux employés et aux mandataires de l'État. Telle qu'elle est conçue, cette solution pourrait aussi permettre la délivrance de clés et de certificats aux citoyens et aux entreprises qui communiquent avec l'État par voie électronique. Cependant, la mise en place de cette solution n'est pas envisagée à court terme compte tenu de l'importance des investissements requis.

- *Common Certification Authority (CCA)*

Parallèlement à la conduite de ses propres travaux, le SCT a été invité à participer à une étude de faisabilité concernant la mise sur pied d'un service de certification pancanadien destiné aux organisations des secteurs publics ainsi qu'aux institutions financières canadiennes.

À la suite des travaux, l'Association canadienne des paiements, représentant les institutions financières, a décidé de ne pas adhérer au modèle élaboré. Cependant, le gouvernement fédéral se montre toujours intéressé à poursuivre des discussions avec les provinces de manière à permettre la mise en commun d'infrastructures technologiques de même que la reconnaissance de l'identifiant électronique fédéral (un certificat portant le nom de *epass*) par les provinces et les municipalités.

Étude de faisabilité du Service québécois d'authentification gouvernementale (SQAG)

Au cours de l'année 2001-2002, la Régie des rentes du Québec a réalisé, en collaboration avec d'autres ministères et organismes, une étude de faisabilité pour le déploiement d'un service québécois d'authentification gouvernementale (SQAG). Cette solution a été proposée afin de soutenir la mise en place d'une infrastructure permettant l'authentification du citoyen désirant s'inscrire aux services en ligne d'un ou de plusieurs ministères ou organismes, tout en s'assurant que ces mécanismes de sécurité maintiennent la convivialité des services et ne lui imposent pas la complexité de l'Administration gouvernementale. D'abord conçu pour les citoyens, le SQAG pourra évoluer pour également desservir les entreprises.

Avec l'appui du Comité stratégique des ressources informationnelles, le SCT a poursuivi le développement de la solution proposée par la Régie des rentes afin d'en rationaliser les coûts et de tirer profit des acquis gouvernementaux en matière de services communs.

5. Orientations gouvernementales sur l'authentification des citoyens et des entreprises dans le cadre du gouvernement électronique

L'une des raisons importantes qui limitent la capacité des ministères et organismes à offrir des services personnalisés réside dans la difficulté de mettre en ligne des services nécessitant un niveau de confiance adéquat au regard de l'authentification des utilisateurs, notamment lorsque ces services exigent la communication de renseignements personnels et confidentiels.

L'évolution des services électroniques du gouvernement exige que des moyens adéquats soient rendus disponibles pour identifier et authentifier les citoyens et les entreprises afin de soutenir des services électroniques personnalisés (qui nécessitent l'authentification de l'utilisateur). Les orientations relatives à la fonction d'authentification qui sont présentées dans cette section visent à répondre aux besoins des ministères et des organismes, qui s'en serviront pour mettre en place les mesures d'authentification requises par leur prestation électronique de services.

5.1. Authentification et anonymat

D'entrée de jeu, il est important de bien distinguer la prestation de services anonymes des services qui nécessitent une authentification. Les différents ministères et organismes du gouvernement du Québec connaissent bien la notion de services anonymes en mode électronique : depuis plusieurs années déjà, une multitude de services informationnels Web sont rendus par ces derniers, qui utilisent ce puissant mode de communication pour offrir aux citoyens et aux entreprises un ensemble de renseignements propres à leur mission. Ces services informationnels sont notamment utilisés pour rendre accessibles en ligne les formulaires gouvernementaux, que les citoyens et entreprises peuvent télécharger, imprimer, puis remplir.

Il faut donc distinguer ces services anonymes des services électroniques qui nécessitent de reconnaître l'utilisateur lors de ses visites en ligne. Ce sont ces derniers qui requièrent l'utilisation d'une fonction d'authentification.

5.2. L'authentification face aux différents besoins de sécurité

La fonction d'authentification doit également être définie par rapport aux différents besoins de sécurité, lesquels varient en fonction des risques. En effet, il faut comprendre que l'authentification

n'est pas un objectif en soi : elle est une fonction de sécurité[7] qu'il est nécessaire d'assurer afin de répondre aux besoins de confidentialité, d'intégrité ou de disponibilité[8] des documents technologiques détenus par les ministères et les organismes ou échangés avec eux.

Dans le cadre d'une prestation électronique de services avec les citoyens et les entreprises, la nécessité de disposer d'un moyen d'authentification prend ainsi sa source dans la sensibilité et la valeur de l'information communiquée. Plus l'information à communiquer est sensible et son contenu important, plus le niveau de confiance requis envers la fonction d'authentification sera élevé.

À cet effet, une catégorisation de l'information est nécessaire pour déterminer, entre autres, les besoins en matière de disponibilité, d'intégrité et de confidentialité (DIC). Le ministère ou l'organisme pourra ensuite entreprendre une analyse de risques[9] afin d'établir le seuil de tolérance acceptable pour son organisation et pour choisir les moyens d'authentification appropriés.

Cette relation entre l'authentification et les besoins de sécurité est importante. Trop souvent, l'authentification est simplement associée au besoin de confidentialité de l'information. Or, il peut également être nécessaire de déployer des mesures d'authentification afin de préserver l'intégrité et l'irrévocabilité d'une information, et ce, même si celle-ci est publique, par exemple pour empêcher une personne non autorisée d'y avoir accès et d'y apporter des modifications. C'est notamment le cas des renseignements inscrits dans les différents registres publics du gouvernement tels que le registre des lobbyistes[10] : alors qu'aucune mesure d'authentification ne sera nécessaire pour consulter le registre, des moyens adéquats d'authentification devront être mis en place afin de contrôler l'accès des personnes qui peuvent y faire des inscriptions.

5.3. Les niveaux de confiance de l'authentification

La fonction d'authentification peut être réalisée selon plusieurs niveaux de confiance établis selon le degré de sensibilité de l'information à protéger et les risques courus.

Les niveaux de confiance varieront notamment selon les processus et les technologies utilisées. Par exemple, il est généralement reconnu qu'un système d'authentification faisant appel à un processus de

---

7 Au même titre que d'autres fonctions de sécurité telles l'habilitation, la surveillance, etc.

8 Selon la nouvelle version du *Guide de catégorisation de l'information* conçu par le SCT, on doit aussi considérer le besoin d'irrévocabilité des documents technologiques lors d'un exercice de catégorisation de l'information. Le guide peut être consulté à l'adresse **www.inforoute-gouvernementale.qc**.

9 Le SCT recommande l'utilisation de la méthode d'analyse de risques Méhari.

10 www.lobby.gouv.qc.ca

vérification d'identité en personne permet d'obtenir une meilleure confiance dans l'authentification qu'un processus de vérification d'identité à distance.

La combinaison de facteurs d'authentification[11] peut aussi contribuer à augmenter le niveau de confiance de l'authentification, au même titre que les processus de vérification de l'identité mis en place et que la robustesse des technologies utilisées. Par exemple, la combinaison d'une information connue de l'utilisateur et d'un jeton matériel (par exemple, un jeton USB ou une carte à puce) permet habituellement d'augmenter le niveau de confiance d'une mesure d'authentification.

Il est possible de classer les niveaux de confiance de l'authentification requis par la prestation électronique de services selon les critères suivants. Ces critères sont toutefois non exhaustifs : il revient à chaque ministère ou organisme de déterminer, compte tenu de ses processus d'affaires et des risques qu'il est prêt à assumer, le niveau de confiance de la mesure d'authentification qu'il entend mettre en place.

Aucune authentification requise (service anonyme)

Un service électronique de type informationnel s'inscrit dans cette catégorie. Dans le cadre d'un service anonyme, aucune donnée n'est recueillie par le ministère ou l'organisme quant à l'identité de l'utilisateur du service électronique. Aucun identifiant n'est requis pour l'utilisateur.

Authentification de niveau de confiance bas

Un service électronique peut nécessiter une authentification de niveau de confiance bas lorsqu'une vérification d'identité formelle n'est pas essentielle, mais qu'il peut être utile de reconnaître l'utilisateur à chaque fois qu'il utilise le service électronique.

C'est notamment le cas des services personnalisés en fonction des préférences de l'utilisateur. À titre d'exemple, on pourrait penser à un service de portail où le citoyen pourrait, à l'aide d'un pseudonyme qu'il choisit, s'inscrire, puis choisir un mode d'affichage personnalisé selon ses goûts et préférences. Dans ce cas, un identifiant lui serait délivré afin de pouvoir le reconnaître à chacune de ses visites.

[11] Les facteurs d'authentification comprennent ce qu'une personne connaît (par exemple, un mot de passe), ce qu'elle possède (par exemple, une carte à puce) et ce qu'elle est (par exemple, une mesure biométrique). Bien que l'augmentation du nombre de facteurs permette habituellement d'augmenter le niveau de confiance de l'authentification, il ne s'agit pas du seul critère qui doive être retenu lorsque vient le moment d'évaluer ce niveau de confiance pour un processus d'authentification donné.

Cependant, dans cet exemple, aucune vérification d'identité n'a besoin d'être faite préalablement à la délivrance de l'identifiant, puisqu'il s'agit d'un pseudonyme.

Pourraient aussi s'inscrire dans cette catégorie les services électroniques destinés à la vente de biens et de services où une inscription est nécessaire afin de conserver des informations de base au sujet de l'utilisateur, notamment des données relatives au mode de paiement privilégié par le client ainsi que son adresse de livraison (pourrait être un casier postal). Dans cet exemple, l'identité de l'utilisateur n'est pas vérifiée préalablement à la délivrance de l'identifiant. Cependant, le service s'assure de la capacité de payer de l'utilisateur par la validation de sa carte de crédit.

Authentification de niveau de confiance moyen

Un service nécessitera un niveau de confiance moyen lorsque le ministère ou l'organisme devra s'assurer, avec un degré de certitude raisonnable, de l'identité de l'utilisateur afin de lui offrir le service.

À titre d'exemple, on peut penser à un site Web où le citoyen pourrait consulter certains renseignements provenant de son dossier. Le ministère ou l'organisme devrait alors utiliser des mesures d'authentification afin de s'assurer que les renseignements inscrits au dossier ne sont visualisés que par la personne concernée.

Un ministère ou un organisme pourra également choisir ce niveau de confiance dans le cadre de services où des données, bien qu'étant publiques, ne peuvent être modifiées que par une personne préalablement identifiée et autorisée : on peut penser aux renseignements inscrits au Registre foncier ou au Registre des droits personnels et réels mobiliers.

Authentification de niveau de confiance élevé

Le niveau de confiance élevé devrait être privilégié lorsque le ministère ou l'organisme doit s'assurer, avec un très grand degré de certitude, de l'identité de l'utilisateur afin de lui offrir un service électronique.

Le niveau de confiance élevé est nécessaire en général pour des services destinés à des employés de l'État ou à des partenaires d'affaires du gouvernement. Il sera particulièrement important pour assurer la protection de renseignements relatifs, par exemple, à la sécurité d'État.

Dans le cas des services aux citoyens et aux entreprises, on peut penser à des services où sont en jeu des sommes d'argent importantes. Il pourrait également s'agir de services permettant à une personne de consulter ou de modifier des renseignements de nature très sensible ou confidentielle qui représentent un risque élevé ou très élevé, par exemple des renseignements de santé.

Il revient à chaque ministère ou organisme de mettre en place une fonction d'authentification appropriée au niveau de confiance recherché, notamment par un exercice de catégorisation de l'information et d'analyse de risques. Il pourra ensuite se référer aux orientations ci-après énoncées pour faire le choix du type d'identifiant approprié.

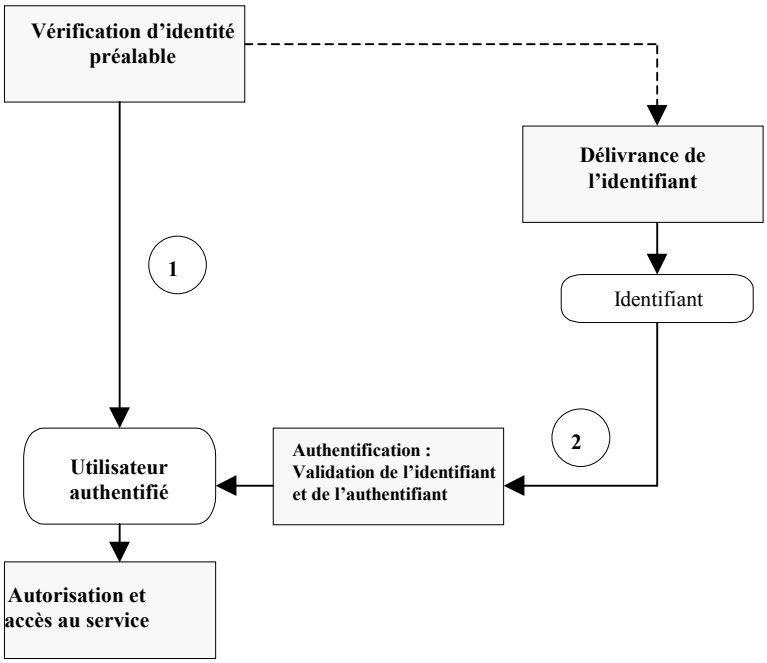
5.4. Éléments constituants de la fonction d'authentification et orientations

Les éléments qui constituent la fonction d'authentification comprennent :

- le processus de vérification d'identité préalable;
- la délivrance d'un identifiant associé à un authentifiant;
- la présentation de l'identifiant et la validation de l'authentifiant (la fonction d'authentification).

Il est important de noter que ces constituants peuvent être facultatifs, selon le type de processus d'authentification privilégié. En effet, la délivrance d'un identifiant de niveau de confiance bas se fait habituellement sans vérification d'identité préalable. De même, l'authentification d'une personne dans le cadre d'un service qui requiert un niveau de confiance moyen pourrait être faite sans l'utilisation d'un identifiant propre à cette fonction. Ce serait le cas si, par exemple, un service était conçu pour procéder à la vérification d'identité complète de l'utilisateur à chacune de ses visites plutôt que de lui délivrer un identifiant pouvant être utilisé subséquemment (par exemple, le service de changement d'adresse du ministère du Revenu).

Le schéma suivant illustre les deux cheminements possibles pour accéder à un service électronique qui nécessite une authentification :



1. **Accès au service directement à la suite d'une vérification d'identité préalable** : le service exige une vérification d'identité dont le résultat n'est valide que pour un seul accès. Au prochain accès, le citoyen devra passer à nouveau par une vérification d'identité. Un service permettant de traiter un événement ponctuel tel un changement d'adresse pourrait fonctionner de cette manière.

   Cette façon de procéder a l'avantage d'éviter d'avoir à gérer la compromission ou l'oubli des identifiants/authentifiants. Cependant, ce processus est plus lourd pour l'utilisateur puisqu'il doit, à chacune de ses visites, entrer un nombre assez important de renseignements.

2. **Accès au service à l'aide d'un identifiant** : l'identifiant peut avoir été délivré avec ou sans processus de vérification d'identité préalable, selon le niveau de confiance recherché. Rappelons cependant que les niveaux de confiance moyen et élevé nécessitent une identification préalable de l'utilisateur.

   Cette façon de procéder nécessite de mettre en place des mécanismes de gestion des identifiants/authentifiants compromis ou oubliés. Toutefois, l'utilisation d'un identifiant

simplifie la confirmation de l'identité lors des accès subséquents au service, c'est-à-dire lors de l'authentification proprement dite. En effet, lors de ses visites subséquentes, l'utilisateur n'a plus à entrer de renseignements personnels pour prouver son identité, il n'a qu'à utiliser son identifiant.

Il peut être intéressant de noter que la vérification d'identité effectuée préalablement à la délivrance d'un identifiant (2) peut faire appel aux mêmes processus que celle effectuée lors d'un accès direct à un service (1). Les recommandations émises dans le présent document pour la vérification d'identité sont valables pour les deux processus.

5.4.1. Les processus de vérification d'identité préalable

La vérification d'identité[12] vise à s'assurer que la personne est bien celle qu'elle prétend être. La méthode de vérification d'identité définit les façons de faire en ce qui concerne les données à vérifier (informations, caractéristiques, connaissances) et les méthodes de collecte (sur place ou à distance) afin de qualifier le niveau de certitude quant à l'identité de la personne. Deux éléments clés étroitement liés de la vérification d'identité sont considérés dans les présentes orientations, soit le mode de vérification et les informations requises.

Le mode de vérification est important, car il détermine les types d'information et de supports qui peuvent être utilisés. En fait, la vérification d'identité peut être faite dans un mode sur place ou dans un mode à distance. Une vérification sur place permet de vérifier visuellement l'identité à partir de pièces délivrées par des autorités reconnues, comme un passeport, un permis de conduire, un certificat de naissance ou autre. La vérification à distance est souvent faite par voie électronique mais peut aussi utiliser des moyens comme le téléphone ou le courrier postal. Elle permet généralement de vérifier des informations qui sont connues à la fois de la personne à identifier et du prestataire de services qui procède à l'identification. Plus l'information présentée pour établir l'identité est secrète, plus la preuve d'identité est fiable.

Les informations nécessaires à la vérification sont différentes selon que l'on identifie une personne en tant que citoyen ou en tant que représentant d'une entreprise. Pour un citoyen, les preuves d'identité

[12] Il importe de distinguer la vérification d'identité destinée à la prestation électronique de services de celle requise pour inscrire le citoyen à un programme ou à un service gouvernemental. La présente section ne vise pas à donner des orientations gouvernementales sur les processus de vérification d'identité pour fins d'inscription aux programmes et services, qui sont souvent prévues par des lois ou des règlements. Les présentes orientations visent plutôt la vérification d'identité permettant de reconnaître, en ligne, un utilisateur déjà connu d'un ministère ou d'un organisme.

admises seront, par exemple, des pièces officielles d'identité avec ou sans photo ou des informations personnelles.

Pour une entreprise[13], les informations requises consistent plutôt en un document d'immatriculation au registre des entreprises[14], un document attestant de l'autorisation de la personne et une preuve de l'identité de la personne qui demande l'obtention d'un identifiant électronique.

Le tableau qui suit énonce les orientations quant au processus de vérification d'identité préalable pour un citoyen. Il s'agit donc de recommandations sur la manière de vérifier l'identité d'une personne préalablement à la délivrance d'un identifiant. C'est cet identifiant qui, subséquemment, sera utilisé par le citoyen pour communiquer électroniquement avec le ministère ou l'organisme.

Niveau de confiance de l'authentification	Mode de vérification d'identité préalable	Informations requises
Élevé	Sur place (en personne)	Deux pièces officielles dont une avec photo
Moyen	À distance	Au moins deux secrets partagés[15], dont une information ayant été envoyée par la poste à l'adresse géographique connue du citoyen[16]
Bas	À distance	Renseignements facultatifs

Tableau 1 – Orientations sur la vérification d'identité préalable du citoyen par niveau de confiance

[13] Les entreprises visées par le présent document sont celles exploitées par des organisations (personnes morales, sociétés ou associations). Le travailleur autonome (c'est-à-dire exploitant une entreprise individuelle) qui agit sous ses nom et prénom verra plutôt sa vérification d'identité effectuée comme celle du citoyen (personne physique).

[14] *Loi sur la publicité légale des entreprises individuelles, des sociétés et des personnes morales* (L.R.Q., c. P-45).

[15] 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 ainsi que par le ministère ou l'organisme. 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).

[16] 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.

Il convient de noter que les orientations en matière de vérification d'identité proposent un processus minimum pour chacun des niveaux de confiance. Cependant, dans le cadre d'un service nécessitant un niveau de confiance moyen, par exemple, un ministère ou un organisme pourrait tout de même choisir de procéder à une vérification d'identité sur place, notamment dans le cas où des processus adéquats sont déjà en place et sont facilement réutilisables.

Pour une entreprise, les vérifications relatives à son identification et à son existence ainsi que celles relatives au lien entre l'entreprise et la personne qui la représente s'ajoutent à la vérification de l'identité de cette dernière. Le tableau qui suit illustre le type d'élément requis selon le niveau de confiance.

Niveau de confiance	Mode de vérification d'identité préalable	Existence de l'entreprise	Identification du représentant	Lien entre le représentant et l'organisation
Élevé	Sur place (en personne)	Extrait du registre, documents constitutifs	Vérification d'identité de niveau élevé (voir Tableau 1)	Document attestant le lien
Moyen	À distance	Extrait du registre	Vérification d'identité de niveau moyen (voir Tableau 1)	Document attestant le lien[17]
Bas	À distance	Extrait du registre	Vérification d'identité de niveau bas (voir Tableau 1)	Document attestant le lien

Tableau 2 - Vérification d'identité préalable de l'entreprise par niveau de confiance

5.4.2. Les processus de délivrance de l'identifiant

Comme la méthode de vérification d'identité, le processus de délivrance de l'identifiant est un élément constituant important de la fonction d'authentification. Il permet d'établir le lien entre le détenteur et l'identifiant. Ce lien est maintenu tout au long du cycle de vie de l'identifiant lors de l'attribution et durant les opérations subséquentes.

[17] 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.

Le processus de délivrance peut dépendre de la méthode de vérification d'identité ainsi que des caractéristiques de l'identifiant, notamment du fait qu'il réside sur un support matériel ou non. Lorsqu'il y a un support transportable, celui-ci doit être remis au détenteur en s'assurant qu'il s'agit bien de la bonne personne. Il peut être remis lors de la vérification d'identité en personne ou par d'autres moyens en s'assurant qu'une trace de la remise est conservée. Dans le cas d'un identifiant sans support transportable, il peut être remis au cours d'une session en ligne en s'assurant qu'il n'y a pas d'interruption de session afin d'éviter toute interception ou erreur de remise. L'identifiant sans support transportable peut également être remis en différé en prenant des mesures pour s'assurer qu'il est bien fourni à la bonne personne. Les situations suivantes sont typiques :

- remise directe de l'identifiant numérique lors d'une vérification d'identité sur place (dans le cas d'un identifiant sur support transportable);
- remise à distance au cours d'une même session sécurisée d'échange par voie électronique;
- remise en différé et à distance (par exemple, transmission d'un mot de passe par courriel ou par téléphone).

L'identifiant se concrétise par une solution technologique qui peut comprendre un ou plusieurs des composants suivants :

- un code d'usager;
- un certificat de clé publique;
- un jeton physique transportable (clé USB, carte à puce, etc.);
- des moyens biométriques.

La délivrance de l'identifiant est souvent associée au choix ou à la remise d'un authentifiant tel un mot de passe ou un NIP. Celui-ci permet de s'assurer que la personne qui présente l'identifiant en est bien le détenteur légitime.

Chaque solution technologique possède des caractéristiques intrinsèques de sécurité qui permettent d'associer au mécanisme d'identification des qualités sur le plan de l'intégrité des données qu'il contient et des fonctions de sécurité qu'il soutient. En se basant sur ces caractéristiques, l'identifiant peut être associé à un niveau de confiance.

L'AGSIN établit une telle association entre les niveaux de confiance et les caractéristiques intrinsèques des technologies utilisées. Cependant, certaines mesures inventoriées par l'AGSIN ne

sont pas toujours appropriées pour des utilisateurs comme les citoyens et les entreprises[18]. Par exemple, alors que l'usage de la biométrie pourrait être envisagé dans certains cas pour des employés de l'État (ex. : pour contrôler l'accès à un système stratégique pour la sécurité de l'État), cette technologie semble moins appropriée pour les citoyens dans le cadre de leurs communications avec le gouvernement[19].

Dans le cadre des communications électroniques avec les citoyens et les entreprises, il est ainsi recommandé d'adopter les mesures d'authentification suivantes :

- Pour le niveau élevé, des mesures d'authentification combinant l'usage 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.
- Pour le niveau moyen, des mesures d'authentification combinant l'usage d'un certificat de clé publique d'identification et d'un secret (mot de passe ou NIP).
- Pour le niveau bas, des mesures d'authentification combinant un code d'usager et un secret (mot de passe ou NIP).

Le type d'identifiant doit être choisi de manière que ses caractéristiques correspondent au niveau de confiance requis pour la prestation électronique de services.

5.4.3. La présentation de l'identifiant et la validation de l'authentifiant

Le processus d'authentification est complété par la présentation de l'identifiant. Cette fonction consiste à s'assurer que l'identifiant est toujours valide et qu'il est utilisé par la bonne personne en vérifiant l'exactitude de l'authentifiant (le mot de passe, par exemple). Tout comme pour les autres composantes du processus d'authentification, la validation de l'authentifiant peut faire appel à des technologies et à des processus qui ont une influence sur le niveau de confiance de l'authentification.

[18] L'AGSIN dresse un inventaire des mesures d'authentification qu'il est possible de mettre en place pour authentifier aussi bien les employés de l'État que les citoyens et les entreprises. Par ailleurs, l'AGSIN couvre les échanges électroniques non seulement avec des utilisateurs externes, mais également entre les employés de l'État. Les présentes orientations ont donc pour objectif de déterminer quelles mesures d'authentification, parmi celles proposées par l'AGSIN, sont les plus appropriées pour les citoyens et les entreprises dans le cadre de leurs échanges avec le gouvernement du Québec.

[19] Notons que les orientations énoncées dans ce document constituent des recommandations d'application générales. Un ministère ou un organisme pourrait, dans un contexte particulier, mettre en place des mesures d'authentification différentes de celles recommandées.

5.5. Synthèse des orientations gouvernementales par niveau de confiance

Les tableaux des pages suivantes fournissent une synthèse des orientations retenues pour chaque élément constituant le processus d'authentification, en tenant compte des différents niveaux de confiance. Le principe de base à respecter dans le choix d'un processus d'authentification consiste à s'assurer que l'ensemble des éléments constituants sont définis et qu'ils correspondent au niveau de confiance requis par la prestation électronique de services.

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[20], dont une information ayant été envoyée par la poste à l'adresse géographique connue du citoyen[21]	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)

[20] 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).

[21] 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[22]	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)

[22] 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.

5.6. Exemples de processus de vérification d'identité dans des services offerts par le gouvernement du Québec

Le gouvernement du Québec offre déjà plusieurs services électroniques par l'intermédiaire d'Internet. La présente section décrit quelques exemples de processus de vérification d'identité utilisés par les ministères et les organismes.

Consultation du dossier de bourse

Les boursiers du Fonds de recherche sur la nature et les technologies[23] peuvent consulter en ligne leur dossier. Pour ce faire, un identifiant ainsi qu'un mot de passe est délivré à la suite d'une vérification d'identité à distance effectuée par corroboration de renseignements. Ainsi, les personnes désirant obtenir un code d'usager doivent remplir un questionnaire en ligne dans lequel sont saisis certains renseignements dont la date de naissance, le nom de fille de la mère et l'année d'obtention du premier diplôme.

Un code d'usager est transmis par courriel au boursier, qui peut alors l'utiliser pour consulter son dossier.

Compte tenu des orientations précédemment énoncées, ce processus d'authentification peut être considéré comme d'un niveau de confiance bas puisqu'il repose sur l'utilisation d'un mot de passe. Il utilise toutefois un processus de vérification d'identité préalable qui lui confère un degré de sécurité plus important que certains autres systèmes de ce type.

Inscription à certains registres publics

Le Registre des droits personnels et réels mobiliers (RDPRM), le Registre foncier et le Registre des lobbyistes sont représentatifs de cas où une signature électronique est requise sur les demandes d'inscription. L'attribution d'un identifiant à un utilisateur pour l'inscription au registre demande une vérification d'identité faite sur place par un responsable désigné, ou encore, faite au moyen d'une confirmation par un tiers de confiance. Ce dernier cas renvoie notamment aux certificats délivrés aux notaires pour l'inscription au Registre foncier.

[23] www.fcar.qc.ca

Dans le cas du RDPRM, dont les utilisateurs sont principalement des entreprises, le processus de vérification d'identité sur place (en personne) comporte également la vérification de l'existence de l'entreprise de même que la vérification du lien entre l'entreprise et son représentant.

L'activation du certificat s'effectue selon une procédure impliquant l'échange de secrets partagés entre la personne et le fournisseur de certificats, dont la remise en main propre d'un code secret. Le certificat, résidant sur le disque dur de l'usager, est utilisé pour signer électroniquement un document. Une fois signé, le document est transmis de manière sécurisée[24]. À la réception du message, la signature du document est validée et le document est conservé avec cette signature. Cette façon de faire permet d'identifier le signataire et de préserver son lien avec le document.

Selon les orientations proposées précédemment, ces services utilisent des mesures d'authentification de niveau de confiance moyen, et ce, même si une vérification d'identité sur place est utilisée. En effet, puisque le certificat est emmagasiné sur le disque dur (et non sur un support transportable), l'authentification qui résultera de son utilisation sera considérée comme de niveau de confiance moyen.

[24] La sécurisation est faite par chiffrement du message ou de la session.

6. Stratégie gouvernementale en matière d'authentification des citoyens et des entreprises pour la mise en place du gouvernement électronique

Les gouvernements d'autres provinces canadiennes, le gouvernement fédéral ainsi que les gouvernements d'autres pays sont engagés dans une modernisation des services de l'État et dans la mise en œuvre d'une prestation électronique de services, afin de tirer pleinement profit des avantages qu'offre l'usage des technologies. Le Québec ne fait pas exception à cette tendance; la section précédente présentait d'ailleurs des exemples d'initiatives de ministères du gouvernement du Québec ayant, au cours des dernières années, amorcé la transformation de leur offre de service afin de permettre la mise en œuvre d'un véritable gouvernement électronique.

Il est maintenant nécessaire de concilier, d'une part, la responsabilité des ministères et organismes de déployer leurs propres mesures de sécurité, dont des mesures d'authentification, et, d'autre part, la volonté ferme du gouvernement de simplifier la vie du citoyen et de tenter de réduire le nombre de processus de vérification d'identité auxquels il devra se soumettre. Dans cette optique, les différents travaux amorcés par le gouvernement du Québec pour permettre la mise en œuvre de l'Administration électronique doivent maintenant être soutenus par une action organisée et cohérente en matière d'authentification des citoyens et des entreprises.

6.1. Enjeux majeurs liés à l'authentification

L'authentification des citoyens et des entreprises aux fins de la prestation électronique de services du gouvernement met en évidence des enjeux majeurs concernant l'évolution des services électroniques gouvernementaux.

Enjeux quant à l'évolution du gouvernement électronique

La disponibilité de moyens d'identification et d'authentification des citoyens et des entreprises est une nécessité pour permettre l'évolution du gouvernement électronique en vue de couvrir davantage de situations d'échanges, dont celles impliquant des renseignements personnels et confidentiels ainsi que celles impliquant des documents ou des consentements.

Cette évolution est d'ailleurs souhaitée par la population du Québec, comme l'indiquent les conclusions d'un récent sondage réalisé par le CEFRIO[25] :

> Ce qui n'empêche toutefois pas les Québécois d'aspirer à mieux en matière de gouvernement électronique. En effet, bon nombre espèrent que l'administration publique *webifie* progressivement une portion croissante de ses services. À titre d'exemple, 78 % des utilisateurs présents et futurs d'Internet jugent « tout à fait » ou « assez prioritaire » que les ministères et organismes rendent possible la demande ou le renouvellement de permis en ligne. De plus, une forte majorité (69 %) des gens d'affaires québécois branchés se disent intéressés par des services électroniques de remplissage ou d'acheminement en ligne de formulaires.
>
> Ainsi, même dans sa plus simple expression, la mise en place de l'administration électronique répond à une réelle demande.

Pour l'instant, peu de services électroniques personnalisés aux citoyens et aux entreprises sont offerts par les ministères et organismes. Pourtant, le volume des échanges d'information à contenu personnalisé est considérable, et des bénéfices importants sont associés à la mise en ligne de ce type de service.

Enjeux quant à la qualité des services électroniques

La mise en œuvre de services électroniques pour les citoyens et les entreprises s'inscrit dans le mouvement de modernisation des services de l'État sous-jacent à la Loi sur l'administration publique. Or, c'est en vue d'affirmer la priorité accordée à la qualité des services aux citoyens que cette loi instaure un nouveau cadre de gestion qui indique, entre autres, aux ministères et organismes de chercher à simplifier le plus possible les règles et les procédures qui régissent la prestation de services.

Simplicité d'utilisation des services électroniques

Dans l'optique de faciliter la vie du citoyen et de répondre aux objectifs de la Loi sur l'administration publique, les moyens d'identification et d'authentification doivent contribuer à simplifier l'utilisation des services électroniques. Le gouvernement du Québec devra, à cet égard, adopter une stratégie permettant une harmonisation dans la façon d'établir son identité auprès des différents ministères et organismes. Cette simplicité d'utilisation des moyens

[25] www.cefrio.qc.ca/rapports/Net_Gouv_2003.pdf, mai 2003, p. 50.

d'authentification est une nécessité pour assurer l'adhésion des citoyens aux services gouvernementaux électroniques.

Mobilité de l'utilisateur

Bien que le gouvernement ait fait beaucoup d'efforts pour permettre aux familles québécoises d'avoir accès à Internet[26], il n'en demeure pas moins qu'actuellement, 49 % des citoyens n'ont pas accès à Internet à la maison, selon une récente étude du CEFRIO[27].

Selon la même étude, la situation est meilleure pour les entreprises québécoises de cinq employés et plus, puisque 71 % d'entre elles sont branchées à Internet. Cependant, près d'un travailleur autonome sur trois (30 %) n'a même pas accès à un ordinateur pour son travail.

Dans ces circonstances, la stratégie gouvernementale d'authentification devra permettre aux usagers des services gouvernementaux d'être mobiles et de communiquer en ligne avec le gouvernement à partir de plusieurs endroits, que ce soit les points de service gouvernementaux, les bibliothèques publiques, les maisons d'enseignement, les cafés Internet ou tout simplement à partir de l'ordinateur d'un parent ou d'un ami.

Confiance des utilisateurs

Il importe que les moyens d'identification et d'authentification retenus permettent de créer un climat de confiance rassurant pour les utilisateurs quant à la sécurité des échanges d'information et au respect rigoureux des lois. En effet, plusieurs enquêtes et sondages[28] ont démontré que de nombreux utilisateurs de services par Internet perçoivent des risques élevés quant à la sécurité des transactions et à la protection des renseignements personnels. Cette perception est suffisamment forte pour qu'un grand nombre d'entre eux s'abstiennent de faire des transactions par Internet. D'ailleurs, les médias contribuent à alimenter cette perception en révélant régulièrement de nouvelles fraudes.

---

[26] Le programme « Branchez les familles », qui s'est échelonné du 1er mai 2000 au 31 mars 2001, a permis 296 000 branchements à Internet et 217 000 achats d'équipement informatique par les familles québécoises.

[27] « La majorité des citoyens adultes (60 %) ont accès à un ordinateur à la maison. Tous ne sont cependant pas branchés : 51 % des citoyens ont accès à Internet à partir de la maison. » (www.cefrio.qc.ca/rapports/Net_Gouv_2003.pdf, mai 2003, p. 16.)

[28] Au Québec, la plus récente étude du CEFRIO montre que le principal frein à l'utilisation d'Internet pour obtenir des services gouvernementaux est la crainte des citoyens et des entreprises relative à la vie privée et à la sécurité (regroupées, ces craintes ont été évoquées par 42 % des citoyens, 27 % des entreprises et 33 % des travailleurs autonomes). (http://www.cefrio.qc.ca/rapports/Net_Gouv_2003.pdf, mai 2003, p. 37.)

Par ailleurs, certaines statistiques montrent qu'il existe effectivement un niveau élevé de risques reliés à Internet, par exemple le taux de fraude par carte de crédit, la propagation épidémique de certains virus informatiques et le nombre élevé de tentatives d'intrusion dans des systèmes ou dans des sites Internet, notamment des sites du gouvernement du Québec. Ces risques sont donc bien réels.

Malgré la croissance continue des services électroniques par Internet, un potentiel important de services en ligne semble donc sous-exploité en raison notamment :

- d'un manque de confiance de la part de nombreux utilisateurs;
- d'un besoin de mécanismes sûrs de sécurisation, simples à utiliser, fortement répandus et peu coûteux pour l'utilisateur;
- d'exigences élevées de sécurité et de protection des renseignements personnels pour plusieurs types de transactions, dont celles demandant une signature.

La perception des citoyens et des entreprises à l'égard des moyens mis à leur disposition par le gouvernement sera donc critique pour le succès de la prestation électronique de services.

Technologies adéquates

Les technologies utilisées contribuent à la qualité des solutions d'authentification. Ainsi, des technologies répondant aux critères suivants sont à privilégier :

- fiabilité démontrée;
- utilisation répandue;
- compatibilité avec les principaux logiciels disponibles sur le marché;
- respect des normes d'industrie et suivi des tendances de l'évolution technologique;
- coûts abordables;
- intégration non intrusive à l'environnement technologique de l'utilisateur.

Enjeux quant à la sécurité juridique et technologique

Le développement de services personnalisés se heurte à la difficulté majeure d'identifier et d'authentifier de façon sûre les citoyens et les entreprises en mode virtuel. En effet, le défi d'offrir des services électroniques personnalisés est de taille, puisque ceux-ci demandent la communication de

renseignements personnels ou confidentiels sur Internet, un réseau ouvert mondialement. Les transactions doivent aussi répondre aux exigences des lois quant à l'établissement d'un lien formel entre un document ou un acte et la personne qui en est l'auteur (citoyen, entreprise, ministère ou organisme, ou autre organisation).

Compte tenu de la Loi sur l'accès, le gouvernement du Québec se doit de faire en sorte que les moyens d'identification et d'authentification qu'il retient pour ses services électroniques personnalisés assurent un niveau de protection adéquat. Sur ce plan, les moyens retenus doivent notamment minimiser les possibilités :

- de collecte de renseignements personnels à partir du moyen d'identification ou des mécanismes reliés à ce moyen;
- de couplage de données lorsque cela n'est pas permis;
- de traçage et de suivi des échanges d'information à des fins non autorisées.

Les moyens d'authentification qui seront mis à la disposition des citoyens et des entreprises devront tenir compte des principes de protection des renseignements personnels édictés par les lois.

Toutefois, la manière traditionnelle d'assurer la protection des renseignements personnels pose des difficultés dans l'univers électronique. Un groupe de travail gouvernemental a donc été mis sur pied à l'automne 2002 afin de fournir des recommandations sur la question de la protection des renseignements personnels dans le contexte de la mise en place du gouvernement électronique. Ce groupe de travail a relevé des questions problématiques relatives à l'applicabilité du cadre juridique actuel aux échanges électroniques, particulièrement dans la prestation de services intégrés impliquant plusieurs ministères et organismes. Il a notamment soulevé la difficulté de partager des renseignements d'identification entre les différents programmes des ministères et des organismes, qui, sauf lorsque cela est prévu dans la loi ou dans des ententes autorisées par la Commission d'accès à l'information, ne peuvent pas partager de renseignements aussi simples que le nom et l'adresse d'un citoyen. Ce principe de cloisonnement des programmes administratifs a pour effet de forcer la collecte répétée des mêmes données auprès du citoyen. Dans un contexte d'authentification gouvernementale, un tel cloisonnement des programmes fera donc en sorte que le citoyen devra se soumettre à une multitude de processus de vérification d'identité.

L'une des recommandations du groupe de travail vise la création d'espaces de circulation de l'information. Ces espaces de circulation permettraient de faciliter le partage limité de certains

renseignements entre des ministères et organismes faisant partie du même espace. La mise en place des espaces de circulation pourrait aider le gouvernement à réduire le nombre de processus de vérification d'identité auxquels le citoyen devra se soumettre dans le cadre de la mise en place du gouvernement électronique. S'il est retenu par le gouvernement, ce nouveau concept devra être intégré à la présente stratégie gouvernementale.

Notons également que les communications faites dans le cadre des services électroniques exigent une protection adaptée à leur sensibilité et aux impacts possibles résultant d'un bris de confidentialité ou d'intégrité. Les moyens d'identification et d'authentification des citoyens et des entreprises doivent correspondre aux niveaux de confiance appropriés à la nature des communications auxquelles ils serviront. Cela implique que les moyens d'authentification retenus devront permettre de répondre non seulement aux exigences de sécurité actuelles, mais devront pouvoir évoluer en fonction des tendances et de la complexité des services en ligne qui seront rendus aux citoyens et aux entreprises au cours des prochaines années.

Enjeux liés au déploiement et aux coûts

Le rythme de déploiement et l'envergure des coûts d'une solution d'authentification dépendent de plusieurs paramètres, dont la nature du processus d'attribution de l'identifiant et la nature de la technologie utilisée. À titre d'exemple, un processus d'attribution comportant une vérification d'identité sur place avec remise d'un identifiant sur un support transportable entraîne des délais de mise en œuvre plus longs et des coûts plus élevés qu'un processus qui ne comporte pas ces éléments. De même, l'utilisation d'un moyen d'authentification qui n'est pas soutenu par les technologies couramment utilisées par les citoyens et les entreprises risque d'avoir des impacts significatifs sur l'adhésion des utilisateurs, le rythme de déploiement et les coûts.

L'optimisation des paramètres de déploiement, de gestion et de fonctionnement lance un défi majeur, d'autant plus que le moyen d'authentification est destiné à une clientèle très vaste (citoyens et entreprises). Une solution d'authentification doit permettre d'établir un juste équilibre entre les besoins, les impacts organisationnels dans les ministères et les organismes, les délais de déploiement et les coûts aussi bien initiaux que récurrents.

Enjeux relatifs à la reconnaissance des moyens d'authentification

La question de l'authentification des personnes aux fins de l'utilisation de services électroniques par Internet se pose dans l'ensemble des pays, aussi bien pour les gouvernements que pour le secteur privé. Certains gouvernements ont déjà défini des orientations sans qu'il se dégage une réelle convergence. Du côté de l'industrie des technologies de l'information, il n'y a pas non plus de solution qui fasse un large consensus.

Toutefois, il est à prévoir que la nécessité d'identifier les personnes pour un volume important de transactions électroniques conduira à l'adoption généralisée de standards et à la dominance de certaines technologies. Une initiative comme Liberty Alliance[29], récemment présentée au groupe de standardisation OASIS[30], vise justement à permettre une reconnaissance à grande échelle des identifiants utilisés par les consommateurs sur Internet.

La solution d'authentification retenue par le gouvernement devra ainsi tenir compte de cette tendance penchant vers une utilisation à large échelle des moyens d'authentification. Plus particulièrement, la solution retenue devra favoriser un arrimage avec les autres moyens d'authentification utilisés par les citoyens québécois, notamment les solutions mises en place par le gouvernement fédéral ainsi que le secteur privé.

6.2. Création d'un service gouvernemental d'authentification

À la lumière de ces enjeux, le SCT a élaboré une stratégie gouvernementale pour l'authentification des citoyens et des entreprises dans le cadre de la prestation électronique de services qui repose sur la création d'un service gouvernemental d'authentification. Ce service comprendra des processus de vérification d'identité, un processus de délivrance d'un identifiant et un système de validation de cet identifiant. Les principes directeurs qui suivent énoncent les mesures d'encadrement qui s'appliquent à ce service d'authentification.

Service regroupé

Un service regroupé d'authentification permet à un citoyen d'utiliser un même identifiant pour l'accès à des services électroniques de plusieurs ministères et organismes. Le fait d'avoir un identifiant

[29] Liberty Alliance est un consortium qui vise à développer des normes ouvertes pour la gestion d'identités dites « fédérées » dans un contexte de services Web. Ces standards sont basés sur les spécifications SAML du groupe OASIS. Pour plus de détails, voir **www.projectliberty.org/**.

reconnu à l'échelle gouvernementale simplifie l'utilisation des services électroniques pour les citoyens et les entreprises. Cette caractéristique améliore la qualité des services au citoyen, car il peut ainsi établir son identité de la même façon, quel que soit le ministère ou l'organisme avec lequel il communique. Le fait d'utiliser régulièrement le même identifiant pour accéder à plusieurs services permettra également de réduire le nombre de cas d'oubli du mot de passe dû à une utilisation peu fréquente de l'identifiant.

Par souci d'accorder le plus de liberté possible au citoyen, ce principe de service regroupé doit cependant permettre à un citoyen qui ne voudrait pas utiliser le même identifiant pour faire affaire avec plusieurs ministères et organismes d'en posséder plusieurs. Il reviendra donc à l'utilisateur de décider du nombre d'identifiants qu'il détiendra pour traiter avec les ministères et organismes de son choix.

Un service regroupé permet également d'optimiser la performance de l'État par une rationalisation des processus et des infrastructures. En effet, un service regroupé comporte un ensemble de composantes développées et utilisées de façon centralisée, ce qui favorisera l'optimisation des paramètres de déploiement, de gestion et de fonctionnement, en plus de réduire les coûts de mise en œuvre à l'échelle gouvernementale.

Pour ces raisons, l'utilisation d'un service regroupé d'authentification est favorisée par le SCT. La mise en place d'un service regroupé, impliquant la participation de plusieurs ministères ou organismes, devra cependant traiter des enjeux de protection des renseignements personnels liés à ce type de service[31].

Service évolutif

Le service d'authentification doit permettre de répondre aux besoins d'échanges d'information personnelle et sensible avec un niveau de confiance adéquat tout en respectant les mesures de sécurité énoncées, entre autres, par l'AGSIN. La première version du service répondra à des besoins généralement définis dans le cadre de projets des ministères et organismes. Le service d'authentification évoluera progressivement pour tenir compte des nouveaux services électroniques des ministères et organismes et des changements technologiques. Le service pourra également évoluer vers un niveau de sécurité plus élevé.

[30] Organization for the Advancement of Structured Information Standards : **www.oasis-open.org**.
[31] Voir la section 6.2., p. 33.

6.3. Considérations quant à la mise en œuvre du service d'authentification

Besoins des ministères et organismes

La première considération de mise en œuvre du service d'authentification a trait aux besoins des ministères et organismes, lesquels seront modulés en fonction des risques qu'ils auront prévus. Ces besoins doivent être considérés en relation avec les différents niveaux de confiance qui peuvent être requis. Tout en prévoyant que des solutions seront mises en place pour plusieurs niveaux, la stratégie gouvernementale doit d'abord mettre l'accent là où les besoins sont prépondérants et où l'adhésion des ministères et des organismes est la plus probable. Étant donné les critères énoncés à la section 5.3., on peut penser que la grande majorité des communications avec les citoyens et les entreprises nécessitera une authentification de niveau moyen ou moindre.

La mise en œuvre d'un service d'authentification doit prendre appui sur un axe prioritaire basé sur le niveau de confiance moyen, compte tenu que ce niveau permet également de répondre à des besoins de niveau inférieur et qu'il permettra au gouvernement de mettre en place plus facilement des services électroniques de nature transactionnelle où sont échangés des renseignements confidentiels.

Dans un objectif à long terme, le service d'authentification pourra évoluer vers la délivrance d'un niveau de confiance élevé, si les besoins le justifient compte tenu des services qui seront déployés par les ministères et organismes.

Pérennité et viabilité de la stratégie de mise en œuvre

La pérennité et la viabilité de la stratégie de mise en œuvre doivent être maintenues malgré le caractère évolutif des services d'authentification et les changements technologiques rapides dans ce domaine. La mise en œuvre sera progressive et alignée sur les orientations gouvernementales, notamment celles de l'AEG et de l'AGSIN ainsi que celles ayant trait à une catégorisation de l'information numérique.

Continuité avec les travaux déjà réalisés

Tout en répondant aux besoins et en misant sur la pérennité de la stratégie, les orientations de mise en œuvre doivent également s'assurer d'une continuité avec les travaux déjà réalisés concernant l'authentification. Les initiatives gouvernementales présentées précédemment ont décrit les services de l'ICPG, particulièrement les travaux effectués par le ministère de la Justice. D'autres travaux ont

aussi été réalisés, tels que ceux relatifs aux services applicatifs communs faits par la Direction générale des services informatiques gouvernementaux du SCT ainsi que ceux relatifs à la mise sur pied de services intégrés, notamment le Service québécois de changement d'adresse. D'autres travaux importants ont également été réalisés dans certains ministères, dont le ministère du Revenu.

La stratégie de mise en œuvre doit faire en sorte d'assurer la cohérence entre les acquis gouvernementaux et de maximiser les possibilités de réutilisation.

Capacité de livraison au moment opportun

Compte tenu que de nombreux projets de prestation électronique de services du gouvernement sont déjà en cours ou sur le point de s'amorcer, il importe que la mise en œuvre du service d'authentification puisse se faire dans un délai rapproché. Les coûts doivent en être raisonnables et la faisabilité technique impose que les technologies utilisées soient disponibles sur le marché.

6.4. Le Service québécois d'authentification gouvernementale

En réponse aux orientations énoncées plus haut et aux tendances canadiennes et internationales recensées, le SCT développera un service gouvernemental d'authentification permettant à un citoyen ou au représentant d'une organisation d'obtenir un identifiant qu'il pourra ensuite utiliser pour s'inscrire et s'authentifier auprès des différents services en ligne gouvernementaux.

Tenant compte des besoins des ministères et organismes et du caractère évolutif des services, la stratégie gouvernementale est d'abord axée sur la mise en place d'un service commun de niveau de confiance moyen. Ce service, appelé Service québécois d'authentification gouvernementale (SQAG), repose sur la délivrance, aux personnes qui en font la demande, de certificats de clé publique pouvant être utilisés pour établir son identité en ligne auprès des différents ministères et organismes ainsi que pour assurer l'intégrité et l'irrévocabilité des documents technologiques.

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[32] 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.

[32] 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 du travail, la Commission de la santé et de la sécurité du

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.

6.4.1. Fonctionnement du SQAG

Le SQAG comporte un ensemble de fonctions visant, d'abord, à rendre accessible un identifiant aux utilisateurs du service, puis à permettre aux ministères et aux organismes de reconnaître cet identifiant.

Vérification d'identité

L'attribution d'un identifiant gouvernemental SQAG aux citoyens et aux entreprises sera amorcée par une demande en ligne lors de l'utilisation d'un premier service électronique transactionnel d'un ministère ou d'un organisme exigeant une identification.

Une vérification d'identité sera faite en comparant des renseignements fournis par l'utilisateur avec des informations déjà en la possession du ministère ou de l'organisme qui effectue la vérification. L'utilisateur du service devra donc être déjà connu du ministère ou de l'organisme qui procédera à la vérification d'identité.

La fonction de vérification d'identité sera assumée par des ministères ou des organismes désignés à cet effet.

Délivrance d'un identifiant

À la suite de la vérification d'identité, un identifiant sera délivré. Cet identifiant prendra la forme d'un certificat de clé publique. Ce type d'identifiant a été retenu notamment parce qu'il permet de répondre aux besoins d'authentification de niveau moyen ou moindre des ministères et organismes et qu'il peut évoluer vers un niveau de confiance élevé[33] lorsqu'il est associé à un support physique transportable (ex. : carte à microprocesseur).

La délivrance des certificats sera effectuée par un fournisseur désigné par le Conseil du trésor.

travail, la Commission administrative des régimes de retraite et d'assurances et la Société de la faune et des parcs du Québec.

[33] À condition que des processus de vérification d'identité de niveau élevé soient mis en place.

L'identifiant SQAG ne contiendra pas de renseignements personnels à propos de l'usager. Il comportera plutôt un pseudonyme. Le ministère ou l'organisme sera responsable d'établir le lien entre le pseudonyme et le numéro de dossier de l'utilisateur : cette étape est appelée « inscription ».

Inscription au service du ministère ou de l'organisme

Dès que le certificat sera délivré, le ministère ou l'organisme procédera à l'inscription de l'utilisateur au service électronique. Cette inscription implique la conservation d'un lien entre le certificat délivré et le numéro de dossier (identifiant administratif) sous lequel la personne est connue 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 devra procéder à une inscription pour chaque service en ligne dont il voudra bénéficier.

Puisque le certificat comportera un pseudonyme, un ministère ou un organisme qui voudra inscrire un utilisateur 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. Cela est nécessaire puisque le certificat ne comporte pas le numéro de dossier de l'utilisateur qui permettrait au ministère ou à l'organisme de le reconnaître dès sa première visite.

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 utilisateur à son service en ligne. Cela offre la possibilité aux ministères et organismes de s'assurer eux-mêmes de l'identité de l'utilisateur, selon le niveau de confiance désiré, avant d'établir le lien entre le certificat de l'utilisateur et le numéro de dossier interne.

Authentification de l'utilisateur

Lorsque la personne accédera de nouveau aux services en ligne d'un ministère ou d'un organisme auxquels elle sera inscrite, l'authentification sera effectuée en session sécurisée. L'utilisateur n'aura alors qu'à présenter son certificat et à entrer son mot de passe, qui sera validé par le SQAG en vue d'authentifier l'usager.

Chaque ministère et organisme sera responsable d'établir et de valider les autorisations de l'utilisateur à la suite de l'authentification.

Gestion de l'identifiant

Les identifiants délivrés par le SQAG seront gérés de façon centralisée. Ainsi, les ministères et les organismes qui adhéreront au service n'auront pas à gérer le cycle de vie des certificats ni les cas de compromission et d'oubli des mots de passe. De plus, de l'aide en ligne sera offerte à l'utilisateur du service qui souhaite modifier ou recouvrer son mot de passe.

6.4.2. Le SQAG et la protection des renseignements personnels

La conception d'un système d'authentification gouvernemental soulève certaines préoccupations relatives à la protection des renseignements personnels. En effet, dans un contexte où les ministères et les organismes sont détenteurs de fichiers comportant une multitude de données nominatives, il devient primordial de s'assurer que la mise en place de nouveaux mécanismes d'identification ne pourra pas servir à des fins détournées de traçage et de couplage de données.

Le SQAG est donc conçu avec un grand souci du respect des principes suivants de protection des renseignements personnels.

Respecter le libre choix du citoyen

L'adhésion au SQAG sera volontaire pour le citoyen. Ainsi, celui-ci pourra toujours opter pour un autre mode de prestation de services, par exemple les services au comptoir ou au téléphone.

Cependant, un ministère ou un organisme pourra exiger la présentation d'un certificat SQAG pour compléter un échange électronique s'il a retenu ce moyen d'identification pour un service donné. Dans ce cas, l'utilisateur aura le choix du certificat qu'il présentera à son interlocuteur.

Par conséquent, une personne pourra, à son choix, détenir plusieurs certificats SQAG et elle pourra choisir quel certificat elle utilisera dans un service particulier ou dans un ministère ou un organisme particulier.

Utiliser des pseudonymes

Le certificat SQAG ne contient pas le nom de l'usager, il contient plutôt un pseudonyme qui prend la forme d'un numéro unique non significatif.

Ni le fournisseur de certificats ni les services centraux qui abriteront le SQAG ne détiendront de base de données comportant le nom ou d'autres renseignements sur l'identité des utilisateurs.

Tel qu'il est conçu, le SQAG fait en sorte que la vérification de l'identité des utilisateurs est d'abord effectuée par un ministère ou un organisme. Lorsque celui-ci a vérifié l'identité d'un individu avec satisfaction, il déclenche alors un processus qui aboutit à la délivrance d'un certificat comportant un pseudonyme. Ce ministère ou cet organisme devra donc établir et maintenir un lien entre le pseudonyme et l'identité de l'individu.

Tel que le requiert la LCCJTI[34], il sera possible pour un ministère ou un organisme de s'adresser au SQAG pour connaître le nom de la personne détentrice d'un certificat. Puisque le SQAG ne stockera pas cette information, la requête sera redirigée directement vers le ministère ou l'organisme qui avait procédé à la vérification d'identité initiale, lequel sera en mesure de fournir au ministère ou à l'organisme demandeur le nom du détenteur du certificat.

Limiter la collecte de renseignements nominatifs

Tel que cela a été mentionné précédemment, la vérification de l'identité des utilisateurs du SQAG sera effectuée par la comparaison de renseignements sur l'utilisateur avec des données déjà en la possession des ministères et organismes. Cette manière de procéder permettra de limiter au strict minimum la collecte de renseignements personnels.

La seule nouvelle collecte de données consistera à recueillir des « secrets partagés », c'est-à-dire des informations qui serviront à la récupération du mot de passe de l'usager en cas d'oubli de sa part. Un tel système est déjà couramment utilisé sur Internet. À titre d'exemple de donnée souvent recueillie, mentionnons le nom de la ville de naissance ou le passe-temps préféré. Dans le cadre du SQAG, ces données seront toutefois recueillies par le fournisseur de certificats, qui ne connaîtra pas l'identité des détenteurs de certificats.

Les seules données à caractère personnel recueillies par le SQAG sont des « secrets partagés », lesquels ne seront, à aucun moment, associés à l'identité réelle des détenteurs de certificats.

[34] Article 48, *in fine*.

Limiter la circulation de renseignements nominatifs

Les ministères et organismes demeureront les seuls détenteurs de renseignements personnels sur les usagers. Ainsi, au moment de la vérification de l'identité d'un utilisateur, les données saisies par l'individu seront comparées, chez le ministère ou l'organisme, avec ses données d'arrière-boutique. De même, au moment de l'inscription, le ministère ou l'organisme s'assurera que les données transmises au SQAG sont chiffrées de manière qu'il soit le seul à y accéder.

Le SQAG comportera un ensemble de mesures technologiques ou administratives afin de s'assurer qu'à aucun moment, des données personnelles 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

L'une des préoccupations couramment avancées en matière de protection de la vie privée concerne la possibilité d'utiliser un identifiant à des fins de couplage de données.

Le SQAG comportera un ensemble de mesures technologiques ou administratives visant à faire en sorte que les ministères et organismes ne puissent pas utiliser le pseudonyme inscrit au certificat pour des fins illicites de couplage de données ou pour toute fin autre que celle prévue par le SQAG.

Tout d'abord, tel que cela a été mentionné précédemment, une personne pourra détenir une multitude de certificats SQAG, donc une multitude de pseudonymes. Cette caractéristique, en plus de respecter le principe de libre choix du citoyen, permet également de s'assurer qu'une personne peut segmenter l'usage du SQAG parmi les ministère et organismes selon ses choix et ses préférences. Par exemple, une personne pourrait utiliser un certificat SQAG pour communiquer avec la Régie des rentes du Québec alors qu'elle en utiliserait un deuxième pour communiquer avec le ministère du Revenu. Elle pourrait aussi, à son choix, utiliser le même. Cette façon de procéder rend difficile un couplage de données à partir de cet identifiant.

Même si la possibilité de détenir plusieurs certificats permet de réduire les risques de couplage de données, des mesures additionnelles seront mises en place afin de diminuer davantage ce risque.

Ainsi, l'identifiant SQAG ne viendra pas se substituer aux numéros de dossiers ministériels : à l'intérieur des programmes et des services, les ministères et organismes continueront d'identifier les

citoyens et les entreprises à l'aide des numéros actuellement utilisés et devront plutôt faire le joint entre ce numéro de dossier et l'identifiant SQAG (étape de l'inscription).

De plus, le SQAG prévoit que ce lien entre le certificat et le numéro de dossier d'un ministère ou d'un organisme 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, ce qui limitera donc la possibilité de croisement de données à partir des certificats SQAG.

Enfin, les ministères et organismes utilisateurs du SQAG s'engageront 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. 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 possibilité de tracer le cheminement d'un individu 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'une personne 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.

Chacune des fonctions du SQAG (vérification d'identité, délivrance de certificats, inscription, authentification, etc.) sera assumée par des entités distinctes. Cette façon de faire permettra ainsi de conserver des journaux de transactions dans des organisations 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.

Le mode de fonctionnement du SQAG fera en sorte qu'il ne sera pas possible de savoir à quel moment ou à quelle fréquence une personne en particulier visite un programme ou un service gouvernemental, à moins d'effectuer une enquête approfondie nécessitant la collaboration de plusieurs entités.

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

6.4.3. Orientations de mise en œuvre du service

Déploiement par étapes

Le SQAG permettra d'abord de délivrer aux utilisateurs des services gouvernementaux un identifiant de niveau de confiance moyen. Cependant, afin de pouvoir répondre à un plus vaste éventail de besoins des ministères et des organismes, le SQAG pourra soutenir, dans une version ultérieure, la délivrance d'un identifiant de niveau de confiance élevé nécessitant alors une vérification d'identité en personne et l'utilisation d'un support matériel transportable (par exemple, une carte à puce).

De même, le SQAG prévoit d'abord recourir à des processus de vérification d'identité à distance, évitant ainsi aux utilisateurs de se déplacer vers des points de service. Cependant, des processus de vérification d'identité en personne seront éventuellement déployés afin, notamment, de pouvoir mieux desservir la clientèle des entreprises ainsi que pour la délivrance des identifiants de niveau de confiance plus élevé.

Désignation des ministères et des organismes responsables de la vérification d'identité

La vérification d'identité des utilisateurs du SQAG sera effectuée par des ministères et des organismes désignés pour assumer un tel rôle. Seuls pourront être désignés les ministères et les organismes effectuant déjà la vérification d'identité dans le cadre de leurs opérations et possédant des processus qui répondent aux orientations gouvernementales précédemment énoncées en matière de vérification d'identité, notamment des processus de vérification d'identité comportant un nombre suffisant de secrets pouvant être validés à distance. Ces processus de vérification d'identité devront être évalués cas par cas au moment de la désignation.

Désignation du fournisseur de certificats

Le Conseil du trésor devra désigner l'organisation qui assumera la fonction de fournisseur de certificats, dont le rôle consistera à délivrer et à gérer les certificats requis dans le cadre du SQAG.

Le choix du fournisseur tiendra compte des critères suivants :

- la capacité du fournisseur de remplir les fonctions requises par le SQAG et de s'arrimer aux processus et aux exigences du gouvernement en matière de vérification d'identité et de gestion des certificats;
- la capacité de satisfaire les exigences gouvernementales relatives à la protection des renseignements personnels;
- le potentiel de récupération des investissements antérieurs et le coût des services;
- la capacité d'« interopérer » avec d'autres certificats, notamment ceux du gouvernement fédéral et du secteur privé;
- la conformité avec les principes édictés par le gouvernement en matière de gestion administrative.

Responsabilité légale des intervenants

Un cadre juridique sera établi afin de définir les responsabilités de chaque intervenant dans le processus de délivrance des identifiants SQAG. Ce cadre juridique énoncera également 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.

7. Conclusion

Dans un contexte gouvernemental où les budgets sont de plus en plus restreints, la création d'un service gouvernemental d'authentification permettra à l'Administration d'optimiser la performance de l'État par l'utilisation de composantes centrales et réutilisables, réduisant ainsi les coûts de développement et de fonctionnement.

Cependant, la clé du succès d'une telle entreprise passe nécessairement par une adhésion des ministères et des organismes à la stratégie gouvernementale retenue. En effet, le principal objectif visé, soit améliorer la qualité des services aux citoyens, ne pourra être atteint que si les ministères et organismes adoptent le modèle d'authentification proposé et y adhèrent. Au lieu de se concentrer sur les mesures de sécurité et d'accès aux services, les ministères et organismes pourront plutôt œuvrer à la conception et à la mise en place de leurs services électroniques, conduisant ainsi plus rapidement l'Administration vers sa mission de déployer un véritable gouvernement électronique.

ANNEXE
Liste des sites Internet cités dans le document

Le Fonds québécois de la recherche sur la nature et les technologies (gouvernement du Québec)
http://www.fcar.qc.ca

À propos du *epass* (gouvernement du Canada)
http://www.ccra-adrc.gc.ca/eservices/tax/individuals/aco/epass-f.html#1

e-Authentication Homepage (États-Unis)
http://www.cio.gov/eauthentication/

Portail fédéral (Belgique)
http://www.belgium.be/eportal

E-government Unit (Nouvelle-Zélande)
http://www.e-government.govt.nz/authentication/index.asp

Office of the *e-Envoy* (Royaume-Uni)
http://www.e-envoy.gov.uk/Responsibilities/Authentication/fs/en

National Office for the Information Economy (Australie)
http://www.noie.gov.au/publications/NOIE/online_authentication/index.htm

Corporate Privacy and Information Access (Colombie-Britannique)
http://www.mser.gov.bc.ca/foi_pop/

CEFRIO
http://www.cefrio.qc.ca/rapports/Net_Gouv_2003.pdf

Projet Liberty Alliance
http://www.projectliberty.org/

OASIS
http://www.oasis-open.org

Secrétariat
du Conseil du trésor
Québec