

DE : Monsieur Éric Caire
Ministre de la Cybersécurité et du Numérique

Le 10 juillet 2024

TITRE : Projet de décret concernant les organismes publics tenus d'utiliser le Service d'authentification gouvernementale du ministre de la Cybersécurité et du Numérique

PARTIE ACCESSIBLE AU PUBLIC

1- Contexte

Mission du ministère de la Cybersécurité et du Numérique :

En application de l'article 4 de la Loi sur le ministère de la Cybersécurité et du Numérique (chapitre M-17.1.1, ci-après « Loi sur le MCN »), le ministre de la Cybersécurité et du Numérique a notamment pour mission de fournir aux organismes publics (OP) au sens de l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03, ci-après « Loi sur les ressources informationnelles »), des services en infrastructures technologiques et en systèmes de soutien communs permettant notamment de soutenir de tels organismes dans l'exercice de leurs fonctions et dans leur prestation de services afin de favoriser leur transformation numérique.

L'article 3 de la Loi sur le MCN prévoit que le ministre de la Cybersécurité et du Numérique assume la responsabilité de développer un ensemble de moyens visant à offrir aux citoyens et aux entreprises une prestation de services numériques de qualité, en s'assurant autant que possible de ne pas causer de fracture numérique et de veiller à l'utilisation optimale des technologies du numérique dans les prestations des services publics.

Actuellement, le ministère de la Cybersécurité et du Numérique (MCN) fournit aux OP le Service d'authentification gouvernementale, lequel remplacera graduellement le service d'authentification clicSÉCUR ainsi que d'autres solutions utilisées pour accéder aux prestations électroniques de services des organismes publics.

En application de sa loi constitutive, le MCN détermine par écrit son offre de services ainsi que la tarification liée à l'utilisation de ces derniers. Toutefois, les OP ne sont pas tenus de recourir à ces services, à moins que le gouvernement en décide autrement, conformément à l'article 22.1 de la Loi sur les ressources informationnelles.

Le projet Accès bonifié aux prestations électroniques de services Citoyens du Programme Service québécois d'identité numérique

Le Programme Service québécois d'identité numérique (SQIN), désigné projet en ressources informationnelles d'intérêt gouvernemental en avril 2020 par le Conseil du trésor, vise notamment à procurer aux citoyens une identité numérique de confiance ainsi qu'une utilisation simplifiée et plus sécuritaire des services gouvernementaux.

Le Programme SQIN permettra notamment d'assurer l'identification de façon unique de chaque citoyen et de supporter la transformation numérique de l'administration publique.

Le Programme SQIN est composé de plusieurs projets, dont le premier, « Accès bonifié aux prestations électroniques de services Citoyens » (ci-après le « Projet Citoyens ») est le projet qui permet notamment le développement de la solution d'authentification Service d'authentification gouvernementale.

La réalisation de ce projet vise, entre autres, à répondre à des besoins spécifiques, à savoir :

- Pour les citoyens :
 - Avoir un moyen simple de se connecter aux prestations électroniques de services (PES) du gouvernement;
 - Avoir un seul identifiant (nom d'utilisateur ou adresse courriel et mot de passe) permettant l'accès à ces PES.
 - Éliminer ainsi la nécessité pour le citoyen de créer un nouveau compte pour chaque PES du gouvernement.
- Pour les organismes publics :
 - Offrir aux citoyens un moyen simple de s'authentifier et de s'identifier pour accéder à leurs PES et ainsi avoir l'assurance que le citoyen qui accède à leurs PES est la bonne personne.
- Pour le gouvernement :
 - Améliorer la prestation de services en ligne aux citoyens;
 - Assurer la continuité des affaires dans un contexte de désuétude technologique de la solution clicSÉCUR.

Le Service d'authentification gouvernementale

L'utilisation d'un seul service d'authentification hautement sécuritaire, qui utiliserait à terme, une source d'information unique et fiable quant aux attributs d'identité des citoyens utilisateurs des PES – ici le registre d'attributs d'identité gouvernemental (RAIG) créé dans le cadre de l'application du décret numéro 870-2022 du 25 mai 2022 (décret concernant la désignation du MCN pour agir comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale) permettra également d'uniformiser les attributs d'identité gouvernementaux (dont les noms, date de naissance, adresse de résidence, etc.).

En regroupant toutes les informations d'authentification dans une seule banque de données sécurisée, les points d'accès potentiels sont réduits et la gestion de la sécurité, est simplifiée, ce qui rend plus facile la protection des données sensibles.

De plus, considérant la sensibilité des informations qui sont traitées par le Service d'authentification gouvernementale, dès les étapes de conception, des experts de sécurité de l'information ont été intégrés dans le projet et continuent d'accompagner la prestation de services afin que le Service d'authentification gouvernementale intègre les exigences de sécurité de l'information (SI) requises pour assurer la sécurité et la confidentialité des données.

Également, le Service d'authentification gouvernementale a été conçu de manière à respecter les orientations prévues aux Règles relatives à l'assurance de l'identité numérique. La conception a été faite de manière à rendre le plus difficile possible le vol de compte par un pirate informatique.

La solution d'authentification Service d'authentification gouvernementale est progressivement utilisée par les organismes publics et peut être utilisée par les citoyens depuis le 14 décembre 2022 pour les PES suivantes :

Organisme public	Prestation électronique de service
Ministère de la Famille	Service québécois de certification du personnel éducateur de la petite enfance
Société de l'assurance automobile du Québec	SAAQclic Citoyens
	SAAQclic Commerçants
	SAAQclic Entreprises
	SAAQclic Mandataires en vérification de véhicules routiers
Ministère de la Santé et des Services sociaux	Grossesse pour autrui hors Québec
Ministère de la Cybersécurité et du Numérique et Secrétariat du Conseil du trésor	Système électronique d'appel d'offres (SEAO)

En date du 20 juin 2024, 1 452 368 utilisateurs uniques ont complété leur vérification d'identité afin d'effectuer des transactions sécurisées avec ces organismes.

2- Raison d'être de l'intervention

L'utilisation par les OP de différentes solutions d'authentification complexifie l'accès aux PES gouvernementales et la navigation dans celles-ci pour le citoyen. À titre d'exemple, un citoyen qui souhaite bénéficier des services en ligne du ministère de l'Éducation, de

Revenu Québec et de la Commission des normes, de l'équité, de la santé et de la sécurité du travail doit s'inscrire et gérer les comptes de trois solutions d'authentification distinctes.

D'un point de vue organisationnel, l'exploitation et l'entretien de multiples solutions d'authentification imposent une charge significative aux OP, tant au niveau financier qu'au niveau des ressources humaines et s'inscrit en opposition avec les orientations liées au principe de mutualisation des solutions technologiques.

Chaque solution d'authentification utilisée nécessite que l'OP investisse dans le développement, le maintien, la mise à jour et la sécurité de la solution d'authentification. Les coûts associés incluent non seulement le développement logiciel et l'acquisition de licences, mais également les dépenses récurrentes de soutien technique, d'entretien et de formation du personnel.

Également, des solutions d'authentification multiples augmentent la complexité de la gestion de la sécurité à l'échelle de l'État. Chaque solution, selon la PES à laquelle elle donne accès, et selon le moment où elle a été développée, peut avoir un niveau de sécurité différent et être sujette à des vulnérabilités distinctes. L'application des mesures de sécurité nécessite donc une attention particulière. L'adoption de nouvelles technologies oblige l'OP à tester et à adapter ces technologies à sa propre solution.

De plus, chaque solution utilisée nécessite de s'assurer que les normes législatives et réglementaires en matière de protection des données soient appliquées.

Actuellement, le Service d'authentification gouvernementale n'est pas utilisé à son plein potentiel. Cela se traduit notamment par un retard dans la matérialisation des bénéfices prévus lors de son développement (tels la réduction des coûts, les gains de productivité, l'augmentation du niveau de précision de l'information, une meilleure sécurité de l'information et une amélioration de la qualité du service aux citoyens).

3- Objectifs poursuivis

L'intervention proposée vise les OP assujettis à la Loi sur les ressources informationnelles afin qu'ils soient tenus, au plus tard le 31 mars 2028, d'utiliser le Service d'authentification gouvernementale comme solution d'authentification des personnes.

De plus, si un OP utilise déjà une autre solution d'authentification des personnes pour une PES, il est exigé que cet OP continue d'utiliser cette autre solution d'authentification jusqu'au rattachement de celle-ci au Service d'authentification gouvernementale au plus tard le 31 mars 2028.

Ces interventions permettront, à terme, de réduire le nombre de solutions d'authentification utilisées par ces OP tout en évitant la multiplication des solutions d'authentification et ainsi réduire les coûts qui y sont associés.

Dans un monde numérique où il est nécessaire d'assurer une protection accrue des renseignements personnels des citoyens et des données détenues par l'administration

publique, l'utilisation du Service d'authentification gouvernementale répond à des exigences de sécurité rehaussées pour assurer cette protection.

La surveillance centralisée de la solution d'authentification permet de détecter rapidement les comportements suspects, renforçant ainsi la résilience du système face aux menaces cybernétiques ou les tentatives d'accès non autorisés pour ainsi contribuer à la réduction des risques d'usurpation d'identité.

Par ailleurs, le passage vers une seule solution d'authentification gouvernementale se traduirait par d'importants bénéfices, non seulement financiers, mais également pour les citoyens en termes d'expérience client. En effet, les citoyens n'auront plus à naviguer entre différentes solutions d'authentification pour accéder aux PES offertes par les OP. Les organismes qui composent l'administration publique doivent travailler de concert pour offrir aux citoyennes et aux citoyens une expérience unifiée. Peu importe le service gouvernemental utilisé, les citoyens doivent vivre une expérience transparente, continue, de qualité équivalente, le tout en s'adressant à un seul gouvernement. Conséquemment, les citoyens n'auront besoin que d'un seul identifiant pour accéder à tous les services gouvernementaux en ligne, ce qui simplifie grandement le processus d'authentification et réduit la charge cognitive associée à la gestion de plusieurs comptes.

De plus, une solution d'authentification unifiée favorise l'interopérabilité entre les différents services gouvernementaux, ce qui facilite l'échange sécurisé de données et la collaboration entre les différentes entités gouvernementales.

Finalement, l'adoption du Service d'authentification gouvernementale comme seule solution d'authentification permettra aux organismes gouvernementaux de se conformer plus aisément aux normes de sécurité et aux réglementations en vigueur, réduisant ainsi les risques de non-conformité.

4- Proposition

Il est proposé que les OP assujettis à la Loi sur les ressources informationnelles soient tenus d'utiliser le Service d'authentification gouvernementale comme solution d'authentification pour les PES qui impliquent une activité d'authentification des personnes, et ce, au plus tard le 31 mars 2028.

Dans l'objectif d'assurer le déploiement graduel du Service d'authentification gouvernementale de manière optimale d'ici le 31 mars 2028, le rattachement des PES se fera sur une base volontaire, à une date convenue entre l'OP et le MCN. Les OP devront toutefois continuer d'utiliser la solution d'authentification des personnes qu'ils utilisent actuellement, et ce, jusqu'à leur rattachement au Service d'authentification gouvernementale. Il ne sera pas possible de migrer vers une autre solution que le Service d'authentification gouvernementale.

Ainsi, lorsqu'un OP développera un nouveau service en ligne, il devra contacter le MCN afin de prévoir le rattachement de cette PES au Service d'authentification gouvernementale considérant que l'OP sera tenu d'utiliser ce service pour l'authentification des personnes au plus tard le 31 mars 2028. Il ne servirait pas l'intérêt

public d'engendrer des coûts d'acquisition, de développement et d'entretien pour la mise en place temporaire d'une solution autre que le Service d'authentification gouvernementale.

Par ailleurs, dès qu'une solution d'authentification deviendra désuète, l'OP devra enclencher les démarches auprès du MCN afin de planifier le rattachement de la PES afférente à la solution d'authentification désuète au Service d'authentification gouvernementale.

5- Autres options

Dans un contexte de mutualisation des ressources, le statut quo n'est pas une option viable. Le statut quo impliquerait que chaque OP choisisse la solution d'authentification qu'il compte utiliser pour ses PES. Cette solution pourrait ne pas respecter les normes et pratiques de cybersécurité et de protection des renseignements personnels équivalentes à celles du Service d'authentification gouvernementale. De plus, cette option ne peut freiner les coûts liés à l'entretien et au développement d'autres solutions et conséquemment, des investissements gouvernementaux nécessaires. Enfin, cela ne permet pas aux citoyens d'utiliser, à terme une seule et même solution d'authentification pour utiliser les PES du gouvernement du Québec, et ne permet pas l'atteinte des objectifs gouvernementaux de mutualiser les services gouvernementaux qui peuvent générer des économies d'échelle significatives.

6- Évaluation intégrée des incidences

En matière d'incidence sur les citoyens, le fait que les OP visés soient tenus d'utiliser le Service d'authentification gouvernementale au plus tard le 31 mars 2028, permettra d'offrir une solution d'authentification sécurisée et une solution uniforme d'authentification.

Quant aux incidences en matière de gouvernance, cela permettra aux OP de concentrer leurs efforts à réaliser leur mission et leurs mandats, plutôt que de faire la gestion d'une solution d'authentification. En effet, le Service d'authentification gouvernementale étant considéré comme un service « horizontal », il peut ainsi être confié au MCN pour qu'il en assure l'exploitation, le maintien et l'évolution dans le cadre de sa mission.

La mutualisation d'un tel service permettra également de mieux utiliser les fonds publics en évitant de payer pour le développement ou l'exploitation de plusieurs services similaires.

7- Consultation entre les ministères et avec d'autres parties prenantes

Le MCN a mis sur pied le Comité stratégique de la transformation numérique gouvernementale qui a pour objectif d'assurer la cohérence et l'efficacité des efforts de transformation numérique à travers différents secteurs de l'administration publique. Ce comité regroupe des représentants du ministère du Conseil exécutif (MCE), de la Société de l'assurance automobile du Québec (SAAQ), du ministère de l'Emploi et de la Solidarité sociale (MESS), de Revenu Québec (RQ), de la Régie de l'assurance maladie du Québec

(RAMQ) et du ministère de la Famille (MFA). Dans le cadre du Projet Citoyens, ces membres sont partenaires ou clients du Service d'authentification gouvernementale et jouent un rôle important dans le déploiement et l'amélioration du service.

Les membres du comité stratégique ont été informés de l'intention de rendre le Service d'authentification gouvernementale obligatoire pour les OP soumis à la Loi sur les ressources informationnelles, lors de la séance du 9 avril 2024.

8- Mise en œuvre, suivi et évaluation

Le rattachement des PES au Service d'authentification gouvernementale se fera graduellement, et ce, jusqu'au 31 mars 2028. Au besoin, le MCN évaluera les solutions utilisées par chaque PES ainsi que leur niveau d'urgence en termes de rattachement.

L'opérationnalisation de chaque rattachement au Service d'authentification gouvernementale suit un processus bien établi qui comporte cinq étapes couvrant le cycle complet, à savoir :

- **Préparation** : Évaluation du niveau d'assurance de la PES ainsi que des besoins de l'OP afin d'effectuer l'architecture préliminaire.
- **Analyse et planification** : Élaboration des architectures affaires et TI, incluant l'analyse des volets de protection des renseignements personnels et de cybersécurité. Planification des travaux à réaliser pour la mise en place de la solution, tant du côté de l'OP que du MCN.
- **Exécution des travaux** : Accompagnement de l'OP dans ses travaux à réaliser et développement dans le Service d'authentification gouvernementale, s'il y a lieu. Réalisation des tests de bout en bout et élaboration de la stratégie de gestion du changement et des communications.
- **Mise en ligne** : Configuration de l'environnement de production et exécution des tests de connectivité. Mise en production du côté du MCN, s'il y a lieu, et mise en ligne de la PES arrimée au SAG.
- **Suivi post implantation** : Surveillance et ajustements selon le passage en mode exploitation. Élaboration du bilan de rattachement avec l'OP.

Le rattachement n'est pas seulement une question de capacité du MCN, mais également celle de l'OP. Ainsi, les travaux sont effectués en collaboration entre l'OP visé et le MCN selon des rôles et responsabilités établis dans le processus.

9- Implications financières

La mise en œuvre de la proposition devra se faire à même les budgets alloués annuellement (investissement et fonctionnement) au MCN et aux OP.

Lorsqu'une PES est rattachée au Service d'authentification gouvernementale, il est de la responsabilité des OP de prendre en charge intégralement les coûts liés à ce rattachement indépendamment du moment où ce rattachement est effectué.

10- Analyse comparative

Conformément au paragraphe 1^o du premier alinéa de l'article 22.1 de la Loi sur les ressources informationnelles, le gouvernement peut, sous certaines conditions, imposer à un OP l'utilisation d'un service en ressources informationnelles fourni par le MCN. C'est en vertu de cette disposition que le MCN a rendu obligatoire l'utilisation du Réseau intégré télécommunication multimédia et du Réseau gouvernemental de télécommunication. Ces services sont maintenant largement utilisés par les OP visés et ont permis de tendre vers l'atteinte des objectifs qu'avait le gouvernement en procédant ainsi.

Par ailleurs, le déploiement du Service d'authentification gouvernementale répond à plusieurs des critères utilisés pour évaluer la pertinence de rendre obligatoire un service comme indiqué dans le « Cadre des services obligatoires »¹ publié en 2017 par le Secrétariat du Conseil du trésor. On pense notamment aux critères suivants :

- Le service commun a une forte probabilité d'atteindre une masse critique de clientèle;
- Le service est standardisé dans plusieurs ministères et organismes ou présente un fort potentiel de standardisation;
- La consolidation des services permet de réaliser des synergies à fort potentiel de rentabilité;
- La mise en commun du service pourrait permettre de créer une masse critique de compétences.

Ministre de la Cybersécurité et du
Numérique,

ÉRIC CAIRE

² Secrétariat du Conseil du trésor. (2017). Cadre des services en ligne obligatoires du gouvernement du Québec. Repéré à https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/cybersecurite_numerique/Publications/AEG/AEG_3.3-Cadre-services-obligatoires_2017-06-05.pdf