

RAPPORT D'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

SERVICE QUÉBÉCOIS D'IDENTITÉ NUMÉRIQUE

PROJET 1 – ACCÈS BONIFIÉ AUX
PRESTATIONS ÉLECTRONIQUES DE
SERVICE – CITOYENS

Version juin 2025

MINISTÈRE DE LA CYBERSÉCURITÉ
ET DU NUMÉRIQUE

PRODUCTION

Direction générale du Service québécois d'identité numérique

Sous-ministériat adjoint au dirigeant principal de l'information et à la gouvernance

INFORMATION

Ministère de la Cybersécurité et du Numérique

900, place D'Youville, 3^e étage

Québec (Québec) G1R 3P7

418 644-1030

Courriel : information@mcn.gouv.qc.ca

Tous droits réservés pour tous pays. La reproduction, par quelque procédé que ce soit, la traduction ou la diffusion de ce document, même partielles, sont interdites. Cependant, la reproduction de ce document ou son utilisation à des fins personnelles, d'étude privée ou de recherche scientifique, mais non commerciales, sont permises à condition d'en mentionner la source.

Table des matières

NOTES PRÉLIMINAIRES	3
DÉFINITIONS	4
ACRONYMES	5
1. DESCRIPTION DU PROJET 1 ET DE L'OBJET DE L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (EFVP)	6
2. PARTIES PRENANTES AU PROJET	8
3. RENSEIGNEMENTS PERSONNELS IMPLIQUÉS	11
4. MOYENS MIS EN PLACE POUR RESPECTER LES OBLIGATIONS ET LES PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS (PRP)	25
5. RISQUES ET STRATÉGIES POUR LES ATTÉNUER	36
6. PLAN D'ACTION	36
7. APPROBATION DU RAPPORT ET VERSIONS	36
ANNEXE 1 – CADRE LÉGAL ET NORMATIF	38
ANNEXE 2 – CONTRATS ET ENTENTES	42
ANNEXE 3 – DÉMONSTRATION QUE LE PROJET 1 EST PROPORTIONNÉ AUX OBJECTIFS ET AUX RISQUES D'ATTEINTE À LA VIE PRIVÉE (NON-PUBLIÉE)	
ANNEXE 4 – MATRICE D'ÉVALUATION DES RISQUES D'ATTEINTE À LA VIE PRIVÉE (NON-PUBLIÉE)	
ANNEXE 5 – ÉVALUATION DES RISQUES D'ATTEINTE À LA VIE PRIVÉE (NON-PUBLIÉE)	
ANNEXE 6 – PLAN D'ACTION (NON PUBLIÉE)	

Notes préliminaires

L'Évaluation des facteurs relatifs à la vie privée est une démarche préventive et évolutive visant à protéger les renseignements personnels pour prévenir une atteinte au droit à la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif en matière de respect de la vie privée des clientèles cibles.

Ces facteurs sont, entre autres :

- La conformité du projet à la législation applicable à la protection des RP et le respect des principes qui l'appuient;
- L'identification des risques d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs impacts;
- La mise en place de stratégies durant tout le cycle de vie du projet pour éviter la réalisation de ces risques ou réduire l'impact de ceux-ci dans l'éventualité où ils se réalisent.

N. B. Pour faciliter la lecture, les acronymes et les définitions ont été regroupés dans les sections ci-après.

Définitions

Sujet	Définition
Attribut d'identité	Information qui permet de prouver l'identité d'une personne. Propriétés à propos d'un sujet sous quelque forme que ce soit qui, prises séparément ou combinées, peuvent être utilisées pour distinguer un sujet.
Authentification	Processus de validation permettant d'assurer que la personne qui entend utiliser ou autrement bénéficier d'un service est bien celle qu'elle prétend être. Elle vise à donner l'assurance qu'une telle personne conserve le contrôle des justificatifs lui permettant l'accès au service concerné et que ceux-ci n'ont pas été compromis.
Consentement	Action de donner son accord, son acceptation, son autorisation à une action, à un projet.
Identification	Processus de vérification permettant d'identifier, de façon unique, une personne qui entend utiliser ou autrement bénéficier d'un service. Un tel processus peut permettre d'établir l'identité dont une personne se réclame afin de pouvoir avoir accès au service concerné.
Justificatif	Données qui lient d'une façon unique les données de validation nécessaires à l'authentification à celles de l'identité
Organisme public (OP) partenaire	OP contribuant ou collaborant à la mise en œuvre et à l'exploitation des services créés et déployés dans le cadre du projet, notamment en : • Procédant à la communication de renseignements, incluant des RP; • Procédant à la validation de secrets d'identification; • Procédant à la vérification d'identité en personne; • Assurant le service à la clientèle; • Assurant la gestion des plaintes et commentaires; • Assurant l'impression et l'expédition des secrets d'identification par la poste.
Organisme public (OP) consommateur	Organisme public (OP) ayant recours au Service d'authentification gouvernementale pour permettre l'accès à ses prestations électroniques de services (PES) aux utilisateurs.
Prestation électronique de services (PES)	Prestation électronique de services (PES) gouvernementaux, sécurisés ou non, offerts aux utilisateurs par l'intermédiaire d'Internet.
Renseignement personnel (RP)	Toute information qui concerne une personne physique et qui permet de l'identifier directement ou indirectement.
Utilisateur	Une personne (ou son représentant) qui crée et utilise un compte au Service d'authentification gouvernementale pour accéder à une prestation électronique de services (PES) d'un organisme public (OP) consommateur. Cette personne peut agir en tant que citoyenne ou citoyen ou encore en tant que personne déléguée dans l'exercice de fonctions professionnelles.

Acronymes

AMF	Autorité des marchés financiers	PES	Prestations électroniques de services
BAnQ	Bibliothèque et Archives nationales du Québec	PRP	Protection des renseignements personnels
CAI	Commission d'accès à l'information	RPRP	Responsable de la protection des renseignements personnels
COCD	Centre organisationnel de cyberdéfense	RAIG	Registre d'attributs d'identité gouvernemental
CSIPRPC	Comité sur la SI, la PRP et la continuité	RAMQ	Régie de l'assurance maladie du Québec
DDN	Date de naissance	RP	Renseignement(s) personnel(s)
EFVP	Évaluation des facteurs relatifs à la vie privée	RPC	Responsable des plaintes et des commentaires
FIPA	Fichier d'inscription des personnes assurée	RQ	Revenu Québec
GAA	Groupement des assureurs automobiles	SAAQ	Société de l'assurance automobile du Québec
LGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03)	SCT	Secrétariat du Conseil du trésor
LFTNAP	Loi favorisant la transformation numérique de l'administration publique	SEAO	Système électronique d'appel d'offres
MCE	Ministère du Conseil exécutif	SI	Sécurité de l'information
MCN	Ministère de la Cybersécurité et du Numérique	SGAA	Solution de gestion des authentifications et des autorisations
MELCCFP	Ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs	SQCA	Service québécois de changement d'adresse
MESS	Ministère de l'Emploi et de la Solidarité sociale	SQIN	Service québécois d'identité numérique
MJQ	Ministère de la Justice du Québec		
MFA	Ministère de la Famille		
NAM	Numéro d'assurance maladie		
NAS	Numéro d'assurance sociale		
OP	Organisme(s) public(s)		

1. Description du projet 1 et de l'objet de l'évaluation des facteurs relatifs à la vie privée (EFVP)

Présentation des grandes lignes

La mise en place du Programme Service québécois d'identité numérique (SQIN) vise à constituer une fondation propulsant le citoyen dans l'ère du numérique en lui procurant une identité numérique de confiance ainsi qu'en lui simplifiant l'accès aux services gouvernementaux. Ce programme comporte des projets en ressources informationnelles d'intérêt gouvernemental, dont le projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens ».

La réalisation du projet 1 vise à instituer le Service d'authentification gouvernementale, incluant la création du Registre d'attributs d'identité gouvernemental (RAIG), aux fins de l'identification et de l'authentification des personnes en vue de leur donner accès aux prestations électroniques de services (PES) gouvernementales tout en contribuant à préserver à la fois l'intégrité et la confidentialité des renseignements personnels (RP) détenus par l'État.

Le Service d'authentification gouvernementale a comme objectif d'offrir des services simplifiés, intégrés et de qualité qui s'appuient sur les technologies de l'information (TI), incluant les technologies numériques, tout en assurant la pérennité du patrimoine numérique gouvernemental.

Historique

Par la prise du décret numéro 511-2020 du 13 mai 2020, le gouvernement a autorisé la phase d'exécution du projet 1 « Accès bonifié aux prestations électroniques de services – Entreprises et Citoyens » du Programme SQIN.

Par le décret numéro 870-2022 du 25 mai 2022, le gouvernement a désigné le ministère de la Cybersécurité et du Numérique (MCN) pour agir comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale, déployé dans le cadre de la réalisation du projet 1 du Programme SQIN. En vertu de ce décret, seules les données numériques gouvernementales requises pour la constitution et la tenue du RAIG sont communiquées au MCN à partir du Fichier d'inscription des personnes assurées (FIPA) de la Régie de l'assurance maladie du Québec (RAMQ)¹. Le 18 décembre 2023, le gestionnaire des données numériques gouvernementales a autorisé la mobilité de ces données numériques gouvernementales détenues par la RAMQ, aux fins du Service d'authentification gouvernementale pour la période du 1er janvier 2024 au 31 décembre 2026.

Expérimentation

Par la prise du décret numéro 1690-2022 du 26 octobre 2022, modifié par le décret numéro 766-2023 du 5 mai 2023, la RAMQ a été désignée pour communiquer au MCN les RP qu'elle détient et qui sont nécessaires aux fins des expérimentations requises avant le déploiement du Service d'authentification gouvernementale, et ce, malgré l'article 63 de la Loi sur l'assurance maladie (chapitre A-29). Le chargement initial des renseignements personnels en provenance du FIPA de la RAMQ vers le RAIG du MCN s'est effectué le 11 novembre 2022.

¹ Vise uniquement les personnes âgées de 14 ans et plus inscrites au FIPA, à l'exception des personnes décédées et des personnes en processus de demande pour qui la RAMQ n'a pas encore vérifié l'identité.

En vertu de ces décrets, des expérimentations ont été effectuées avec le ministère de la Famille (MFA) et la Société de l'assurance automobile du Québec (SAAQ) afin de tester le fonctionnement et l'efficacité du Service d'authentification gouvernementale. Les expérimentations requises avant le déploiement du Service d'authentification gouvernementale ont été terminées le 31 décembre 2023.

Changements significatifs

Par la prise du décret numéro 765-2023 du 3 mai 2023, le gouvernement a autorisé un changement significatif à la portée du projet 1 du Programme SQIN afin d'ajouter une plateforme de développement moderne spécifique à ce programme ainsi que des fonctionnalités nécessaires à la vérification de l'identité d'une personne dans un centre de services et au déploiement du Service d'authentification gouvernementale. Par la prise de ce décret, la phase d'exécution du projet 1 a été prolongée jusqu'au 31 décembre 2023.

Par la prise du décret numéro 1848-2023 du 20 décembre 2023, le gouvernement a autorisé un changement significatif à la portée du projet 1 du Programme SQIN afin de retirer le bloc « Accès bonifié aux prestations électroniques de services – Entreprises » du projet 1 et a autorisé la poursuite de la réalisation de la phase d'exécution du nouveau projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens ». Par la prise de ce décret, la phase d'exécution du projet 1 a été prolongée jusqu'au 13 mai 2025.

Par la prise du décret 1084-2024 du 10 juillet 2024, les organismes publics visés à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) seront tenus, au plus tard le 31 mars 2028, d'utiliser le Service d'authentification gouvernementale, comme service d'authentification des personnes, pour chacune de leurs PES. Il en est de même pour l'organisme public qui utilise déjà un autre service d'authentification des personnes pour une PES. Cette nouvelle exigence vise à faciliter les démarches des citoyens, en plus de permettre l'utilisation du plein potentiel du Service d'authentification gouvernementale, dans une perspective d'optimisation de l'efficacité gouvernementale de l'Administration en ligne.

Par l'indication d'application numéro IA-RI-2024-001-OP du 12 juillet 2024, le MCN a précisé certaines activités liées à l'identification et à l'authentification des personnes qui, aux fins du Service d'authentification gouvernementale, doivent être exécutées par les organismes publics visés. Cette indication d'application appuie le décret n° 870-2022 du 25 mai 2022.

Objectifs et motivation du projet 1

Le projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens » du Programme SQIN vise notamment à remplacer le service d'authentification clicSÉCUR, afin de permettre à un plus grand nombre de citoyens d'accéder plus facilement et de manière plus sécuritaire aux PES gouvernementales. Par l'institution du Service d'authentification gouvernementale, il vise aussi l'uniformisation des façons de faire des organismes publics (OP) en matière d'authentification des utilisateurs de leurs services en ligne.

Les OP recueillent et entreposent les données d'identification nécessaires à leur prestation de services et en fonction de la clientèle qu'ils servent. Ainsi, chaque organisme possède des renseignements qui concernent une portion des citoyennes et des citoyens. Conséquemment, les données d'identification des citoyens sont, dans plusieurs cas, présentes dans diverses bases de données gouvernementales.

À terme, les diverses bases de données gouvernementales comprenant les données d'identification des citoyens ne seront plus requises et le nombre de solutions permettant l'accès aux prestations de services gouvernementales sera considérablement réduit, diminuant d'autant les risques en sécurité de l'information (SI) et d'atteinte à la vie privée.

Les principaux objectifs du projet 1 sont les suivants :

- Améliorer la sécurité des RP des citoyens;
- Simplifier le processus d'authentification gouvernementale et de vérification d'identité;
- Élargir le bassin de la clientèle potentielle aux PES gouvernementales du Québec;
- Implanter un service unifié d'authentification gouvernementale qui contribue à la confiance du public dans les solutions technologiques de l'administration publique;
- Fournir aux utilisateurs un service d'authentification gouvernementale convivial, moderne, évolutif, extensible, sécuritaire et disponible.

Démonstration que le projet 1 est proportionné aux objectifs et aux risques d'atteinte à la vie privée

La démonstration de proportionnalité du projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens » aux objectifs et aux risques d'atteinte à la vie privée a été réalisée et est présentée à l'annexe 3 (non-publiée).

Détermination de l'objet de l'évaluation

La présente EFVP porte sur l'exécution du projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens », incluant la constitution et la tenue du RAIG aux fins du Service d'authentification gouvernementale.

2. Parties prenantes au projet

Partie prenante	Période d'implication dans le cycle de vie du projet 1	Rôle et responsabilité
MCN	Avant-projet et réalisation (planification et exécution)	• Agit comme maître d'ouvrage et maître d'œuvre du Programme SQIN • Assure la conformité du programme et des projets qui le composent aux règles applicables, incluant celles découlant des décrets liés au projet 1, du cadre légal et normatif, ainsi que des meilleures pratiques • Établit les normes de protection et assure la mise en œuvre des mesures de sécurité associées • Développe et exploite les solutions d'affaires et technologiques
Ministère de la Justice du Québec (MJQ)	Avant-projet et réalisation (planification et exécution)	• Assure le rôle de juriconsulte du gouvernement

Partie prenante	Période d'implication dans le cycle de vie du projet 1	Rôle et responsabilité
Ministère du Conseil exécutif (MCE)	Planification et réalisation (exécution)	Assure la cohérence des activités de communication gouvernementale en assumant la coordination des communications numériques, des campagnes de communication et des annonces publiques
Ministère de l'Emploi et de la Solidarité sociale (MESS – Services Québec)	Planification et réalisation (exécution)	- Agit comme OP partenaire - Assure le service à la clientèle de première ligne et la gestion des plaintes et commentaires - Participe au comité directeur du projet 1 et au comité stratégique
MFA	Planification et réalisation (exécution)	- Agit comme OP consommateur dès la période d'expérimentation - Participe au comité directeur du projet 1 et au comité stratégique
OP ayant recours au Service d'authentification gouvernementale pour permettre l'accès à leurs PES	Réalisation (exécution)	- Agit comme OP consommateur - Respecte les règles encadrant les activités du Service d'authentification gouvernementale
RAMQ	Réalisation (planification et exécution)	- Agit comme OP partenaire - Communique les renseignements nécessaires à la constitution et à la tenue du RAIG [REDACTED] - Offre le service à la clientèle quant aux renseignements dont il est responsable, incluant pour les demandes de rectification des RP qui sont communiqués pour la tenue du RAIG - Participe au comité directeur du projet 1 et au comité stratégique
Revenu Québec (RQ)	Réalisation (planification et exécution)	- Agit comme OP partenaire [REDACTED] - Offre le service à la clientèle quant aux renseignements dont il est responsable [REDACTED] - Participe au comité directeur du projet 1 et au comité stratégique

Partie prenante	Période d'implication dans le cycle de vie du projet 1	Rôle et responsabilité
SAAQ	Réalisation (planification et exécution)	• Agit comme OP consommateur dès la période d'expérimentation • Agit comme OP partenaire • [REDACTED] • Offre le service à la clientèle quant aux RP dont il est responsable • Offre le service de réalisation du processus d'identification en personne • Participe au comité directeur du projet 1 et au comité stratégique
Utilisateur	Réalisation (exécution)	• Consomme les services créés et déployés dans le cadre du projet 1 • Consent à la collecte, à la communication et à l'utilisation de ses RP aux fins du Service d'authentification gouvernementale

3. Renseignements personnels impliqués

Vue d'ensemble de la circulation des RP

RP recueillis, utilisés ou communiqués au MCN			
Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
RP prévus au décret² : Nom Nom du mari pour les femmes mariées avant le 2 avril 1981 Date de naissance (DDN) Date du décès Adresse de résidence active Adresse de résidence future Indicateur de présence d'un répondant Numéro d'assurance maladie (NAM)	RAMQ (FIPA)	Constitution et mise à jour du RAIG RP communiqués au MCN pour la création et la mise à jour du RAIG, soit ceux nécessaires à l'identification des personnes pour leur donner accès aux PES gouvernementales. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les RP suivants : Date du décès : RP communiqué au MCN aux fins de désactivation d'un compte au Service d'authentification gouvernementale à la suite d'un décès. Adresse de résidence : RP communiqué au MCN aux fins de correspondance. Indicateur de présence d'un répondant : renseignement communiqué au MCN aux fins de gestion de l'adresse de résidence (identification d'une période pendant laquelle l'adresse peut être celle d'une tierce personne).	Chargement initial des RP en provenance du FIPA de la RAMQ vers le RAIG du MCN³ et transmission de mises à jour de RP [REDACTED] dans un canal sécurisé (aucune transmission inverse possible). <i>N. B. Le NAM et le NAS sont des RP sensibles qui font l'objet d'une protection équivalente à celle contenue dans les règles particulières de protection mises en place dans le cadre des expérimentations⁴.</i> [REDACTED]

² Conformément au décret numéro 870-2022 du 25 mai 2022, au décret numéro 1690-2022 du 26 octobre 2022 modifié par le décret 766-2023 du 3 mai 2023 et à l'autorisation de mobilité des données numériques gouvernementales 2023-01 du gestionnaire de données numériques gouvernementales du 18 décembre 2023.

³ Ibid.

⁴ Ibid. Règles particulières de protection du NAS et du NAM dans le cadre des expérimentations requises avant le déploiement du Service d'authentification gouvernementale du projet d'intérêt gouvernemental, Programme SQIN.

RP recueillis, utilisés ou communiqués au MCN

Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
Numéro d'assurance sociale (NAS) Identifiant sectoriel de la RAMQ			
Indicateur de changement d'adresse de résidence effectué par l'entremise du Service québécois de changement d'adresse (SQCA) Date de début et de fin de validité de l'adresse de résidence	RAMQ	Mise à jour du RAIG (gestion de l'adresse de résidence) Spécifiquement pour les RP suivants : Indicateur de changement d'adresse de résidence effectué par l'entremise du SQCA : renseignement communiqué au MCN aux fins de gestion de l'adresse de résidence Date de début et de fin de validité de l'adresse de résidence : renseignement communiqué au MCN aux fins de gestion de l'adresse de résidence (identification d'une période de validité de l'adresse de résidence active).	Transmission de mises à jour de RP dans un canal sécurisé (aucune transmission inverse possible).

RP recueillis, utilisés ou communiqués au MCN

Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
Adresse courriel Nom d'utilisateur Mot de passe Code de sécurité	Utilisateurs du Service d'authentification gouvernementale	Création, modification et accès au compte au Service d'authentification gouvernementale RP recueillis et utilisés, sur la base d'un consentement, pour la création, la modification ou l'accès au compte au Service d'authentification gouvernementale, et aux fins d'authentification des personnes en vue de leur donner accès aux PES gouvernementales. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les RP suivants : Adresse courriel : RP utilisé aux fins de correspondance. Code de sécurité : renseignement [REDACTED] recueilli et utilisé aux fins d'authentification (deuxième facteur d'authentification). [REDACTED] [REDACTED]	Interface d'échanges informatisé du Service d'authentification gouvernementale. Transactions informatiques sécurisée [REDACTED] [REDACTED] Génération automatique d'un code de sécurité. Transmission automatique par courriel d'un code de sécurité [REDACTED] [REDACTED]

RP recueillis, utilisés ou communiqués au MCN

Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
Nom DDN NAM NAS Numéro d'avis de cotisation Numéro de référence de la carte d'assurance maladie Numéro de référence du permis de conduire	Utilisateurs du Service d'authentification gouvernementale	Processus d'identification en ligne RP recueillis ou utilisés, sur la base d'un consentement, aux fins de l'identification des personnes en vue de leur donner accès aux PES gouvernementales. Au surplus de la finalité mentionnée ci-dessus et spécifiquement pour les RP suivants : [REDACTED] Nom, DDN, NAS, numéro de référence de la carte d'assurance maladie ou numéro de référence du permis de conduire : RP recueillis et utilisés lorsque le mot de passe est oublié.	Interface d'échanges automatisés du Service d'authentification gouvernementale. Transactions informatiques sécurisées [REDACTED] [REDACTED]

RP recueillis, utilisés ou communiqués au MCN

Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
Adresse de résidence Indicateur de présence d'un répondant Secret d'identification par la poste [REDACTED]	Utilisateurs du Service d'authentification gouvernementale MCN [REDACTED]	Création et validation d'un secret d'identification par la poste RP recueillis ou utilisés, sur la base d'un consentement, pour l'identification des personnes en vue de leur donner accès aux PES gouvernementales. Au surplus de la finalité mentionnée ci-dessus et spécifiquement pour les RP suivants : Indicateur de présence d'un répondant : RP utilisé aux fins de vérification de l'adresse. Adresse de résidence : RP recueilli et utilisé aux fins de correspondance. Secret d'identification par la poste : renseignement [REDACTED] recueilli et utilisé [REDACTED] pour l'identification des personnes. [REDACTED]	Interface d'échanges automatisés du Service d'authentification gouvernementale. Transactions informatiques sécurisées [REDACTED] [REDACTED] Génération d'un secret d'identification par la poste ayant une durée de validité limitée. [REDACTED] Génération automatique d'une lettre.

RP recueillis, utilisés ou communiqués au MCN

Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
Nom DDN NAM Adresse courriel Code de sécurité (deuxième facteur d'authentification) Types des pièces d'identité fournies, dont une avec photo	Utilisateurs du Service d'authentification gouvernementale	Processus d'identification en personne RP recueillis et utilisés, sur la base d'un consentement, pour l'identification des personnes en vue de leur donner accès aux PES gouvernementales⁶. Spécifiquement pour les RP suivants : Adresse courriel et code de sécurité : RP utilisés pour valider que l'utilisateur est détenteur d'un compte au Service d'authentification gouvernementale. Type des pièces d'identité fournies : RP recueilli aux fins de vérification à posteriori.	Entente de collaboration entre l'OP partenaire et le MCN. Échanges dans un point de service. Interface d'échanges automatisés [REDACTED] Transactions informatiques sécurisées [REDACTED]
Nom DDN NAM Adresse courriel Adresse de résidence Renseignements en lien avec l'utilisation du compte au Service d'authentification gouvernementale Numéro de téléphone	Utilisateurs du Service d'authentification gouvernementale MESS (Services Québec)	Demande d'intervention au compte RP communiqués au MCN et utilisés, sur la base du consentement, pour l'identification des utilisateurs en vue de traiter des demandes téléphoniques d'intervention au compte, soit pour bloquer ou réactiver un compte, modifier une adresse courriel ou signaler un problème technique. Au surplus de la finalité mentionnée ci-dessus et spécifiquement pour le RP suivant : Adresse courriel : RP utilisé aux fins de correspondance. Spécifiquement pour le RP suivant : Numéro de téléphone : RP utilisé aux fins de correspondance.	Collaboration avec un OP partenaire pour assurer le service à la clientèle de première ligne, incluant les demandes d'intervention au compte et la gestion des plaintes et commentaires. Communication téléphonique. Notifications transmises par courriel. Formulaire électronique de demande d'intervention au compte. Partage sécurisé de document. Interface d'échanges automatisés [REDACTED]. Transactions informatiques sécurisées [REDACTED].

⁶ En vertu du décret numéro 765-2023 du 3 mai 2023.

RP recueillis, utilisés ou communiqués au MCN

Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
		Plainte ou commentaire Seuls les renseignements fournis parmi les suivants sont communiqués au MCN et utilisés, sur la base du consentement, aux fins de correspondance en vue de traiter une plainte ou un commentaire : nom, adresse courriel et numéro de téléphone.	Formulaire Web de plainte ou de commentaire.
Identifiants : [REDACTED] [REDACTED] au Service d'authentification gouvernementale [REDACTED] [REDACTED] Adresse IP Ville et pays	Utilisateurs du Service d'authentification gouvernementale MCN [REDACTED]	Sécurité et soutien aux opérations RP utilisés à des fins de sécurité et de soutien aux opérations [REDACTED] Spécifiquement pour les RP suivants : Ville et pays : RP inférés à partir de l'adresse IP.	[REDACTED] Transactions informatiques sécurisées [REDACTED]. [REDACTED]
Identifiants [REDACTED] [REDACTED] [REDACTED]	MCN [REDACTED]	Statistiques de performance et de qualité RP utilisés aux fins de production de statistiques en vue d'évaluer la performance et de mesurer la qualité du Service d'authentification gouvernementale, dans une perspective d'amélioration continue.	Transactions informatiques sécurisées [REDACTED] Procédés techniques automatisés de dépersonnalisation.

RP recueillis, utilisés ou communiqués au MCN

Description des RP	Provenance	Description des finalités	Moyen d'interaction et modalité
Adresse courriel	MFA MCN	Comparaison de données⁷ RP communiqué au MCN et utilisé aux fins de comparaison de données pendant la période requise de transition pour le rattachement de certaines PES gouvernementales.	Transfert sécurisé de fichier. Transactions informatiques sécurisées [REDACTED]
Identifiant [REDACTED] [REDACTED] [REDACTED] Adresse courriel ou nom d'utilisateur Langue d'affichage : FR (pour français) ou EN (pour anglais)	Utilisateurs du Service d'authentification gouvernementale MCN [REDACTED]	Témoins de connexion RP utilisés afin d'assurer le bon fonctionnement du site Web du Service d'authentification gouvernementale et afin d'améliorer et de personnaliser l'expérience utilisateur.	Transactions informatiques sécurisées [REDACTED] [REDACTED]

RP communiqués par le MCN

Description des RP	Destinataire	Description des finalités	Moyen d'interaction et modalité
Code de sécurité	Utilisateurs du Service d'authentification gouvernementale	Création, modification et accès au compte au Service d'authentification gouvernementale Renseignement communiqué, sur la base du consentement, aux fins d'authentification (deuxième facteur d'authentification) en vue de créer, de modifier ou d'accéder au compte au Service d'authentification gouvernementale.	Génération automatique du code [REDACTED] [REDACTED] Transmission automatique par courriel du code.

⁷ En vertu de l'Indication d'application numéro IA-RI-2024-001-OP du 12 juillet 2024.

RP communiqués par le MCN

Description des RP	Destinataire	Description des finalités	Moyen d'interaction et modalité
Nom DDN NAS Numéro d'avis de cotisation	RQ	Validation d'un secret d'identification RP communiqués, sur la base d'un consentement, aux fins du processus d'identification en ligne pour la validation d'un secret d'identification.	Transmission dans un canal sécurisé.
 Numéro de référence de la carte d'assurance maladie	RAMQ	Validation d'un secret d'identification RP communiqués, sur la base d'un consentement, aux fins du processus d'identification en ligne pour la validation d'un secret d'identification.	Transmission dans un canal sécurisé.
Nom DDN Numéro de référence du permis de conduire	SAAQ	Validation d'un secret d'identification RP communiqués, sur la base d'un consentement, aux fins du processus d'identification en ligne pour la validation d'un secret d'identification.	Transmission dans un canal sécurisé. 
Nom Adresse de résidence Secret d'identification par la poste	 OP partenaire	Transmission d'un secret d'identification par la poste RP communiqués, sur la base d'un consentement, aux fins du processus d'identification en ligne pour l'impression et l'expédition d'une lettre.	Transfert d'information sécurisé. Transmission  des lettres en lot. Impression des lettres sur papier. Lettres transmises par courrier postal.

RP communiqués par le MCN

Description des RP	Destinataire	Description des finalités	Moyen d'interaction et modalité
Identifiant [REDACTED] [REDACTED] Adresse courriel professionnelle	SAAQ MCN (SEAO)	Accès à une PES (niveau 1)⁸ RP à caractère public communiqués aux fins d'identification des personnes déléguées dans l'exercice de fonctions professionnelles en vue de leur donner accès à certaines PES gouvernementales de niveau 1. Spécifiquement pour le RP suivant : Adresse courriel professionnelle : RP à caractère public communiqué lors de tous les accès aux PES concernées du MCN (SEAO). Au surplus de la finalité mentionnée ci-dessus et spécifiquement pour le RP suivant : Adresse courriel professionnelle : RP à caractère public communiqué aux fins de correspondance lors du premier accès aux PES concernées de la SAAQ.	Transmission dans un canal sécurisé.

⁸ Les niveaux d'assurance de l'identité sont détaillés dans les Règles relatives à l'assurance de l'identité numérique.

RP communiqués par le MCN

Description des RP	Destinataire	Description des finalités	Moyen d'interaction et modalité
Identifiants   Nom DDN NAM Adresse de résidence Adresse courriel NAS partiel	SAAQ MFA Autorité des marchés financiers (AMF) RAMQ MSSS Ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs (MELCCFP) Groupement des assureurs automobiles (GAA)	Accès à une PES (niveau 2) ⁹ RP communiqués, sur la base d'un consentement, aux fins d'identification des personnes en vue de leur donner accès à certaines PES gouvernementales de niveau 2. Spécifiquement pour les RP suivants : Nom, DDN : RP communiqués lors du premier accès aux PES concernées de la SAAQ, du MFA, de l'AMF et du GAA. Adresse de résidence : RP communiqué lors du premier accès aux PES concernées du MFA et de l'AMF. Adresse courriel : RP communiqué lors du premier accès aux PES concernées de l'AMF. NAM : RP communiqué lors du premier accès aux PES concernées du MSSS. NAS partiel : RP communiqué lors du premier accès aux PES concernées du MELCCFP. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les RP suivants : Nom, DDN : RP communiqués aux fins de remplissage automatisé d'un formulaire d'inscription pour la création d'un compte utilisateur lors du premier accès aux PES concernées du MFA et de l'AMF. Nom, DDN, adresse de résidence et adresse courriel : RP communiqués aux fins du service à la clientèle lors du premier accès aux PES concernées de l'AMF.	Transmission dans un canal sécurisé.

⁹ *Ibid.*

RP communiqués par le MCN

Description des RP	Destinataire	Description des finalités	Moyen d'interaction et modalité
RP détenus aux fins du Service d'authentification gouvernementale : [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	Fournisseurs de services infonuagiques	Hébergement des données RP hébergés dans les infrastructures de fournisseurs de services infonuagiques.	Transactions informatiques sécurisées. [REDACTED]
Identifiant [REDACTED] [REDACTED] Adresse courriel ou nom d'utilisateur Langue d'affichage : FR (pour français) ou EN (pour anglais)	Fichier témoin du navigateur Web des utilisateurs du Service d'authentification gouvernementale	Témoins de connexion RP communiqués afin d'assurer le bon fonctionnement du site Web du Service d'authentification gouvernementale, d'améliorer et de personnaliser l'expérience utilisateur.	Transactions informatiques sécurisées [REDACTED] [REDACTED] [REDACTED] au Service d'authentification gouvernementale [REDACTED]

RP conservés et détruits			
Catégorie de RP	Type de support	Description	Moyen d'interaction et modalité
RP détenus aux fins du au Service d'authentification gouvernementale [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	Infonuagique	Hébergement des données RP conservés par des fournisseurs en services infonuagiques conformément aux règles de conservation de RP établies par le MCN.	RP conservés le temps nécessaire pour atteindre les finalités pour lesquelles ils ont été recueillis et pour respecter les obligations découlant de la Loi sur l'accès et du calendrier de conservation du MCN ¹⁰ . RP détruits lorsque les finalités pour lesquelles ils ont été recueillis sont atteintes.
RP contenus dans le fichier témoin du navigateur Web des utilisateurs	Numérique	Témoins de connexion Spécifiquement pour les RP suivants : Identifiant [REDACTED] t langue d'affichage : RP conservés pour la durée d'une session, soit jusqu'à la fermeture de la fenêtre du navigateur Web ou jusqu'à ce que la session soit expirée. Adresse courriel ou nom d'utilisateur : RP conservé jusqu'à l'expiration du témoin de connexion.	RP détruits au moment de la suppression par l'utilisateur ou à la fin de la session.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

¹⁰ Élaboré et approuvé conformément à la Loi sur les archives (RLRQ, c. A-21.1).

RP conservés et détruits

Catégorie de RP	Type de support	Description	Moyen d'interaction et modalité
RP contenus dans la demande d'intervention au compte	Numérique	RP conservés par le MCN à la suite de la transmission de la demande d'intervention au compte par le MESS (Services Québec) conformément aux règles de conservation de RP établies par le MCN.	RP conservés le temps nécessaire pour atteindre les finalités pour lesquelles ils ont été recueillis et pour respecter les obligations découlant de la Loi sur l'accès et du calendrier de conservation du MCN¹². RP détruits lorsque les finalités pour lesquelles ils ont été recueillis sont atteintes.
RP contenus dans la plainte ou le commentaire	Numérique	RP conservés par le MCN à la suite de la transmission de la plainte ou du commentaire par le MESS (Services Québec) conformément aux règles de conservation de RP établies par le MCN.	RP conservés le temps nécessaire pour atteindre les finalités pour lesquelles ils ont été recueillis et pour respecter les obligations découlant de la Loi sur l'accès et du calendrier de conservation du MCN¹³. RP détruits lorsque les finalités pour lesquelles ils ont été recueillis sont atteintes.

¹¹ *Ibid.*

¹² *Ibid.*

¹³ *Ibid.*

4. Moyens mis en place pour respecter les obligations et les principes de protection des renseignements personnels (PRP)

Les obligations et les principes de protection des renseignements personnels (PRP) applicables au projet 1 sont notamment prévus dans le cadre légal et normatif énumérés à l'annexe 1. On y retrouve notamment les documents de gouvernance du MCN concernant la PRP en vigueur ainsi que les différents décrets applicables.

Les principales obligations et principes de PRP qui ont été appliqués au projet 1 ainsi que des exemples de moyens pour y répondre sont les suivants :

- **Responsabilité.** Le MCN est imputable quant à la gestion des RP qu'il détient et reconnaît son devoir de les protéger, que leur conservation soit assurée par lui-même ou par un tiers.
- **Détermination des finalités.** Les finalités pour lesquelles le MCN recueille des RP sont légitimes et établies avant la collecte.
- **Limitation de la collecte.** Le MCN recueille uniquement les RP nécessaires aux fins déterminées.
- **Protection dès la conception et par défaut.** Le Service d'authentification gouvernementale est conçu dans le respect de la vie privée des utilisateurs et les paramètres de confidentialité qu'il comprend protègent la vie privée par défaut.
- **Consentement.** Les utilisateurs sont adéquatement informés des finalités déterminées et y consentent librement, à moins d'exception.
- **Limitation de l'utilisation, de la communication et de la conservation.** Le MCN utilise et communique les RP recueillis aux fins déterminées ou à des fins compatibles, sauf consentement ou exception légale. Il limite l'accès à ces RP aux personnes autorisées et ne les conserve pas plus longtemps que nécessaire.
- **Exactitude.** Le MCN tient les RP à jour et s'assure qu'ils sont exacts et complets au moment où il les utilise ou il les communique.
- **Sécurité.** Le MCN prend des mesures de sécurité appropriées pour protéger en tout temps les RP qu'il détient contre la perte, le vol, la modification, la communication ou la destruction non autorisée. En cas d'incident, le MCN réagit promptement et avertit les personnes concernées et les autorités, sauf exception.
- **Transparence.** Le MCN fournit les informations pertinentes aux utilisateurs au moment de la collecte ou du consentement.
- **Droits à l'égard des RP.** Les utilisateurs peuvent accéder aux RP qui les concernent et en demander la rectification ou, dans certains cas, la suppression. Ils peuvent également formuler une plainte ou un commentaire. Le MCN a établi des processus accessibles pour permettre l'exercice de ces droits.

Responsabilité

Énoncé	Moyen mis en place
Règles de gouvernance encadrant les RP détenus aux fins du projet 1	Règles adoptées et accessibles au personnel concerné. Règles transmises à la Commission d'accès à l'information (CAI) pour information.
Formation et sensibilisation en matière de PRP	Activités de formation et de sensibilisation offertes aux employés concernés de la direction générale responsable du projet 1. Processus d'accueil et d'intégration pour tout nouvel employé de la direction générale responsable du projet 1. Registre des activités de sensibilisation et de formation en matière de PRP, accessible au personnel concerné. Révision en continu du plan de formation et de sensibilisation.
Ressources dédiées à la PRP	Soutien-conseil en continu pour le développement et l'exploitation du Service d'authentification gouvernementale dans le respect des obligations tout au long du cycle de vie des RP.
Ententes contractuelles avec les tiers sur l'encadrement notamment la communication de RP à l'extérieur du Québec	Directive sur l'encadrement des exigences de sécurité vis-à-vis des tiers, accessible au personnel concerné. Lignes directrices du Courtier infonuagique qui favorisent le respect des obligations relatives au maintien d'une protection adéquate pour l'hébergement des RP. Audit externe réalisé par les fournisseurs en infonuagique préalablement à la signature d'un contrat, lequel vise le respect des plus hautes normes et des meilleures pratiques en matière de sécurité de l'information et de protection, notamment celles des RP. Clauses contractuelles qui prévoient les mesures PRP appliquées par les tiers, qui sont mandatés pour l'hébergement des données, notamment en matière de conservation de données de journalisation et de continuité du Service d'authentification gouvernementale advenant un sinistre majeur. Dépôt annuel, par les fournisseurs de services en infonuagique, de pièces justificatives requises auprès du MCN (ex. : rapport d'audit de SI basé sur le standard SSAE 16/SOC 2 Type II, attestations de destruction) pour démontrer leur conformité. Travaux en cours auprès des OP partenaires pour la mise en œuvre des activités d'audit externe. Registre en application de l'article 67.3 (entente de collecte en collaboration avec un autre organisme et communication sans consentement), accessible au personnel concerné.

Énoncé	Moyen mis en place
Rapports en application des lois applicables	Rapport d'EFVP publié conformément aux exigences de la Loi favorisant la transformation numérique de l'administration publique (LFTNAP) et transmis selon les exigences de la LGGRI. Rapport annuel concernant les RP recueillis, utilisés et communiqués aux fins du Service d'authentification gouvernementale et du SQIN en application de la LFTNAP et de la LGGRI publié et transmis selon les exigences des lois applicables.
Confiance du public dans le développement de solutions technologiques assurant le respect de la vie privée	Étude menée par la firme SOM au sujet du Service d'authentification gouvernementale (de septembre à décembre 2023) et mise en place d'un plan d'action (février 2024). Campagne de promotion au sujet du respect de la vie privée dans le cadre des activités du Service d'authentification gouvernementale (de juillet 2024 à mars 2025).

Détermination des finalités

Énoncé	Moyen mis en place
Finalités déterminées avant la collecte	Finalités de la collecte de RP aux fins du Service d'authentification gouvernementale, déterminées par décret. Description de certaines activités (finalités) liées à l'identification et à l'authentification des personnes qui, aux fins du Service d'authentification gouvernementale, doivent être exécutées par les organismes publics visés (indication d'application concernant les activités liées à l'identification et à l'authentification des personnes aux fins du Service d'authentification gouvernementale). Finalités pour lesquelles les RP font l'objet d'une autorisation de mobilité par le gestionnaire des données numériques gouvernementales déterminées par décret. Finalités précisées dans les règles encadrant la gouvernance des RP aux fins du Service d'authentification gouvernementale Collecte des RP en conformité avec les Règles relatives à l'assurance de l'identité numérique. Vue d'ensemble de la circulation des RP impliqués dans le Service d'authentification gouvernementale présentant la description des finalités, accessible au personnel concerné.

Limitation de la collecte

Énoncé	Moyen mis en place
Légitimité à collecter les RP aux fins déterminées	Projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens » du Programme SQIN désigné par la prise du décret numéro 115-2018 du 14 février 2018 comme projet en ressources informationnelles d'intérêt gouvernemental. Désignation du MCN, par la prise du décret numéro 870-2022 du 25 mai 2022, pour agir comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale. Autorisation de mobilité des données numériques gouvernementales 2023-01 du gestionnaire de données numériques gouvernementales du 18 décembre 2023.
Limitation de la collecte de RP à ce qui est nécessaire aux fins déterminées	Évaluation de la nécessité de la collecte des RP par rapport aux objectifs du projet 1 et à la solution proposée, et ce, avant la prise du décret numéro 870-2022 du 25 mai 2022. Analyse approfondie des RP nécessaires à l'exercice des attributions du MCN et à la mise en œuvre des processus d'authentification et d'identification des personnes qui souhaitent accéder à certaines PES gouvernementales par l'entremise du Service d'authentification gouvernementale. Ce processus comprend notamment la constitution et la tenue du RAIG, la création, la modification et l'accès au compte au Service d'authentification gouvernementale ainsi que le processus d'identification en ligne et en personne. Propositions faites à l'utilisateur afin de limiter la collecte de ses RP (Politique de confidentialité du Service d'authentification gouvernementale). Champs à remplissage obligatoires prédéterminés dans l'interface d'échanges automatisés du Service d'authentification gouvernementale sans possibilité d'ajouter d'autres RP. Application de règles d'affaires pour valider le contenu de la saisie dans les champs à remplissage obligatoires prédéterminés.
Limitation de la collecte des <u>RP sensibles</u> aux fins déterminées	Analyse de plusieurs combinaisons de RP pour la réalisation du processus d'identification en ligne (ex. : nom, DDN et code postal; nom, DDN et nom de la mère) en tenant compte de l'existence des cas répertoriés de personnes ayant les mêmes noms, prénoms et DDN. Cette analyse a permis de démontrer que la combinaison du NAS et du NAM limite les risques de fraude par ingénierie sociale. Absence de pièce d'identité citoyenne québécoise (avec un numéro unique pour chaque citoyen) rendant difficile la corroboration des attributs de base (nom, prénom, DDN) auprès de la source de confiance et de les relier à une seule identité.

Énoncé	Moyen mis en place
	Réalisation d'une analyse basée sur des identifiants existants démontrant qu'à part le NAS et le NAM, aucun autre identifiant présent dans les bases de données des OP ne peut donner l'assurance de l'unicité de l'identité d'un citoyen.  Combinaison du NAS et du NAM permettant de garantir la qualité des données en assurant en amont la fiabilité lors de l'identification en ligne de l'utilisateur et en aval lors de l'utilisation par l'ensemble des OP de la même information d'identité.

Protection dès la conception et par défaut

Énoncé	Moyen mis en place
Protection de la vie privée dès la conception	Réalisation d'une EFVP. Accompagnement des équipes spécialisées dans toutes les phases du projet 1 afin d'assurer l'intégration des mesures relatives à la protection de la vie privée.
Protection de la vie privée par défaut	Solution administrée selon les règles et les protocoles établis en vue d'assurer le plus haut niveau de confidentialité sans intervention des utilisateurs. Paramétrage des fonctionnalités assurant le plus haut niveau de confidentialité sans intervention des utilisateurs. Évaluation en continu des témoins de connexion utilisés aux fins du Service d'authentification gouvernementale. Informations fournies aux utilisateurs quant à l'utilisation des témoins de connexion, notamment le témoin de profilage (fenêtre informative et Politique de confidentialité du Service d'authentification gouvernementale). Informations fournies à l'utilisateur quant aux moyens pour activer la fonction de localisation ou la refuser (fenêtre informative et Politique de confidentialité du Service d'authentification gouvernementale).

Consentement

Énoncé	Moyen mis en place
Consentement valide	Accompagnement des équipes spécialisées dans toutes les phases du projet 1 afin d'assurer le respect des critères de validité du consentement.

Énoncé	Moyen mis en place
	Forme du consentement et méthode d'obtention appropriées à la sensibilité des RP impliqués et adaptés aux personnes visées, au contexte et au type d'interface. Informations requises fournies à l'utilisateur au moment de la demande de consentement spécifiant notamment les finalités de l'utilisation ou de la communication concernée. Informations fournies à l'utilisateur concernant les conséquences d'un refus ou, le cas échéant, d'un retrait de son consentement suivant une demande facultative.
Exceptions au consentement	Obtention du consentement pour toute utilisation et communication de RP aux fins déterminées, sauf exception comme pour la comparaison de données pendant la période requise de transition.
Documentation de l'obtention du consentement	Journalisation des événements liés au consentement.
Retrait du consentement	Informations fournies à l'utilisateur concernant son droit de retrait du consentement (Politique de confidentialité du Service d'authentification gouvernementale).

Limitation de l'utilisation, de la communication et de la conservation

Énoncé	Moyen mis en place
Utilisation et communication aux seules fins déterminées	Politique de confidentialité et de protection des renseignements personnels du MCN agissant à titre de source officielle de données numériques gouvernementales, accessible au personnel concerné. Procédure encadrant la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels dans le cadre du Service québécois d'identité numérique, accessible au personnel concerné. Limitation de la communication des RP à des tiers situés à l'extérieur du Québec aux seules fins de prévention, de détection ou de diminution des impacts en cas d'atteinte ou de risque d'atteinte de confidentialité, de disponibilité ou d'intégrité. Analyse par les équipes spécialisées des demandes d'utilisation et de communication de RP détenus aux fins du Service d'authentification gouvernementale à des fins compatibles (primaires et secondaires) pour réaliser certaines activités en accord avec le décret à l'aide du formulaire de demande de communication de RP du Service d'authentification gouvernementale vers l'OP.

Énoncé	Moyen mis en place
	Limitation de l'utilisation secondaire des RP aux seules fins statistiques avec dépersonnalisation dans le but d'évaluer la performance ou de mesurer la qualité du Service d'authentification gouvernementale dans une perspective d'amélioration continue. Limitation de la communication des RP nécessaire au suivi d'une demande d'intervention au compte au Service d'authentification gouvernementale, seul le numéro de la demande est communiqué à l'utilisateur. Registre en application de l'article 67.3 (utilisation à une autre fin), accessible au personnel concerné. Vue d'ensemble de la circulation des RP impliqués dans le Service d'authentification gouvernementale présentant la description des finalités, accessible au personnel concerné.
Conservation des RP pour la réalisation des fins déterminées	Politique de confidentialité et de protection des renseignements personnels du ministère de la Cybersécurité et du Numérique agissant à titre de source officielle de données numériques gouvernementales, accessible au personnel concerné. Procédure encadrant la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels dans le cadre du Service québécois d'identité numérique, accessible au personnel concerné. Calendrier de conservation du MCN et règle de conservation pour les RP contenus dans le RAIG, établie par le MCN et approuvée par la Bibliothèque et Archives nationales du Québec (BAnQ). Toute modification apportée à un RP au FIPA de la RAMQ entraîne une modification du RP concerné au RAIG (aucune conservation d'historique des RP modifiés). Programme d'élaboration du Plan de conservation et de destruction de RP détenus aux fins du Service d'authentification gouvernementale.

Exactitude

Énoncé	Moyen mis en place
Assurance de la qualité des RP détenus aux fins du Service d'authentification gouvernementale	Procédure encadrant la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels dans le cadre du Service québécois d'identité numérique. Informations fournies à l'utilisateur au regard de sa responsabilité concernant la mise à jour de ses RP (Politique de confidentialité du Service d'authentification gouvernementale). Transmission de mises à jour des RP [REDACTED] en provenance de la RAMQ dans un canal sécurisé (aucune transmission inverse possible). Analyse approfondie des processus de collecte en provenance d'une source de confiance avant la sélection de la source. Champ à remplissage prédéfini pour la saisie des RP dans l'interface d'échanges automatisés du Service d'authentification gouvernementale. Règles d'affaires mises en application pour valider la qualité des données, comprenant des RP (validation des formats et des contextes rendant notamment impossible l'inscription de certaines dates dans le futur dans le RAIG). Règles d'affaires mises en application pour la gestion des adresses de résidence en vue de la transmission de correspondance. Mise à jour de l'adresse courriel et du mot de passe par l'entremise de la gestion de compte en ligne. Mise à jour de l'adresse courriel par l'entremise d'une demande téléphonique d'intervention au compte. Journalisation des événements liés à certaines mises à jour.

Sécurité

Énoncé	Moyen mis en place
Mesures de sécurité physiques, techniques et organisationnelles	Application des mesures pour assurer le caractère confidentiel de tous les RP détenus aux fins du Service d'authentification gouvernementale qui prennent effet en amont de la collecte, notamment par le déploiement d'une infrastructure technologique sécuritaire. Mesures minimales de sécurité au regard des données lors de l'utilisation de solutions technologiques [REDACTED] Cadre normatif en matière de RP, de SI et des conflits d'intérêts.

Énoncé	Moyen mis en place
	Plusieurs types de mesures¹⁴ appliquées pour protéger les RP contre tout accès, utilisation, communication ou destruction non autorisés, toute perte ou toute autre forme d'atteinte à leur protection. Avis de sécurité de l'information émis par le MCN permettant d'identifier les mesures de sécurité appropriées pour protéger les RP durant tout leur cycle de vie, incluant : • des mesures physiques, comme la restriction des accès aux locaux; • des mesures techniques ou technologiques, comme le chiffrement, le hachage [REDACTED] ou de mécanismes d'authentification à facteurs multiples; • des mesures organisationnelles, comme l'adoption et l'application de règles en matière de SI et de PRP, plan de reprise en cas de sinistre. Notifications transmises automatiquement par courriel aux utilisateurs pour les informer de la survenance d'événements liés au compte.
Mesures de sécurité proportionnelles au degré de sensibilité des RP	Mesures de protection équivalentes à celles des règles particulières de protection du NAM et du NAS mises en place dans le cadre des expérimentations requises avant le déploiement du Service d'authentification gouvernementale. Mécanismes de contrôle et de vérification de l'efficacité et du respect des mesures de sécurité appliquées au Service d'authentification gouvernementale.
Gestion des accès	Processus de révision de l'identité et des droits d'accès, accessible au personnel concerné. RP accessibles aux personnes qui détiennent les autorisations requises lorsque cela est nécessaire à l'exécution de leurs tâches. Rôles et responsabilités des intervenants établis dans le Service d'authentification gouvernementale (profils d'accès fondés sur les tâches, en mode consultation). [REDACTED] Droit d'accès aux RP sensibles octroyés de façon ponctuelle et temporaire pour répondre à une demande précise et assortie d'un délai prédéfini. Mécanismes de contrôle et de surveillance des droits d'accès afin de détecter les abus de droit, le cas échéant : • Journalisation de tout accès aux RP; • Analyse automatisée et périodique des journaux afin de déceler les anomalies ou les irrégularités;

¹⁴ La liste complète des mesures applicables au Service d'authentification gouvernementale et au RAIG n'est pas accessible pour des raisons de sécurité.

Énoncé	Moyen mis en place
	- Alerte déclenchée pour tout accès aux RP contenus dans le RAIG et vérification visant à confirmer le droit d'accès; - Registre des membres du personnel ayant un accès physique ou informatique aux RP détenus aux fins du Service d'authentification gouvernementale, accessible au personnel autorisé. Inventaire des catégories de personnes qui ont accès aux RP, accessible au personnel concerné.
Règles de gouvernance concernant les incidents de sécurité, incluant les incidents de confidentialité	Directive sur la gestion des menaces, des vulnérabilités, des incidents de sécurité de l'information et des incidents impliquant des renseignements personnels, accessible au personnel concerné. Processus de signalement d'un incident en passant par les canaux de communication prédéterminés (téléphone ou courriel), accessible à l'ensemble du personnel du MCN. Processus de gestion des incidents de SI, qui relève du Centre organisationnel de cyberdéfense (COCD), prévoyant l'implication du RPRP lorsque des RP sont impliqués. Lorsque requis, les personnes concernées par un incident de confidentialité ainsi que la CAI sont avisées. Processus de signalement de compromission d'un compte au Service d'authentification gouvernementale, accessible au personnel concerné. Outils de surveillance utilisés pour la détection d'incident de sécurité. Actions correctrices identifiées en concertation avec les intervenants appropriés et réalisation des travaux dans les temps et les modalités prescrites en fonction de la situation. Registre des incidents de confidentialité.

Transparence

Énoncé	Moyen mis en place
Informations fournies aux utilisateurs concernant les règles de gouvernance encadrant les RP détenus aux fins du projet 1	Plan de communication pour promouvoir les aspects de PRP et de sécurité de l'information en lien avec le Service d'authentification gouvernementale.
Informations fournies aux utilisateurs concernant les pratiques de gestion et de protection des RP	Section dédiée au Service d'authentification gouvernementale accessible sur Québec.ca, dans laquelle des informations sont fournies au sujet de la création d'un compte et des documents requis aux fins du processus d'identification.

Énoncé	Moyen mis en place
détenus aux fins du Service d'authentification gouvernementale	Capsule vidéo présentant les processus de création d'un compte et d'identification, diffusée dans la section dédiée au Service d'authentification gouvernementale sur Québec.ca. Documents en lien avec la gestion des RP détenus aux fins du Service d'authentification gouvernementale présentés de manière claire et compréhensible diffusés sur le site du Service d'authentification gouvernementale (Politique de confidentialité du Service d'authentification gouvernementale et Conditions d'utilisation du Service d'authentification gouvernementale). Informations requises fournies aux utilisateurs par un agent aux fins du processus d'identification en personne ou d'une demande téléphonique d'intervention au compte. Informations générales concernant le consentement accessibles dans le bandeau de bas de page du site Web du Service d'authentification gouvernementale.

Droits à l'égard des RP

Énoncé	Moyen
Demandes d'accès et de rectification	Accessibilité pour consultation à certains RP détenus aux fins du Service d'authentification gouvernementale par l'entremise de la gestion de compte en ligne. Politique de confidentialité du Service d'authentification gouvernementale détaillant les droits d'accès aux RP et de rectification, laquelle est publiée sur le site du Service d'authentification gouvernementale. Procédure de traitement des demandes d'accès et de rectification des RP en lien avec le Service d'authentification gouvernementale, laquelle est accessible au personnel concerné.
Plainte ou commentaire concernant la gestion des RP	Moyens pour formuler une plainte ou un commentaire concernant la gestion des RP : téléphone, formulaire électronique transmis par courriel ou par la poste (Politique de confidentialité du Service d'authentification gouvernementale). Politique et processus de gestion des plaintes et des commentaires pour le Service d'authentification gouvernementale prévoyant la transmission au RPRP de toute plainte et commentaire concernant la gestion des RP, lesquels sont accessibles au personnel concerné. Les rôles et responsabilités sont définis pour tous les secteurs impliqués. MESS (Services Québec) mandaté pour la gestion des plaintes et des commentaires en lien avec l'utilisation du Service d'authentification gouvernementale et des demandes d'intervention au compte. Registre des plaintes.

5. Risques et stratégies pour les atténuer

Une analyse a été effectuée pour cerner les risques d'atteinte à la vie privée susceptibles de causer une perte ou un préjudice aux personnes concernées par le déploiement du Service d'authentification gouvernementale aux fins du projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens » du Programme SQIN et recenser les stratégies mises en place pour les atténuer et, plus particulièrement, au regard des risques dépassant le seuil de tolérance de l'organisation.

Une équipe multidisciplinaire a collaboré à la documentation et a participé à l'évaluation des risques.

La matrice d'évaluation des risques d'atteinte à la vie privée est présentée à l'annexe 4 (non publiée). L'évaluation des risques d'atteinte à la vie privée est présentée à l'annexe 5 (non publiée).

Réévaluation de la proportionnalité

À la lumière de l'ensemble de l'EFVP, le MCN considère que le déploiement du Service d'authentification gouvernementale aux fins du projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens » est proportionnel, compte tenu des risques d'atteinte à la vie privée ciblés et du niveau de risque résiduel, pour atteindre les objectifs fixés.

Le MCN s'est assuré, tout au long du déploiement du Service d'authentification gouvernementale, notamment de la mise en place de moyens pour respecter ses obligations et les principes de PRP.

De plus, l'effet combiné des mesures en place et des mesures additionnelles incluant celles inscrites dans le plan d'action permet d'atténuer à un niveau estimé acceptable les risques d'atteinte à la vie privée des personnes concernées engendrés par le projet.

6. Plan d'action

Au terme de cette EFVP, il en ressort que dans la majorité des scénarios de risques d'atteinte à la vie privée, la source principale de risque est humaine, qu'elle provienne de l'interne ou de l'externe du MCN, qu'elle soit produite de manière accidentelle ou de façon délibérée. De plus, des travaux sont planifiés en continu pour respecter les obligations en matière de PRP. Les mesures du plan d'action ont été définies en conséquence.

Le plan d'action est présenté à l'annexe 6 (non publiée).

7. Approbation du rapport et versions

Le rapport d'EFVP est un document évolutif qui sert à documenter et à consolider les résultats de l'évaluation, il est donc mis à jour en continu pour exposer tout changement significatif au projet 1 ou tout élément s'y appliquant, et qui ont un impact sur la vie privée des personnes concernées. Les rapports mis à jour seront transmis à la CAI, conformément à l'article 12.16 de la LGGRI.

La vérification, en vue d'assurer la mise en œuvre des moyens nécessaires pour respecter les obligations du MCN et les principes de PRP, de l'analyse de risques d'atteinte à la vie privée pour le projet 1 et les stratégies retenues pour éliminer ces risques ou les réduire efficacement ainsi que la mise à jour du rapport d'EFVP, est prise en charge par les parties prenantes qui en sont responsables conformément au cadre de gouvernance applicable au projet 1.

Approbation

J'atteste que les informations contenues dans les sections du présent rapport ainsi que les contrôles afférents à ces informations sont fiables et qu'ils correspondent à la situation telle qu'elle se présentait à la date de signature de ce rapport d'EFVP.

Madame Mylène Martel, sous-ministre adjointe au dirigeant principal de l'information et à la gouvernance

Signature de l'autorité responsable

Date d'approbation : 16 octobre 2025

Historique des versions

Date	Modification	Description des modifications
2023-02-17	Création	S. O.
2023-12-18	Mise à jour	Parties prenantes au projet. Inventaire et vue d'ensemble de la circulation des RP. Moyens mis en place pour assurer le respect des obligations et des principes de PRP. Risques identifiés et résiduels – stratégies, mécanismes et mesures de sécurité déployés pour les éliminer ou les réduire. Acronymes. Définitions. Annexes.
2025-10-16	Mise à jour	Définitions. Acronymes. Description du projet 1 et de l'objet de l'EFVP. Parties prenantes au projet. Renseignements personnels impliqués. Moyens mis en place pour respecter les obligations et les principes de protection des renseignements personnels (PRP). Risques et stratégies pour les atténuer. Plan d'action. Annexes.

Annexe 1 – Cadre légal et normatif

Document	Émetteur ou provenance du document	Version
Autorisation de mobilité des données numériques gouvernementales 2023-01 du gestionnaire de données numériques gouvernementales	MCN	2023-12-18
Cadre de gouvernance et de gestion de la sécurité de l'information	MCN	2022-03-29
Calendrier de conservation	MCN	S. O.
Conditions d'utilisation du Service d'authentification gouvernementale	MCN	2024-06-12
Code de bonnes pratiques du numéro d'assurance sociale	Gouvernement du Canada – Emploi et Développement social Canada	2023-01-09
Décret numéro 115-2018	MCE	2018-02-14
Décret numéro 511-2020	MCE	2022-05-13
Décret numéro 870-2022	MCE	2022-05-25
Décret numéro 1159-2022	MCE	2022-06-22
Décret numéro 1690-2022	MCE	2022-10-26
Décret numéro 1848-2023	MCE	2023-12-20
Décret numéro 765-2023	MCE	2023-05-03
Décret numéro 766-2023	MCE	2023-05-03
Décret numéro 1084-2024	MCN	2024-07-10
Directive sur la gestion et la classification des actifs informationnels	MCN	2023-02-17
Directive sur la gestion des menaces, des vulnérabilités, des incidents de sécurité de l'information et des incidents impliquant des renseignements personnels	MCN	2023-02-17
Directive – Continuité des services	MCN	2023-06-01
Directive – Gestion des accès physiques	MCN	2023-02-17

Document	Émetteur ou provenance du document	Version
Directive sur la conformité des services en matière de sécurité de l'information	MCN	2023-02-17
Directive sur la sécurité applicative	MCN	2023-10-31
Directive sur la sécurité des réseaux et des télécommunications	MCN	2023-10-31
Directive sur la sécurité de l'information des ressources humaines	MCN	2023-10-31
Directive sur les obligations relatives à la confidentialité et à la déclaration de conflit d'intérêts	MCN	2023-06-28
Directive sur l'encadrement des exigences de sécurité vis-à-vis des tiers	MCN	2023-02-17
Directive sur le numéro d'assurance sociale (ISBN : 978-0-660-09689-6)	Gouvernement du Canada	2022-10-26
Directive sur l'usage de la cryptographie	MCN	2023-10-31
Mesures minimales de sécurité au regard des données lors de l'utilisation de solutions technologiques [REDACTED]	MCN	2023-02-01
Gouvernement du Canada - Considérations relatives à l'utilisation de la cryptographie dans les services d'informatique en nuage commerciaux (BT22-254/2020F-PDF; ISBN 978-0-660-34789-9)	Secrétariat du Conseil du trésor du Canada	2020-04-28
Indication d'application concernant les activités liées à l'identification et à l'authentification des personnes aux fins du Service d'authentification gouvernementale (IA-RI-2024-001-OP)	MCN	2024-07-12
Indication d'application concernant les Règles relatives à l'assurance de l'identité numérique	MCN	2022-10-04
L'éthique dans la fonction publique québécoise (ISBN 2-550-40764-4)	MCE	2003
Loi concernant la cadre juridique des technologies de l'information (RLRQ, c. C-1.1)	MCE	Mise à jour en continu – Publications du Québec
Loi favorisant la transformation numérique de l'administration publique (RLRQ, c. T-11.003)	MCE	Mise à jour en continu – Publications du Québec
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)	MCE	Mise à jour en continu – Publications du Québec

Document	Émetteur ou provenance du document	Version
Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03)	MCE	Mise à jour en continu – Publications du Québec
Loi sur l'assurance maladie (RLRQ, c. A-29)	MCE	Mise à jour en continu – Publications du Québec
Loi sur le ministère de la Cybersécurité et du Numérique (RLRQ, c. M-17.1.1)	MCE	Mise à jour en continu – Publications du Québec
Loi sur les archives (RLRQ, c. A-21.1)	MCE	Mise à jour en continu – Publications du Québec
Politique-cadre en matière de télétravail pour les employés de la fonction publique	SCT	2022-04-04
Politique de confidentialité et de protection des renseignements personnels du ministère de la Cybersécurité et du Numérique agissant à titre de source officielle de données numériques gouvernementales	MCN	2023-10-31
Politique de confidentialité du Service d'authentification gouvernementale	MCN	2023-10-31
Politique de sécurité de l'information	MCN	2023-06-01
Politique de gestion des plaintes et des commentaires pour le Service d'authentification gouvernementale	MCN	2023-10-31
Politique sur les conflits d'intérêts	MCN	2023-06-28
Procédure encadrant la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels dans le cadre du Service québécois d'identité numérique	MCN	2023-02-17
Processus de gestion de l'identité et des droits d'accès	MCN	2023-11
Processus de gestion des plaintes relatives aux renseignements personnels en lien avec le Service d'authentification gouvernementale	MCN	2023-10-31
Processus de révision de l'identité et des droits d'accès	MCN	2023-10
Processus de signalement d'une compromission d'un compte du Service d'authentification gouvernementale	MCN	2023-10-31
Procédure de traitement des demandes d'accès et de rectification des renseignements personnels en lien avec le Service d'authentification gouvernementale	MCN	2023-09-29

Document	Émetteur ou provenance du document	Version
Règles de sécurité de l'information destinées au personnel du MCN	MCN	S. O.
Règles de sécurité destinées aux ressources externes	MCN	S. O.
Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, c. A-2.1, r. 2)	MCE	Mise à jour en continu – Publications du Québec
Règles relatives à l'assurance de l'identité numérique	MCN	2024-07-06
Règles relatives à la gestion des projets en ressources informationnelles	MCN	2024-06-22

Annexe 2 – Contrats et ententes

Titre du contrat ou de l'entente	Objectif du contrat ou de l'entente	Nom des tiers	Rôle des partenaires	Date de début	Date de fin	Renouvellement prévu
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Entente SAAQ/MCN	Le MCN mandate la SAAQ à effectuer les opérations relatives au processus d'identification en personne aux fins du Service d'authentification gouvernementale.	SAAQ MCN	La SAAQ doit effectuer les opérations relatives au processus d'identification en personne aux fins du Service d'authentification gouvernementale, excluant la vérification des secrets partagés, dans ses différents centres de service.	2023-03-10	2026-03-31	L'entente se renouvelle tacitement d'année en année
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

N. B. Indiqués ci-dessus, ententes et contrats signés uniquement.

