RAPPORT D'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

SERVICE QUÉBÉCOIS D'IDENTITÉ NUMÉRIQUE

ACCÈS BONIFIÉ AUX PRESTATION ÉLECTRONIQUES DE SERVICE – CITOYENS

17 février 2023

Votre gouvernement

Québec

Table des matières

Rapport d'évaluation des facteurs relatifs à la vie privée[1]

1. Notes préliminaires

L'EFVP est une démarche préventive et évolutive visant à protéger les RP dans le but de 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.

À noter : afin de faciliter la lecture, les acronymes et les définitions ont été regroupés dans des sections qui leurs sont dédiées à la fin du présent rapport.

2. Description du projet

Le Programme SQIN vise à procurer aux citoyens et aux entreprises une identité numérique gouvernementale de confiance leur permettant d'accéder plus facilement et plus sécuritairement aux services offerts par l'administration publique.

Le SAG du SQIN, a comme objectif d'offrir des services simplifiés, intégrés et de qualité qui s'appuient sur les TI, incluant les technologies numériques, tout en assurant la pérennité du patrimoine numérique gouvernemental. Le déploiement de ce service est essentiel à la transformation numérique du gouvernement et prévoit :

- La création et la tenue du RAIG;
- L'identification des personnes pour leur donner accès aux PES gouvernementales;
- L'authentification des personnes qui entendent utiliser ou autrement bénéficier d'un service auprès d'un MO prestataire d'un tel service.

3. Motivation du projet et objectifs poursuivis

Projet 1 du Programme SQIN

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. Ce projet vise à remplacer le service d'authentification clicSÉQUR, afin de permettre à un plus grand nombre de citoyens et de représentants d'entreprises d'accéder plus facilement et de manière plus sécuritaire aux services en ligne du gouvernement. Il vise aussi l'uniformisation des façons de faire des MO en matière de PES gouvernementales, laquelle doit être prise en charge par le MCN.

Les principaux objectifs du projet 1 sont :

- Améliorer la sécurité des RP des citoyens et des entreprises;
- Simplifier le processus d'authentification gouvernementale et de vérification d'identité;
- Élargir le bassin de la clientèle potentielle aux PES du gouvernement du Québec;
- Implanter un service universel d'authentification gouvernementale;
- Fournir aux utilisateurs un service d'authentification gouvernemental convivial, moderne, évolutif, extensible, sécuritaire et disponible.

Constituant à terme des services communs fournis aux MO par le MCN, l'authentification des citoyens constitue la première étape de réalisation du projet 1 du Programme SQIN, et l'authentification des entreprises sera la seconde.

MCN source officielle de données numériques gouvernementales

Actuellement, les MO recueillent et entreposent les données d'identification nécessaires à leur prestation de services et en fonction de la clientèle qu'ils desservent. Ainsi, chaque organisme possède des renseignements concernant une portion de la population québécoise. Conséquemment, les données d'identification des citoyens sont, dans plusieurs cas, présentes dans diverses bases de données gouvernementales.

[1] Requise en vertu de l'article 9 de la Loi favorisant la transformation numérique de l'administration publique (RLRC, c T-11.003).

Par le décret numéro 870-2022 du 25 mai 2022, le gouvernement a désigné le MCN pour agir comme source officielle de données numériques gouvernementales aux fins du SAG, déployé dans le cadre de la réalisation du projet 1 du Programme SQIN. En vertu de ce décret, les données numériques gouvernementales requises pour la constitution et la tenue du RAIG, qui sont communiquées à partir du FIPA de la RAMQ[2], sont les suivants : le nom; pour les femmes mariées avant le 2 avril 1981, le nom du mari; la DDN; la date du décès; l'adresse de résidence active et future; l'indicateur de présence d'un répondant; le NAM; le NAS; l'identifiant sectoriel de la RAMQ. L'analyse du risque d'atteinte à la vie privée (nécessité) par rapport aux objectifs du projet et à la solution proposée a été effectuée avant la prise du décret numéro 870-2022, quant aux données numériques gouvernementales qui peuvent être dans le RAIG.

En conformité avec sa mission, le MCN effectue les travaux nécessaires pour devenir une source fiable et digne de confiance des attributs d'identité nécessaires à l'identification des citoyens, assurant ainsi l'unicité des individus qui accèdent aux PES gouvernementales par l'entremise du SAG. Ces travaux sont effectués dans l'objectif d'améliorer la SI gouvernementale, incluant la PRP des citoyens.

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 PES gouvernementales sera considérablement réduit, réduisant d'autant les risques au niveau de la SI et de la PRP.

Phases d'expérimentation du SAG

Afin de tester le fonctionnement et l'efficience du SAG, des expérimentations sont effectuées avec le Service québécois de certification du personnel éducateur de la petite enfance du MFA, vers la fin de l'année 2022, et le Projet CASA de la SAAQ, au début de l'année 2023.

[2] 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.

4. Parties prenantes au projet

Parties prenantes ressources du ministère, différents partenaires du projet et clientèle	**Période d'implication** mise en œuvre et/ou par la suite	**Rôles et responsabilités des parties prenantes**
MCN	Mise en œuvre et par la suite	• Maître d'ouvrage et maître d'œuvre du Programme SQIN; • S'assure que le projet est conforme aux règles applicables, incluant celles découlant des décrets pris en lien avec le projet, 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.
MESS	Mise en œuvre et par la suite	• MO Partenaire; • Assure le service à la clientèle de première ligne pour le SQIN; • Participe au comité stratégique du projet.
MFA	Mise en œuvre et par la suite	• Premier MO Consommateur ayant recours au SAG pour l'accès à ses PES; • Participe au comité directeur et au comité stratégique du projet.
RAMQ	Mise en œuvre et par la suite	• MO Partenaire (source de confiance); • Communique les renseignements nécessaires à la constitution et à la tenue du RAIG; • Valide le secret partagé communiqué par le citoyen dont elle est l'émettrice et offre le service à la clientèle quant à ce secret; • Offre le service à la clientèle quant aux renseignements dont elle est responsable; • Participe au comité directeur et au comité stratégique du projet.
RQ	Mise en œuvre et par la suite	• MO Partenaire (valideur de secret); • Valide le secret partagé communiqué par le citoyen dont il est l'émetteur et offre le service à la clientèle quant à ce secret; • Participe au comité directeur et au comité stratégique du projet.
SAAQ	Mise en œuvre et par la suite	• Deuxième MO Consommateur ayant recours au SAG pour l'accès à ses PES; • Valide le secret partagé communiqué par le citoyen dont il est l'émetteur et offre le service à la clientèle quant à ce secret; • Participe au comité directeur et au comité stratégique du projet.
Utilisateurs	Mise en œuvre et par la suite	• Utilisent le SAG pour accéder aux PES visées par le projet; • Consentent au partage de leurs RP.

5. Inventaire et vue d'ensemble de la circulation des RP

Phase du projet et ses particularités	**RP concernés** regroupés par catégories lorsqu'applicable[3]	**Interaction avec les RP tout au long de leur cycle de vie**	**Personne ou secteur qui interagit avec les RP**	**Moyen(s) utilisé(s) pour l'interaction**
Développement	RP servant à la constitution du RAIG[4]	Communication	RAMQ SMATNG – DGSCE – groupe restreint d'employés autorisés responsables de la phase de développement	Transmission d'un chargement massif des RP dans un canal sécurisé, en provenance du FIPA de la RAMQ vers le RAIG du MCN (aucune transmission inverse possible)
Développement et exploitation	RP servant à la mise à jour du RAIG[5]	Communication	RAMQ SMATNG - DGSCE – groupe restreint d'employés autorisés responsables de la phase de développement et d'exploitation	Transmission d'une mise à jour des RP aux 15 minutes dans un canal sécurisé, en provenance du FIPA de la RAMQ vers le RAIG du MCN (aucune transmission inverse possible)
Exploitation	RP servant à la création d'un compte SAG et à l'authentification de l'utilisateur[6]	Collecte, communication, utilisation et conservation	Utilisateur SMATNG – DGSCE	Interface d'échange informatisé (SAG) Courriel Transaction informatique entre l'interface d'échange informatisé (SAG) et la solution de gestion de l'authentification et des autorisations
Développement et exploitation	RP servant à la réalisation du processus d'identification[7]	Collecte et utilisation	Utilisateur SMATNG – DGSCE Agent vérificateur du MCN	Interface d'échange informatisé (SAG) Transaction informatique entre l'interface d'échange informatisé (SAG) et le RAIG Communication téléphonique
Développement et exploitation	RP servant pour la validation d'un secret	Collecte	Utilisateur	Interface d'échange informatisé (SAG)

[3] Catégorie de RP : RP qui possèdent des caractéristiques communes et/ou qui sont regroupés afin d'accomplir une fonction ou atteindre un objectif.

[4] Cette catégorie contient : le nom; pour les femmes mariées avant le 2 avril 1981, le nom du mari; la DDN; la date du décès; l'adresse de résidence; l'indicateur de présence d'un répondant; le NAM; le NAS; l'identifiant sectoriel de la RAMQ.

[5] Cette catégorie contient : le nom; pour les femmes mariées avant le 2 avril 1981, le nom du mari; la DDN; la date du décès; l'adresse de résidence; l'indicateur de présence d'un répondant; le NAM; le NAS; l'identifiant sectoriel de la RAMQ.

[6] Cette catégorie contient : le nom d'utilisateur, l'adresse courriel, le mot de passe, le code de sécurité transmis automatiquement par courriel à l'utilisateur.

[7] Cette catégorie contient : le nom, pour les femmes mariées avant le 2 avril 1981, le nom du mari, la DDN, le NAM, le NAS.

	partagé dans le cadre du processus d'identification[8]		SMATNG – DGSCE	
Développement et exploitation	RP servant à la validation d'un secret partagé dans le cadre du processus d'identification[9]	Communication	SMATNG – DGSCE MO Partenaire(s) - validateur(s) de secret partagé	Transmission dans un canal sécurisé
Développement et exploitation	RP servant à l'obtention d'un secret à usage unique dans le cadre du processus d'identification[10]	Communication	SMATNG – DGSCE – émetteur de secret à usage unique RQ Utilisateur	Génération d'une lettre automatisée Transaction informatique entre l'interface d'échange informatisé (SAG) et le Dépôt des demandes[11] Transmission quotidienne des lettres en lot par l'entremise d'un transfert d'information sécurisé (Axway) Impression des lettres sur papier Lettres transmises par la poste (Poste Canada)
Développement et exploitation	RP servant à la validation d'un secret à usage unique dans le cadre du processus d'identification[12]	Utilisation	Utilisateur SMATNG – DGSCE – valideur de secret à usage unique	Interface d'échange informatisé (SAG) Transaction informatique entre l'interface d'échange informatisé (SAG) et le Dépôt des demandes
Développement et exploitation	RP servant pour une utilisation subséquente du SAG[13]	Collecte, communication et utilisation	Utilisateur SMATNG – DGSCE	Interface d'échange informatisé (SAG) Courriels

[8] Cette catégorie contient : l'un des secrets suivants : un numéro d'avis de cotisation parmi les deux dernières années (obligatoire sous réserve de l'utilisation d'un secret à usage unique), le numéro de référence situé à l'arrière de la carte d'assurance maladie (optionnel) ou le numéro de référence du permis de conduire (optionnel).

[9] Cette catégorie contient : l'un des secrets suivants : un numéro d'avis de cotisation parmi les deux dernières années (obligatoire), le numéro de référence situé à l'arrière de la carte d'assurance maladie (optionnel) ou le numéro de référence du permis de conduire (optionnel) et, selon le MO Partenaire (validateur de secret), le nom, la DDN, le NAS et l'identifiant unique sectoriel de la RAMQ.

[10] Cette catégorie contient : le nom, l'adresse de résidence et le secret à usage unique.

[11] Pour les demandes de secret à usage unique.

[12] Cette catégorie contient : un secret à usage unique ayant une durée de validité limitée.

[13] Cette catégorie contient : le nom d'utilisateur ou l'adresse courriel, le mot de passe et le code de sécurité transmis automatiquement par courriel à l'utilisateur; ainsi que le code de sécurité transmis par courriel automatisé en cas d'oubli du mot de passe. Les informations d'accès au SAG journalisés sont quant à elles constituées de : l'identifiant unique du SAG, (généré dans la solution de gestion d'authentification et des autorisation), l'adresse courriel et l'adresse IP.

Développement et exploitation	RP servant à accéder à une PES d'un MO Consommateur[14]	Communication et utilisation	SMATNG – DGSCE MO Consommateur(s)	Transmission dans un canal sécurisé
Développement et exploitation	RP contenus dans le RAIG[15]	Utilisation et conservation	SMATNG – DGSCE – groupe retreint d'employés responsables du pilotage du SAG SMASIGC – DGSSI – groupe restreint d'employés qui auront à effectuer des audits DGSG – Équipe de l'ADPRP – groupe restreint d'employés qui auront à traiter les demandes d'accès ou de rectification SMAITB – groupe restreint d'employés qui ont accès aux CTI concernés AWS – groupe restreint de personnes qui ont accès aux CTI d'AWS concernés	Transaction informatique sécurisée Création d'une image en format PDF chiffrée et transmission d'un courriel contenant la clé de chiffrement dans le cadre des demandes d'accès ou de rectification Accès physique ou logique aux locaux dans lesquels sont situés les équipements et les infrastructures hébergeant les données du RAIG
Exploitation	RP contenus dans le RAIG	Conservation	SMATNG – DGSCE	Transactions informatisées automatisées *À venir : travaux en cours pour approbation des orientations proposées et établissement des solutions*
Exploitation	RP contenus dans le RAIG	Destruction	SMATNG – DGSCE	La destruction des RP peut se produire aux moments suivants : 1. lors de la mise à jour des RP en provenance du FIPA de la RAMQ vers le RAIG du MCN par transmission dans un canal sécurisé 2. en appliquant les règles prévues au calendrier de conservation des données

[14] Cette catégorie contient, selon le MO Consommateur concerné : le nom, la DDN, l'adresse de résidence, l'identifiant unique du SAG (généré lors de la création du compte) et l'adresse courriel.

[15] Cette catégorie contient : le nom; pour les femmes mariées avant le 2 avril 1981, le nom du mari; la DDN; la date du décès; l'adresse de résidence; l'indicateur de présence d'un répondant; le NAM; le NAS; l'identifiant sectoriel de la RAMQ.

6. Moyens mis en place pour assurer le respect des obligations et des principes de PRP

Les obligations et les principes de PRP applicables au projet sont notamment prévus dans les divers documents du cadre normatif énumérés à l'annexe 1 du présent rapport, L'on y retrouve notamment les documents de gouvernance du MCN concernant la PRP, en vigueur ou à venir, ainsi que le décret numéro 1690-2022 du 26 octobre 2022 contenant les règles particulières encadrant l'utilisation du NAS et du NAM.

Les principales obligations et principes de PRP qui s'appliquent au projet sont :

- Assumer les responsabilités;
- Déterminer les fins de la collecte de RP;
- Limiter la collecte des RP (nécessité);
- Informer la personne concernée;
- Limiter l'accès aux RP;
- Requérir les consentements des utilisateurs;
- Assurer la qualité des RP;
- Mettre en place des mesures de sécurité appropriées;
- Permettre l'exercice des droits d'accès à l'information;
- Permettre l'exercice des droits de rectification;
- Limiter la durée de conservation des renseignements;
- Répondre dans les délais légaux;
- Assurer la réalisation d'audits externes;
- Mettre en place une protection par défaut maximale;
- Mettre en application les règles particulières concernant le NAS;
- Mettre en application les règles particulières concernant le NAM;
- Recourir aux services d'un fournisseur en infonuagique conforme aux exigences de sécurité applicables au projet.

Quant aux moyens mis en place pour assurer le respect des obligations et principes, ils sont résumés dans le tableau à la page suivante.

RP concernés regroupés par catégories lorsqu'applicable[16]	**Interaction avec les RP tout au long de leur cycle de vie**	**Description des moyens mis en place pour assurer le respect des obligations et des principes de PRP**
RP servant à la constitution du RAIG	Communication	Les RP chargés dans le RAIG en provenance du FIPA ont fait l'objet d'une analyse approfondie et seuls les RP jugés nécessaires à la réalisation du projet ont fait l'objet d'un chargement. Parmi ces RP, le NAS et le NAM, qui sont des RP essentiels dans le cadre des expérimentations visant à s'assurer de l'efficacité du SAG, sont considérés comme des RP sensibles[17]. Le MCN met en place des mesures de sécurité physiques, logiques et administratives additionnelles pour assurer leur protection, telles que prévues en annexe du décret numéro 1690-2022. Le ROCD est responsable de valider le respect des mesures mises en place par un processus d'audit de sécurité. Si requis, un rapport est préparé et transmis à la Directrice générale des solutions citoyennes et entreprises et au CSIO; une décision concernant la mise en ligne de la solution ou son retrait est prise; un plan contenant des mesures pour la sécurisation des données sensibles est mis en œuvre; le CSIO donne son accord préalablement à la remise en ligne de la solution, le cas échéant.
RP servant à la mise à jour du RAIG	Communication	Lorsqu'il y a une modification de RP au FIPA cela entraîne une modification du RP au RAIG. Au moment de la mise à jour, seul le RP modifié sera mis à jour dans le RAIG. Aucun historique des RP modifiés n'est conservé; le RP mis à jour supprime et remplace le précédent RP. Le canal de données utilisé fait l'objet d'un chiffrement robuste afin de prévenir les risques d'incidents de confidentialité et les altérations non autorisées.
RP servant à la création d'un compte SAG et à l'authentification de l'utilisateur	Collecte, communication, utilisation et conservation	L'utilisateur saisit ses RP dans l'interface du SAG et doit consentir à leur utilisation par le MCN. Les RP servant à la création et à l'authentification du compte SAG transitent par une plateforme de gestion de l'authentification et de l'autorisation.

[16] Voir le détail des catégories dans les notes de bas de page de la section 4 du présent rapport.

[17] Plusieurs combinaisons ont été explorées pour la réalisation du processus d'identification (ex. : nom, DDN et code postal; nom, DDN et nom de la mère). À cet effet, l'adresse de résidence ne peut pas être utilisée puisqu'il n'y a pas de référentiel d'adresses au sein du gouvernement qui puisse garantir l'unicité de l'adresse des utilisateurs dans les registres ou les bases de données des MO. Les différents essais ont démontré d'une part que la combinaison du NAS et du NAM limite les risques d'atteinte à la vie privée par ingénierie sociale et, d'autre part, qu'elle est la seule option permettant de distinguer des utilisateurs ayant les mêmes noms et DDN. De plus, les essais ont mis en lumière qu'il n'existe aucun autre identifiant présent dans les registres et les bases de données des MO pouvant donner l'assurance de l'unicité de l'identité d'un utilisateur.

Pour toute ces raisons, le NAS et le NAM sont des RP nécessaires pour résoudre l'identité d'un utilisateur du SAG. Également, le NAS est un RP servant à la validation du secret partagé avec RQ.

Bien que l'utilisation du NAS et du NAM ne soit pas prévue aux fins d'une identification telle que celle mise en place dans le cadre du projet, il est impératif de s'assurer d'avoir une clé d'identité forte et sûre, à défaut d'un éventuel identifiant gouvernemental unique. La valorisation des données, qui constitue une obligation du MCN dans le cadre de la réalisation du projet, passe, entre autres, par la qualité des données. Le Programme SQIN contribue à améliorer la qualité des données utilisées par les MO; en amont, avec fiabilité lors de l'identification de l'utilisateur, et en aval, par l'utilisation dans l'ensemble des MO de la même information d'identité, d'adresse et de contact.

RP concernés regroupés par catégories lorsqu'applicable[16]	**Interaction avec les RP tout au long de leur cycle de vie**	**Description des moyens mis en place pour assurer le respect des obligations et des principes de PRP**
RP servant à la réalisation du processus d'identification	Collecte et utilisation	En vue de détecter les menaces et de mettre en œuvre des mesures de sécurité appropriées, le système journalise les tentatives de saisie des attributs nécessaires à la réalisation du processus d'identification. Si l'utilisateur fait un certain nombre de tentatives de saisie erronées le système verrouillera le compte pour une durée prédéterminée; en cas d'une deuxième suspension, le délai de celle-ci sera augmenté; en cas d'une troisième suspension, l'utilisateur devra communiquer avec le centre de service à la clientèle de Service Québec (MESS).
RP requis pour la validation d'un secret partagé dans le cadre du processus d'identification	Collecte	L'utilisateur saisit deux secrets partagés dans l'interface du SAG et doit consentir à ce qu'ils soient communiqués aux MO Partenaires (valideur de secret) concernés pour validation et utilisation par ces derniers pour vérifier leur exactitude. Si l'utilisateur fait un certain nombre de tentatives de saisie erronées de ses secrets, le système verrouillera le processus d'identification pour une durée prédéterminée; en cas d'une deuxième suspension, le délai de celle-ci sera augmenté; en cas d'une troisième suspension, l'utilisateur devra communiquer avec le centre de service à la clientèle de Service Québec (MESS).
RP requis pour la validation d'un secret partagé dans le cadre du processus d'identification	Communication	La validation des secrets sert uniquement à déterminer que les secrets partagés sont exacts lorsqu'ils sont comparés aux informations détenues par le MO Partenaire (valideur de secret). Le secret partagé et certains RP saisis par l'utilisateur via l'interface du SAG sont transmis de manière sécurisée au MO Partenaires (valideur de secret) source de ce secret. Un consentement pour la vérification de chaque secret est requis à cette étape. Une fois la comparaison effectuée, le MO retourne le résultat de cette comparaison au SAG. Si la réponse reçue est positive pour chacun des deux secrets, le processus d'identification sera considéré comme valide et complété. Le secret saisi n'est pas conservé au RAIG ni dans aucune autre base de données du MCN.
RP servant à l'obtention d'un secret à usage unique dans le cadre du processus d'identification	Communication	Lorsque l'utilisateur n'est pas en mesure de fournir l'un des deux secrets partagés, il peut demander qu'un secret à usage unique lui soit transmis par lettre postale afin de pouvoir compléter le processus d'identification. Pour ce faire, il saisit son numéro d'immeuble et son code postal afin qu'ils soient comparés avec ceux présents dans le RAIG. Un consentement est requis de l'utilisateur afin que le MCN communique son nom et son adresse à RQ pour impression et expédition de la lettre. S'il y a corroboration, l'utilisateur sera informé que sa demande a été reçue et la lettre, une fois créée, sera transmise à RQ en lot par transfert sécurisé. RQ recevra le lot de lettres PDF, les imprimera et les postera. Dans l'éventualité où la lettre ne peut pas être remise à l'utilisateur, celle-ci est retournée au MESS pour destruction sécuritaire, sans que l'enveloppe ne soit ouverte. L'utilisateur doit effectuer une nouvelle demande s'il souhaite obtenir un nouveau secret à usage unique, le cas échéant.
RP servant à la validation d'un secret à usage unique dans le cadre du processus d'identification	Utilisation	En vue de détecter les menaces et de mettre en œuvre des mesures de sécurité appropriées, le système journalise les demandes de génération de secret à usage unique. Lorsque le nombre maximum préétabli de tentatives de saisie du secret à usage unique est atteint, le secret n'est plus valide. L'utilisateur devra présenter une nouvelle demande de secret à usage unique en vue d'en obtenir un nouveau.

RP concernés regroupés par catégories lorsqu'applicable[16]	**Interaction avec les RP tout au long de leur cycle de vie**	**Description des moyens mis en place pour assurer le respect des obligations et des principes de PRP**
RP servant pour une utilisation subséquente du SAG	Collecte, communication et utilisation	L'utilisateur saisit ses RP dans l'interface du SAG et doit consentir à leur utilisation par le MCN. <u>Mot de passe oublié :</u> L'utilisateur qui a complété son inscription au SAG qui oublie son mot de passe peut demander une réinitialisation de celui-ci dans l'interface d'authentification du SAG. Un code de sécurité valide pour une durée limitée est transmis à l'adresse courriel indiquée par l'utilisateur, si elle est liée à un compte existant du SAG. Le code de sécurité reçu à cette adresse courriel peut être utilisé pour procéder à la réinitialisation du mot de passe par l'utilisateur. Si le processus d'identification pour ce compte était complété, l'utilisateur doit l'effectuer à nouveau en conséquence de la réinitialisation.
RP servant à accéder à une PES d'un MO Consommateur	Communication et utilisation	Afin d'accéder à la PES d'un MO Consommateur, l'utilisateur doit consentir via l'interface du SAG à ce que le MCN communique au MO Consommateur les RP que celui-ci requiert, ainsi que l'identifiant unique du SAG de l'utilisateur. Lorsque l'utilisateur se connecte pour une première fois à la PES d'un MO Consommateur, deux cas de figure peuvent se présenter : 1. Le MO possède déjà des RP d'identification concernant l'utilisateur : l'appariement entre les RP du RAIG et celles de la base de données du MO est effectuée; o Ce cas de figure est celui qui s'applique à la SAAQ dans le cadre du projet. 2. Le MO ne possède pas les RP d'identification concernant l'utilisateur : le SAG peut communiquer les RP d'identification au MO, qui peut créer sa base de données avec ces RP[18]. o Ce cas de figure est celui qui s'applique au MFA dans le cadre du projet. Dans les deux cas, le MO Consommateur conservera l'identifiant unique du SAG dans sa base de données aux fins d'identification future de l'utilisateur. Lors des connexions subséquentes par l'entremise du SAG, seul ce RP sera communiqué et utilisé pour rechercher et analyser l'identité de l'utilisateur.[19] En vue de détecter les menaces et de mettre en œuvre des mesures de sécurité, le système journalise les tentatives de vérification d'identité. Si l'utilisateur échoue un nombre prédéterminé de cycles de connexion comprenant chacun un nombre également prédéterminé de tentatives de validation de son identité, le compte sera suspendu.

[18] Par l'effet combiné des articles 12.12 (1) (4°) et 12.15 (2) de la LGGRI et du décret 870-2022, la communication de données d'identification détenues dans le RAIG à un autre MO peut être autorisée lorsque c'est nécessaire aux fins d'une PES à laquelle l'utilisateur désire accéder. La confection d'une telle base de données répond à l'intention du législateur du Projet de loi n° 95 qui était d'éviter que les MO qui désirent offrir de nouveaux services électroniques redemandent aux utilisateurs de fournir des renseignements déjà détenus par l'État.

[19] L'identifiant unique du SAG n'est pas communiqué à l'utilisateur.

RP concernés regroupés par catégories lorsqu'applicable[16]	**Interaction avec les RP tout au long de leur cycle de vie**	**Description des moyens mis en place pour assurer le respect des obligations et des principes de PRP**
RP contenus dans le RAIG	Utilisation et conservation	L'accès aux RP du RAIG est limité aux employés du MCN responsables du pilotage de celui-ci ainsi qu'aux employés qui effectueront des audits. Les autorisations d'accès sont restreintes afin de prévenir les accès non autorisés, et une journalisation de ceux-ci est mise en place afin de détecter les abus de droits, le cas échéant. Les autorisations des accès se font par l'octroi de rôles : pilotage ou auditeur. Le gestionnaire des employés concernés approuve les demandes d'ajout de rôles. Ces accès seront octroyés de façon ponctuelle pour répondre à une demande de consultation concernant les RP d'un utilisateur et sont assortis d'un délai prédéfini. Une revue des accès est réalisée selon une fréquence définie. Également, un accès en consultation peut être autorisé pour des fins de diagnostique d'anomalies. Le gestionnaire assigné au pilotage du RAIG approuve les demandes d'accès ainsi que les requêtes faites pour obtenir des RP. Les demandes d'accès sont conservées et l'accès aux RP sont journalisés. Les accès aux données sont journalisés et l'accès à cette journalisation se fera dans l'application de pilotage par les employés ayant le rôle auditeur. Chaque consultation des RP dans le RAIG engendrera une alerte dans le système et une vérification visant à corroborer la consultation préalablement autorisée.
RP contenus dans le RAIG	Conservation	Journalisation : À l'exception des renseignements nécessaires à l'authentification, requis à des fins de surveillance du bon fonctionnement de la solution, le MCN proscrit l'inclusion des RP dans les journaux système du SAG. Les accès et les opérations effectués par un des acteurs de l'exploitation de la solution ou déclenchés de manière systématique sont journalisés. Stockage de données : Sauf exceptions, les données du RAIG sont hachées ou chiffrées afin de prévenir les risques d'incidents de confidentialité générés par toute personne autorisée ou non qui aurait accès à la base de données. Actifs informationnels hébergés par le fournisseur infonuagique AWS : Le MCN a mis en place une séparation logique des configurations et des données des actifs informationnels qu'il gère et qui sont hébergés par le fournisseur infonuagique AWS. Ceux-ci sont également séparés de ceux des autres clients du fournisseur et les serveurs de base de données utilisés sont dédiés au SAG. Plan de reprise : Compte tenu de la nature sensible des RP concernés par la solution, le MCN a édicté des orientations concernant les bonnes pratiques en matière de plan de reprise pour le SAG. Dans un cas de survenance d'un sinistre majeur, les données pourraient être transférées sur un site d'AWS situé dans une localisation ayant un cadre juridique équivalent ou supérieur. Pour les données transactionnelles et sensibles, une copie de sécurité chiffrée est conservée par le MCN. En ce qui concerne les journaux d'exploitation, il est prévu qu'une copie soit hébergée dans la Ville de Toronto.
RP contenus dans le RAIG	Destruction	Mise à jour : Lors de la mise à jour du RAIG, l'ancien RP devient inactif dans le registre, il est remplacé et sera supprimé des bases de données. Également, le RAIG comprend les adresses actives et futures. Au moment où une adresse active arrive à échéance, l'adresse future devient l'adresse active et l'ancienne sera retirée du RAIG. Un traitement régulier s'assurera d'éliminer toutes les adresses devenues inactives. Calendrier de conservation : Les RP constituant le RAIG sont conservés 91 ans ou 3 ans après le décès de l'utilisateur. Un rapport de destruction est remis à la Directrice générale des solutions citoyennes et entreprises et à la DRMI.

7. Risques identifiés et résiduels – stratégies, mécanismes et mesures de sécurité déployés pour les éliminer ou les réduire

Une analyse de risques a été effectuée pour recenser les risques susceptibles de causer une perte ou un préjudice aux personnes concernées par le déploiement du SAG ainsi que les mesures mises en place afin d'atténuer ces risques au maximum. Une matrice d'évaluation des impacts et des probabilités a été définie par le MCN afin d'assurer l'uniformité des évaluations. L'exigence du respect du seuil de tolérance de niveau 2 a été établi pour le projet, considérant notamment la sensibilité des renseignements recueillis. L'analyse de risques a été réalisée en collaboration avec les personnes des différents secteurs du MCN impliquée dans le projet.

Au terme de cette analyse, il est constaté que sur les quatorze risques recensés, dix respectent le seuil de tolérance établie (71,43 %). Il ressort également de cette démarche que dans la majorité des scénarios, 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. Pour cette raison, les mesures de sécurité et les documents de gouvernance tiennent compte et sont conçus de manière à atténuer le plus possible ces risques. Les mesures proposées ont été pensées en fonction de ce que le MCN peut contrôler[20].

Matrice d'évaluation des risques relatifs à la PRP

Impact

5 - Critique (Inacceptable (5) : le risque engendre des conséquences trop importantes et/ou implique une non-conformité aux lois)	Modéré Niveau 5	Modéré Niveau 10	Élevé Niveau 15	Critique Niveau 20	Critique Niveau 25
4 - Élevé (Très grand (4) : le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes)	Faible Niveau 4	Modéré Niveau 8	Élevé Niveau 12	Critique Niveau 16	Critique Niveau 20
3 - Modéré (Grand (3) : le risque engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes)	Faible Niveau 3	Modéré Niveau 6	Modéré Niveau 9	Élevé Niveau 12	Élevé Niveau 15
2 - Mineur (Faible (2) : le risque engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes)	Faible Niveau 2	Faible Niveau 4	Modéré Niveau 6	Modéré Niveau 8	Modéré Niveau 10
1 - Négligeable (Très faible et/ou inexistant (1) : le risque n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne)	Faible Niveau 1	Faible Niveau 2	Faible Niveau 3	Faible Niveau 4	Modéré Niveau 5
	1 - Rare (Très faible et/ou inexistant (1) : Le risque n'a aucune chance de se concrétiser)	**2 - Improbable** (Faible (2) : le risque a peu de chance de se concrétiser ou un événement similaire ne s'est jamais produit)	**3 - Possible** (Moyen (3) : le risque a une probabilité raisonnable de se réaliser, mais possibilité tout aussi réelle qu'il ne se réalise ou peut se produire à un moment donné, à une fréquence annuelle)	**4 - Probable** (Grand (4) : le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelques reprises, à une fréquence mensuelle)	**5 - Certain** (Très grand (5) : le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises à une fréquence quotidienne ou hebdomadaire)

Probabilité

[20] L'un des risques a été identifié comme cygne noir (risque 5), puisque le MCN n'a aucun contrôle sur les causes de ce risque (catastrophe naturelle).

Actions selon les niveaux de la matrice du risque

Critique	Exige une action rapide pour atténuer le risque et mettre en place une surveillance régulière de ce dernier.
Élevé	Une intervention est nécessaire pour atténuer le risque et assurer une surveillance de son évolution.
Modéré	Ce niveau de risque peut être accepté ou il peut être atténué par une ou des interventions supplémentaires; dans les deux cas une surveillance de son évolution est effectuée.
Faible	Géré avec les pratiques et procédures actuelles - les impacts sont traités par des opérations de routine dont l'efficacité doit être contrôlée.

Analyse des risques – Programme SQIN – projet 1												
Cycle de vie	**Risque brut / Scénario**	**Cause / Source**	**Impact / Conséquence sur la personne concernée**	**Évaluation du risque brut (avant mesures)**			**Mesures mises en place**	**Évaluation du risque net (après mesures)**			**Commentaires**
				Impact	Probabilité	Niveau du risque brut		Impact	Probabilité	Niveau du risque net	
Collecte	Sentiment d'intrusion dans la vie privée de la personne concernée disproportionnée par rapport à l'objectif du projet	• L'objectif du projet est trop large ou non clairement défini • Les fins ne sont pas déterminées en début de projet	• Sentiment d'intrusion dans la vie privée • Perte d'intimité • Stress	2	3	6	• L'objectif du projet est clairement défini • Les fins pour lesquelles les RP sont collectés ont été déterminées en début de projet • Uniquement les RP nécessaires ont été communiqués par la RAMQ au MCN pour la constitution du RAIG • Révision périodique des documents de gouvernance	2	1	2	
	Collecte trop large ou abusive de RP	• L'analyse n'a pas été effectuée en fonction du critère de nécessité	• Sentiment d'intrusion dans la vie privée • Perte d'intimité • Stress	2	3	6	• Les fins pour lesquelles les RP sont collectés ont été déterminées en début de projet • Uniquement les RP nécessaires sont transférés par la RAMQ • Les champs sont prédéterminés, il n'y a pas de possibilité d'ajouter des renseignements • Révision périodique des documents de gouvernance	2	1	2	
Utilisation	Utilisation des RP à d'autres fins que celles prévues, pour lesquelles l'utilisateur a donné son consentement	• Manque d'encadrement de gestion • Manque de sensibilisation	• Perte de confiance envers le gouvernement • L'utilisateur ne peut exercer son droit de consentir à l'utilisation de ses RP à une autre fin	2	3	6	• Élaboration d'un processus d'approbation pour l'exploitation des RP • Les actions sont journalisées et les journaux sont exploités • L'accès est restreint uniquement aux personnes dont les fonctions le nécessitent • Les données sont cryptées • Sensibilisation du personnel à l'égard de l'utilisation et de la PRP • Formation de certains employés au principe de PRP dès la conception de la solution	1	2	2	• Risque à surveiller en continu puisque qu'il existe un manque de contrôle sur les causes. L'évaluation a été effectuée en tenant compte des événements survenus dans certaines institutions et MO au cours des dernières années. • Les mesures suivantes seront en place au moment de la mise en production : - Processus de gestion des fraudes - Équipe dédiée à la mise en place des outils de détection des menaces (mode prévention en continu) - Processus de détection des menaces pour l'exploitation de la solution

Analyse des risques – Programme SQIN – projet 1												
Cycle de vie	**Risque brut / Scénario**	**Cause / Source**	**Impact / Conséquence sur la personne concernée**	**Évaluation du risque brut (avant mesures)**			**Mesures mises en place**	**Évaluation du risque net (après mesures)**			**Commentaires**
				Impact	Probabilité	Niveau du risque brut		Impact	Probabilité	Niveau du risque net	
Accès aux RP	Vol de RP	• Un employé malveillant • Une personne qui réussit à s'introduire dans le système • Usage non sécuritaire par la personne concernée	• Vol d'identité • Fraude • Sentiment d'intrusion dans la vie privée • Perte d'intimidé • Stress • Induire des démarches pour le citoyen pour reprendre le contrôle de ses RP	4	3	12	• Les personnes ayant accès aux RP feront l'objet d'une habilitation sécuritaire de la SQ • Les actions sont journalisées et les journaux sont exploités • L'accès est restreint uniquement aux personnes dont les fonctions le nécessitent • La gestion des autorisations suit un processus d'approbation • Le citoyen est informé des accès à son justificatif par notification • Les données sont cryptées	2	3	6	• Risque Cygne noir • Le MCN n'a aucun contrôle sur les causes de ce risque
	Donnée non disponible pour le MCN ou l'utilisateur	• Séisme • Catastrophe naturelle	• Stress • Impossibilité pour la personne d'avoir accès au service	3	3	9	• Une copie de sauvegarde sécurisée des données sera exportée vers une localisation géographique distante et offrant une protection équivalant à celle prévue à la Loi sur l'accès[21] afin d'être en mesure de procéder à la relève du système, en cas de besoin • L'infrastructure est conçue de manière à offrir un très haut niveau de disponibilité (redondance) • Le service d'infrastructure répond aux exigences de haute disponibilité du gouvernement	3	2	6	
	Accès non autorisé aux RP	• Personne négligente à l'interne ou à l'externe du MCN • Vol ou perte d'équipement	• Vol d'identité • Fraude • Sentiment d'intrusion dans la vie privée • Perte d'intimidé • Stress	4	3	12	• Sensibilisation du personnel à l'égard de la PRP • Sensibilisation des utilisateurs aux bonnes pratiques numériques • Notification de l'utilisateur lors de changements significatifs à son compte d'authentification • Authentification à double facteur nécessaire pour utiliser le compte d'authentification	1	2	2	

[21] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c A-2.1; dans le présent rapport : « Loi sur l'accès »)

Analyse des risques – Programme SQIN – projet 1												
Cycle de vie	**Risque brut / Scénario**	**Cause / Source**	**Impact / Conséquence sur la personne concernée**	**Évaluation du risque brut (avant mesures)**			**Mesures mises en place**	**Évaluation du risque net (après mesures)**			**Commentaires**
				Impact	Probabilité	Niveau du risque brut		Impact	Probabilité	Niveau du risque net	
		• Personne malveillante • Employé en télétravail	• Induire des démarches pour le citoyen pour reprendre le contrôle de ses RP • Perte de confiance envers le gouvernement				• Chiffrement des ordinateurs portables et appareils mobiles utilisés par les employés du MCN • Les données sont cryptées • Pseudonymisation de certaines bases de données				
	Réidentification des renseignements préalablement anonymisés	• Une anonymisation insuffisante qui permet à un employé malveillant de faire marche arrière	• Vol d'identité • Fraude • Sentiment d'intrusion dans la vie privée • Perte d'intimidé • Stress • Induire des démarches pour le citoyen pour reprendre le contrôle de ses RP • Perte de confiance envers le gouvernement	4	2	8	• Mise en place du hachage des données • Algorithmes robustes d'anonymisation des données • Création de données fictives pour les expérimentations • Formation de certains employés aux principes de PRP dès la conception de la solution	2	1	2	• Risque à surveiller en continu puisque qu'il existe un manque de contrôle sur les causes. L'évaluation a été effectuée en tenant compte des événements survenus dans certaines institutions et MO au cours des dernières années. • Les mesures suivantes seront en place au moment de la mise en production : - Processus de gestion des fraudes - Équipe dédiée à la mise en place des outils de détection des menaces (mode prévention en continu) - Processus de détection des menaces pour l'exploitation de la solution

Analyse des risques – Programme SQIN – projet 1												
Cycle de vie	**Risque brut / Scénario**	**Cause / Source**	**Impact / Conséquence sur la personne concernée**	**Évaluation du risque brut (avant mesures)**			**Mesures mises en place**	**Évaluation du risque net (après mesures)**			**Commentaires**
				Impact	Probabilité	Niveau du risque brut		Impact	Probabilité	Niveau du risque net	
Communication	Divulgation non autorisée des RP	• Erreur d'identification • Erreur de destinataire • Utilisation d'un mode de communication non conforme • Non-respect des procédures	• Vol d'identité • Fraude • Sentiment d'intrusion dans la vie privée • Perte d'intimidé • Stress • Induire des démarches pour le citoyen pour reprendre contrôle de ses RP • Perte de confiance envers le gouvernement	3	3	9	• Sensibilisation du personnel à l'égard de la PRP • Processus d'identification des personnes en place • Fichier sécurisé par mot de passe • Transmission du mot de passe séparément • Envoie de courriel sécurisé	2	3	6	• Risque à surveiller en continu puisque qu'il existe un manque de contrôle sur les causes. L'évaluation a été effectuée en tenant compte des événements survenus dans certaines institutions et MO au cours des dernières années. • Les mesures suivantes seront en place au moment de la mise en production : - Processus de gestion des fraudes - Équipe dédiée à la mise en place des outils de détection des menaces (mode prévention en continu) - Processus de détection des menaces pour l'exploitation de la solution

Analyse des risques – Programme SQIN – projet 1												
Cycle de vie	**Risque brut / Scénario**	**Cause / Source**	**Impact / Conséquence sur la personne concernée**	**Évaluation du risque brut (avant mesures)**			**Mesures mises en place**	**Évaluation du risque net (après mesures)**			**Commentaires**
				Impact	Probabilité	Niveau du risque brut		Impact	Probabilité	Niveau du risque net	
	Atteinte à la cybersécurité	• Piratage • Espionnage • Sabotage • Vulnérabilité liée aux librairies applicatives utilisées dans la solution	• Vol d'identité • Fraude • Sentiment d'intrusion dans la vie privée • Perte d'intimidé • Stress • Induire des démarches pour le citoyen pour reprendre le contrôle de ses RP • Perte de confiance envers le gouvernement • Impossibilité pour la personne d'avoir accès au service • Perte de temps • Frustration	4	4	16	• Formation continue du personnel dédié à la cybersécurité • Programme de prime aux bogues • Les actions sont journalisées et les journaux sont exploités • Gestion des droits d'accès • Utilisation d'équipement permettant de prévenir et de détecter les intrusions • Équipe dédiée à la cybersécurité qui surveille les infrastructures du MCN et du gouvernement • Les personnes ayant accès aux données feront l'objet d'une habilitation sécuritaire de la SQ • Mise en place de mécanismes obligatoires et automatisés d'analyse de sécurité lors de la compilation des applications • Réalisation d'une analyse de vulnérabilité prévue plusieurs fois par année • Essais d'intrusions prévus plusieurs fois par année • Les données sont cryptées	3	3	9	• Atteinte à la cybersécurité
Conservation	Conservation de renseignements lorsque leur utilité n'est plus démontrée	• Il n'y a pas de règle de conservation • Règle de conservation non appliquée	• Vol d'identité • Fraude • Perte financière • Sentiment d'intrusion dans la vie privée • Perte d'intimidé • Stress • Induire des démarches pour le citoyen pour reprendre le contrôle de ses RP	4	3	12	• Une règle de conservation a été élaborée • Une directive de conservation a été élaborée • Calendrier de conservation mis en place • Élaboration d'un processus d'affaires sur les dossiers actifs/inactifs • Mesures chapeautées par la gouvernance et les règles revues aux deux ans • Destruction des données périodiquement prévue au processus de destruction • Sensibilisation du personnel à l'égard de la PRP	2	1	2	

8. Réévaluation périodique

Le rapport d'ÉFVP est évolutif, il sera donc révisé lors de chaque changement au projet ou aux éléments qui s'appliquent à celui-ci ayant un impact sur les RP. Les versions révisées du rapport seront transmises à la CAI, conformément à la LGGRI.

La vérification de la mise en place des actions permettant d'assurer la mise en œuvre des stratégies et des moyens retenus pour assurer la PRP, ainsi que de la mise à jour du rapport d'EFVP, sera assurée par les parties prenantes qui en sont responsables conformément au cadre de gouvernance applicable au projet.

9. Approbation

Le présent rapport d'EFVP a été approuvé par la Responsable de l'accès aux documents et de la protection des renseignement personnels, Madame Renée Giguère, ainsi que par le sous-ministre de la Cybersécurité et du Numérique et dirigeant principal de l'information, Monsieur Pierre E. Rodrigue, en date du 17 février 2023.

10. Acronymes

ADPRP	Accès aux documents et PRP
AWS	Amazon Web Services
CAI	Commission d'accès à l'information
CASA	Carrefour des services d'affaires
CDSI	Chef délégué de la SI
CGCD	Centre gouvernemental de cyberdéfense
COCD	Centre organisationnel de cyberdéfense
CSIO	Chef de la SI organisationnelle
COMSI	Coordonnateur organisationnel des mesures de SI
CSIPRPC	Comité sur la SI , la PRP et la continuité
CSPQ	Centre de services partagés du Québec
CTI	Centre de traitement de l'information
DDN	Date de naissance
DGSCE	Direction générale des solutions citoyennes et entreprises
DGSG	Direction générale du Secrétariat général
DGSSI	Direction générale de la sécurité des services et de l'information
DI	Dirigeant de l'information
DPI	Dirigeant principal de l'information
DRMI	Direction des ressources matérielles et informationnelles
EFVP	Évaluation des facteurs relatifs à la vie privée
FIPA	Fichier d'inscription des personnes assurée
ITQ	Infrastructures technologiques Québec
LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
MCE	Ministère du Conseil exécutif
MCN	Ministère de la Cybersécurité et du Numérique
MESS	Ministère de l'Emploi et de la Solidarité sociale
MFA	Ministère de la Famille
NAM	Numéro d'assurance maladie
NAS	Numéro d'assurance sociale
MO	Ministère(s) et organisme(s) public(s)
PDF	Portable Document Format
PES	Prestations électroniques de services
PRP	Protection des renseignements personnels
RADPRP	Responsable de l'accès aux documents et de la protection des renseignement personnels
RAIG	Registre d'attributs d'identité gouvernemental
RAMQ	Régie de l'assurance maladie du Québec
RITM	Réseau intégré de télécommunication multimédia
ROCD	Responsable opérationnel de la cyberdéfense
RP	Renseignement(s) personnel(s)
RPC	Responsable des plaintes et des commentaires
RQ	Revenu Québec
SAAQ	Société de l'assurance automobile du Québec
SAG	Service d'authentification gouvernementale
SI	Sécurité de l'information
SM	Sous-ministre de la Cybersécurité et du Numérique
SMAITB	Sous-ministériat adjoint aux infrastructures technologique et à la bureautique
SMASIGC	Sous-ministériat adjoint à la SI gouvernementale et à la cybersécurité
SMATNG	Sous-ministériat adjoint à la transformation numérique gouvernementale
SQ	Sûreté du Québec
SQIN	Service québécois d'identité numérique
SRIDAI	Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité
TI	Technologies de l'information

11. 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.
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 de l'authentifiant à celles de l'identité.
MO Partenaire (source de confiance)	MO qui communique des renseignements nécessaires à la constitution et à la tenue du RAIG.
MO Partenaire (valideur de secret)	MO contribuant à la validation de l'identité d'un citoyen.
MO Consommateur	MO ayant recours au SAG.
Prestation électronique de service	Prestation de services gouvernementaux, sécurisés ou non, offerts aux utilisateurs par l'intermédiaire d'Internet.
RP	Toute information qui concerne une personne physique et qui permet de l'identifier directement ou indirectement.
Utilisateur	Une personne (ou son représentant) qui souhaite accéder intentionnellement à un service numérique.

Annexe 1 – Cadre légal et normatif

Document	Émetteur ou provenance du document	Version
Cadre de gouvernance et de gestion de la sécurité de l'information	MCN	2022-03-29
Code de bonnes pratiques du numéro d'assurance sociale[22]	Gouvernement du Canada – Emploi et Développement social Canada	2023-01-09
Décret numéro 511-2020 du 13 mai 2020	MCE	2022-05-13
Décret numéro 870-2022 du 25 mai 2022	MCE	2022-05-25
Décret numéro 1690-2022 du 26 octobre 2022	MCE	2022-10-26
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 – Gestion des accès physique	MCN	2023-02-17
Directive sur la conformité des services en matière de sécurité de l'information	MCN	2023-02-17
Directive sur la prévention et la gestion des conflits d'intérêts (EL-00-00-03-00-00)	ITQ	2021-10-27
Directive sur l'encadrement des exigences de sécurité vis-à-vis des tiers	MCN	2023-02-17
Directive sur le numéro d'assurance sociale[23] (ISBN: 978-0-660-09689-6)	Gouvernement du Canada	2022-10-26
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
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

[22] https://www.canada.ca/fr/emploi-developpement-social/services/numero-assurance-sociale/rapports/code-pratiques.html
[23] https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=13342&section=html

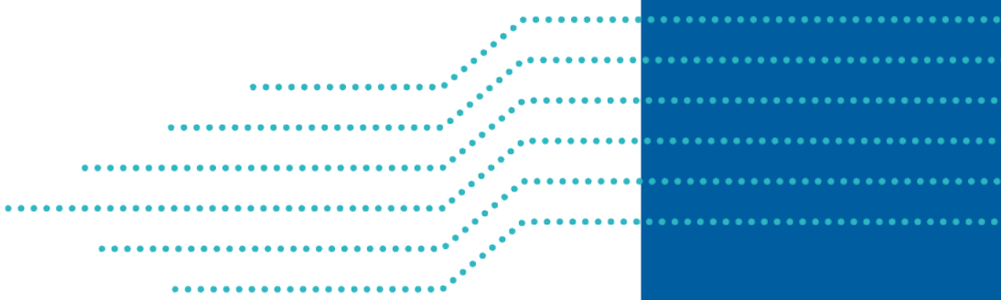
Document	Émetteur ou provenance du document	Version
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)	MCE	Mise à jour en continu – Publications du Québec
Loi sur la gouvernance et la gestion des ressources informationnelles des organismes 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 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	2023-02-17
Politique de sécurité de l'information	MCN	2022-03-29
Politique – Gestion des plaintes et des commentaires (AI-01-00-00-00-00)	CSPQ	2019-09-13
Procédure de gestion des incidents de confidentialité	Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité du MCE	S.O.
Procédure de traitement des demandes d'accès et de rectification des renseignements personnels en lien avec le Service d'authentification gouvernementale	MCN	2023-02-17
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
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[24]	Ministre de la Cybersécurité et du Numérique	2022-08-26

[24] Arrêté numéro 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022, publié à la *Gazette officielle du Québec* le 7 septembre 2022, page 6065.

Annexe 2 – Contrats et ententes avec les partenaires du projet

Titre du contrat ou de l'entente	Objectifs du contrat ou de l'entente	Nom des partenaires	Rôles des partenaires	Date de début	Date de fin	Renouvellements prévus
Entente SAAQ/MCN hébergement temporaire des données	La SAAQ confie au MCN le développement et l'exploitation d'une solution temporaire permettant de valider le secret partagé de la SAAQ.	SAAQ MCN	Le MCN doit effectuer des travaux de développement et assurer l'exploitation d'une solution temporaire en vue d'assurer le transfert et l'hébergement de données de la SAAQ requises dans le cadre du projet, ainsi que pour assurer le traitement des vérifications du secret partagé.	2022-10-27	2022-12-31	L'entente se renouvelle de plein droit pour une période de six mois.

À noter : Uniquement les ententes et les contrats signés sont indiqués ci-dessus.



Québec