

RE: Pour commentaires : documents rencontre de démarrage équipe projet SQIN

From: "Boutin, Catherine" <catherine.boutin@mce.gouv.qc.ca>
To: "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>
Cc: "Sauvé, Marie-Pier" <marie-pier.sauve@mce.gouv.qc.ca>, "Germain-Lauzon, Jennily" <jennily.germain-lauzon@mcn.gouv.qc.ca>, "Perron, Sophie" <sophie.perron@mcn.gouv.qc.ca>
Date: Tue, 12 Jul 2022 14:43:05 +0000
Attachments: Unnamed Attachment (68 bytes); Unnamed Attachment (68 bytes); Mandat - Équipe projet - SQIN (VF).docx (39.12 kB); Coordonnées Membres EP - SQIN.docx (31.69 kB); ODJ 14 juillet 2022 - Équipe projet - SQIN (VF).doc (65.02 kB)



Bonjour Karine,

Nous regardons la grille rapidement et vous revenons avec nos commentaires, le cas échéant. Par ailleurs, tu trouveras ci-joint le mandat de l'ÉP, ajusté selon les commentaires finaux de M. Audin. Le document sera présenté et transmis à tous en marge de la rencontre de jeudi. L'invitation sera d'ailleurs transmise ce matin, avec l'ordre du jour. À cet égard, nous souhaiterions convenir avec vous de l'information à communiquer au point 5 « Prochaines étapes », et en informer M. Audin. Est-ce qu'avec Sophie vous avez de la disponibilité cet après-midi? Je suis libre sauf entre 14h30-15h. Merci et à plus tard!
Catherine

De : Morin, Karine
Envoyé : 11 juillet 2022 15:26
À : Boutin, Catherine
Cc : Sauvé, Marie-Pier ; Germain-Lauzon, Jennily ; Perron, Sophie
Objet : RE: Pour commentaires : documents rencontre de démarrage équipe projet SQIN
Importance : Haute



Bonjour,

Voici maintenant notre grille pour la cueillette d'information. Elle a besoin d'explications que nous pourrions fournir pendant la rencontre. Le contenu qui sera fourni par les MO concernés aidera à établir les actions de communication les mieux adaptées. Nous attendons votre convocation. Merci !

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer,

d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

De : Morin, Karine <Karine.Morin@mcn.gouv.qc.ca>

Envoyé : 11 juillet 2022 14:51

À : Boutin, Catherine <Catherine.Boutin@mce.gouv.qc.ca>

Cc : Sauvé, Marie-Pier <Marie-Pier.Sauve@mce.gouv.qc.ca>; Germain-Lauzon, Jennily <Jennily.Germain-Lauzon@mcn.gouv.qc.ca>; Perron, Sophie <Sophie.Perron@mcn.gouv.qc.ca>

Objet : RE: Pour commentaires : documents rencontre de démarrage équipe projet SQIN

Importance : Haute

Cybersécurité
et Numérique



Bonjour,

Voici nos commentaires sur les documents soumis.

En fin de journée, vous aurez notre grille de cueillette d'information et demain matin, ma collègue du projet me fera parvenir la PPT de présentation du projet. Elle est avisée de la démarche et sera présente à la rencontre. Il s'agit d'Isabelle Guillemette, directrice à la direction générale du Service québécois d'identité numérique.

Merci !

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

De : Boutin, Catherine <Catherine.Boutin@mce.gouv.qc.ca>

Envoyé : 11 juillet 2022 10:25

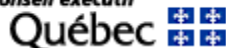
À : Germain-Lauzon, Jennily <Jennily.Germain-Lauzon@mcn.gouv.qc.ca>

Cc : Morin, Karine <Karine.Morin@mcn.gouv.qc.ca>; Sauvé, Marie-Pier <Marie-Pier.Sauve@mce.gouv.qc.ca>

Objet : Pour commentaires : documents rencontre de démarrage équipe projet SQIN

Importance : Haute

Ministère
du Conseil exécutif



Bonjour Jennily,

Comme convenu, nous vous partageons quelques documents en vue de la tenue d'une rencontre de démarrage de l'équipe projet SQIN dès cette semaine. Nous visons ce jeudi 14 juillet. Vos commentaires seraient très appréciés.

Il y aura aussi sans doute des préparatifs de votre côté, notamment pour une présentation du projet. Je te laisse faire le point avec Karine qui revient aujourd'hui et on se reconfirme le tout dès que possible.

Merci et bonne journée!

Catherine

Catherine Boutin

Conseillère I Coordination des communications stratégiques

Ministère du Conseil exécutif

Secrétariat à la communication gouvernementale

875, Grande Allée Est, bureau 5.771

Québec (Québec) G1R 4Y8

catherine.boutin@mce.gouv.qc.ca



418 643-2001, poste 3060

Ce courriel est à usage restreint. S'il ne vous est pas destiné, veuillez svp le détruire et en informer l'expéditeur.

ÉQUIPE PROJET EN COMMUNICATION SUR LE PROGRAMME SERVICE QUÉBÉCOIS D'IDENTITÉ NUMÉRIQUE

Coordonnatrices

MCN	Sophie Perron	
SCG	Catherine Boutin	

Coordonnées des membres – Équipe complète

Ministères et organismes	Représentants	Coordonnées
SCG (communications numériques)	Mathieu Imbeault	
MFA	Cynthia Richard et Simon Fortin	
	Jo-Anne Massé	
MTESS	Annie Bérubé	
	Laurent Slupik	
	Joël Gauthier	
	Émilie Charest (remplace Joël rencontre #1)	
Retraite Québec	Virginie Auger	
Régie de l'assurance maladie	Isabelle Landry	
	Chantale Garant-Noël	
Revenu Québec	Marie-Claude Gagnon	
	Catherine Ouellet	
Société de l'assurance automobile du Québec	Lucie Laviolette	
	Émilie Ferland-Paradis	

Mandat de l'équipe projet : Programme Service québécois d'identité numérique

Contexte de mise en œuvre
• La Stratégie de transformation numérique gouvernementale 2019-2023 prévoit offrir des services publics rapides et intuitifs propulsés par le numérique, où la confidentialité et la sécurité des données seront rehaussées. • Une nouvelle solution d'authentification gouvernementale « Service d'authentification gouvernementale » sera déployée graduellement auprès des organismes publics en 2022 et 2023. • Il permettra une meilleure accessibilité aux prestations électroniques de services du gouvernement du Québec, notamment par une meilleure compatibilité sur diverses plateformes technologiques (ordinateur, tablette et mobile). • Ce service vise à remplacer progressivement la solution clicSÉCUR afin de répondre aux nouvelles exigences de sécurité qui ont été rehaussées pour protéger l'identité numérique des Québécoises et Québécois.
Contribution des membres et mandat de l'équipe projet
• Élaborer une stratégie globale de communication gouvernementale multiplateformes, divisée en plusieurs volets, notamment la communication interne (gestion du changement) et la communication grand public, et s'adressant à plusieurs cibles (communication interne : organismes publics / communication grand public : utilisateurs du service d'authentification). • Outiller les ministères et les organismes concernés pour les communications avec leurs clientèles respectives. • Assurer une excellente cohésion et coordination des initiatives de communication des ministères et organismes concernés par le dossier. • Se doter de mécanismes de partage et de concertation en ce qui a trait à toute information pertinente dans le cadre de ce dossier. • Développer les messages gouvernementaux en lien avec le projet et ses différentes phases de mise en application. • Développer les messages propres à chacune des organisations concernées par le projet. • Mise en œuvre du plan de communication et de gestion du changement.
Composition de l'équipe

Mandat de l'équipe projet : Programme Service québécois d'identité numérique

- **Coordination** : Les travaux sont coordonnés par la direction des communications du MCN, en collaboration avec le SCG. Ils sont représentés respectivement par Sophie Perron (sophie.perron@mcn.gouv.qc.ca) et Catherine Boutin (catherine.boutin@mce.gouv.qc.ca).
- **Composition** : MCN, MCE (communications numériques et SCG), MFA, MTESS, RAMQ, Retraite Québec, Revenu Québec, SAAQ.

**RENCONTRE DE L'ÉQUIPE PROJET EN COMMUNICATION
SUR LE PROGRAMME SERVICE QUÉBÉCOIS D'IDENTITÉ NUMÉRIQUE**

Date : Le 14 juillet 2022
Lieu : Rencontre TEAMS
Heure : 13h30 à 15h

ORDRE DU JOUR

1. Mot de bienvenue (Thierry Audin)
2. Rôle de l'équipe projet et présentation du mandat (Marie-Pier Sauvé)
3. Présentation du dossier (Isabelle Guillemette et Karine Morin, MCN)
4. Tour de table (tous) :
 - Présentation des membres de l'équipe projet
 - Rôle du ministère ou de l'organisme dans le projet
 - Exposition des principaux défis internes et des enjeux externes
5. Prochaines étapes :
 - Premiers livrables
 - Prochaine rencontre
 - Fréquence des rencontres
6. Période de questions

Équipe projet en communication - Programme Service québécois d'identité numérique

From: "Perron, Sophie" <sophie.perron@mcn.gouv.qc.ca>
To: mathieu.imbeault2 <mathieu.imbeault2@mce.gouv.qc.ca>, Jo-Anne Masse <jo-anne.masse@education.gouv.qc.ca>, "Slupik, Laurent" <laurent.slupik@mtess.gouv.qc.ca>, "Gauthier, Joël" <joel.gauthier@servicesquebec.gouv.qc.ca>, virginie.auger <virginie.auger@retraitequebec.gouv.qc.ca>, Garant-Noël Chantale <chantale.garant-noel@ramq.gouv.qc.ca>, francine.bilodeau@ramq.gouv.qc.ca, Catherine.Ouellet <catherine.ouellet@revenuquebec.ca>, "Ferland-Paradis, Émilie" <emilie.ferland-paradis@saaq.gouv.qc.ca>
Cc: catherine.boutin <catherine.boutin@mce.gouv.qc.ca>, "Demers, Nathalie" <nathalie.demers@mcn.gouv.qc.ca>, "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>
Date: Fri, 19 Aug 2022 17:47:04 +0000
Attachments: PLCOM_SAG_2022_V19 août.pdf (289.16 kB)



Bonjour,

À l'aube de la rencontre du 22 août prochain, vous trouverez ci-joint le plan de communication en version projet.

Il est important de noter qu'il s'agit d'un document de travail. SVP ne le partagez qu'au sein de vos équipes DCOM pour l'instant.

En guise de rappel, l'objectif de la rencontre de lundi est d'échanger sur ce document.

Merci et au plaisir.

Sophie Perron
Coordonnatrice p. i. || Services-conseils en communication
Ministère de la Cybersécurité et du Numérique

800, Place d'Youville, 4e étage, suite 4.01, Québec (Québec) G1R 3P4
Tél. : 418 528-0880, poste 4827 | Téléc. : 418 644-0462
Sophie.Perron@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer

l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Plan de communication

**Service d'authentification gouvernementale :
Projet Accès bonifié aux prestations électroniques de
services (PES) – Citoyens**

Avis : Ce document fait l'objet d'une diffusion restreinte. L'information qu'il contient est sujette à des changements en fonction du déploiement du service, des changements contextuels, des priorités d'action et des résultats des actions de communication. La Direction des communications du MCN est responsable et gardienne de la version finale du plan.

Équipe projet - Programme Service québécois d'identité numérique
Version du 19 août 2022

CONTEXTE

La [Stratégie de transformation numérique gouvernementale 2019-2023](#) prévoit offrir des services publics rapides et intuitifs, propulsés par le numérique, où la confidentialité et la sécurité des données seront rehaussées.

Pour y arriver, une nouvelle solution d'authentification gouvernementale, s'inscrivant dans le projet Accès bonifié aux prestations électroniques de services (PES) – Citoyens¹, du [Programme Service québécois d'identité numérique](#), sera déployée graduellement à compter d'octobre 2022². Nommée Service d'authentification gouvernementale à l'issu de travaux et de tests utilisateurs³, elle permettra un accès aux services en ligne du gouvernement du Québec à partir de diverses plateformes technologiques, dans un environnement performant et sécuritaire.

Le projet Service d'authentification gouvernementale est réalisé par le ministère de la Cybersécurité et du Numérique, en collaboration avec des ministères et organismes (MO) parties prenantes de certaines étapes du développement et de sa mise en œuvre :

- le ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS), par l'entremise de Services Québec, pour le soutien téléphonique aux citoyens;
- la Régie de l'assurance maladie du Québec (RAMQ), fournisseur de la nouvelle source de confiance (validation de l'identité);
- Revenu Québec, la Société de l'assurance automobile du Québec (SAAQ, à confirmer) et la RAMQ, fournisseurs de secret (information contenue dans un document officiel, ex. avis de cotisation, pour la validation de l'identité).

Le Service d'authentification gouvernementale remplacera progressivement la solution actuelle [clicSÉCUR](#)⁴, implanté en 2005, pour pouvoir répondre aux orientations gouvernementales en matière de sécurité et d'expérience utilisateur. Mentionnons que l'adhésion des ministères et organismes (MO) au Service d'authentification gouvernementale s'effectue présentement sur une base volontaire.

Le déploiement du Service d'authentification gouvernementale s'effectuera par PES, identifiées par les MO, selon un calendrier déterminé (*annexe 1 à venir*). Lorsqu'une PES aura migré vers le service d'authentification, elle ne sera plus accessible par l'intermédiaire de son ancienne solution. Ainsi, dans l'inventaire global des différentes PES, il y aura une période de chevauchement entre l'ancienne et la nouvelle solution.

Le premier déploiement aura lieu dans le contexte de l'implantation d'une première PES au ministère de la Famille (MFA), en octobre, auprès d'éducatrices et d'éducateurs en petite enfance. Puis, dès janvier 2023, dans le cadre de sa transformation numérique, la SAAQ déploiera 5 portails de services en ligne sous l'appellation *saaqclic*, dont 4 utiliseront le Service d'authentification gouvernementale – Citoyens.

¹ Un projet Entreprises est également prévu ultérieurement, qui ne fait pas partie de la portée du présent plan de communication.

² Date exacte à déterminer.

³ Dénomination retenue, selon les [orientations gouvernementales](#) et ayant fait l'objet de tests auprès d'utilisateurs.

⁴ clicSÉCUR : service québécois d'authentification gouvernementale actuel permettant aux citoyens d'accéder à certaines prestations électroniques de services gouvernementales.

Utilisation des services en ligne

(Voir si d'autres données pertinentes sont disponibles)

Selon les données de l'Académie de la transformation numérique⁵, en 2021, deux adultes sur trois (67 %) évaluent qu'il est « très ou assez facile » d'utiliser les services offerts en ligne par le gouvernement. Ce point de vue est principalement partagé par les internautes âgés de 25 à 34 ans (77 %), ceux âgés de 35 à 44 ans (78 %) de même que par les diplômés universitaires (74 %). La création d'un système d'authentification unique qui donnerait accès à tous les services gouvernementaux arrive au troisième rang (71 %) des six initiatives numériques évaluées que le gouvernement devrait mettre en place.

DÉFIS DE COMMUNICATION INTERNE

Intégration d'une nouvelle offre de service

Plusieurs facteurs pourraient freiner l'adhésion des gestionnaires et du personnel des MO à l'implantation de la nouvelle solution. Notamment, la méconnaissance de la nouvelle solution, sa pertinence par rapport aux solutions existantes, la perception d'une charge de travail additionnelle (nouveaux apprentissages, cohabitation avec la solution actuelle ou une solution maison). L'adhésion des MO sur une base volontaire, du moins pour le moment, n'est pas un facteur à négliger.

Incidence sur la communication : mobiliser les autorités et gestionnaires, transmettre un message fort sur l'orientation de migrer vers une solution unique et les avantages; rassurer sur l'accompagnement qui sera offert

Résultats des projets pilotes

Des écueils pourraient survenir dans l'implantation des PES et de la nouvelle solution d'authentification, qui pourraient constituer un frein à l'adhésion des autres MO.

Incidence sur la communication : informer en continu, miser sur les bons coups pour générer un effet de levier

ENJEUX DE COMMUNICATION EXTERNE

Spécificités des offres de services

Le déploiement de la nouvelle solution s'effectuera en fonction d'un calendrier déterminé par les MO, en fonction de leurs objectifs organisationnels et des spécificités de leur offre de services. Ces spécificités se reflètent également dans le fait que ce sont divers événements de vie qui amènent le citoyen à s'adresser à un MO pour obtenir un service.

Incidences sur la communication : privilégier des initiatives de communication sectorielles, en phase avec le déploiement de l'offre de services des MO, de leurs spécificités et des besoins des utilisateurs

Coexistence des solutions actuelles et de la nouvelle

La coexistence de clicSÉCUR, de solutions maison et du Service d'authentification gouvernementale, en raison du déploiement graduel d'un MO à un autre, pour l'ensemble de ses PES ou certaines de celles-ci, pourrait créer de la confusion chez les utilisateurs, étant donné les façons différentes de s'authentifier pendant la période de transition.

L'inscription des citoyens au Service d'authentification gouvernementale ne pourra s'effectuer qu'au moment d'accéder à une PES (c'est aussi le cas pour l'actuel

⁵ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Les services gouvernementaux en ligne et l'identité numérique*, [En ligne], 27 avril 2022.

clicSÉCUR). Ainsi, l'inscription à la nouvelle solution sera possible seulement une fois que le Service d'authentification gouvernementale aura été déployé dans le MO donné.

La coexistence des solutions facilitera aussi la comparaison entre les deux services, qui pourrait susciter des questionnements sur la pertinence d'implanter une nouvelle solution.

Incidences sur la communication : communiquer la bonne information au bon moment, démontrer le bénéfice citoyen

Effritement de la confiance des utilisateurs envers clicSÉCUR

La désuétude de la technologie de clicSÉCUR pourrait effriter la confiance à l'égard de la solution. Elle pourrait aussi générer des questions quant à la durée de vie de la nouvelle solution (rapport investissement/durée de vie). Par ailleurs, le fait de parler de rehaussement des exigences de vérification d'identité pourrait avoir l'effet pervers de discréditer l'ancienne solution alors que celle-ci demeurera pendant un certain temps.

Incidences sur la communication : trouver le juste équilibre dans la manière de faire valoir la nouvelle solution sans le faire au détriment de l'autre, rassurer à l'effet que clicSÉCUR reste fonctionnel et sécuritaire, avec un entretien continu.

Résistances résultant de la première connexion

(schéma du parcours utilisateurs à venir en annexe)

L'obligation de créer un nouveau compte pour certains utilisateurs pourrait être un irritant, notamment pour ceux dont l'inscription à clicSÉCUR est récente. Les comptes des deux solutions ne seront pas jumelés.

Par ailleurs, le rehaussement des exigences de vérification d'identité lors de la première connexion des utilisateurs pourrait représenter un frein à leur adhésion au Service d'authentification gouvernementale. Mentionnons que certaines clientèles pourraient ne pas avoir accès à tous les documents demandés.

En effet, en plus du numéro d'assurance sociale qui pourra être fourni par l'utilisateur, de l'information détenue par la Régie de l'assurance maladie du Québec (RAMQ), Revenu Québec et la Société de l'assurance automobile du Québec (SAAQ, à confirmer) sera demandée afin de procéder à la vérification d'identité. S'il n'a pas l'information requise, l'utilisateur pourra demander un « secret d'identification » auprès de ces organismes. Il recevra alors l'information par la poste, ce qui pourrait prendre jusqu'à 10 jours ouvrables. Cela pourrait sembler paradoxal aux yeux de clientèles habituées à l'instantanéité qui caractérise les transactions Web et surtout, retarder l'inscription et l'obtention de la PES.

Incidence sur la communication : la nature de l'information demandée devra être connue au bon moment et si nécessaire, être en mesure de répondre au citoyen

Crainte quant à la confidentialité des données et la sécurité de l'information

La confidentialité des données et la sécurité de l'information sont des sujets sensibles pour tous, tant pour les organisations que la population. La nouvelle solution fera sûrement l'objet d'une couverture médiatique soutenue et d'une attention particulière de la part de certains groupes d'intérêt (ex. Commission d'accès à l'information). D'ailleurs, la couverture médiatique en lien avec la confidentialité des données et la sécurité de l'information, ou encore avec le « bordel informatique », pourrait miner la crédibilité du projet et freiner l'adhésion des utilisateurs.

Incidences sur la communication : rassurer sur les mécanismes de sécurité en place

Disfonctionnements de la nouvelle solution

L'implantation du Service d'authentification gouvernementale pourrait s'accompagner de disfonctionnements et de retards, ce qui pourrait entraîner des répercussions importantes pour les citoyens et des craintes pour la migration des autres PES. Cette situation pourrait

provoquer du mécontentement, engendrer des plaintes et même une surcharge de travail pour les services à la clientèle. La situation serait doublement problématique : accès impossible à la solution en ligne et temps d'attente plus long pour obtenir de l'aide. Par ailleurs, la solution actuelle clicSÉCUR n'est pas à l'abri d'un bris de service.

Incidences sur la communication : maintenir un lien constant entre les équipes de déploiement et les directions de communication, être prêts à communiquer en mode gestion de crise

RÉSULTATS ATTENDUS

À compléter, ex : objectifs d'affaires, cibles organisationnelles, résultats attendus déterminés selon les PES, nombre de plaintes reçues

PRINCIPES DIRECTEURS

En fonction de ce qui précède, les initiatives de communication entourant ce projet, tant pour la communication externe que publique, devront s'appuyer sur les principes directeurs suivants :

- la transparence;
- la cohérence des messages véhiculés par les MO, articulés autour d'un positionnement gouvernemental;
- une réponse efficace aux questions des citoyens.

OBJECTIFS DE COMMUNICATION

Objectifs généraux

- Faire connaître la nouvelle solution et démontrer ses avantages.
- Établir un niveau élevé de confiance envers la nouvelle solution.
- Faire adhérer les citoyens et les MO à la nouvelle solution.
- Démontrer que le gouvernement du Québec est engagé à offrir des services publics intuitifs et faciles d'utilisation pour la population, en améliorant l'efficacité de l'État.

Objectif spécifique à la communication interne

- Mobiliser et faire adhérer le personnel des MO au projet.

Objectifs spécifiques à la communication externe

- Démystifier la nouvelle solution de l'ancienne.
- Rassurer les utilisateurs sur le fait que la nouvelle solution assurera la protection de leurs données personnelles, entre autres par le rehaussement des exigences de vérification d'identité.
- Maintenir la confiance des utilisateurs de l'actuelle solution clicSÉCUR pendant la période de transition.

Objectifs de communication mesurables

À déterminer, communication gouvernementale et plans de communication sectoriels.

Par exemple, pour la communication gouvernementale :

- Pourcentage d'utilisateurs de la nouvelle solution qui estimeront avoir été bien outillés pour réaliser leur inscription.

PUBLICS CIBLES

Internes

- Les **MO consommateurs** qui souhaitent transférer certaines PES sur le Service d'authentification gouvernementale. Plus précisément, les équipes de projet des 9 ministères et organismes⁶ qui utilisent déjà clicSÉQUR – Citoyens et regroupées par expertise :
 - Affaires
 - Communication et Web
 - Gestion du changement
 - Services à la clientèle
 - TI
- Les **MO non-consommateurs de clicSÉQUR – Citoyens** :
 - Ministère de la Famille (MFA);
 - Société de l'assurance automobile du Québec (SAAQ);
 - Les MO qui offrent déjà une solution d'authentification développée à l'interne ou qui élaborent leur dossier d'affaires pour la mise en place de leur PES, et qui souhaitent connaître les modalités du Service d'authentification gouvernementale.
- Les syndicats d'employées et employés.
- Les groupes d'intérêts (ex. Commission d'accès à l'information, Protecteur du citoyen).
- Autres?

Externes

- Les **utilisateurs des PES susceptibles de recourir au Service d'authentification gouvernementale**.
 - Ce public cible sera segmenté par les MO pour que chacun puisse atteindre sa cible dans ses communications respectives. Une diversité de PES répond à une diversité de besoins et de profils d'utilisateurs.
- Les **utilisateurs de clicSÉQUR** qui ont créés plus de 2,5 millions de comptes et ceux qui en créeront un d'ici les déploiements dans les MO. Ceux-ci pourraient être à la fois utilisateurs des deux solutions.

STRATÉGIE

Puisque l'implantation de la nouvelle solution doit se faire graduellement par MO, selon un calendrier de PES, et considérant les spécificités de chaque PES, la stratégie de communication sera ponctuelle et ciblée auprès des utilisateurs concernés.

La diffusion de l'information se fera à deux niveaux, de façon à accompagner les utilisateurs au moment opportun dans leur démarche de transaction avec l'État :

- une information gouvernementale sur le service en général;
- une information sectorielle pour chaque PES.

⁶ Autorité des marchés financiers (AMF) / Conseil des arts et des lettres du Québec (CALQ) / Groupement des assureurs automobiles (GAA) / Ministère de l'Environnement et de la Lutte contre les changements climatiques (MELCC) / Ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) / Office de la protection du consommateur (OPC) / Régie de l'assurance maladie du Québec (RAMQ) / Retraite Québec / Revenu Québec (RQ)

(Évaluer la pertinence de proposer une séquence de communication type par PES basée sur les principes directeurs)

L'information gouvernementale sera prise en compte dans les plans de communication propres à chacun des MO qui planteront une PES utilisant le Service d'authentification gouvernementale. Cela comprendra notamment l'information sur le processus de connexion et l'accompagnement pour les utilisateurs, par Services Québec ou le MO concerné.

Cette approche d'intégration de l'information gouvernementale dans les communications sectorielles favorisera une communication de proximité avec l'utilisateur, au bon moment, en cohérence avec la démarche de celui-ci, qui est d'abord motivée par le besoin d'obtenir un service d'un MO. L'authentification de l'utilisateur étant une étape à franchir pour obtenir le service.

Orientations spécifiques pour la communication interne

Information – Mobilisation – Adhésion

- Communiquer régulièrement l'avancement des travaux et ses différents jalons.
- Transformer le personnel des MO consommateurs en ambassadeurs. Les équipes des MO devront pouvoir s'approprier les nouveautés au moment opportun afin de les communiquer auprès de leurs clientèles.
- Transmettre des communications aux MO non-consommateurs sur les résultats des projets pilotes en vue de susciter leur adhésion au Service d'authentification gouvernementale.

Orientations spécifiques pour la communication externe

Information – Accompagnement - Adhésion

- Diffuser l'information gouvernementale sur la nouvelle solution sur Québec.ca.
- Expliquer les modalités d'utilisation des deux solutions pendant la transition.
- Profiter des canaux de communication des MO consommateurs avec leurs clientèles à des moments clés pour le recours aux PES.
- Prévoir des canaux de communication pour rejoindre l'ensemble des utilisateurs potentiels.
- Profiter des communications aux utilisateurs de la solution actuelle clicSÉCUR pour communiquer sur le Service d'authentification gouvernementale.
- Véhiculer l'image d'une plateforme sécuritaire qui permet d'augmenter la rapidité de traitement lors de démarches administratives avec le gouvernement, en éliminant notamment les délais postaux.
- Mettre en place des procédures de communication pour chaque MO afin de faire face aux risques de panne de la plateforme (gestion de crise pour les situations de dysfonctionnement).

AXE DE COMMUNICATION

Le Service d'authentification gouvernementale est une solution moderne, évolutive, accessible et tout aussi sécuritaire, qui facilite la communication entre l'État et le citoyen.

MESSAGES

Messages généraux

- Le Service d'authentification gouvernementale simplifiera la vie des citoyens et des MO en rendant les démarches administratives beaucoup plus simples et rapides.
- Le Service d'authentification gouvernementale assure une évolution technologique afin de réaliser la transformation numérique gouvernementale.

Pour les publics internes

- Le Service d'authentification gouvernementale contribue à augmenter la cohérence des systèmes et l'accès aux services en ligne gouvernementaux.
- Le Service d'authentification gouvernementale offre des avantages non négligeables pour votre clientèle concernant la sécurité de leurs données et une rapidité de traitement lors de démarches administratives, en éliminant notamment les délais postaux.
- Le gouvernement du Québec prend en considération les spécificités des MO pour proposer une solution optimale pour tous.
- De la formation au personnel est disponible afin que tous puissent communiquer de façon efficiente sur le Service d'authentification gouvernementale.

Pour les publics externes :

- Le Service d'authentification gouvernementale est plus performant quant à son accessibilité technologique, et rehausse le niveau de confidentialité et la sécurité des données pour l'ensemble des PES du gouvernement du Québec (bien que la sécurité de la solution actuelle soit conforme).
- Le gouvernement du Québec met toute son expertise au service de la sécurité numérique des citoyens par l'intermédiaire du nouveau Service d'authentification gouvernementale.
- La solution clicSÉCUR reste opérationnelle et entretenue pour garantir un niveau conforme de sécurité.

MOYENS DE COMMUNICATION

Différents moyens de communication seront utilisés selon les publics cibles, la nature de l'information à transmettre et les étapes du projet. À venir dans la phase subséquente des travaux, en fonction de la stratégie retenue.

BUDGET

À venir en fonction de la stratégie et des moyens retenus.

RECHERCHE ET ÉVALUATION

À venir dans la phase subséquente des travaux.

SÉQUENCE DE COMMUNICATION

À venir dans la phase subséquente des travaux.

Équipe projet en communication - Programme Service québécois d'identité numérique

From: "Perron, Sophie" <sophie.perron@mcn.gouv.qc.ca>
To: mathieu.imbeault2 <mathieu.imbeault2@mce.gouv.qc.ca>, Jo-Anne Masse <jo-anne.masse@education.gouv.qc.ca>, "Slupik, Laurent" <laurent.slupik@mtess.gouv.qc.ca>, "Gauthier, Joël" <joel.gauthier@servicesquebec.gouv.qc.ca>, virginie.auger <virginie.auger@retraitequebec.gouv.qc.ca>, Garant-Noël Chantale <chantale.garant-noel@ramq.gouv.qc.ca>, francine.bilodeau@ramq.gouv.qc.ca, Catherine.Ouellet <catherine.ouellet@revenuquebec.ca>, "Ferland-Paradis, Émilie" <emilie.ferland-paradis@saaq.gouv.qc.ca>, "Desgagné, Marie-Eve" <marie-eve.desgagne3@saaq.gouv.qc.ca>, Létourneau Vanessa <vanessa.letourneau@retraitequebec.gouv.qc.ca>, "Talbot, Stéphanie" <stephanie.talbot@saaq.gouv.qc.ca>
Cc: "Boutin, Catherine" <catherine.boutin@mce.gouv.qc.ca>, "Demers, Nathalie" <nathalie.demers@mcn.gouv.qc.ca>, "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>
Date: Mon, 22 Aug 2022 20:14:33 +0000
Attachments: Compte rendu du processus de dénomination SQIN 1.pdf (418.55 kB);
PLCOM_SAG_2022_V19 août.pdf (289.16 kB)

Cybersécurité
et Numérique



Bonjour,

Tel que mentionné lors de notre rencontre, vous trouverez en pièce jointe le compte-rendu du processus de dénomination.

J'en profite pour vous rappeler que vos commentaires sur la version de travail (parti 1) du plan de communication sont attendus d'ici **ce vendredi, 26 août**.

J'ajoute également l'hyperlien vous permettant de travailler en mode collaboratif dans notre équipe

Teams :  [PLCOM_SAG_2022_V19 août.docx](#)

Finalement, je vous remercie à l'avance de conserver Nathalie (nathalie.demers@mcn.gouv.qc.ca) en copie de vos retours courriel.

Merci et bonne fin de journée!

Sophie Perron

Coordonnatrice p. i. || Services-conseils en communication

Ministère de la Cybersécurité et du Numérique

800, Place d'Youville, 4e étage, suite 4.01, Québec (Québec) G1R 3P4

Tél. : 418 528-0880, poste 4827 | Téléc. : 418 644-0462

Sophie.Perron@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer

l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Plan de communication

**Service d'authentification gouvernementale :
Projet Accès bonifié aux prestations électroniques de
services (PES) – Citoyens**

Avis : Ce document fait l'objet d'une diffusion restreinte. L'information qu'il contient est sujette à des changements en fonction du déploiement du service, des changements contextuels, des priorités d'action et des résultats des actions de communication. La Direction des communications du MCN est responsable et gardienne de la version finale du plan.

Équipe projet - Programme Service québécois d'identité numérique
Version du 19 août 2022

CONTEXTE

La [Stratégie de transformation numérique gouvernementale 2019-2023](#) prévoit offrir des services publics rapides et intuitifs, propulsés par le numérique, où la confidentialité et la sécurité des données seront rehaussées.

Pour y arriver, une nouvelle solution d'authentification gouvernementale, s'inscrivant dans le projet Accès bonifié aux prestations électroniques de services (PES) – Citoyens¹, du [Programme Service québécois d'identité numérique](#), sera déployée graduellement à compter d'octobre 2022². Nommée Service d'authentification gouvernementale à l'issu de travaux et de tests utilisateurs³, elle permettra un accès aux services en ligne du gouvernement du Québec à partir de diverses plateformes technologiques, dans un environnement performant et sécuritaire.

Le projet Service d'authentification gouvernementale est réalisé par le ministère de la Cybersécurité et du Numérique, en collaboration avec des ministères et organismes (MO) parties prenantes de certaines étapes du développement et de sa mise en œuvre :

- le ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS), par l'entremise de Services Québec, pour le soutien téléphonique aux citoyens;
- la Régie de l'assurance maladie du Québec (RAMQ), fournisseur de la nouvelle source de confiance (validation de l'identité);
- Revenu Québec, la Société de l'assurance automobile du Québec (SAAQ, à confirmer) et la RAMQ, fournisseurs de secret (information contenue dans un document officiel, ex. avis de cotisation, pour la validation de l'identité).

Le Service d'authentification gouvernementale remplacera progressivement la solution actuelle [clicSÉCUR](#)⁴, implanté en 2005, pour pouvoir répondre aux orientations gouvernementales en matière de sécurité et d'expérience utilisateur. Mentionnons que l'adhésion des ministères et organismes (MO) au Service d'authentification gouvernementale s'effectue présentement sur une base volontaire.

Le déploiement du Service d'authentification gouvernementale s'effectuera par PES, identifiées par les MO, selon un calendrier déterminé (*annexe 1 à venir*). Lorsqu'une PES aura migré vers le service d'authentification, elle ne sera plus accessible par l'intermédiaire de son ancienne solution. Ainsi, dans l'inventaire global des différentes PES, il y aura une période de chevauchement entre l'ancienne et la nouvelle solution.

Le premier déploiement aura lieu dans le contexte de l'implantation d'une première PES au ministère de la Famille (MFA), en octobre, auprès d'éducatrices et d'éducateurs en petite enfance. Puis, dès janvier 2023, dans le cadre de sa transformation numérique, la SAAQ déploiera 5 portails de services en ligne sous l'appellation *saaqclic*, dont 4 utiliseront le Service d'authentification gouvernementale – Citoyens.

¹ Un projet Entreprises est également prévu ultérieurement, qui ne fait pas partie de la portée du présent plan de communication.

² Date exacte à déterminer.

³ Dénomination retenue, selon les [orientations gouvernementales](#) et ayant fait l'objet de tests auprès d'utilisateurs.

⁴ clicSÉCUR : service québécois d'authentification gouvernementale actuel permettant aux citoyens d'accéder à certaines prestations électroniques de services gouvernementales.

Utilisation des services en ligne

(Voir si d'autres données pertinentes sont disponibles)

Selon les données de l'Académie de la transformation numérique⁵, en 2021, deux adultes sur trois (67 %) évaluent qu'il est « très ou assez facile » d'utiliser les services offerts en ligne par le gouvernement. Ce point de vue est principalement partagé par les internautes âgés de 25 à 34 ans (77 %), ceux âgés de 35 à 44 ans (78 %) de même que par les diplômés universitaires (74 %). La création d'un système d'authentification unique qui donnerait accès à tous les services gouvernementaux arrive au troisième rang (71 %) des six initiatives numériques évaluées que le gouvernement devrait mettre en place.

DÉFIS DE COMMUNICATION INTERNE

Intégration d'une nouvelle offre de service

Plusieurs facteurs pourraient freiner l'adhésion des gestionnaires et du personnel des MO à l'implantation de la nouvelle solution. Notamment, la méconnaissance de la nouvelle solution, sa pertinence par rapport aux solutions existantes, la perception d'une charge de travail additionnelle (nouveaux apprentissages, cohabitation avec la solution actuelle ou une solution maison). L'adhésion des MO sur une base volontaire, du moins pour le moment, n'est pas un facteur à négliger.

Incidence sur la communication : mobiliser les autorités et gestionnaires, transmettre un message fort sur l'orientation de migrer vers une solution unique et les avantages; rassurer sur l'accompagnement qui sera offert

Résultats des projets pilotes

Des écueils pourraient survenir dans l'implantation des PES et de la nouvelle solution d'authentification, qui pourraient constituer un frein à l'adhésion des autres MO.

Incidence sur la communication : informer en continu, miser sur les bons coups pour générer un effet de levier

ENJEUX DE COMMUNICATION EXTERNE

Spécificités des offres de services

Le déploiement de la nouvelle solution s'effectuera en fonction d'un calendrier déterminé par les MO, en fonction de leurs objectifs organisationnels et des spécificités de leur offre de services. Ces spécificités se reflètent également dans le fait que ce sont divers événements de vie qui amènent le citoyen à s'adresser à un MO pour obtenir un service.

Incidences sur la communication : privilégier des initiatives de communication sectorielles, en phase avec le déploiement de l'offre de services des MO, de leurs spécificités et des besoins des utilisateurs

Coexistence des solutions actuelles et de la nouvelle

La coexistence de clicSÉCUR, de solutions maison et du Service d'authentification gouvernementale, en raison du déploiement graduel d'un MO à un autre, pour l'ensemble de ses PES ou certaines de celles-ci, pourrait créer de la confusion chez les utilisateurs, étant donné les façons différentes de s'authentifier pendant la période de transition.

L'inscription des citoyens au Service d'authentification gouvernementale ne pourra s'effectuer qu'au moment d'accéder à une PES (c'est aussi le cas pour l'actuel

⁵ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Les services gouvernementaux en ligne et l'identité numérique*, [En ligne], 27 avril 2022.

clicSÉCUR). Ainsi, l'inscription à la nouvelle solution sera possible seulement une fois que le Service d'authentification gouvernementale aura été déployé dans le MO donné.

La coexistence des solutions facilitera aussi la comparaison entre les deux services, qui pourrait susciter des questionnements sur la pertinence d'implanter une nouvelle solution.

Incidences sur la communication : communiquer la bonne information au bon moment, démontrer le bénéfice citoyen

Effritement de la confiance des utilisateurs envers clicSÉCUR

La désuétude de la technologie de clicSÉCUR pourrait effriter la confiance à l'égard de la solution. Elle pourrait aussi générer des questions quant à la durée de vie de la nouvelle solution (rapport investissement/durée de vie). Par ailleurs, le fait de parler de rehaussement des exigences de vérification d'identité pourrait avoir l'effet pervers de discréditer l'ancienne solution alors que celle-ci demeurera pendant un certain temps.

Incidences sur la communication : trouver le juste équilibre dans la manière de faire valoir la nouvelle solution sans le faire au détriment de l'autre, rassurer à l'effet que clicSÉCUR reste fonctionnel et sécuritaire, avec un entretien continu.

Résistances résultant de la première connexion

(schéma du parcours utilisateurs à venir en annexe)

L'obligation de créer un nouveau compte pour certains utilisateurs pourrait être un irritant, notamment pour ceux dont l'inscription à clicSÉCUR est récente. Les comptes des deux solutions ne seront pas jumelés.

Par ailleurs, le rehaussement des exigences de vérification d'identité lors de la première connexion des utilisateurs pourrait représenter un frein à leur adhésion au Service d'authentification gouvernementale. Mentionnons que certaines clientèles pourraient ne pas avoir accès à tous les documents demandés.

En effet, en plus du numéro d'assurance sociale qui pourra être fourni par l'utilisateur, de l'information détenue par la Régie de l'assurance maladie du Québec (RAMQ), Revenu Québec et la Société de l'assurance automobile du Québec (SAAQ, à confirmer) sera demandée afin de procéder à la vérification d'identité. S'il n'a pas l'information requise, l'utilisateur pourra demander un « secret d'identification » auprès de ces organismes. Il recevra alors l'information par la poste, ce qui pourrait prendre jusqu'à 10 jours ouvrables. Cela pourrait sembler paradoxal aux yeux de clientèles habituées à l'instantanéité qui caractérise les transactions Web et surtout, retarder l'inscription et l'obtention de la PES.

Incidence sur la communication : la nature de l'information demandée devra être connue au bon moment et si nécessaire, être en mesure de répondre au citoyen

Crainte quant à la confidentialité des données et la sécurité de l'information

La confidentialité des données et la sécurité de l'information sont des sujets sensibles pour tous, tant pour les organisations que la population. La nouvelle solution fera sûrement l'objet d'une couverture médiatique soutenue et d'une attention particulière de la part de certains groupes d'intérêt (ex. Commission d'accès à l'information). D'ailleurs, la couverture médiatique en lien avec la confidentialité des données et la sécurité de l'information, ou encore avec le « bordel informatique », pourrait miner la crédibilité du projet et freiner l'adhésion des utilisateurs.

Incidences sur la communication : rassurer sur les mécanismes de sécurité en place

Disfonctionnements de la nouvelle solution

L'implantation du Service d'authentification gouvernementale pourrait s'accompagner de disfonctionnements et de retards, ce qui pourrait entraîner des répercussions importantes pour les citoyens et des craintes pour la migration des autres PES. Cette situation pourrait

provoquer du mécontentement, engendrer des plaintes et même une surcharge de travail pour les services à la clientèle. La situation serait doublement problématique : accès impossible à la solution en ligne et temps d'attente plus long pour obtenir de l'aide. Par ailleurs, la solution actuelle clicSÉCUR n'est pas à l'abri d'un bris de service.

Incidences sur la communication : maintenir un lien constant entre les équipes de déploiement et les directions de communication, être prêts à communiquer en mode gestion de crise

RÉSULTATS ATTENDUS

À compléter, ex : objectifs d'affaires, cibles organisationnelles, résultats attendus déterminés selon les PES, nombre de plaintes reçues

PRINCIPES DIRECTEURS

En fonction de ce qui précède, les initiatives de communication entourant ce projet, tant pour la communication externe que publique, devront s'appuyer sur les principes directeurs suivants :

- la transparence;
- la cohérence des messages véhiculés par les MO, articulés autour d'un positionnement gouvernemental;
- une réponse efficace aux questions des citoyens.

OBJECTIFS DE COMMUNICATION

Objectifs généraux

- Faire connaître la nouvelle solution et démontrer ses avantages.
- Établir un niveau élevé de confiance envers la nouvelle solution.
- Faire adhérer les citoyens et les MO à la nouvelle solution.
- Démontrer que le gouvernement du Québec est engagé à offrir des services publics intuitifs et faciles d'utilisation pour la population, en améliorant l'efficacité de l'État.

Objectif spécifique à la communication interne

- Mobiliser et faire adhérer le personnel des MO au projet.

Objectifs spécifiques à la communication externe

- Démystifier la nouvelle solution de l'ancienne.
- Rassurer les utilisateurs sur le fait que la nouvelle solution assurera la protection de leurs données personnelles, entre autres par le rehaussement des exigences de vérification d'identité.
- Maintenir la confiance des utilisateurs de l'actuelle solution clicSÉCUR pendant la période de transition.

Objectifs de communication mesurables

À déterminer, communication gouvernementale et plans de communication sectoriels.

Par exemple, pour la communication gouvernementale :

- Pourcentage d'utilisateurs de la nouvelle solution qui estimeront avoir été bien outillés pour réaliser leur inscription.

PUBLICS CIBLES

Internes

- Les **MO consommateurs** qui souhaitent transférer certaines PES sur le Service d'authentification gouvernementale. Plus précisément, les équipes de projet des 9 ministères et organismes⁶ qui utilisent déjà clicSÉQUR – Citoyens et regroupées par expertise :
 - Affaires
 - Communication et Web
 - Gestion du changement
 - Services à la clientèle
 - TI
- Les **MO non-consommateurs de clicSÉQUR – Citoyens** :
 - Ministère de la Famille (MFA);
 - Société de l'assurance automobile du Québec (SAAQ);
 - Les MO qui offrent déjà une solution d'authentification développée à l'interne ou qui élaborent leur dossier d'affaires pour la mise en place de leur PES, et qui souhaitent connaître les modalités du Service d'authentification gouvernementale.
- Les syndicats d'employées et employés.
- Les groupes d'intérêts (ex. Commission d'accès à l'information, Protecteur du citoyen).
- Autres?

Externes

- Les **utilisateurs des PES susceptibles de recourir au Service d'authentification gouvernementale**.
 - Ce public cible sera segmenté par les MO pour que chacun puisse atteindre sa cible dans ses communications respectives. Une diversité de PES répond à une diversité de besoins et de profils d'utilisateurs.
- Les **utilisateurs de clicSÉQUR** qui ont créés plus de 2,5 millions de comptes et ceux qui en créeront un d'ici les déploiements dans les MO. Ceux-ci pourraient être à la fois utilisateurs des deux solutions.

STRATÉGIE

Puisque l'implantation de la nouvelle solution doit se faire graduellement par MO, selon un calendrier de PES, et considérant les spécificités de chaque PES, la stratégie de communication sera ponctuelle et ciblée auprès des utilisateurs concernés.

La diffusion de l'information se fera à deux niveaux, de façon à accompagner les utilisateurs au moment opportun dans leur démarche de transaction avec l'État :

- une information gouvernementale sur le service en général;
- une information sectorielle pour chaque PES.

⁶ Autorité des marchés financiers (AMF) / Conseil des arts et des lettres du Québec (CALQ) / Groupement des assureurs automobiles (GAA) / Ministère de l'Environnement et de la Lutte contre les changements climatiques (MELCC) / Ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) / Office de la protection du consommateur (OPC) / Régie de l'assurance maladie du Québec (RAMQ) / Retraite Québec / Revenu Québec (RQ)

(Évaluer la pertinence de proposer une séquence de communication type par PES basée sur les principes directeurs)

L'information gouvernementale sera prise en compte dans les plans de communication propres à chacun des MO qui planteront une PES utilisant le Service d'authentification gouvernementale. Cela comprendra notamment l'information sur le processus de connexion et l'accompagnement pour les utilisateurs, par Services Québec ou le MO concerné.

Cette approche d'intégration de l'information gouvernementale dans les communications sectorielles favorisera une communication de proximité avec l'utilisateur, au bon moment, en cohérence avec la démarche de celui-ci, qui est d'abord motivée par le besoin d'obtenir un service d'un MO. L'authentification de l'utilisateur étant une étape à franchir pour obtenir le service.

Orientations spécifiques pour la communication interne

Information – Mobilisation – Adhésion

- Communiquer régulièrement l'avancement des travaux et ses différents jalons.
- Transformer le personnel des MO consommateurs en ambassadeurs. Les équipes des MO devront pouvoir s'approprier les nouveautés au moment opportun afin de les communiquer auprès de leurs clientèles.
- Transmettre des communications aux MO non-consommateurs sur les résultats des projets pilotes en vue de susciter leur adhésion au Service d'authentification gouvernementale.

Orientations spécifiques pour la communication externe

Information – Accompagnement - Adhésion

- Diffuser l'information gouvernementale sur la nouvelle solution sur Québec.ca.
- Expliquer les modalités d'utilisation des deux solutions pendant la transition.
- Profiter des canaux de communication des MO consommateurs avec leurs clientèles à des moments clés pour le recours aux PES.
- Prévoir des canaux de communication pour rejoindre l'ensemble des utilisateurs potentiels.
- Profiter des communications aux utilisateurs de la solution actuelle clicSÉCUR pour communiquer sur le Service d'authentification gouvernementale.
- Véhiculer l'image d'une plateforme sécuritaire qui permet d'augmenter la rapidité de traitement lors de démarches administratives avec le gouvernement, en éliminant notamment les délais postaux.
- Mettre en place des procédures de communication pour chaque MO afin de faire face aux risques de panne de la plateforme (gestion de crise pour les situations de dysfonctionnement).

AXE DE COMMUNICATION

Le Service d'authentification gouvernementale est une solution moderne, évolutive, accessible et tout aussi sécuritaire, qui facilite la communication entre l'État et le citoyen.

MESSAGES

Messages généraux

- Le Service d'authentification gouvernementale simplifiera la vie des citoyens et des MO en rendant les démarches administratives beaucoup plus simples et rapides.
- Le Service d'authentification gouvernementale assure une évolution technologique afin de réaliser la transformation numérique gouvernementale.

Pour les publics internes

- Le Service d'authentification gouvernementale contribue à augmenter la cohérence des systèmes et l'accès aux services en ligne gouvernementaux.
- Le Service d'authentification gouvernementale offre des avantages non négligeables pour votre clientèle concernant la sécurité de leurs données et une rapidité de traitement lors de démarches administratives, en éliminant notamment les délais postaux.
- Le gouvernement du Québec prend en considération les spécificités des MO pour proposer une solution optimale pour tous.
- De la formation au personnel est disponible afin que tous puissent communiquer de façon efficiente sur le Service d'authentification gouvernementale.

Pour les publics externes :

- Le Service d'authentification gouvernementale est plus performant quant à son accessibilité technologique, et rehausse le niveau de confidentialité et la sécurité des données pour l'ensemble des PES du gouvernement du Québec (bien que la sécurité de la solution actuelle soit conforme).
- Le gouvernement du Québec met toute son expertise au service de la sécurité numérique des citoyens par l'intermédiaire du nouveau Service d'authentification gouvernementale.
- La solution clicSÉCUR reste opérationnelle et entretenue pour garantir un niveau conforme de sécurité.

MOYENS DE COMMUNICATION

Différents moyens de communication seront utilisés selon les publics cibles, la nature de l'information à transmettre et les étapes du projet. À venir dans la phase subséquente des travaux, en fonction de la stratégie retenue.

BUDGET

À venir en fonction de la stratégie et des moyens retenus.

RECHERCHE ET ÉVALUATION

À venir dans la phase subséquente des travaux.

SÉQUENCE DE COMMUNICATION

À venir dans la phase subséquente des travaux.

RAPPEL - Équipe projet en communication - Programme Service québécois d'identité numérique

From: "Demers, Nathalie" <nathalie.demers@mcn.gouv.qc.ca>
To: "Imbeault, Mathieu" <mathieu.imbeault2@mce.gouv.qc.ca>, Jo-Anne Masse <jo-anne.masse@education.gouv.qc.ca>, "Slupik, Laurent" <laurent.slupik@mtess.gouv.qc.ca>, "Gauthier, Joël" <joel.gauthier@servicesquebec.gouv.qc.ca>, virginie.auger <virginie.auger@retraitequebec.gouv.qc.ca>, Garant-Noël Chantale <chantale.garant-noel@ramq.gouv.qc.ca>, Bilodeau Francine <francine.bilodeau@ramq.gouv.qc.ca>, Catherine.Ouellet <catherine.ouellet@revenuquebec.ca>, "Ferland-Paradis , Émilie" <emilie.ferland-paradis@saaq.gouv.qc.ca>, marie-eve.desgagne3 <marie-eve.desgagne3@saaq.gouv.qc.ca>, Létourneau Vanessa <vanessa.letourneau@retraitequebec.gouv.qc.ca>, "Talbot, Stéphanie" <stephanie.talbot@saaq.gouv.qc.ca>
Cc: "Boutin, Catherine" <catherine.boutin@mce.gouv.qc.ca>, "Demers, Nathalie" <nathalie.demers@mcn.gouv.qc.ca>, "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>
Date: Wed, 24 Aug 2022 19:44:13 +0000
Attachments: Compte rendu du processus de dénomination SQIN 1.pdf (418.55 kB);
PLCOM_SAG_2022_V19 août.pdf (289.16 kB)

Cybersécurité
et Numérique



Bonjour à toute l'équipe,
Juste un mot pour vous adresser un rappel.
Nous attendons vos commentaires, comprenant ceux de votre directeur.trice des communications, d'ici ce vendredi, s'il y a lieu.
Si vous n'en avez pas, nous apprécierions obtenir un petit courriel à cet effet.
Pour plus de précisions, voir SVP le message courriel ci-dessous ainsi que les pièces jointes.
Très belle fin de journée.
Nathalie

Nathalie Demers
Conseillère en communication
Ministère de la Cybersécurité et du Numérique

800, Place d'Youville, 4e étage, suite 4.01, Québec (Québec) G1R 3P4
Tél. : 418 528-0880, poste 4835 | Téléc. : 418 644-0462
Nathalie.Demers@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

De : Perron, Sophie

Envoyé : 22 août 2022 16:15

À : Imbeault, Mathieu ; Jo-Anne Masse ; Slupik, Laurent ; Gauthier, Joël ; virginie.auger ; Garant-Noël Chantale ; Bilodeau Francine ; Catherine.Ouellet ; Ferland-Paradis , Émilie ; marie-eve.desgagne3 ; Létourneau Vanessa ; Talbot, Stéphanie

Cc : Boutin, Catherine ; Demers, Nathalie ; Morin, Karine

Objet : Équipe projet en communication - Programme Service québécois d'identité numérique

***ATTENTION** Ce courriel ne provient pas de notre organisation. Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe sans préalablement vous assurer de la légitimité de ce courriel. Votre adresse courriel gouvernementale (@ramq.gouv.qc.ca) ne doit servir qu'à des activités professionnelles.

Cybersécurité
et Numérique

Québec 

Bonjour,

Tel que mentionné lors de notre rencontre, vous trouverez en pièce jointe le compte-rendu du processus de dénomination.

J'en profite pour vous rappeler que vos commentaires sur la version de travail (partie 1) du plan de communication sont attendus d'ici **ce vendredi, 26 août**.

J'ajoute également l'hyperlien vous permettant de travailler en mode collaboratif dans notre équipe

Teams :  [PLCOM SAG 2022 V19 août.docx](#)

Finalement, je vous remercie à l'avance de conserver Nathalie (nathalie.demers@mcn.gouv.qc.ca) en copie de vos retours courriel.

Merci et bonne fin de journée!

Sophie Perron

Coordonnatrice p. i. || Services-conseils en communication

Ministère de la Cybersécurité et du Numérique

800, Place d'Youville, 4e étage, suite 4.01, Québec (Québec) G1R 3P4

Tél. : 418 528-0880, poste 4827 | Téléc. : 418 644-0462

Sophie.Perron@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Plan de communication

**Service d'authentification gouvernementale :
Projet Accès bonifié aux prestations électroniques de
services (PES) – Citoyens**

Avis : Ce document fait l'objet d'une diffusion restreinte. L'information qu'il contient est sujette à des changements en fonction du déploiement du service, des changements contextuels, des priorités d'action et des résultats des actions de communication. La Direction des communications du MCN est responsable et gardienne de la version finale du plan.

Équipe projet - Programme Service québécois d'identité numérique
Version du 19 août 2022

CONTEXTE

La [Stratégie de transformation numérique gouvernementale 2019-2023](#) prévoit offrir des services publics rapides et intuitifs, propulsés par le numérique, où la confidentialité et la sécurité des données seront rehaussées.

Pour y arriver, une nouvelle solution d'authentification gouvernementale, s'inscrivant dans le projet Accès bonifié aux prestations électroniques de services (PES) – Citoyens¹, du [Programme Service québécois d'identité numérique](#), sera déployée graduellement à compter d'octobre 2022². Nommée Service d'authentification gouvernementale à l'issu de travaux et de tests utilisateurs³, elle permettra un accès aux services en ligne du gouvernement du Québec à partir de diverses plateformes technologiques, dans un environnement performant et sécuritaire.

Le projet Service d'authentification gouvernementale est réalisé par le ministère de la Cybersécurité et du Numérique, en collaboration avec des ministères et organismes (MO) parties prenantes de certaines étapes du développement et de sa mise en œuvre :

- le ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS), par l'entremise de Services Québec, pour le soutien téléphonique aux citoyens;
- la Régie de l'assurance maladie du Québec (RAMQ), fournisseur de la nouvelle source de confiance (validation de l'identité);
- Revenu Québec, la Société de l'assurance automobile du Québec (SAAQ, à confirmer) et la RAMQ, fournisseurs de secret (information contenue dans un document officiel, ex. avis de cotisation, pour la validation de l'identité).

Le Service d'authentification gouvernementale remplacera progressivement la solution actuelle [clicSÉCUR](#)⁴, implanté en 2005, pour pouvoir répondre aux orientations gouvernementales en matière de sécurité et d'expérience utilisateur. Mentionnons que l'adhésion des ministères et organismes (MO) au Service d'authentification gouvernementale s'effectue présentement sur une base volontaire.

Le déploiement du Service d'authentification gouvernementale s'effectuera par PES, identifiées par les MO, selon un calendrier déterminé (*annexe 1 à venir*). Lorsqu'une PES aura migré vers le service d'authentification, elle ne sera plus accessible par l'intermédiaire de son ancienne solution. Ainsi, dans l'inventaire global des différentes PES, il y aura une période de chevauchement entre l'ancienne et la nouvelle solution.

Le premier déploiement aura lieu dans le contexte de l'implantation d'une première PES au ministère de la Famille (MFA), en octobre, auprès d'éducatrices et d'éducateurs en petite enfance. Puis, dès janvier 2023, dans le cadre de sa transformation numérique, la SAAQ déploiera 5 portails de services en ligne sous l'appellation *saaqclic*, dont 4 utiliseront le Service d'authentification gouvernementale – Citoyens.

¹ Un projet Entreprises est également prévu ultérieurement, qui ne fait pas partie de la portée du présent plan de communication.

² Date exacte à déterminer.

³ Dénomination retenue, selon les [orientations gouvernementales](#) et ayant fait l'objet de tests auprès d'utilisateurs.

⁴ clicSÉCUR : service québécois d'authentification gouvernementale actuel permettant aux citoyens d'accéder à certaines prestations électroniques de services gouvernementales.

Utilisation des services en ligne

(Voir si d'autres données pertinentes sont disponibles)

Selon les données de l'Académie de la transformation numérique⁵, en 2021, deux adultes sur trois (67 %) évaluent qu'il est « très ou assez facile » d'utiliser les services offerts en ligne par le gouvernement. Ce point de vue est principalement partagé par les internautes âgés de 25 à 34 ans (77 %), ceux âgés de 35 à 44 ans (78 %) de même que par les diplômés universitaires (74 %). La création d'un système d'authentification unique qui donnerait accès à tous les services gouvernementaux arrive au troisième rang (71 %) des six initiatives numériques évaluées que le gouvernement devrait mettre en place.

DÉFIS DE COMMUNICATION INTERNE

Intégration d'une nouvelle offre de service

Plusieurs facteurs pourraient freiner l'adhésion des gestionnaires et du personnel des MO à l'implantation de la nouvelle solution. Notamment, la méconnaissance de la nouvelle solution, sa pertinence par rapport aux solutions existantes, la perception d'une charge de travail additionnelle (nouveaux apprentissages, cohabitation avec la solution actuelle ou une solution maison). L'adhésion des MO sur une base volontaire, du moins pour le moment, n'est pas un facteur à négliger.

Incidence sur la communication : mobiliser les autorités et gestionnaires, transmettre un message fort sur l'orientation de migrer vers une solution unique et les avantages; rassurer sur l'accompagnement qui sera offert

Résultats des projets pilotes

Des écueils pourraient survenir dans l'implantation des PES et de la nouvelle solution d'authentification, qui pourraient constituer un frein à l'adhésion des autres MO.

Incidence sur la communication : informer en continu, miser sur les bons coups pour générer un effet de levier

ENJEUX DE COMMUNICATION EXTERNE

Spécificités des offres de services

Le déploiement de la nouvelle solution s'effectuera en fonction d'un calendrier déterminé par les MO, en fonction de leurs objectifs organisationnels et des spécificités de leur offre de services. Ces spécificités se reflètent également dans le fait que ce sont divers événements de vie qui amènent le citoyen à s'adresser à un MO pour obtenir un service.

Incidences sur la communication : privilégier des initiatives de communication sectorielles, en phase avec le déploiement de l'offre de services des MO, de leurs spécificités et des besoins des utilisateurs

Coexistence des solutions actuelles et de la nouvelle

La coexistence de clicSÉCUR, de solutions maison et du Service d'authentification gouvernementale, en raison du déploiement graduel d'un MO à un autre, pour l'ensemble de ses PES ou certaines de celles-ci, pourrait créer de la confusion chez les utilisateurs, étant donné les façons différentes de s'authentifier pendant la période de transition.

L'inscription des citoyens au Service d'authentification gouvernementale ne pourra s'effectuer qu'au moment d'accéder à une PES (c'est aussi le cas pour l'actuel

⁵ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Les services gouvernementaux en ligne et l'identité numérique*, [En ligne], 27 avril 2022.

clicSÉCUR). Ainsi, l'inscription à la nouvelle solution sera possible seulement une fois que le Service d'authentification gouvernementale aura été déployé dans le MO donné.

La coexistence des solutions facilitera aussi la comparaison entre les deux services, qui pourrait susciter des questionnements sur la pertinence d'implanter une nouvelle solution.

Incidences sur la communication : communiquer la bonne information au bon moment, démontrer le bénéfice citoyen

Effritement de la confiance des utilisateurs envers clicSÉCUR

La désuétude de la technologie de clicSÉCUR pourrait effriter la confiance à l'égard de la solution. Elle pourrait aussi générer des questions quant à la durée de vie de la nouvelle solution (rapport investissement/durée de vie). Par ailleurs, le fait de parler de rehaussement des exigences de vérification d'identité pourrait avoir l'effet pervers de discréditer l'ancienne solution alors que celle-ci demeurera pendant un certain temps.

Incidences sur la communication : trouver le juste équilibre dans la manière de faire valoir la nouvelle solution sans le faire au détriment de l'autre, rassurer à l'effet que clicSÉCUR reste fonctionnel et sécuritaire, avec un entretien continu.

Résistances résultant de la première connexion

(schéma du parcours utilisateurs à venir en annexe)

L'obligation de créer un nouveau compte pour certains utilisateurs pourrait être un irritant, notamment pour ceux dont l'inscription à clicSÉCUR est récente. Les comptes des deux solutions ne seront pas jumelés.

Par ailleurs, le rehaussement des exigences de vérification d'identité lors de la première connexion des utilisateurs pourrait représenter un frein à leur adhésion au Service d'authentification gouvernementale. Mentionnons que certaines clientèles pourraient ne pas avoir accès à tous les documents demandés.

En effet, en plus du numéro d'assurance sociale qui pourra être fourni par l'utilisateur, de l'information détenue par la Régie de l'assurance maladie du Québec (RAMQ), Revenu Québec et la Société de l'assurance automobile du Québec (SAAQ, à confirmer) sera demandée afin de procéder à la vérification d'identité. S'il n'a pas l'information requise, l'utilisateur pourra demander un « secret d'identification » auprès de ces organismes. Il recevra alors l'information par la poste, ce qui pourrait prendre jusqu'à 10 jours ouvrables. Cela pourrait sembler paradoxal aux yeux de clientèles habituées à l'instantanéité qui caractérise les transactions Web et surtout, retarder l'inscription et l'obtention de la PES.

Incidence sur la communication : la nature de l'information demandée devra être connue au bon moment et si nécessaire, être en mesure de répondre au citoyen

Crainte quant à la confidentialité des données et la sécurité de l'information

La confidentialité des données et la sécurité de l'information sont des sujets sensibles pour tous, tant pour les organisations que la population. La nouvelle solution fera sûrement l'objet d'une couverture médiatique soutenue et d'une attention particulière de la part de certains groupes d'intérêt (ex. Commission d'accès à l'information). D'ailleurs, la couverture médiatique en lien avec la confidentialité des données et la sécurité de l'information, ou encore avec le « bordel informatique », pourrait miner la crédibilité du projet et freiner l'adhésion des utilisateurs.

Incidences sur la communication : rassurer sur les mécanismes de sécurité en place

Disfonctionnements de la nouvelle solution

L'implantation du Service d'authentification gouvernementale pourrait s'accompagner de disfonctionnements et de retards, ce qui pourrait entraîner des répercussions importantes pour les citoyens et des craintes pour la migration des autres PES. Cette situation pourrait

provoquer du mécontentement, engendrer des plaintes et même une surcharge de travail pour les services à la clientèle. La situation serait doublement problématique : accès impossible à la solution en ligne et temps d'attente plus long pour obtenir de l'aide. Par ailleurs, la solution actuelle clicSÉCUR n'est pas à l'abri d'un bris de service.

Incidences sur la communication : maintenir un lien constant entre les équipes de déploiement et les directions de communication, être prêts à communiquer en mode gestion de crise

RÉSULTATS ATTENDUS

À compléter, ex : objectifs d'affaires, cibles organisationnelles, résultats attendus déterminés selon les PES, nombre de plaintes reçues

PRINCIPES DIRECTEURS

En fonction de ce qui précède, les initiatives de communication entourant ce projet, tant pour la communication externe que publique, devront s'appuyer sur les principes directeurs suivants :

- la transparence;
- la cohérence des messages véhiculés par les MO, articulés autour d'un positionnement gouvernemental;
- une réponse efficace aux questions des citoyens.

OBJECTIFS DE COMMUNICATION

Objectifs généraux

- Faire connaître la nouvelle solution et démontrer ses avantages.
- Établir un niveau élevé de confiance envers la nouvelle solution.
- Faire adhérer les citoyens et les MO à la nouvelle solution.
- Démontrer que le gouvernement du Québec est engagé à offrir des services publics intuitifs et faciles d'utilisation pour la population, en améliorant l'efficacité de l'État.

Objectif spécifique à la communication interne

- Mobiliser et faire adhérer le personnel des MO au projet.

Objectifs spécifiques à la communication externe

- Démystifier la nouvelle solution de l'ancienne.
- Rassurer les utilisateurs sur le fait que la nouvelle solution assurera la protection de leurs données personnelles, entre autres par le rehaussement des exigences de vérification d'identité.
- Maintenir la confiance des utilisateurs de l'actuelle solution clicSÉCUR pendant la période de transition.

Objectifs de communication mesurables

À déterminer, communication gouvernementale et plans de communication sectoriels.

Par exemple, pour la communication gouvernementale :

- Pourcentage d'utilisateurs de la nouvelle solution qui estimeront avoir été bien outillés pour réaliser leur inscription.

PUBLICS CIBLES

Internes

- Les **MO consommateurs** qui souhaitent transférer certaines PES sur le Service d'authentification gouvernementale. Plus précisément, les équipes de projet des 9 ministères et organismes⁶ qui utilisent déjà clicSÉQUR – Citoyens et regroupées par expertise :
 - Affaires
 - Communication et Web
 - Gestion du changement
 - Services à la clientèle
 - TI
- Les **MO non-consommateurs de clicSÉQUR – Citoyens** :
 - Ministère de la Famille (MFA);
 - Société de l'assurance automobile du Québec (SAAQ);
 - Les MO qui offrent déjà une solution d'authentification développée à l'interne ou qui élaborent leur dossier d'affaires pour la mise en place de leur PES, et qui souhaitent connaître les modalités du Service d'authentification gouvernementale.
- Les syndicats d'employées et employés.
- Les groupes d'intérêts (ex. Commission d'accès à l'information, Protecteur du citoyen).
- Autres?

Externes

- Les **utilisateurs des PES susceptibles de recourir au Service d'authentification gouvernementale**.
 - Ce public cible sera segmenté par les MO pour que chacun puisse atteindre sa cible dans ses communications respectives. Une diversité de PES répond à une diversité de besoins et de profils d'utilisateurs.
- Les **utilisateurs de clicSÉQUR** qui ont créés plus de 2,5 millions de comptes et ceux qui en créeront un d'ici les déploiements dans les MO. Ceux-ci pourraient être à la fois utilisateurs des deux solutions.

STRATÉGIE

Puisque l'implantation de la nouvelle solution doit se faire graduellement par MO, selon un calendrier de PES, et considérant les spécificités de chaque PES, la stratégie de communication sera ponctuelle et ciblée auprès des utilisateurs concernés.

La diffusion de l'information se fera à deux niveaux, de façon à accompagner les utilisateurs au moment opportun dans leur démarche de transaction avec l'État :

- une information gouvernementale sur le service en général;
- une information sectorielle pour chaque PES.

⁶ Autorité des marchés financiers (AMF) / Conseil des arts et des lettres du Québec (CALQ) / Groupement des assureurs automobiles (GAA) / Ministère de l'Environnement et de la Lutte contre les changements climatiques (MELCC) / Ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) / Office de la protection du consommateur (OPC) / Régie de l'assurance maladie du Québec (RAMQ) / Retraite Québec / Revenu Québec (RQ)

(Évaluer la pertinence de proposer une séquence de communication type par PES basée sur les principes directeurs)

L'information gouvernementale sera prise en compte dans les plans de communication propres à chacun des MO qui planteront une PES utilisant le Service d'authentification gouvernementale. Cela comprendra notamment l'information sur le processus de connexion et l'accompagnement pour les utilisateurs, par Services Québec ou le MO concerné.

Cette approche d'intégration de l'information gouvernementale dans les communications sectorielles favorisera une communication de proximité avec l'utilisateur, au bon moment, en cohérence avec la démarche de celui-ci, qui est d'abord motivée par le besoin d'obtenir un service d'un MO. L'authentification de l'utilisateur étant une étape à franchir pour obtenir le service.

Orientations spécifiques pour la communication interne

Information – Mobilisation – Adhésion

- Communiquer régulièrement l'avancement des travaux et ses différents jalons.
- Transformer le personnel des MO consommateurs en ambassadeurs. Les équipes des MO devront pouvoir s'approprier les nouveautés au moment opportun afin de les communiquer auprès de leurs clientèles.
- Transmettre des communications aux MO non-consommateurs sur les résultats des projets pilotes en vue de susciter leur adhésion au Service d'authentification gouvernementale.

Orientations spécifiques pour la communication externe

Information – Accompagnement - Adhésion

- Diffuser l'information gouvernementale sur la nouvelle solution sur Québec.ca.
- Expliquer les modalités d'utilisation des deux solutions pendant la transition.
- Profiter des canaux de communication des MO consommateurs avec leurs clientèles à des moments clés pour le recours aux PES.
- Prévoir des canaux de communication pour rejoindre l'ensemble des utilisateurs potentiels.
- Profiter des communications aux utilisateurs de la solution actuelle clicSÉCUR pour communiquer sur le Service d'authentification gouvernementale.
- Véhiculer l'image d'une plateforme sécuritaire qui permet d'augmenter la rapidité de traitement lors de démarches administratives avec le gouvernement, en éliminant notamment les délais postaux.
- Mettre en place des procédures de communication pour chaque MO afin de faire face aux risques de panne de la plateforme (gestion de crise pour les situations de dysfonctionnement).

AXE DE COMMUNICATION

Le Service d'authentification gouvernementale est une solution moderne, évolutive, accessible et tout aussi sécuritaire, qui facilite la communication entre l'État et le citoyen.

MESSAGES

Messages généraux

- Le Service d'authentification gouvernementale simplifiera la vie des citoyens et des MO en rendant les démarches administratives beaucoup plus simples et rapides.
- Le Service d'authentification gouvernementale assure une évolution technologique afin de réaliser la transformation numérique gouvernementale.

Pour les publics internes

- Le Service d'authentification gouvernementale contribue à augmenter la cohérence des systèmes et l'accès aux services en ligne gouvernementaux.
- Le Service d'authentification gouvernementale offre des avantages non négligeables pour votre clientèle concernant la sécurité de leurs données et une rapidité de traitement lors de démarches administratives, en éliminant notamment les délais postaux.
- Le gouvernement du Québec prend en considération les spécificités des MO pour proposer une solution optimale pour tous.
- De la formation au personnel est disponible afin que tous puissent communiquer de façon efficiente sur le Service d'authentification gouvernementale.

Pour les publics externes :

- Le Service d'authentification gouvernementale est plus performant quant à son accessibilité technologique, et rehausse le niveau de confidentialité et la sécurité des données pour l'ensemble des PES du gouvernement du Québec (bien que la sécurité de la solution actuelle soit conforme).
- Le gouvernement du Québec met toute son expertise au service de la sécurité numérique des citoyens par l'intermédiaire du nouveau Service d'authentification gouvernementale.
- La solution clicSÉCUR reste opérationnelle et entretenue pour garantir un niveau conforme de sécurité.

MOYENS DE COMMUNICATION

Différents moyens de communication seront utilisés selon les publics cibles, la nature de l'information à transmettre et les étapes du projet. À venir dans la phase subséquente des travaux, en fonction de la stratégie retenue.

BUDGET

À venir en fonction de la stratégie et des moyens retenus.

RECHERCHE ET ÉVALUATION

À venir dans la phase subséquente des travaux.

SÉQUENCE DE COMMUNICATION

À venir dans la phase subséquente des travaux.

Compte rendu du processus de dénomination de SQIN 1

Rapport abrégé	0
Mise en contexte	1
Contexte actuel	1
Dénomination actuelle	1
Liens vers les prestations de services en ligne (PES)	1
Description du service	1
Évaluation des commentaires de pages dans Québec.ca concernant clicSÉCUR	1
Utilisation projetée de la dénomination	2
Exemples d'utilisation de la dénomination	2
Accéder à une PES souhaitée	2
Gestion de compte	3
Points de contacts	4
Processus de dénomination	6
Comité expert	6
Sondage de compréhension de terme (littératie)	6
Tests utilisateurs	6
Recommandations	7
Dénomination	7
Déclinaisons d'utilisation	7

Mise en contexte

Le programme SQIN est divisé en trois projets majeurs, mais la dénomination ne concerne que le projet 1, ayant pour objectif de mettre en place une solution gouvernementale qui modernisera les services actuels (clicSÉQR), autant pour les citoyens que pour les entreprises.

Contexte actuel

Dénomination actuelle

ClicSÉQR est le service québécois d'authentification gouvernementale en place actuellement. Un travail de notoriété a été fait sur la dénomination clicSÉQR afin de le faire connaître aux utilisateurs. Cette notoriété crée de la confusion dans l'esprit des utilisateurs, car clicSÉQR n'est pas un service de destination. De plus, les utilisateurs ont de la difficulté à écrire le nom du service et donc à le retrouver.

Bien que le service d'authentification ne soit qu'un « passage » vers un service numérique donné (une PES), il convient de le nommer pour des raisons pratiques de soutien aux utilisateurs et pour faciliter la complétion de tâche.

Liens vers les prestations de services en ligne (PES)

Un recensement sommaire des pages de PES qui mène vers clicSÉQR a été fait. Dans la plupart des cas, conformément à l'orientation gouvernementale, les liens font référence à la tâche et non au nom du service.

Constat : la dénomination du service a peu d'influence sur le parcours (flow) de la tâche principale de l'utilisateur.

Description du service

Dans plusieurs des cas, une explication supplémentaire du service est nécessaire pour aider l'utilisateur à la compréhension du service.

Le terme « Authentification » est actuellement utilisé dans tous les cas. Cet ajout à la dénomination existante démontre que le nom actuel « clicSÉQR » n'est pas assez explicatif et descriptif pour vivre seule.

Constat : Le nom du service devrait être autosuffisant.

Évaluation des commentaires de pages dans Québec.ca concernant clicSÉQR

- Les utilisateurs ont de la difficulté à écrire le terme “clicSÉQR” et le formulent de différentes façons.
- Les termes employés dans les communications sur clicSÉQR («Compte», «clicSÉQR», etc) sont fréquemment utilisés dans les commentaires des utilisateurs.

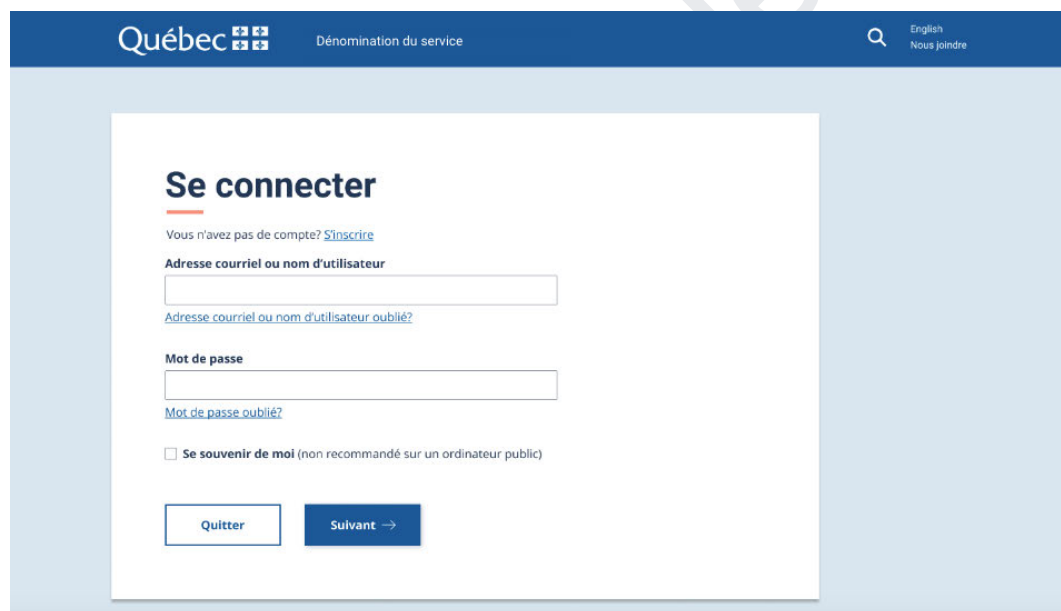
Constat : Les utilisateurs reprennent dans leur recherches les mots qui sont induits dans les communications sur un sujet. C’est à ce moment que des mots simples seraient utiles pour diriger les utilisateurs selon la tâche précise qu’ils doivent effectuer.

Utilisation projetée de la dénomination

Exemples d’utilisation de la dénomination

À l’aide de l’ITQ, nous avons compilé les points de contact principaux avec SQIN.

Accéder à une PES souhaitée

A screenshot of a projected login interface for the Québec government website. The header is dark blue with the Québec logo, the text 'Dénomination du service', a search icon, and a language selector for 'English' with the option 'Nous joindre'. The main content area is white and contains the heading 'Se connecter'. Below this, there is a link 'Vous n'avez pas de compte? S'inscrire'. The first input field is labeled 'Adresse courriel ou nom d'utilisateur' and has a link 'Adresse courriel ou nom d'utilisateur oublié?'. The second input field is labeled 'Mot de passe' and has a link 'Mot de passe oublié?'. There is a checkbox labeled 'Se souvenir de moi (non recommandé sur un ordinateur public)'. At the bottom are two buttons: 'Quitter' and 'Suivant ->'.

Québec Dénomination du service English Nous joindre

Se connecter

[Vous n'avez pas de compte? S'inscrire](#)

Adresse courriel ou nom d'utilisateur

[Adresse courriel ou nom d'utilisateur oublié?](#)

Mot de passe

[Mot de passe oublié?](#)

☐ Se souvenir de moi (non recommandé sur un ordinateur public)

Quitter Suivant →

Maquette projetée d'une interface de connexion

Le passage par SQIN 1 doit être le plus transparent possible pour l'utilisateur.

Les besoins de l'utilisateur à cette étape sont :

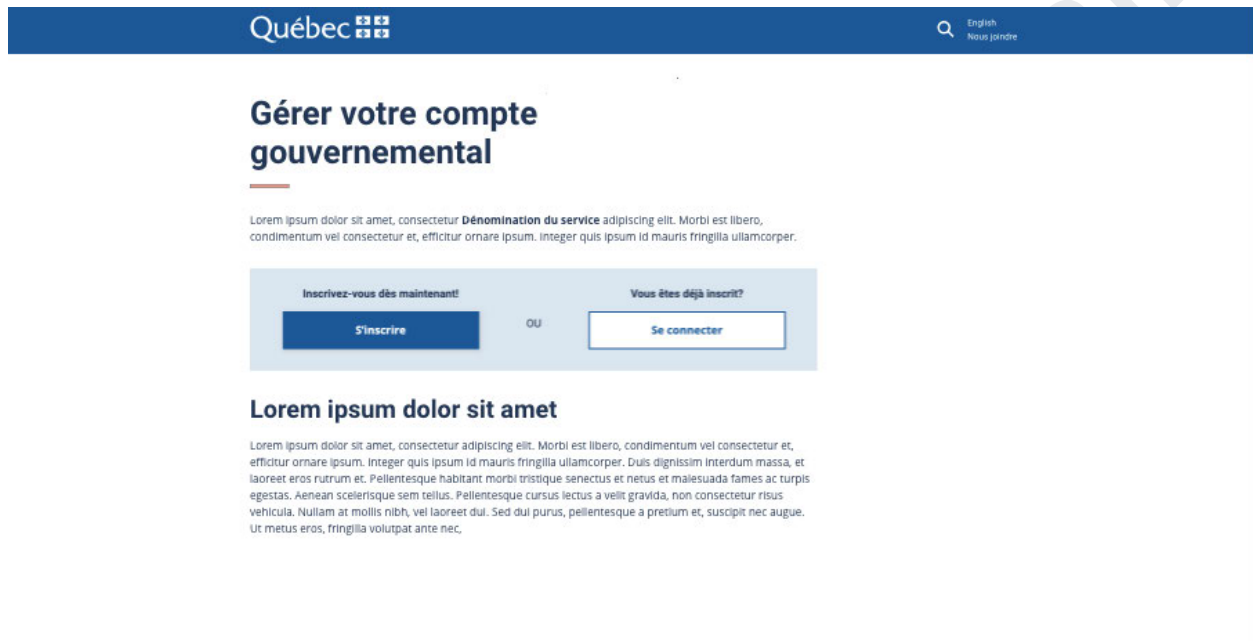
- D'accéder facilement à la PES désirée
- De s'authentifier à un compte unique
- De savoir qu'il se trouve sur un site gouvernemental

- De savoir que la connexion est sécuritaire
- Que le parcours soit fluide du site d'origine à la PES, en passant par SQIN
- De savoir qu'il doit utiliser ses données d'identifications gouvernementales

Ce dont il n'a pas besoin :

- De différencier l'authentification du reste de son parcours
- De connaître le nom de la solution d'authentification

Gestion de compte



Maquette projetée d'une interface de gestion de compte

L'utilisateur qui souhaite gérer son compte (changer l'adresse courriel, son mot de passe, ses phrases secrètes, etc)

Les besoins de l'utilisateur à cette étape sont :

- Avoir accès facilement à son compte à partir d'une PES ou d'un fureteur Web
- De savoir qu'il se trouve sur un site gouvernemental
- De savoir que le site est sécuritaire
- De savoir qu'il s'agit de ses données d'identification gouvernementale

Points de contact

REVENU QUÉBEC

AUTHENTIFICATION

COMMENT FAIRE

Pour accéder au service, vous devez préalablement vous authentifier au moyen d'un des deux services d'authentification ci-dessous.

Service d'authentification d'un partenaire de connexion CONNEXION

Ouvrez une session en inscrivant les informations d'authentification demandées par votre institution financière.

Lors de votre première utilisation du service, vous devez fournir votre numéro d'assurance sociale, votre date de naissance et l'un des renseignements suivants :

- votre **code d'accès temporaire**; ou
- le **numéro d'avis de cotisation** de l'un des deux plus récents avis de cotisation qui vous ont été délivrés au cours des cinq dernières années d'imposition.

Vos informations financières ou bancaires ne nous seront pas divulguées. De plus, le partenaire de connexion ne saura pas quel service du gouvernement vous utilisez.

Il est fortement recommandé de **ne divulguer à personne** les renseignements que vous utilisez pour accéder à nos services au moyen d'un partenaire de connexion.

Dénomination du service CONNEXION

Ouvrez votre compte en inscrivant votre code d'utilisateur et votre mot de passe habituels.

Créez un compte si vous n'avez jamais utilisé le service.

[Annuler](#)

NOUS JOINDRE

À QUEL SUJET?

[Accessibilité](#) | [Configuration requise](#) | [Sécurité](#) | [Politique de confidentialité](#)

© Revenu Québec, 2018

Image de la page de connexion Revenu Québec. Le lien vers le service d'authentification est dans le bandeau bleu dans le bas.

Québec

Retraite Québec

À propos de nous
Nous joindre
English

Accueil > Nos services > Services en ligne

Mon dossier

Adapté à ma réalité

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi est libero, condimentum vel consectetur et, efficitur ornare ipsum. Integer quis ipsum id mauris fringilla ullamcorper.

Services en ligne

- Planification financière de la retraite
- Régime de rentes du Québec
- Régimes de retraite du secteur public (REGOP, RRPE, etc.)
- Allocation famille
- Régimes complémentaires de retraite
- CRI et FRV
- Services en ligne et sécurité
- Foire aux questions

Inscrivez-vous dès maintenant!

S'inscrire

OU

Vous êtes déjà inscrit?

Se connecter

Lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi est libero, condimentum vel consectetur et, efficitur ornare ipsum. Integer quis ipsum id mauris fringilla ullamcorper. Duis dignissim interdum massa, et laoreet eros rutrum et. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean scelerisque sem tellus. Pellentesque cursus lectus a velit gravida, non consectetur risus vehicula. Nullam at mollis nibh, vel laoreet dui. Sed dui purus, pellentesque a pretium et, suscipit nec augue. Ut metus eros, fringilla volutpat ante nec.

Exemple de page de connexion Retraite Québec. La dénomination n'est pas mentionnée dans la page.

Processus de dénomination

En septembre 2021, le SCG obtient le mandat de dénomination de la solution. Le SCG est donc responsable de la démarche de définir le nom de la solution et doit fournir des propositions officielles respectant les orientations.

Le processus de dénomination inclut notamment un comité expert et des tests auprès des utilisateurs. Voici les constats des principales étapes du processus.

Comité expert

Constat : «Authentification» est le terme le plus représentatif. Il est toutefois jugé comme étant moins accessible aux citoyens. Il est donc important de tester ce terme auprès des citoyens (voir l'étape suivante).

Sondage de compréhension de terme (littératie)

Constat : «Authentification» est le terme le plus fréquemment choisi comme étant représentatif du service SQIN 1. Il est aussi le terme le plus employé dans les définitions de termes dans les questions ouvertes.

Tests utilisateurs

Constat : «Authentification» est jugé par l'ensemble des répondants comme étant le terme le plus crédible et le terme qui correspond le mieux au service.

Ne pas nommer le service à aussi été évoqué par certains répondants.

Recommandations

Dénomination

Le SCG recommande la dénomination Service d'authentification gouvernementale.

Ce nom a été choisi pour les raisons suivantes :

- La dénomination est descriptive
- La dénomination contient des mots clés explicites, liés à la tâche de l'utilisateur
- La dénomination est succincte et claire
- La dénomination évite les acronymes ou jeux de mots
- La dénomination n'est pas créée dans une logique de marque
- Le terme «Authentification» est le terme le plus représentatif du service
- Le terme «Authentification» est un terme compris par les citoyens
- Le terme «Gouvernementale» représente l'aspect transversal du service

Déclinaisons d'utilisation

Les communications entourant le service ont peu ou pas d'impact sur le tâche principale de l'utilisateur. Toutefois, pour les tâches secondaires, le travail de vulgarisation sera très important dans les communications afférentes afin de simplifier l'accès aux tâches des utilisateurs.

À noter :

- Utiliser des mots clairs et simples, reliés à la tâche de l'utilisateur, selon son contexte, dans les communications verbales et écrites

Voir la fiche [Dénomination et références aux services](#) dans le Système de design gouvernemental pour plus d'informations.

Équipe projet en communication - Programme Service québécois d'identité numérique

From: "Perron, Sophie" <sophie.perron@mcn.gouv.qc.ca>
To: "Imbeault, Mathieu" <mathieu.imbeault2@mce.gouv.qc.ca>, Jo-Anne Masse <jo-anne.masse@education.gouv.qc.ca>, "Slupik, Laurent" <laurent.slupik@mtess.gouv.qc.ca>, "Gauthier, Joël" <joel.gauthier@servicesquebec.gouv.qc.ca>, "Charest, Émilie" <emilie.charest@servicesquebec.gouv.qc.ca>, virginie.auger <virginie.auger@retraitequebec.gouv.qc.ca>, Garant-Noël Chantale <chantale.garant-noel@ramq.gouv.qc.ca>, Catherine.Ouellet <catherine.ouellet@revenuquebec.ca>, "Ferland-Paradis, Émilie" <emilie.ferland-paradis@saaq.gouv.qc.ca>, "Courchesne, Marie-Anne" <marie-anne.courchesne@mce.gouv.qc.ca>, Doré Dominique <dominique.dore@revenuquebec.ca>
Cc: Lavoie Alexandre <alexandre.lavoie@revenuquebec.ca>, "Demers, Nathalie" <nathalie.demers@mcn.gouv.qc.ca>, Dion Alexandre <alexandre.dion.ext@retraitequebec.gouv.qc.ca>, "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>, "Boutin, Catherine" <catherine.boutin@mce.gouv.qc.ca>
Date: Tue, 06 Sep 2022 16:50:20 +0000
Attachments: PLCOM_SAG_2022_20220906.docx (1.38 MB); Annexe 2_Moyens-de-communication_20220906.doc (100.35 kB); Annexe 3_Séquence de communication_20220906.docx (38.51 kB)



Bonjour,

En prévision de la rencontre de ce jeudi, vous trouverez en attachement :

- Le plan de communication ajusté en considération des commentaires formulés;
- Le tableau des moyens;
- La séquence de communication.

Merci et à bientôt!

Sophie Perron

Coordonnatrice p. i. || Services-conseils en communication

Ministère de la Cybersécurité et du Numérique

800, Place d'Youville, 4e étage, suite 4.01, Québec (Québec) G1R 3P4

Tél. : 418 528-0880, poste 4827 | Téléc. : 418 644-0462

Sophie.Perron@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Annexe 3 - Séquence de communication

	Déploiement MFA			Déploiement SAAQ	
	Septembre 2022	Octobre	Novembre	Décembre	Janvier 2023
Site Québec.ca	- Actualité pour annoncer le début du déploiement - Mise en ligne d'une page d'information sur le Service d'authentification gouvernemental - Diffusion d'un tutoriel de connexion pour les citoyens		Actualité pour faire le bilan du 1 ^{er} déploiement au MFA.	Actualité pour annoncer le prochain déploiement	Janvier 2023 Actualité pour faire le bilan 2 ^e déploiement à la SAAQ. • <i>Calendrier de déploiement pour la poursuite du projet</i>
Site du MO		MFA : Diffuser le tutoriel et les moyens pour communiquer avec le service à la clientèle avec visuel.	Actualité pour faire le bilan du 1 ^{er} déploiement au MFA.		SAAQ : Diffuser le tutoriel et les moyens pour communiquer avec le service à la clientèle avec visuel. Actualité pour faire le bilan du 2 ^e déploiement à la SAAQ.
Médias sociaux	Publication pour annoncer la page d'information sur Québec.ca et le tutoriel de connexion sur la page LinkedIn du MCN et demande de partage sur les comptes des MO visés <i>Stratégie de publication de contenu à déterminer en collaboration avec les DCOM visées et la DCNG</i>	Veille et gestion des commentaires sur le sujet	Publication pour faire le bilan du 1 ^{er} déploiement au MFA.	Publication pour annoncer le prochain déploiement sur la page LinkedIn du MCN et demande de partage sur les comptes des MO visés <i>Stratégie de publication de contenu à déterminer en</i>	Publication pour faire le bilan du 2 ^e déploiement à la SAAQ. • <i>Calendrier de déploiement pour la poursuite du projet</i>

					<i>collaboration avec les DCOM visées et la DCNG</i>			
Plateforme collaborative SharePoint du MCN à l'usage exclusif des MO	Annoncer la disponibilité des outils : - Foire aux questions. - Aide-mémoire. - Documents de formation. - Série de webinaires. - Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels). - Plan de gestion de crise pour chaque MO en cas de disfonctionnement de la plateforme. - Tutoriel de connexion adapté au personnel des services à la clientèle. - Modèle de papillon avec texte et image pour insertion dans des communications en format papier.			- Actualité pour faire le bilan du 1^{er} déploiement - Mise en valeur des bons coups - Ajustements en vue du prochain déploiement (solution, approche, matériel pour le service à la clientèle)	Diffusion des documents ajustés, au besoin.		- Actualité pour faire le bilan du 2^e déploiement - Mise en valeur des bons coups - Ajustements en vue du prochain déploiement (solution, approche, matériel pour le service à la clientèle) <i>Calendrier de déploiement pour la poursuite du projet</i>	
Relations publiques	- Lignes de presse - Document de type « questions-réponses »	- Brefing technique - Point de presse	- Communiqué de presse (bilan du déploiement) - Bonification des documents (lignes de presse et Questions-Réponses) selon l'expérience				- Communiqué de presse (bilan du déploiement) - Bonification des documents (lignes de presse et Questions-Réponses) selon l'expérience	

			vécue avec le 1 ^{er} déploiement			vécue avec le 2 ^e déploiement • <i>Annnonce du calendrier de déploiement pour la poursuite du projet</i>
Forum des sous-ministres	• Présentation sur les déploiements prévus • Stratégie de gestion du changement • Stratégie de communication					
Page de connexion de clicSEQUR						Diffusion d'un bandeau d'information qui réfère à la page sur le Service d'authentification gouvernementale (éviter la confusion)
Communications administratives de l'organisation visée	MFA : Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, papillon, etc.). MFA : Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, papillon, etc.).		SAAQ : Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, papillon, etc.). <i>*Selon la fréquence des communications établie avec la clientèle cible.</i>			A établir avec le prochain MO visé, selon le calendrier de déploiement.
Communications internes dans les MO visés	Actualité pour annoncer le déploiement à venir		MFA : • Actualité pour faire le bilan du 1^{er} déploiement • Mise en valeur des bons coups	Actualité pour annoncer le déploiement à venir		SAAQ : • Actualité pour faire le bilan du déploiement • Mise en valeur des bons coups

ANNEXE 2 - MOYENS DE COMMUNICATION

Outils/Moyens		Détails	Porteur/ collaborateur	Publics cibles	Échéancier
Web/numérique	Site Québec.ca. - Fil d'actualités du MCN. - Page sur le Service d'authentification gouvernementale. - Tutoriel pas à pas, une version pour les citoyens.	Objectif : Accompagner les utilisateurs du Service d'authentification gouvernementale.	DCOM du MCN avec GdC du MCN	Citoyens susceptibles d'utiliser le Service d'authentification gouvernementale	En cours et en continu, selon les phases de la stratégie de gestion du changement, avant le déploiement au MIFA.
	Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, etc.). Une trousse de communication sera fournie aux MO. Des propositions de messages accompagnés de visuels seront remis. Il s'agira de moyens numériques.	En fonction du calendrier de déploiement, une communication identique sera soumise aux MO. Objectif : Informer les citoyens qu'ils doivent procéder à une nouvelle authentification selon le calendrier de déploiement par MO et par PES	DCOM du MCN	Utilisateurs de la nouvelle solution	Selon le calendrier de déploiement
	Message sur la page d'accueil du site du MO au moment où le Service d'authentification gouvernementale sera déployé (une page menant à la page de connexion) avec visuel.	Objectif : Informer les citoyens qu'ils doivent procéder à une nouvelle authentification dès maintenant.	DCOM du MCN, par l'entremise de chaque DCOM des MO	Clientèles du MO utilisatrices du Service d'authentification gouvernementale	Selon le calendrier de déploiement.
	Message sur la page de connexion de clicSÉCUR avec hyperlien vers la page d'information sur le Service d'authentification gouvernementale sur Québec.ca.	Objectif : Informer les citoyens de l'évolution de clicSÉCUR et qu'ils devront procéder à une nouvelle authentification au cours des prochains mois, ainsi que de la coexistence de clicSÉCUR et du Service d'authentification gouvernementale.	DCOM du MCN, par l'entremise de Services Québec (MTESS)	Utilisateurs de clicSÉCUR	Décembre 2022

Médias sociaux	Publications sur la page LinkedIn du MCN.	Objectif : Annoncer la séquence de déploiement. Demande de partages aux MO visés.	DCOM du MCN DCOM des MO	Grand public	2023 (à préciser)
	Comptes de médias sociaux des MO visés	Stratégie de publication de contenus à déterminer en collaboration avec les DCOM visés et la DCNG.	DCOM du MCN DCOM des MO DCNG		
Outils de communication à l'intention des MO	Plateforme collaborative SharePoint du MCN à l'usage exclusif des ministères et organismes (MO) – RH, gestion du changement et communications: - Foires aux questions. - Aide-mémoire. - Documents de formation (PowerPoint). - Série de webinaires. - Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels). - Plan de gestion de crise pour chaque MO en cas de disfonctionnement de la plateforme. - Tutoriel de connexion adapté au personnel des services à la clientèle. - Modèle de papillon avec texte et image pour insertion dans des communications en format papier.	Objectifs : - Accompagner le personnel impliqué dans le déploiement du Service d'authentification gouvernementale. - Présenter l'état d'avancement des travaux. - Annoncer la disponibilité des outils	GdC du MCN avec DCOM du MCN	Pour les équipes des MO consommateurs et non-consommateurs	En cours et en continu
Communications internes	- Actualités intranet - Témoignages des ambassadeurs	Objectif : Annoncer le déploiement, faire le bilan de l'opération et mettre en valeur les bons coups.	DCOM des MO visés	Employés des MO visés par un déploiement du Service d'authentification gouvernementale	Dès septembre 2022

Forum des sous-ministres	• Présentation sur les déploiements prévus • Stratégie de gestion du changement • Stratégie de communication	Objectif : Renseigner et rassurer les sous-ministres à l'égard du déploiement du Service d'authentification gouvernementale.	DCOM du MCN	Sous-ministres	Septembre 2022
Relations publiques	• Lignes de presse • Document de type « questions-réponses »	Objectifs : unifier le message et gérer le risque médiatique.	DCOM du MCN en soutien aux DCOM concernées	Grand public	1 mois avant le premier déploiement
	• Breffage technique (<i>à la discrétion du cabinet du ministre du MCN</i>) • Point de presse (<i>à la discrétion du cabinet du ministre du MCN</i>)	Objectif : Annoncer le déploiement et expliquer le projet	DCOM du MCN	Grand public	Mi-octobre
	• Communiqué de presse (<i>à la discrétion du cabinet du ministre du MCN</i>)	Objectif : Faire le bilan du déploiement	DCOM du MCN	Grand public	Novembre (MFA) Février (SAAQ)

Plan de communication

**Service d'authentification gouvernementale :
Projet Accès bonifié aux prestations électroniques de
services (PES) – Citoyens**

Avis : Ce document fait l'objet d'une diffusion restreinte. L'information qu'il contient est sujette à des changements en fonction du déploiement du service, des changements contextuels, des priorités d'action et des résultats des actions de communication. La Direction des communications du MCN est responsable et gardienne de la version finale du plan.

Équipe projet - Programme Service québécois d'identité numérique
Version du 31 août 2022

Québec 

CONTEXTE

La [Stratégie de transformation numérique gouvernementale 2019-2023](#) prévoit offrir aux citoyens du Québec des services publics rapides et intuitifs, propulsés par le numérique.

Pour y arriver, une nouvelle solution d'authentification gouvernementale, s'inscrivant dans le projet Accès bonifié aux prestations électroniques de services (PES) – Citoyens¹, du [Programme Service québécois d'identité numérique](#), sera déployée graduellement à compter d'octobre 2022². Nommée Service d'authentification gouvernementale à l'issu de travaux et de tests utilisateurs³, elle permettra un accès aux services en ligne du gouvernement du Québec à partir de diverses plateformes technologiques, dans un environnement performant et sécuritaire.

Les objectifs du Service d'authentification gouvernementale sont de :

- conserver les plus hauts standards de sécurité;
- harmoniser les systèmes;
- optimiser le traitement des données;
- améliorer l'accessibilité technologique (adaptabilité sur divers types d'appareils : mobile, tablette);
- harmoniser les processus d'accès et d'utilisation des services en ligne offerts par les ministères et organismes du gouvernement du Québec (MO);
- contribuer à la transformation numérique gouvernementale.

Le projet est réalisé par le ministère de la Cybersécurité et du Numérique (MCN), en collaboration avec des MO parties prenantes de certaines étapes du développement et de sa mise en œuvre :

- le ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS), par l'entremise de Services Québec, pour le soutien téléphonique aux citoyens;
- la Régie de l'assurance maladie du Québec (RAMQ), fournisseur de la nouvelle source de confiance (validation de l'identité au moment de la création du compte, soit le.s prénom.s et le.s nom.s de famille);
- Revenu Québec, la Société de l'assurance automobile du Québec (SAAQ) et la RAMQ, fournisseurs de secret (vérification d'identité au moment de la création du compte comprenant notamment l'information contenue dans un document officiel, ex. numéro de référence de l'avis de cotisation émis par Revenu Québec).

¹ Un projet Entreprises est également prévu ultérieurement, qui ne fait pas partie de la portée du présent plan de communication.

² Date exacte à déterminer.

³ Dénomination retenue, selon les [orientations gouvernementales](#) et ayant fait l'objet de tests auprès d'utilisateurs.

Le Service d'authentification gouvernementale remplacera progressivement la solution actuelle [clicSÉCUR](#)⁴, implantée en 2005, pour pouvoir répondre aux orientations gouvernementales en matière de sécurité et d'expérience utilisateur. Mentionnons que l'adhésion des MO au Service d'authentification gouvernementale s'effectue présentement sur une base volontaire.

Son déploiement s'effectuera par PES, identifiées par les MO, selon un calendrier déterminé. Lorsqu'une PES aura migré vers le service d'authentification, elle ne sera plus accessible par l'intermédiaire de son ancienne solution.

Le premier déploiement aura lieu dans le contexte de l'implantation d'une première PES au ministère de la Famille (MFA), en octobre 2022, auprès d'éducatrices et d'éducateurs de la petite enfance. Puis, dès janvier 2023, dans le cadre de sa transformation numérique, la SAAQ déploiera cinq portails de services en ligne sous l'appellation *saaqclic*, dont quatre utiliseront le Service d'authentification gouvernementale – Citoyens.

Utilisation des services en ligne

Selon les données de l'Académie de la transformation numérique⁵, en 2021, deux adultes sur trois (67 %) évaluent qu'il est « très ou assez facile » d'utiliser les services offerts en ligne par le gouvernement du Québec. Ce point de vue est principalement partagé par les internautes âgés de 25 à 34 ans (77 %), ceux âgés de 35 à 44 ans (78 %) de même que par les diplômés universitaires (74 %). La création d'un système d'authentification unique qui donnerait accès à tous les services gouvernementaux arrive au troisième rang (71 %) des six initiatives numériques évaluées que le gouvernement devrait mettre en place.

Il est intéressant de constater que la popularité de l'utilisation du mobile par les citoyens est confirmée par les données de Québec.ca. Plus de la moitié des adultes (60 %) au cours de la dernière année utilise principalement un appareil mobile pour consulter Québec.ca (la plateforme Web gouvernementale unifiée).

DÉFIS DE COMMUNICATION INTERNE

Intégration d'une nouvelle offre de service

Plusieurs facteurs pourraient freiner l'adhésion des gestionnaires et du personnel des MO à l'implantation du Service d'authentification gouvernementale, notamment, la méconnaissance de la nouvelle solution, sa pertinence par rapport aux solutions

⁴ clicSÉCUR : service québécois d'authentification gouvernementale actuel permettant aux citoyens d'accéder à certaines prestations électroniques de services gouvernementales.

⁵ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Les services gouvernementaux en ligne et l'identité numérique*, [En ligne], 27 avril 2022.

existantes, la perception d'une charge de travail additionnelle (nouveaux apprentissages, cohabitation avec la solution actuelle ou une solution maison). L'adhésion des MO sur une base volontaire, du moins pour le moment, n'est pas un facteur à négliger.

Incidence sur la communication : mobiliser les autorités et les gestionnaires, transmettre un message fort sur l'orientation de migrer vers une solution unique et ses avantages; rassurer sur l'accompagnement qui sera offert; bien définir les rôles et responsabilités au niveau des moyens de communication.

Résultats des deux premiers déploiements

Des écueils pourraient survenir dans l'implantation des PES et de la nouvelle solution d'authentification, qui pourraient constituer un frein à l'adhésion des autres MO.

Incidence sur la communication : informer et rassurer en continu, miser sur les bons coups pour générer un effet de levier, expliquer les ajustements apportés pour les prochains déploiements.

ENJEUX DE COMMUNICATION EXTERNE

Spécificités des offres de services

Le déploiement de la nouvelle solution s'effectuera en fonction d'un calendrier déterminé avec les MO, en fonction de leurs objectifs organisationnels et des spécificités de leur offre de service. Ces spécificités se reflètent également dans le fait que ce sont divers événements de vie qui amènent le citoyen à s'adresser à un MO pour obtenir un service.

Incidence sur la communication : privilégier des initiatives de communication sectorielles, en phase avec le déploiement de l'offre de service des MO, de leurs spécificités et des besoins des utilisateurs.

Risque de confusion associée à la coexistence des solutions actuelles et de la nouvelle

La coexistence de clicSÉCUR, de solutions maison et du Service d'authentification gouvernementale, en raison du déploiement graduel d'un MO à un autre, pour l'ensemble de ses PES ou certaines de celles-ci, pourrait créer de la confusion chez les utilisateurs, étant donné les façons différentes de s'authentifier pendant la période de transition.

L'inscription des citoyens au Service d'authentification gouvernementale ne pourra s'effectuer qu'au moment d'accéder à une PES (c'est aussi le cas pour l'actuel clicSÉCUR). Ainsi, l'inscription à la nouvelle solution sera possible seulement une fois que le Service d'authentification gouvernementale aura été déployé dans le MO donné, et uniquement pour la PES qui aura migré son service d'authentification.

La coexistence des solutions facilitera aussi la comparaison entre les deux services, qui pourrait susciter des questionnements sur la pertinence d'implanter une nouvelle solution.

Incidence sur la communication : communiquer la bonne information au bon moment, démontrer le bénéfice citoyen, s'assurer de référer le citoyen au bon service d'authentification, en fonction de la PES utilisée.

Perte de la confiance des utilisateurs envers clicSÉQUR

La désuétude de la technologie de clicSÉQUR pourrait effriter la confiance à l'égard de la solution. Pour contrer l'effet, nous misons sur l'évolution de la solution. Elle pourrait aussi générer des questions quant à la durée de vie de la nouvelle solution (rapport investissement/durée de vie). Par ailleurs, le fait de parler de rehaussement des exigences de vérification d'identité pourrait avoir l'effet pervers de discréditer l'ancienne solution alors que celle-ci demeurera pendant un certain temps.

Incidence sur la communication : trouver le juste équilibre dans la manière de faire valoir la nouvelle solution sans le faire au détriment de l'autre, rassurer à l'effet que clicSÉQUR reste fonctionnel et sécuritaire, avec un entretien continu, miser sur les nouvelles habitudes de navigation des citoyens et l'adaptabilité essentielle des services gouvernementaux en ligne aux appareils mobiles.

Résistances résultant de la première connexion

(Schéma du parcours utilisateur – annexe 1)

L'obligation de créer un nouveau compte pour certains utilisateurs pourrait être un irritant, notamment pour ceux dont l'inscription à clicSÉQUR est récente. Les comptes des deux solutions ne seront pas jumelés et il est possible qu'un citoyen doive utiliser ses deux comptes (clicSéQUR et Service d'authentification gouvernementale), selon les PES auxquelles il est inscrit.

Par ailleurs, le rehaussement des exigences de vérification d'identité lors de la première connexion des utilisateurs pourrait représenter un frein à leur adhésion au Service d'authentification gouvernementale. Mentionnons que certaines clientèles pourraient ne pas avoir accès à tous les documents demandés (ex. les nouveaux arrivants et les jeunes de moins de 18 ans). Bien que le citoyen pourra obtenir le service du gouvernement par les autres moyens connus.

En effet, en plus du numéro d'assurance sociale qui pourra être fourni par l'utilisateur, de l'information détenue par la RAMQ, Revenu Québec et la SAAQ, sera demandée afin de procéder à la vérification d'identité. S'il n'a pas l'information requise, l'utilisateur pourra demander un « secret d'identification » auprès de ces organismes. Il recevra alors l'information par la poste ce qui occasionnera un délai supplémentaire. Le fait de ne pas

pouvoir compléter la démarche sur le champ pourrait engendrer un irritant, en retardant l'inscription et l'obtention de la PES.

Finalement, le citoyen pourrait ne pas se connecter au Service d'authentification gouvernementale par manque d'habiletés ou manque d'intérêt pour l'univers technologique.

Incidence sur la communication : la nature de l'information demandée devra être connue au bon moment.

Crainte quant à la confidentialité des données et la sécurité de l'information

La confidentialité des données et la sécurité de l'information sont des sujets sensibles pour tous, tant pour les organisations que la population. La nouvelle solution fera sûrement l'objet d'une couverture médiatique soutenue et d'une attention particulière de la part de certains groupes d'intérêt (ex. Commission d'accès à l'information). D'ailleurs, la couverture médiatique en lien avec la confidentialité des données et la sécurité de l'information, ou encore avec le « bordel informatique », pourrait miner la crédibilité du projet et freiner l'adhésion des utilisateurs.

Des liens pourraient être faits avec la disponibilité de la solution sur le site des chercheurs en sécurité de l'information (Programme de Primes aux bogues) et les découvertes de vulnérabilités potentielles pourraient miner la crédibilité de la solution.

Incidence sur la communication: rassurer sur les mécanismes de sécurité en place et rappeler les objectifs de la mise en disponibilité de la solution dans le Programme de Primes aux bogues.

Mécontentement et plaintes possibles de la clientèle à la suite d'un dysfonctionnement de la nouvelle solution

L'implantation du Service d'authentification gouvernementale pourrait s'accompagner de dysfonctionnements et de retards, ce qui pourrait entraîner des répercussions importantes pour les citoyens et des craintes pour la migration des autres PES.

Cette situation pourrait provoquer du mécontentement, engendrer des plaintes et même une surcharge de travail pour les services à la clientèle. La situation serait doublement problématique : accès impossible à la solution en ligne et temps d'attente plus long pour obtenir de l'aide. Par ailleurs, la solution actuelle clicSÉCUR n'est pas à l'abri d'un bris de service.

Incidence sur la communication : prévoir un plan de gestion de crise de communication en situation d'incidents de sécurité et circonscrire l'incident aux PES touchées.

RÉSULTATS ATTENDUS

Les résultats attendus seront déterminés avec les MO dans le cadre du déploiement de leurs PES, en fonction de leurs objectifs d'affaires et de leurs cibles organisationnelles.

PRINCIPES DIRECTEURS

En fonction de ce qui précède, les initiatives de communication entourant ce projet, tant pour la communication interne qu'externe, devront s'appuyer sur les principes directeurs suivants :

- la transparence;
- la cohérence des messages véhiculés par les MO, articulés autour d'un positionnement gouvernemental;
- une réponse efficace aux questions des citoyens;
- une action rapide et des communications claires et ciblées en cas d'incidence de sécurité ou de défaillance des systèmes.

OBJECTIFS DE COMMUNICATION

Objectifs de communication interne

- Informer, mobiliser et faire adhérer le personnel des MO au projet.

Objectifs de communication externe

- Faire connaître aux citoyens concernés la nouvelle solution et démontrer ses avantages.
- Convaincre les citoyens de se créer un compte citoyen Service d'authentification gouvernementale pour transiger avec l'État.
- Rassurer les utilisateurs sur le fait que la nouvelle solution assurera la protection de leurs données personnelles, entre autres par le rehaussement des exigences de vérification d'identité.
- Maintenir la confiance des utilisateurs de l'actuelle solution clicSÉCUR pendant la période de transition.
- Démontrer que le gouvernement du Québec est engagé à offrir des services publics intuitifs pour la population, en améliorant l'efficacité de l'État.

Objectifs de communication mesurables

À déterminer, pour les actions de communication gouvernementale et sectorielles.

Pour la communication gouvernementale, les objectifs s'articuleront autour des variables suivantes :

- pourcentage d'utilisateurs de la nouvelle solution qui estimeront avoir été bien outillés pour réaliser leur inscription;
- statistiques d'achalandage de la page d'information de Québec.ca;
- nombre de visionnement du tutoriel de connexion;
- nombre de vues de l'actualité;
- interactions (partage, j'aime et commentaires) sur les publications du LinkedIn MCN;
- teneur des retombées médiatiques des actions de relations publiques.

PUBLICS CIBLES

Internes

- Les **MO consommateurs** qui souhaitent transférer des PES sur le Service d'authentification gouvernementale. Plus précisément, les équipes de projet des neuf MO⁶ qui utilisent déjà clicSÉQUR – Citoyens et regroupées par expertise :
 - affaires;
 - communication et Web;
 - gestion du changement;
 - services à la clientèle;
 - technologies de l'information.
- Les **MO non-consommateurs de clicSÉQUR – Citoyens** :
 - MFA;
 - SAAQ;
 - Les MO qui offrent déjà une solution d'authentification développée à l'interne ou qui élaborent leur dossier d'affaires pour la mise en place de leur PES, et qui souhaitent connaître les modalités du Service d'authentification gouvernementale.
- Les syndicats d'employées et employés.

⁶ Autorité des marchés financiers (AMF) / Conseil des arts et des lettres du Québec (CALQ) / Groupement des assureurs automobiles (GAA) / Ministère de l'Environnement et de la Lutte contre les changements climatiques (MELCC) / Ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) / Office de la protection du consommateur (OPC) / Régie de l'assurance maladie du Québec (RAMQ) / Retraite Québec / Revenu Québec (RQ)

- Les organismes de surveillance et de protection des intérêts des citoyens (ex. Commission d'accès à l'information, Protecteur du citoyen).

Externes

Les citoyens souhaitant transiger en ligne avec l'État, plus spécifiquement :

- Les **utilisateurs, actuels et futurs, des PES susceptibles de recourir au Service d'authentification gouvernementale.**
 - Ce public cible sera segmenté par les MO pour que chacun puisse atteindre sa cible dans ses communications respectives. Une diversité de PES répond à une diversité de besoins et de profils d'utilisateurs.
- Les **utilisateurs de clicSÉCUR** qui ont créé plus de 2,5 millions de comptes et ceux qui en créeront un d'ici les déploiements dans les MO. Ceux-ci pourraient être à la fois utilisateurs des deux solutions.

STRATÉGIE

Puisque l'implantation de la nouvelle solution doit se faire graduellement par MO, selon un calendrier de PES, et considérant les spécificités de chaque PES, la stratégie de communication sera ponctuelle et ciblée auprès des utilisateurs concernés.

La diffusion de l'information se fera à deux niveaux, de façon à accompagner les utilisateurs au moment opportun dans leur démarche de transaction avec l'État :

- une information gouvernementale sur le service en général;
- une information sectorielle pour chaque PES.

L'information gouvernementale sera prise en compte dans les plans de communication propres à chacun des MO qui planteront une PES utilisant le Service d'authentification gouvernementale. Cela comprendra notamment l'information sur le processus de connexion et l'accompagnement pour les utilisateurs, par Services Québec ou le MO concerné.

Cette approche d'intégration de l'information gouvernementale dans les communications sectorielles favorisera une communication de proximité avec l'utilisateur, au bon moment, en cohérence avec la démarche de celui-ci, qui est d'abord motivée par le besoin d'obtenir un service d'un MO. L'authentification de l'utilisateur étant une étape à franchir pour obtenir le service.

Orientations spécifiques pour la communication interne

Information – Mobilisation – Adhésion

- Communiquer régulièrement l'avancement des travaux et ses différents jalons.
- Tenir compte de l'opinion du personnel impliqué lors de l'évaluation des implantations et la recherche d'améliorations.
- Faire du personnel des MO consommateurs des ambassadeurs de la nouvelle solution. Les équipes des MO devront pouvoir s'approprier les nouveautés au moment opportun afin de les communiquer auprès de leurs clientèles.
- Transmettre des communications aux MO non-consommateurs sur les résultats des deux premiers déploiements en vue de susciter leur adhésion au Service d'authentification gouvernementale.

Orientations spécifiques pour la communication externe

Information – Accompagnement – Adhésion

- Diffuser l'information gouvernementale sur la nouvelle solution sur Québec.ca.
- Expliquer les modalités d'utilisation des deux solutions pendant la transition.
- Profiter des canaux de communication des MO consommateurs avec leurs clientèles à des moments clés pour le recours aux PES.
- Prévoir des canaux de communication pour rejoindre l'ensemble des utilisateurs potentiels.
- Profiter des communications aux utilisateurs de la solution actuelle clicSÉCUR pour communiquer sur le Service d'authentification gouvernementale.
- Véhiculer l'image d'une plateforme sécuritaire qui permet d'augmenter la rapidité de traitement lors de démarches administratives avec le gouvernement (une fois le compte créé), en éliminant notamment les délais postaux.
- Mettre en place des procédures de communication pour chaque MO afin de faire face aux risques de panne de la plateforme (gestion de crise pour les situations de dysfonctionnement).

AXE DE COMMUNICATION

Le Service d'authentification gouvernementale est une solution moderne, évolutive, accessible et sécuritaire, qui facilite la communication entre l'État et le citoyen.

MESSAGES

Messages généraux

- L'accès aux différents services en ligne du gouvernement sera simplifié grâce au nouveau Service d'authentification gouvernementale.

- Le Service d'authentification gouvernementale assure une évolution technologique afin de réaliser la transformation numérique gouvernementale.
- Le Service d'authentification gouvernementale offre plus de possibilités pour tenir compte des habitudes de navigation des citoyens.

Pour les publics internes

- Le Service d'authentification gouvernementale contribue à augmenter la cohérence des systèmes et l'accès aux services en ligne gouvernementaux.
- Le Service d'authentification gouvernementale offre des avantages non négligeables pour votre clientèle concernant la sécurité de leurs données et une rapidité de traitement lors de démarches administratives.
- Le gouvernement du Québec prend en considération les spécificités des MO pour proposer une solution optimale pour tous.
- De la formation est disponible pour le personnel afin que tous puissent communiquer de façon juste sur le Service d'authentification gouvernementale.

Pour les publics externes :

- Le Service d'authentification gouvernementale est plus performant quant à son accessibilité technologique (mobile, tablette et ordinateur).
- Le gouvernement du Québec met toute son expertise au service de la sécurité numérique des citoyens par l'intermédiaire du nouveau Service d'authentification gouvernementale.
- La solution clicSÉCUR reste opérationnelle et entretenue pour garantir un niveau conforme de sécurité.

MOYENS DE COMMUNICATION

Différents moyens de communication seront utilisés selon les publics cibles, la nature de l'information à transmettre et les étapes du projet. Ces moyens sont détaillés à l'annexe 2.

BUDGET

À venir en fonction de la stratégie et des moyens retenus.

RECHERCHE ET ÉVALUATION

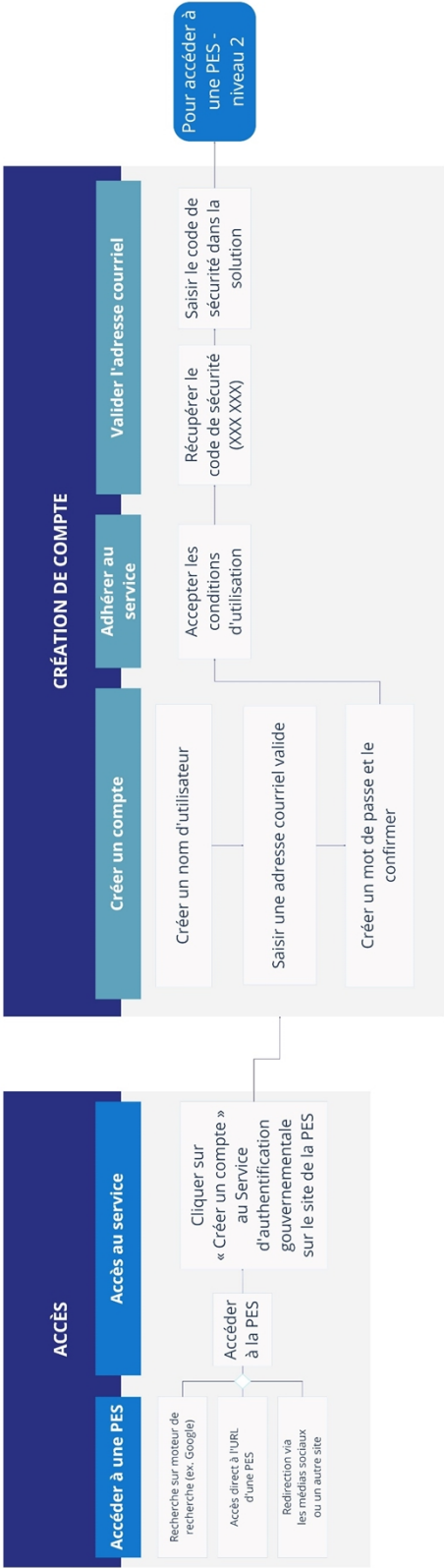
À venir dans la phase subséquente des travaux.

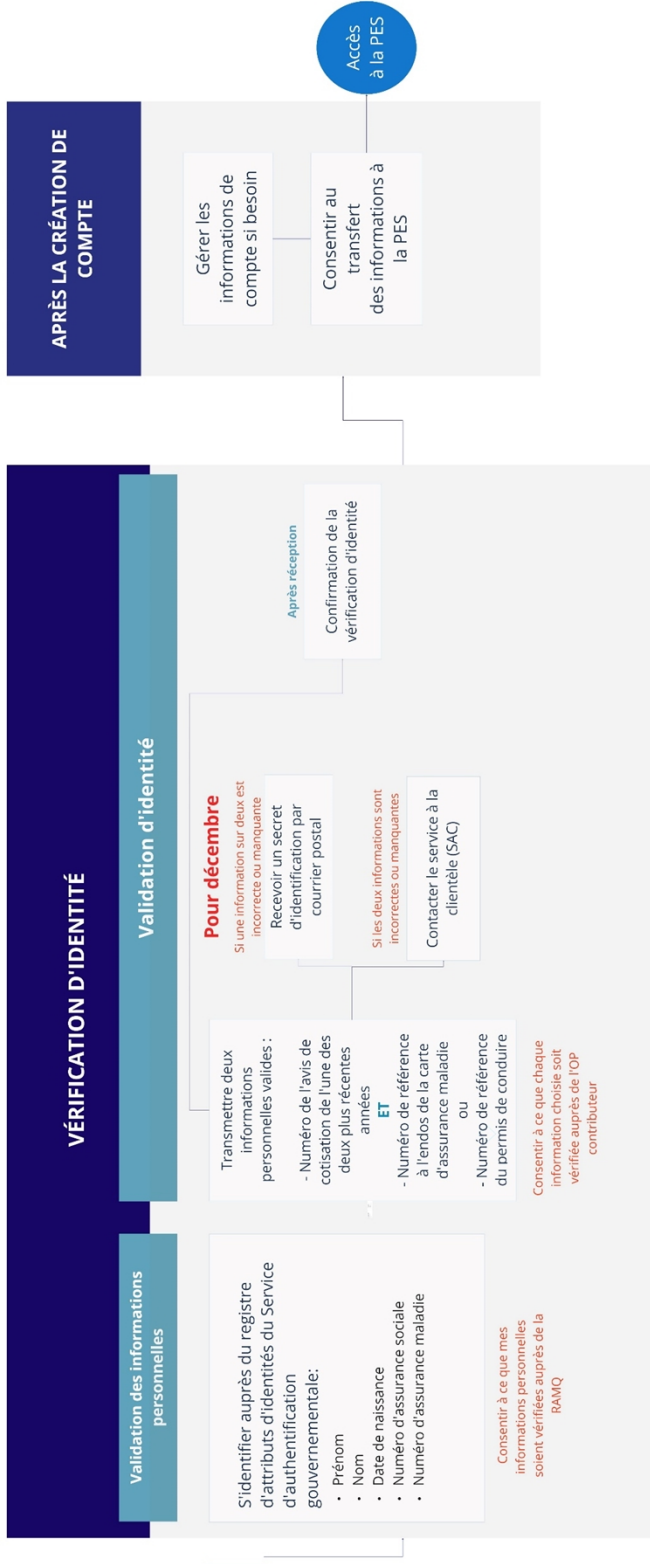
SÉQUENCE DE COMMUNICATION

Voir l'annexe 3.

DOCUMENT DE TRAVAIL

Annexe 1 – Parcours utilisateur





RE: Équipe projet en communication - Programme Service québécois d'identité numérique

From: "Perron, Sophie" <sophie.perron@mcn.gouv.qc.ca>
To: "Imbeault, Mathieu" <mathieu.imbeault2@mce.gouv.qc.ca>, Jo-Anne Masse <joanne.masse@education.gouv.qc.ca>, "Slupik, Laurent" <laurent.slupik@mtess.gouv.qc.ca>, "Gauthier, Joël" <joel.gauthier@servicesquebec.gouv.qc.ca>, "Charest, Émilie" <emilie.charest@servicesquebec.gouv.qc.ca>, virginie.auger <virginie.auger@retraitequebec.gouv.qc.ca>, Garant-Noël Chantale <chantale.garant-noel@ramq.gouv.qc.ca>, Catherine.Ouellet <catherine.ouellet@revenuquebec.ca>, "Ferland-Paradis, Émilie" <emilie.ferland-paradis@saaq.gouv.qc.ca>, "Courchesne, Marie-Anne" <marie-anne.courchesne@mce.gouv.qc.ca>, Doré Dominique <dominique.dore@revenuquebec.ca>
Cc: Lavoie Alexandre <alexandre.lavoie@revenuquebec.ca>, "Demers, Nathalie" <nathalie.demers@mcn.gouv.qc.ca>, Dion Alexandre <alexandre.dion.ext@retraitequebec.gouv.qc.ca>, "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>, "Boutin, Catherine" <catherine.boutin@mce.gouv.qc.ca>
Date: Fri, 09 Sep 2022 17:14:04 +0000
Attachments: PLCOM_SAG_2022_20220906.docx (1.38 MB); Annexe 2_Moyens-de-communication_20220908.doc (103.42 kB); Annexe 3_Séquence de communication_20220908.docx (37.9 kB)



Bonjour,
Pour faire suite à la dernière rencontre, vous trouverez en pièces jointes les documents ajustés en fonction de nos discussions.
Merci

Sophie Perron
Coordonnatrice p. i. || Services-conseils en communication
Ministère de la Cybersécurité et du Numérique

800, Place d'Youville, 4e étage, suite 4.01, Québec (Québec) G1R 3P4
Tél. : 418 528-0880, poste 4827 | Téléc. : 418 644-0462
Sophie.Perron@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

De : Perron, Sophie

Envoyé : 6 septembre 2022 12:50

À : Imbeault, Mathieu ; Jo-Anne Masse ; Slupik, Laurent ; Gauthier, Joël ; Charest, Émilie ; virginie.auger ; Garant-Noël Chantale ; Catherine.Ouellet ; Ferland-Paradis , Émilie ; Courchesne, Marie-Anne ; Doré Dominique

Cc : Lavoie Alexandre ; Demers, Nathalie ; Dion Alexandre ; Morin, Karine ; Boutin, Catherine

Objet : Équipe projet en communication - Programme Service québécois d'identité numérique

Cybersécurité
et Numérique



Bonjour,

En prévision de la rencontre de ce jeudi, vous trouverez en attachement :

- Le plan de communication ajusté en considération des commentaires formulés;
- Le tableau des moyens;
- La séquence de communication.

Merci et à bientôt!

Sophie Perron

Coordonnatrice p. i. || Services-conseils en communication

Ministère de la Cybersécurité et du Numérique

800, Place d'Youville, 4e étage, suite 4.01, Québec (Québec) G1R 3P4

Tél. : 418 528-0880, poste 4827 | Téléc. : 418 644-0462

Sophie.Perron@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Annexe 3 - Séquence de communication

	Déploiement MFA				Déploiement SAAQ	
	Septembre 2022	Octobre	Novembre	Décembre	Janvier 2023	Février
Site Québec.ca	- Actualité pour annoncer le début du déploiement - Mise en ligne d'une page d'information sur le Service d'authentification gouvernemental - Diffusion d'un tutoriel de connexion pour les citoyens		Actualité pour faire le bilan du 1 ^{er} déploiement au MFA.	Actualité pour annoncer le prochain déploiement		- Actualité pour faire le bilan 2^e déploiement à la SAAQ. <i>Calendrier de déploiement pour la poursuite du projet</i>
Site du MO		MFA : Diffuser le tutoriel et les moyens pour communiquer avec le service à la clientèle	Actualité pour faire le bilan du 1 ^{er} déploiement au MFA.		SAAQ : Diffuser le tutoriel et les moyens pour communiquer avec le service à la clientèle	Actualité pour faire le bilan du 2^e déploiement à la SAAQ.
Médias sociaux	Une publication pour annoncer la page d'information sur Québec.ca et le tutoriel de connexion sur la page LinkedIn du MCN et demande de partage sur les comptes des MO visés <i>Stratégie de publication de contenu à déterminer en collaboration avec les DCOM visées et la DCNG</i>	Veille et gestion des commentaires sur le sujet			Veille et gestion des commentaires sur le sujet	Une publication pour annoncer la séquence de déploiement sur la page LinkedIn du MCN et demande de partage sur les comptes des MO visés <i>Stratégie de publication de contenu à déterminer en collaboration avec les DCOM visées et la DCNG</i>
Plateforme collaborative SharePoint du MCN	Annoncer la disponibilité des outils :		Ajustements en vue du prochain	Diffusion des documents		Ajustements en vue du prochain

à l'usage exclusif des MO	- Foire aux questions. - Aide-mémoire. - Documents de formation. - Série de webinaires. - Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels). - Modèle de papillon avec texte et image pour insertion dans des communications en format papier.		déploiement (solution, approche, matériel pour le service à la clientèle)	ajustés, au besoin.		déploiement (solution, approche, matériel pour le service à la clientèle) Calendrier de déploiement pour la poursuite du projet
Relations publiques	- Lignes de presse au plan gouvernemental - Document de type « questions-réponses »	- Brefpage technique - Point de presse	- Communiqué de presse (bilan du déploiement) - Bonification des documents (lignes de presse et Questions-Réponses) selon l'expérience vécue avec le 1^{er} déploiement			- Communiqué de presse (bilan du déploiement) - Bonification des documents (lignes de presse et Questions-Réponses) selon l'expérience vécue avec le 2^e déploiement - Annonce du calendrier de déploiement pour la poursuite du projet
Forum des sous-ministres			- Présentation sur les déploiements prévus - Stratégie de gestion du changement - Stratégie de communication			
Page de connexion de clicSÉCUR					Diffusion d'un bandeau d'information qui réfère à la page sur le Service d'authentification gouvernementale (éviter la confusion)	

Communications administratives de l'organisation visée	MFA : Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, papillon, etc.).		SAAQ : Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, papillon, etc.). <i>*Selon la fréquence des communications établie avec la clientèle cible.</i>		À établir avec le prochain MO visé, selon le calendrier de déploiement.
--	---	--	--	--	---

ANNEXE 2 – MOYENS DE COMMUNICATION

Outils/Moyens		Détails	Porteur/ collaborateur	Publics cibles	Échéancier
Web/numérique	Site Québec.ca. - Fil d'actualités du MCN. - Page sur le Service d'authentification gouvernementale. - Tutoriel pas à pas, une version pour les citoyens.	Objectif : Accompagner les utilisateurs du Service d'authentification gouvernementale.	DCOM du MCN avec GdC du MCN	Citoyens susceptibles d'utiliser le Service d'authentification gouvernementale	En cours et en continu, selon les phases de la stratégie de gestion du changement, avant le déploiement au MFA.
	Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, etc.). Une trousse de communication sera fournie aux MO. Des propositions de messages accompagnés de visuels seront remis. Il s'agira de moyens numériques.	En fonction du calendrier de déploiement, une communication identique sera soumise aux MO. Objectif : Informer les citoyens qu'ils doivent procéder à une nouvelle authentification selon le calendrier de déploiement par MO et par PES	DCOM du MCN	Utilisateurs de la nouvelle solution	Selon le calendrier de déploiement Note : Le MFA utilisera ces outils à compter de novembre 2022
	Pour les MO qui ont leur propre site Web : Message sur les sites Web des MO au moment où le Service d'authentification gouvernementale sera déployé dans leur organisation respective (une page menant à la page de connexion) avec visuel.	Objectifs : Informer les citoyens qu'ils doivent procéder à une nouvelle authentification dès maintenant. Préciser comment obtenir son numéro de référence contenu sur un des deux derniers avis de cotisation et d'avoir en main leur carte de la Régie d'assurance maladie du Québec (RAMQ) et leur permis de conduire (numéro de référence).	DCOM du MCN, par l'entremise de chaque DCOM des MO	Clientèles du MO utilisatrices du Service d'authentification gouvernementale	Selon le calendrier de déploiement. Note : Le MFA utilisera ces outils à compter de novembre 2022

		Bon à savoir : Revenu Québec demandera un consentement aux citoyens lors de la production de leur déclaration fiscale dès le printemps 2022, afin qu'il soit rendu accessible en ligne. Objectifs : Informer les citoyens de l'évolution de clicSÉQUR et qu'ils devront procéder à une nouvelle authentification au cours des prochains mois, ainsi que de la coexistence de clicSÉQUR et du Service d'authentification gouvernementale. Préciser comment obtenir son numéro de référence contenu sur un des deux derniers avis de cotisation et d'avoir en main leur carte de la Régie d'assurance maladie du Québec (RAMQ) Bon à savoir : Revenu Québec demande un consentement aux citoyens lors de la production de leur déclaration fiscale depuis le printemps 2022, afin qu'il soit rendu accessible en ligne. Une promotion de cette demande de consentement s'accentuera.	DCOM du MCN, par l'entremise de Services Québec (MTESS)	Utilisateurs de clicSÉQUR	Décembre 2022
Message sur la page de connexion de clicSÉQUR avec hyperlien vers la page d'information sur le Service d'authentification gouvernementale sur Québec.ca.	Une publication sur la page LinkedIn du MCN. Une publication sur la page Facebook et le Twitter du gouvernement du Québec.	Objectif : Annoncer la séquence de déploiement. Demande de partages aux MO visés.	DCOM du MCN DCOM des MO	Grand public	2023 (à préciser) Suivant le déploiement de la SAAQ

Médias sociaux

	Comptes de médias sociaux des MO visés.	Stratégie de publication de contenus à déterminer en collaboration avec les DCOM visés et la DCNG.	DCOM du MCN DCOM des MO DCNG	
Outils de communication à l'intention des MO	Plateforme collaborative SharePoint du MCN à l'usage exclusif des ministères et organismes (MO) – équipes de gestion du changement (pour partage avec les équipes internes tel que les services à la clientèle, relations d'affaires et communications : Pour diffusion aux équipes internes : • Foire aux questions. • Aide-mémoire. • Documents de formation (PowerPoint). • Série de webinaires. Pour diffusion externe : • Modèle de papillon avec texte et image pour insertion dans des communications en format papier. Pour diffusion dans les intranets : • Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels).	Objectifs : • Accompagner le personnel impliqué dans le déploiement du Service d'authentification gouvernementale. • Présenter l'état d'avancement des travaux. • Annoncer la disponibilité des outils	GdC du MCN avec DCOM du MCN	Pour les équipes des MO consommateurs et non-consommateurs
		Objectif : Renseigner et rassurer les sous-ministres à l'égard du déploiement du Service d'authentification gouvernementale.	DCOM du MCN	Sous-ministres
		Objectifs : unifier le message et gérer le risque médiatique.	DCOM du MCN	Grand public
Forum des sous-ministres	• Présentation sur les déploiements prévus • Stratégie de gestion du changement • Stratégie de communication			Octobre 2022 ou après
Relations publiques	• Lignes de presse au plan gouvernemental Document de type « questions-réponses »			1 mois avant le premier déploiement, soit fin septembre

					2022
	- Breffage technique (<i>à la discrétion du cabinet du ministre du MCN</i>) - Point de presse (<i>à la discrétion du cabinet du ministre du MCN</i>) <i>Voir à le cabinet du MFA</i>	Objectif : Annoncer le déploiement et expliquer le projet	DCOM du MCN	Grand public	Fin-octobre
	Communiqué de presse (<i>à la discrétion du cabinet du ministre du MCN</i>) <i>Voir à s'arrimer avec le cabinet du MFA et de du MTQ</i>	Objectif : Faire le bilan du déploiement	DCOM du MCN	Grand public	Novembre 2022 (MFA) Février 2022 (SAAQ)

Programme Service québécois d'identité numérique — Plan de communication

From: "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>
To: "Rodrigue, Pierre" <pierre.rodrigue@mcn.gouv.qc.ca>, "Léveillé, Michel" <michel.leveille@mce.gouv.qc.ca>
Cc: "Audin, Thierry" <thierry.audin@mce.gouv.qc.ca>, Marie-Pier.Sauve <marie-pier.sauve@mce.gouv.qc.ca>, "Boutin, Catherine" <catherine.boutin@mce.gouv.qc.ca>, "Bilodeau, Marie" <marie.bilodeau@mce.gouv.qc.ca>, "Perron, Sophie" <sophie.perron@mcn.gouv.qc.ca>, "Prévost-Dallaire, Stéphane" <stephane.prevast-dallaire@mcn.gouv.qc.ca>
Date: Mon, 12 Sep 2022 18:21:43 +0000
Attachments: PLCOM_SAG_20220912.docx (1.38 MB); Annexe 3_Séquence de communication_20220912.docx (36.12 kB); Annexe 2_Moyens-de-communication_20220912.doc (102.91 kB)



Bonjour messieurs,

Voici la version finale du plan de communication pour le déploiement du Service d'authentification gouvernementale (SAG), dans le cadre du Programme Service québécois d'identité numérique.

Le plan a été rédigé en collaboration avec l'équipe projet en communication, laquelle rassemble les communicateurs des ministères et organismes impliqués dans le déploiement du SAG. Il est accompagné d'un tableau des moyens retenu de même que la séquence de communication prévue.

Si vous avez des questions, n'hésitez surtout pas à communiquer avec moi.

Merci et bonne fin de journée !

Karine Morin

Directrice p. i.

Direction des communications

Ministère de la Cybersécurité et du Numérique

800, place D'Youville, 4^e étage

Québec (Québec) G1R 3P4

Téléphone : 418 655-1154

karine.morin@mcn.gouv.qc.ca

contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Plan de communication

**Service d'authentification gouvernementale :
Projet Accès bonifié aux prestations électroniques de
services (PES) – Citoyens**

Avis : Ce document fait l'objet d'une diffusion restreinte. L'information qu'il contient est sujette à des changements en fonction du déploiement du service, des changements contextuels, des priorités d'action et des résultats des actions de communication. La Direction des communications du MCN est responsable et gardienne de la version finale du plan.

Équipe projet - Programme Service québécois d'identité numérique
Version du 31 août 2022

Québec  
 

CONTEXTE

La [Stratégie de transformation numérique gouvernementale 2019-2023](#) prévoit offrir aux citoyens du Québec des services publics rapides et intuitifs, propulsés par le numérique.

Pour y arriver, une nouvelle solution d'authentification gouvernementale, s'inscrivant dans le projet Accès bonifié aux prestations électroniques de services (PES) – Citoyens¹, du [Programme Service québécois d'identité numérique](#), sera déployée graduellement à compter d'octobre 2022². Nommée Service d'authentification gouvernementale à l'issu de travaux et de tests utilisateurs³, elle permettra un accès aux services en ligne du gouvernement du Québec à partir de diverses plateformes technologiques, dans un environnement performant et sécuritaire.

Les objectifs du Service d'authentification gouvernementale sont de:

- conserver les plus hauts standards de sécurité;
- harmoniser les systèmes;
- optimiser le traitement des données;
- améliorer l'accessibilité technologique (adaptabilité sur divers types d'appareils : mobile, tablette);
- harmoniser les processus d'accès et d'utilisation des services en ligne offerts par les ministères et organismes du gouvernement du Québec (MO);
- contribuer à la transformation numérique gouvernementale.

Le projet est réalisé par le ministère de la Cybersécurité et du Numérique (MCN), en collaboration avec des MO parties prenantes de certaines étapes du développement et de sa mise en œuvre :

- le ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS), par l'entremise de Services Québec, pour le soutien téléphonique aux citoyens;
- la Régie de l'assurance maladie du Québec (RAMQ), fournisseur de la nouvelle source de confiance (validation de l'identité au moment de la création du compte, soit le.s prénom.s et le.s nom.s de famille);
- Revenu Québec, la Société de l'assurance automobile du Québec (SAAQ) et la RAMQ, fournisseurs de secret (vérification d'identité au moment de la création du compte comprenant notamment l'information contenue dans un document officiel, ex. numéro de référence de l'avis de cotisation émis par Revenu Québec).

¹ Un projet Entreprises est également prévu ultérieurement, qui ne fait pas partie de la portée du présent plan de communication.

² Date exacte à déterminer.

³ Dénomination retenue, selon les [orientations gouvernementales](#) et ayant fait l'objet de tests auprès d'utilisateurs.

Le Service d'authentification gouvernementale remplacera progressivement la solution actuelle [clicSÉCUR](#)⁴, implantée en 2005, pour pouvoir répondre aux orientations gouvernementales en matière de sécurité et d'expérience utilisateur. Mentionnons que l'adhésion des MO au Service d'authentification gouvernementale s'effectue présentement sur une base volontaire.

Son déploiement s'effectuera par PES, identifiées par les MO, selon un calendrier déterminé. Lorsqu'une PES aura migré vers le service d'authentification, elle ne sera plus accessible par l'intermédiaire de son ancienne solution.

Le premier déploiement aura lieu dans le contexte de l'implantation d'une première PES au ministère de la Famille (MFA), en octobre 2022, auprès d'éducatrices et d'éducateurs de la petite enfance. Puis, dès janvier 2023, dans le cadre de sa transformation numérique, la SAAQ déploiera cinq portails de services en ligne sous l'appellation *saaqclic*, dont quatre utiliseront le Service d'authentification gouvernementale – Citoyens.

Utilisation des services en ligne

Selon les données de l'Académie de la transformation numérique⁵, en 2021, deux adultes sur trois (67 %) évaluent qu'il est « très ou assez facile » d'utiliser les services offerts en ligne par le gouvernement du Québec. Ce point de vue est principalement partagé par les internautes âgés de 25 à 34 ans (77 %), ceux âgés de 35 à 44 ans (78 %) de même que par les diplômés universitaires (74 %). La création d'un système d'authentification unique qui donnerait accès à tous les services gouvernementaux arrive au troisième rang (71 %) des six initiatives numériques évaluées que le gouvernement devrait mettre en place.

Il est intéressant de constater que la popularité de l'utilisation du mobile par les citoyens est confirmée par les données de Québec.ca. Plus de la moitié des adultes (60 %) au cours de la dernière année utilise principalement un appareil mobile pour consulter Québec.ca (la plateforme Web gouvernementale unifiée).

DÉFIS DE COMMUNICATION INTERNE

Intégration d'une nouvelle offre de service

Plusieurs facteurs pourraient freiner l'adhésion des gestionnaires et du personnel des MO à l'implantation du Service d'authentification gouvernementale, notamment, la méconnaissance de la nouvelle solution, sa pertinence par rapport aux solutions

⁴ clicSÉCUR : service québécois d'authentification gouvernementale actuel permettant aux citoyens d'accéder à certaines prestations électroniques de services gouvernementales.

⁵ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Les services gouvernementaux en ligne et l'identité numérique*, [En ligne], 27 avril 2022.

existantes, la perception d'une charge de travail additionnelle (nouveaux apprentissages, cohabitation avec la solution actuelle ou une solution maison). L'adhésion des MO sur une base volontaire, du moins pour le moment, n'est pas un facteur à négliger.

Incidence sur la communication : mobiliser les autorités et les gestionnaires, transmettre un message fort sur l'orientation de migrer vers une solution unique et ses avantages; rassurer sur l'accompagnement qui sera offert; bien définir les rôles et responsabilités au niveau des moyens de communication.

Résultats des deux premiers déploiements

Des écueils pourraient survenir dans l'implantation des PES et de la nouvelle solution d'authentification, qui pourraient constituer un frein à l'adhésion des autres MO.

Incidence sur la communication : informer et rassurer en continu, miser sur les bons coups pour générer un effet de levier, expliquer les ajustements apportés pour les prochains déploiements.

ENJEUX DE COMMUNICATION EXTERNE

Spécificités des offres de services

Le déploiement de la nouvelle solution s'effectuera en fonction d'un calendrier déterminé avec les MO, en fonction de leurs objectifs organisationnels et des spécificités de leur offre de service. Ces spécificités se reflètent également dans le fait que ce sont divers événements de vie qui amènent le citoyen à s'adresser à un MO pour obtenir un service.

Incidence sur la communication : privilégier des initiatives de communication sectorielles, en phase avec le déploiement de l'offre de service des MO, de leurs spécificités et des besoins des utilisateurs.

Risque de confusion associée à la coexistence des solutions actuelles et de la nouvelle

La coexistence de clicSÉQUR, de solutions maison et du Service d'authentification gouvernementale, en raison du déploiement graduel d'un MO à un autre, pour l'ensemble de ses PES ou certaines de celles-ci, pourrait créer de la confusion chez les utilisateurs, étant donné les façons différentes de s'authentifier pendant la période de transition.

L'inscription des citoyens au Service d'authentification gouvernementale ne pourra s'effectuer qu'au moment d'accéder à une PES (c'est aussi le cas pour l'actuel clicSÉQUR). Ainsi, l'inscription à la nouvelle solution sera possible seulement une fois que le Service d'authentification gouvernementale aura été déployé dans le MO donné, et uniquement pour la PES qui aura migré son service d'authentification.

La coexistence des solutions facilitera aussi la comparaison entre les deux services, qui pourrait susciter des questionnements sur la pertinence d'implanter une nouvelle solution.

Incidence sur la communication : communiquer la bonne information au bon moment, démontrer le bénéfice citoyen, s'assurer de référer le citoyen au bon service d'authentification, en fonction de la PES utilisée.

Perte de la confiance des utilisateurs envers clicSÉCUR

La désuétude de la technologie de clicSÉCUR pourrait effriter la confiance à l'égard de la solution. Pour contrer l'effet, nous misons sur l'évolution de la solution. Elle pourrait aussi générer des questions quant à la durée de vie de la nouvelle solution (rapport investissement/durée de vie). Par ailleurs, le fait de parler de rehaussement des exigences de vérification d'identité pourrait avoir l'effet pervers de discréditer l'ancienne solution alors que celle-ci demeurera pendant un certain temps.

Incidence sur la communication : trouver le juste équilibre dans la manière de faire valoir la nouvelle solution sans le faire au détriment de l'autre, rassurer à l'effet que clicSÉCUR reste fonctionnel et sécuritaire, avec un entretien continu, miser sur les nouvelles habitudes de navigation des citoyens et l'adaptabilité essentielle des services gouvernementaux en ligne aux appareils mobiles.

Résistances résultant de la première connexion

(Schéma du parcours utilisateur – annexe 1)

L'obligation de créer un nouveau compte pour certains utilisateurs pourrait être un irritant, notamment pour ceux dont l'inscription à clicSÉCUR est récente. Les comptes des deux solutions ne seront pas jumelés et il est possible qu'un citoyen doive utiliser ses deux comptes (clicSÉCUR et Service d'authentification gouvernementale), selon les PES auxquelles il est inscrit.

Par ailleurs, le rehaussement des exigences de vérification d'identité lors de la première connexion des utilisateurs pourrait représenter un frein à leur adhésion au Service d'authentification gouvernementale. Mentionnons que certaines clientèles pourraient ne pas avoir accès à tous les documents demandés (ex. les nouveaux arrivants et les jeunes de moins de 18 ans). Bien que le citoyen pourra obtenir le service du gouvernement par les autres moyens connus.

En effet, en plus du numéro d'assurance sociale qui pourra être fourni par l'utilisateur, de l'information détenue par la RAMQ, Revenu Québec et la SAAQ, sera demandée afin de procéder à la vérification d'identité. S'il n'a pas l'information requise, l'utilisateur pourra demander un « secret d'identification » auprès de ces organismes. Il recevra alors l'information par la poste ce qui occasionnera un délai supplémentaire. Le fait de ne pas

pouvoir compléter la démarche sur le champ pourrait engendrer un irritant, en retardant l'inscription et l'obtention de la PES.

Finalement, le citoyen pourrait ne pas se connecter au Service d'authentification gouvernementale par manque d'habiletés ou manque d'intérêt pour l'univers technologique.

Incidence sur la communication : la nature de l'information demandée devra être connue au bon moment.

Crainte quant à la confidentialité des données et la sécurité de l'information

La confidentialité des données et la sécurité de l'information sont des sujets sensibles pour tous, tant pour les organisations que la population. La nouvelle solution fera sûrement l'objet d'une couverture médiatique soutenue et d'une attention particulière de la part de certains groupes d'intérêt (ex. Commission d'accès à l'information). D'ailleurs, la couverture médiatique en lien avec la confidentialité des données et la sécurité de l'information, ou encore avec le « bordel informatique », pourrait miner la crédibilité du projet et freiner l'adhésion des utilisateurs.

Des liens pourraient être faits avec la disponibilité de la solution sur le site des chercheurs en sécurité de l'information (Programme de Primes aux bogues) et les découvertes de vulnérabilités potentielles pourraient miner la crédibilité de la solution.

Incidence sur la communication: rassurer sur les mécanismes de sécurité en place et rappeler les objectifs de la mise en disponibilité de la solution dans le Programme de Primes aux bogues.

Mécontentement et plaintes possibles de la clientèle à la suite d'un dysfonctionnement de la nouvelle solution

L'implantation du Service d'authentification gouvernementale pourrait s'accompagner de dysfonctionnements et de retards, ce qui pourrait entraîner des répercussions importantes pour les citoyens et des craintes pour la migration des autres PES.

Cette situation pourrait provoquer du mécontentement, engendrer des plaintes et même une surcharge de travail pour les services à la clientèle. La situation serait doublement problématique : accès impossible à la solution en ligne et temps d'attente plus long pour obtenir de l'aide. Par ailleurs, la solution actuelle clicSÉCUR n'est pas à l'abri d'un bris de service.

Incidence sur la communication : prévoir un plan de gestion de crise de communication en situation d'incidents de sécurité et circonscrire l'incident aux PES touchées.

RÉSULTATS ATTENDUS

Les résultats attendus seront déterminés avec les MO dans le cadre du déploiement de leurs PES, en fonction de leurs objectifs d'affaires et de leurs cibles organisationnelles.

PRINCIPES DIRECTEURS

En fonction de ce qui précède, les initiatives de communication entourant ce projet, tant pour la communication interne qu'externe, devront s'appuyer sur les principes directeurs suivants :

- la transparence;
- la cohérence des messages véhiculés par les MO, articulés autour d'un positionnement gouvernemental;
- une réponse efficace aux questions des citoyens;
- une action rapide et des communications claires et ciblées en cas d'incidence de sécurité ou de défaillance des systèmes.

OBJECTIFS DE COMMUNICATION

Objectifs de communication interne

- Informer, mobiliser et faire adhérer le personnel des MO au projet.

Objectifs de communication externe

- Faire connaître aux citoyens concernés la nouvelle solution et démontrer ses avantages.
- Convaincre les citoyens de se créer un compte citoyen Service d'authentification gouvernementale pour transiger avec l'État.
- Rassurer les utilisateurs sur le fait que la nouvelle solution assurera la protection de leurs données personnelles, entre autres par le rehaussement des exigences de vérification d'identité.
- Maintenir la confiance des utilisateurs de l'actuelle solution clicSÉCUR pendant la période de transition.
- Démontrer que le gouvernement du Québec est engagé à offrir des services publics intuitifs pour la population, en améliorant l'efficacité de l'État.

Objectifs de communication mesurables

À déterminer, pour les actions de communication gouvernementale et sectorielles.

Pour la communication gouvernementale, les objectifs s'articuleront autour des variables suivantes :

- pourcentage d'utilisateurs de la nouvelle solution qui estimeront avoir été bien outillés pour réaliser leur inscription;
- statistiques d'achalandage de la page d'information de Québec.ca;
- nombre de visionnement du tutoriel de connexion;
- nombre de vues de l'actualité;
- interactions (partage, j'aime et commentaires) sur les publications du LinkedIn MCN;
- teneur des retombées médiatiques des actions de relations publiques.

PUBLICS CIBLES

Internes

- Les **MO consommateurs** qui souhaitent transférer des PES sur le Service d'authentification gouvernementale. Plus précisément, les équipes de projet des neuf MO⁶ qui utilisent déjà clicSÉQUR – Citoyens et regroupées par expertise :
 - affaires;
 - communication et Web;
 - gestion du changement;
 - services à la clientèle;
 - technologies de l'information.
- Les **MO non-consommateurs de clicSÉQUR – Citoyens** :
 - MFA;
 - SAAQ;
 - Les MO qui offrent déjà une solution d'authentification développée à l'interne ou qui élaborent leur dossier d'affaires pour la mise en place de leur PES, et qui souhaitent connaître les modalités du Service d'authentification gouvernementale.
- Les syndicats d'employées et employés.

⁶ Autorité des marchés financiers (AMF) / Conseil des arts et des lettres du Québec (CALQ) / Groupement des assureurs automobiles (GAA) / Ministère de l'Environnement et de la Lutte contre les changements climatiques (MELCC) / Ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) / Office de la protection du consommateur (OPC) / Régie de l'assurance maladie du Québec (RAMQ) / Retraite Québec / Revenu Québec (RQ)

- Les organismes de surveillance et de protection des intérêts des citoyens (ex. Commission d'accès à l'information, Protecteur du citoyen).

Externes

Les citoyens souhaitant transiger en ligne avec l'État, plus spécifiquement :

- Les **utilisateurs, actuels et futurs, des PES susceptibles de recourir au Service d'authentification gouvernementale.**
 - Ce public cible sera segmenté par les MO pour que chacun puisse atteindre sa cible dans ses communications respectives. Une diversité de PES répond à une diversité de besoins et de profils d'utilisateurs.
- Les **utilisateurs de clicSÉCUR** qui ont créé plus de 2,5 millions de comptes et ceux qui en créeront un d'ici les déploiements dans les MO. Ceux-ci pourraient être à la fois utilisateurs des deux solutions.

STRATÉGIE

Puisque l'implantation de la nouvelle solution doit se faire graduellement par MO, selon un calendrier de PES, et considérant les spécificités de chaque PES, la stratégie de communication sera ponctuelle et ciblée auprès des utilisateurs concernés.

La diffusion de l'information se fera à deux niveaux, de façon à accompagner les utilisateurs au moment opportun dans leur démarche de transaction avec l'État :

- une information gouvernementale sur le service en général;
- une information sectorielle pour chaque PES.

L'information gouvernementale sera prise en compte dans les plans de communication propres à chacun des MO qui planteront une PES utilisant le Service d'authentification gouvernementale. Cela comprendra notamment l'information sur le processus de connexion et l'accompagnement pour les utilisateurs, par Services Québec ou le MO concerné.

Cette approche d'intégration de l'information gouvernementale dans les communications sectorielles favorisera une communication de proximité avec l'utilisateur, au bon moment, en cohérence avec la démarche de celui-ci, qui est d'abord motivée par le besoin d'obtenir un service d'un MO. L'authentification de l'utilisateur étant une étape à franchir pour obtenir le service.

Orientations spécifiques pour la communication interne

Information – Mobilisation – Adhésion

- Communiquer régulièrement l'avancement des travaux et ses différents jalons.
- Tenir compte de l'opinion du personnel impliqué lors de l'évaluation des implantations et la recherche d'améliorations.
- Faire du personnel des MO consommateurs des ambassadeurs de la nouvelle solution. Les équipes des MO devront pouvoir s'approprier les nouveautés au moment opportun afin de les communiquer auprès de leurs clientèles.
- Transmettre des communications aux MO non-consommateurs sur les résultats des deux premiers déploiements en vue de susciter leur adhésion au Service d'authentification gouvernementale.

Orientations spécifiques pour la communication externe

Information – Accompagnement – Adhésion

- Diffuser l'information gouvernementale sur la nouvelle solution sur Québec.ca.
- Expliquer les modalités d'utilisation des deux solutions pendant la transition.
- Profiter des canaux de communication des MO consommateurs avec leurs clientèles à des moments clés pour le recours aux PES.
- Prévoir des canaux de communication pour rejoindre l'ensemble des utilisateurs potentiels.
- Profiter des communications aux utilisateurs de la solution actuelle clicSÉCUR pour communiquer sur le Service d'authentification gouvernementale.
- Véhiculer l'image d'une plateforme sécuritaire qui permet d'augmenter la rapidité de traitement lors de démarches administratives avec le gouvernement (une fois le compte créé), en éliminant notamment les délais postaux.
- Mettre en place des procédures de communication pour chaque MO afin de faire face aux risques de panne de la plateforme (gestion de crise pour les situations de dysfonctionnement).

AXE DE COMMUNICATION

Le Service d'authentification gouvernementale est une solution moderne, évolutive, accessible et sécuritaire, qui facilite la communication entre l'État et le citoyen.

MESSAGES

Messages généraux

- L'accès aux différents services en ligne du gouvernement sera simplifié grâce au nouveau Service d'authentification gouvernementale.

- Le Service d'authentification gouvernementale assure une évolution technologique afin de réaliser la transformation numérique gouvernementale.
- Le Service d'authentification gouvernementale offre plus de possibilités pour tenir compte des habitudes de navigation des citoyens.

Pour les publics internes

- Le Service d'authentification gouvernementale contribue à augmenter la cohérence des systèmes et l'accès aux services en ligne gouvernementaux.
- Le Service d'authentification gouvernementale offre des avantages non négligeables pour votre clientèle concernant la sécurité de leurs données et une rapidité de traitement lors de démarches administratives.
- Le gouvernement du Québec prend en considération les spécificités des MO pour proposer une solution optimale pour tous.
- De la formation est disponible pour le personnel afin que tous puissent communiquer de façon juste sur le Service d'authentification gouvernementale.

Pour les publics externes :

- Le Service d'authentification gouvernementale est plus performant quant à son accessibilité technologique (mobile, tablette et ordinateur).
- Le gouvernement du Québec met toute son expertise au service de la sécurité numérique des citoyens par l'intermédiaire du nouveau Service d'authentification gouvernementale.
- La solution clicSÉCUR reste opérationnelle et entretenue pour garantir un niveau conforme de sécurité.

MOYENS DE COMMUNICATION

Différents moyens de communication seront utilisés selon les publics cibles, la nature de l'information à transmettre et les étapes du projet. Ces moyens sont détaillés à l'annexe 2.

BUDGET

À venir en fonction de la stratégie et des moyens retenus.

RECHERCHE ET ÉVALUATION

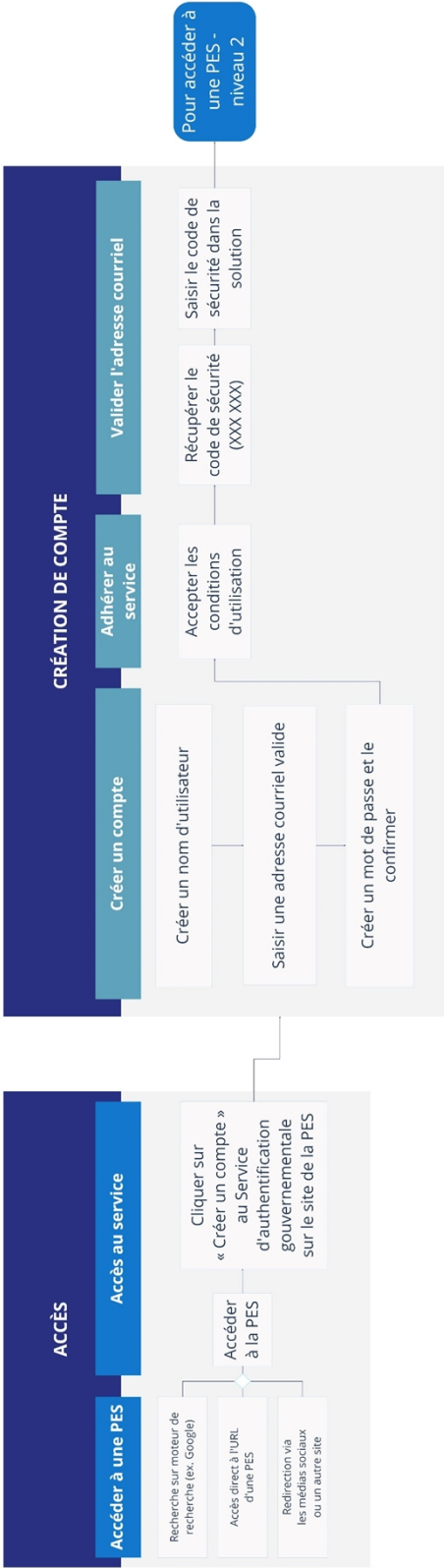
À venir dans la phase subséquente des travaux.

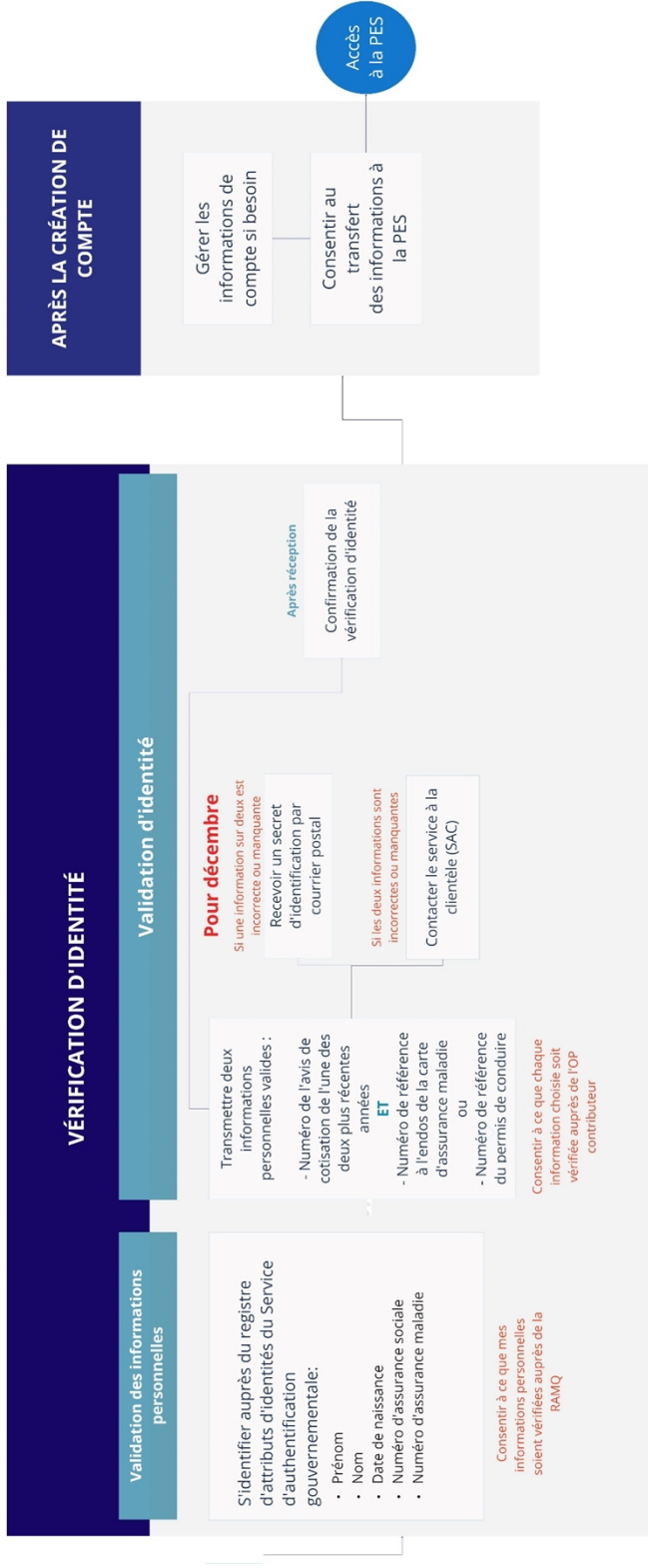
SÉQUENCE DE COMMUNICATION

Voir l'annexe 3.

DOCUMENT DE TRAVAIL

Annexe 1 – Parcours utilisateur





TR: Programme Service québécois d'identité numérique — Plan de communication

From: "Rodrigue, Pierre" <pierre.rodrique@mcn.gouv.qc.ca>
To: "Kelly, Jonathan" <jonathan.kelly@mcn.gouv.qc.ca>, "Bélanger, Julie" <julie.belanger@mcn.gouv.qc.ca>
Date: Tue, 13 Sep 2022 01:14:30 +0000
Attachments: PLCOM_SAG_20220912.docx (1.38 MB); Annexe 3_Séquence de communication_20220912.docx (36.12 kB); Annexe 2_Moyens-de-communication_20220912.doc (102.91 kB)

Cybersécurité
et Numérique



POUR INFORMATION ET SUITES APPROPRIÉES

Pierre E. Rodrigue

Sous-ministre et dirigeant principal de l'information

Ministère de la Cybersécurité et du Numérique

900, Place D'Youville, 9^e étage

Québec (Québec) G1R 3P7

Tél. : 418 644-1030, poste 5600

Quebec.ca/gouv/ministere/cybersecurite-numerique

De : Morin, Karine

Envoyé : 12 septembre 2022 14:22

À : Rodrigue, Pierre ; Léveillé, Michel

Cc : Audin, Thierry ; Marie-Pier.Sauve ; Boutin, Catherine ; Bilodeau, Marie ; Perron, Sophie ; Prévost-Dallaire, Stéphane

Objet : Programme Service québécois d'identité numérique — Plan de communication

Importance : Haute

Cybersécurité
et Numérique



Bonjour messieurs,

Voici la version finale du plan de communication pour le déploiement du Service d'authentification gouvernementale (SAG), dans le cadre du Programme Service québécois d'identité numérique.

Le plan a été rédigé en collaboration avec l'équipe projet en communication, laquelle rassemble les communicateurs des ministères et organismes impliqués dans le déploiement du SAG. Il est accompagné d'un tableau des moyens retenus de même que la séquence de communication prévue. Si vous avez des questions, n'hésitez surtout pas à communiquer avec moi.

Merci et bonne fin de journée !

Karine Morin

Directrice p. i.

Direction des communications

Ministère de la Cybersécurité et du Numérique

800, place D'Youville, 4^e étage
Québec (Québec) G1R 3P4
Téléphone : 418 655-1154
karine.morin@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Équipe projet en communication - Programme Service québécois d'identité numérique

From: "Morin, Karine" <karine.morin@mcn.gouv.qc.ca>
To: "Boucher, Martin" <martin.boucher@mce.gouv.qc.ca>, "Foster, Nathalie" <nathalie.foster@education.gouv.qc.ca>, "Hurtevent, Isabelle" <isabelle.hurtevent@mtess.gouv.qc.ca>, Bilodeau Francine <francine.bilodeau@ramq.gouv.qc.ca>, "Delisle, Josée" <josée.delisle@retraitequebec.gouv.qc.ca>, marie-claude.gagnon <marie-claude.gagnon@revenuquebec.ca>, "Farand, Béatrice" <beatrice.farand@saaq.gouv.qc.ca>
Cc: "Audin, Thierry" <thierry.audin@mce.gouv.qc.ca>, "Demers, Nathalie" <nathalie.demers@mcn.gouv.qc.ca>, "Demers, Robert" <robert.demers@mce.gouv.qc.ca>, catherine.gauthier <catherine.gauthier@mce.gouv.qc.ca>, "Boutin, Catherine" <catherine.boutin@mce.gouv.qc.ca>, "Perron, Sophie" <sophie.perron@mcn.gouv.qc.ca>, "Guillemette, Isabelle" <isabelle.guillemette@mcn.gouv.qc.ca>, "Bélanger, Julie" <julie.belanger@mcn.gouv.qc.ca>
Date: Fri, 23 Sep 2022 20:15:27 +0000
Attachments: PLCOM_SAG_20220912.docx (1.38 MB); Annexe 2_Moyens-de-communication_20220912.doc (102.91 kB); Annexe 3_Séquence de communication_20220912.docx (36.12 kB)



Bonjour,

Voici la version finale du plan de communication pour le déploiement du Service d'authentification gouvernementale (SAG), dans le cadre du Programme Service québécois d'identité numérique.

Le plan a été rédigé en collaboration avec l'équipe projet en communication, laquelle rassemble les communicateurs de vos ministères et organismes. Il est accompagné d'un tableau des moyens retenu de même que la séquence de communication prévue.

Si vous avez des questions, n'hésitez surtout pas à communiquer avec moi.

Merci et bonne fin de semaine !

Karine Morin
Directrice p. i.
Direction des communications
Ministère de la Cybersécurité et du Numérique
800, place D'Youville, 4^e étage
Québec (Québec) G1R 3P4
Téléphone : 418 655-1154
karine.morin@mcn.gouv.qc.ca

Ce message est confidentiel et est à l'usage exclusif du destinataire identifié ci-dessus. Toute autre personne est, par les présentes, avisée qu'il lui est strictement interdit de le diffuser, de le distribuer, d'en dévoiler le contenu ou de le reproduire. Si vous avez reçu cette communication par erreur, veuillez en informer l'expéditeur par courrier électronique immédiatement et détruire l'original de ce message ainsi que toute copie.

Plan de communication

**Service d'authentification gouvernementale :
Projet Accès bonifié aux prestations électroniques de
services (PES) – Citoyens**

Avis : Ce document fait l'objet d'une diffusion restreinte. L'information qu'il contient est sujette à des changements en fonction du déploiement du service, des changements contextuels, des priorités d'action et des résultats des actions de communication. La Direction des communications du MCN est responsable et gardienne de la version finale du plan.

Équipe projet - Programme Service québécois d'identité numérique
Version du 12 septembre 2022

Québec 

CONTEXTE

La [Stratégie de transformation numérique gouvernementale 2019-2023](#) prévoit offrir aux citoyens du Québec des services publics rapides et intuitifs, propulsés par le numérique.

Pour y arriver, une nouvelle solution d'authentification gouvernementale, s'inscrivant dans le projet Accès bonifié aux prestations électroniques de services (PES) – Citoyens¹, du [Programme Service québécois d'identité numérique](#), sera déployée graduellement à compter d'octobre 2022². Nommée Service d'authentification gouvernementale à l'issu de travaux et de tests utilisateurs³, elle permettra un accès aux services en ligne du gouvernement du Québec à partir de diverses plateformes technologiques, dans un environnement performant et sécuritaire.

Les objectifs du Service d'authentification gouvernementale sont de:

- conserver les plus hauts standards de sécurité;
- harmoniser les systèmes;
- optimiser le traitement des données;
- améliorer l'accessibilité technologique (adaptabilité sur divers types d'appareils : mobile, tablette);
- harmoniser les processus d'accès et d'utilisation des services en ligne offerts par les ministères et organismes du gouvernement du Québec (MO);
- contribuer à la transformation numérique gouvernementale.

Le projet est réalisé par le ministère de la Cybersécurité et du Numérique (MCN), en collaboration avec des MO parties prenantes de certaines étapes du développement et de sa mise en œuvre :

- le ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS), par l'entremise de Services Québec, pour le soutien téléphonique aux citoyens;
- la Régie de l'assurance maladie du Québec (RAMQ), fournisseur de la nouvelle source de confiance (validation de l'identité au moment de la création du compte, soit le.s prénom.s et le.s nom.s de famille);
- Revenu Québec, la Société de l'assurance automobile du Québec (SAAQ) et la RAMQ, fournisseurs de secret (vérification d'identité au moment de la création du compte comprenant notamment l'information contenue dans un document officiel, ex. numéro de référence de l'avis de cotisation émis par Revenu Québec).

¹ Un projet Entreprises est également prévu ultérieurement, qui ne fait pas partie de la portée du présent plan de communication.

² Date exacte à déterminer.

³ Dénomination retenue, selon les [orientations gouvernementales](#) et ayant fait l'objet de tests auprès d'utilisateurs.

Le Service d'authentification gouvernementale remplacera progressivement la solution actuelle [clicSÉCUR](#)⁴, implantée en 2005, pour pouvoir répondre aux orientations gouvernementales en matière de sécurité et d'expérience utilisateur. Mentionnons que l'adhésion des MO au Service d'authentification gouvernementale s'effectue présentement sur une base volontaire.

Son déploiement s'effectuera par PES, identifiées par les MO, selon un calendrier déterminé. Lorsqu'une PES aura migré vers le service d'authentification, elle ne sera plus accessible par l'intermédiaire de son ancienne solution.

Le premier déploiement aura lieu dans le contexte de l'implantation d'une première PES au ministère de la Famille (MFA), en octobre 2022, auprès d'éducatrices et d'éducateurs de la petite enfance. Puis, dès janvier 2023, dans le cadre de sa transformation numérique, la SAAQ déploiera cinq portails de services en ligne sous l'appellation *saaqclic*, dont quatre utiliseront le Service d'authentification gouvernementale – Citoyens.

Utilisation des services en ligne

Selon les données de l'Académie de la transformation numérique⁵, en 2021, deux adultes sur trois (67 %) évaluent qu'il est « très ou assez facile » d'utiliser les services offerts en ligne par le gouvernement du Québec. Ce point de vue est principalement partagé par les internautes âgés de 25 à 34 ans (77 %), ceux âgés de 35 à 44 ans (78 %) de même que par les diplômés universitaires (74 %). La création d'un système d'authentification unique qui donnerait accès à tous les services gouvernementaux arrive au troisième rang (71 %) des six initiatives numériques évaluées que le gouvernement devrait mettre en place.

Il est intéressant de constater que la popularité de l'utilisation du mobile par les citoyens est confirmée par les données de Québec.ca. Plus de la moitié des adultes (60 %) au cours de la dernière année utilise principalement un appareil mobile pour consulter Québec.ca (la plateforme Web gouvernementale unifiée).

DÉFIS DE COMMUNICATION INTERNE

Intégration d'une nouvelle offre de service

Plusieurs facteurs pourraient freiner l'adhésion des gestionnaires et du personnel des MO à l'implantation du Service d'authentification gouvernementale, notamment, la méconnaissance de la nouvelle solution, sa pertinence par rapport aux solutions

⁴ clicSÉCUR : service québécois d'authentification gouvernementale actuel permettant aux citoyens d'accéder à certaines prestations électroniques de services gouvernementales.

⁵ ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Les services gouvernementaux en ligne et l'identité numérique*, [\[En ligne\]](#), 27 avril 2022.

existantes, la perception d'une charge de travail additionnelle (nouveaux apprentissages, cohabitation avec la solution actuelle ou une solution maison). L'adhésion des MO sur une base volontaire, du moins pour le moment, n'est pas un facteur à négliger.

Incidence sur la communication : mobiliser les autorités et les gestionnaires, transmettre un message fort sur l'orientation de migrer vers une solution unique et ses avantages; rassurer sur l'accompagnement qui sera offert; bien définir les rôles et responsabilités au niveau des moyens de communication.

Résultats des deux premiers déploiements

Des écueils pourraient survenir dans l'implantation des PES et de la nouvelle solution d'authentification, qui pourraient constituer un frein à l'adhésion des autres MO.

Incidence sur la communication : informer et rassurer en continu, miser sur les bons coups pour générer un effet de levier, expliquer les ajustements apportés pour les prochains déploiements.

ENJEUX DE COMMUNICATION EXTERNE

Spécificités des offres de services

Le déploiement de la nouvelle solution s'effectuera en fonction d'un calendrier déterminé avec les MO, en fonction de leurs objectifs organisationnels et des spécificités de leur offre de service. Ces spécificités se reflètent également dans le fait que ce sont divers événements de vie qui amènent le citoyen à s'adresser à un MO pour obtenir un service.

Incidence sur la communication : privilégier des initiatives de communication sectorielles, en phase avec le déploiement de l'offre de service des MO, de leurs spécificités et des besoins des utilisateurs.

Risque de confusion associée à la coexistence des solutions actuelles et de la nouvelle

La coexistence de clicSÉCUR, de solutions maison et du Service d'authentification gouvernementale, en raison du déploiement graduel d'un MO à un autre, pour l'ensemble de ses PES ou certaines de celles-ci, pourrait créer de la confusion chez les utilisateurs, étant donné les façons différentes de s'authentifier pendant la période de transition.

L'inscription des citoyens au Service d'authentification gouvernementale ne pourra s'effectuer qu'au moment d'accéder à une PES (c'est aussi le cas pour l'actuel clicSÉCUR). Ainsi, l'inscription à la nouvelle solution sera possible seulement une fois que le Service d'authentification gouvernementale aura été déployé dans le MO donné, et uniquement pour la PES qui aura migré son service d'authentification.

La coexistence des solutions facilitera aussi la comparaison entre les deux services, qui pourrait susciter des questionnements sur la pertinence d'implanter une nouvelle solution.

Incidence sur la communication : communiquer la bonne information au bon moment, démontrer le bénéfice citoyen, s'assurer de référer le citoyen au bon service d'authentification, en fonction de la PES utilisée.

Perte de la confiance des utilisateurs envers clicSÉCUR

La désuétude de la technologie de clicSÉCUR pourrait effriter la confiance à l'égard de la solution. Pour contrer l'effet, nous misons sur l'évolution de la solution. Elle pourrait aussi générer des questions quant à la durée de vie de la nouvelle solution (rapport investissement/durée de vie). Par ailleurs, le fait de parler de rehaussement des exigences de vérification d'identité pourrait avoir l'effet pervers de discréditer l'ancienne solution alors que celle-ci demeurera pendant un certain temps.

Incidence sur la communication : trouver le juste équilibre dans la manière de faire valoir la nouvelle solution sans le faire au détriment de l'autre, rassurer à l'effet que clicSÉCUR reste fonctionnel et sécuritaire, avec un entretien continu, miser sur les nouvelles habitudes de navigation des citoyens et l'adaptabilité essentielle des services gouvernementaux en ligne aux appareils mobiles.

Résistances résultant de la première connexion

(Schéma du parcours utilisateur – annexe 1)

L'obligation de créer un nouveau compte pour certains utilisateurs pourrait être un irritant, notamment pour ceux dont l'inscription à clicSÉCUR est récente. Les comptes des deux solutions ne seront pas jumelés et il est possible qu'un citoyen doive utiliser ses deux comptes (clicSéCUR et Service d'authentification gouvernementale), selon les PES auxquelles il est inscrit.

Par ailleurs, le rehaussement des exigences de vérification d'identité lors de la première connexion des utilisateurs pourrait représenter un frein à leur adhésion au Service d'authentification gouvernementale. Mentionnons que certaines clientèles pourraient ne pas avoir accès à tous les documents demandés (ex. les nouveaux arrivants et les jeunes de moins de 18 ans). Bien que le citoyen pourra obtenir le service du gouvernement par les autres moyens connus.

En effet, en plus du numéro d'assurance sociale qui pourra être fourni par l'utilisateur, de l'information détenue par la RAMQ, Revenu Québec et la SAAQ, sera demandée afin de procéder à la vérification d'identité. S'il n'a pas l'information requise, l'utilisateur pourra demander un « secret d'identification » auprès de ces organismes. Il recevra alors l'information par la poste ce qui occasionnera un délai supplémentaire. Le fait de ne pas

pouvoir compléter la démarche sur le champ pourrait engendrer un irritant, en retardant l'inscription et l'obtention de la PES.

Finalement, le citoyen pourrait ne pas se connecter au Service d'authentification gouvernementale par manque d'habiletés ou manque d'intérêt pour l'univers technologique.

Incidence sur la communication : la nature de l'information demandée devra être connue au bon moment.

Crainte quant à la confidentialité des données et la sécurité de l'information

La confidentialité des données et la sécurité de l'information sont des sujets sensibles pour tous, tant pour les organisations que la population. La nouvelle solution fera sûrement l'objet d'une couverture médiatique soutenue et d'une attention particulière de la part de certains groupes d'intérêt (ex. Commission d'accès à l'information). D'ailleurs, la couverture médiatique en lien avec la confidentialité des données et la sécurité de l'information, ou encore avec le « bordel informatique », pourrait miner la crédibilité du projet et freiner l'adhésion des utilisateurs.

Des liens pourraient être faits avec la disponibilité de la solution sur le site des chercheurs en sécurité de l'information (Programme de Primes aux bogues) et les découvertes de vulnérabilités potentielles pourraient miner la crédibilité de la solution.

Incidence sur la communication: rassurer sur les mécanismes de sécurité en place et rappeler les objectifs de la mise en disponibilité de la solution dans le Programme de Primes aux bogues.

Mécontentement et plaintes possibles de la clientèle à la suite d'un dysfonctionnement de la nouvelle solution

L'implantation du Service d'authentification gouvernementale pourrait s'accompagner de dysfonctionnements et de retards, ce qui pourrait entraîner des répercussions importantes pour les citoyens et des craintes pour la migration des autres PES.

Cette situation pourrait provoquer du mécontentement, engendrer des plaintes et même une surcharge de travail pour les services à la clientèle. La situation serait doublement problématique : accès impossible à la solution en ligne et temps d'attente plus long pour obtenir de l'aide. Par ailleurs, la solution actuelle clicSÉCUR n'est pas à l'abri d'un bris de service.

Incidence sur la communication : prévoir un service de première ligne pour répondre aux questions et plaintes des citoyens et un plan de gestion de crise de communication en situation d'incidents de sécurité et circonscrire l'incident aux PES touchées.

RÉSULTATS ATTENDUS

Les résultats attendus seront déterminés avec les MO dans le cadre du déploiement de leurs PES, en fonction de leurs objectifs d'affaires et de leurs cibles organisationnelles.

PRINCIPES DIRECTEURS

En fonction de ce qui précède, les initiatives de communication entourant ce projet, tant pour la communication interne qu'externe, devront s'appuyer sur les principes directeurs suivants :

- la transparence;
- la cohérence des messages véhiculés par les MO, articulés autour d'un positionnement gouvernemental;
- une réponse efficace aux questions des citoyens;
- une action rapide et des communications claires et ciblées en cas d'incidence de sécurité ou de défaillance des systèmes.

OBJECTIFS DE COMMUNICATION

Objectifs de communication interne

- Informer, mobiliser et faire adhérer le personnel des MO au projet.

Objectifs de communication externe

- Faire connaître aux citoyens concernés la nouvelle solution et démontrer ses avantages.
- Convaincre les citoyens de se créer un compte citoyen Service d'authentification gouvernementale pour transiger avec l'État.
- Rassurer les utilisateurs sur le fait que la nouvelle solution assurera la protection de leurs données personnelles, entre autres par le rehaussement des exigences de vérification d'identité.
- Maintenir la confiance des utilisateurs de l'actuelle solution clicSÉCUR pendant la période de transition.
- Démontrer que le gouvernement du Québec est engagé à offrir des services publics intuitifs pour la population, en améliorant l'efficacité de l'État.

Objectifs de communication mesurables

À déterminer, pour les actions de communication gouvernementale et sectorielles.

Pour la communication gouvernementale, les objectifs s'articuleront autour des variables suivantes :

- pourcentage d'utilisateurs de la nouvelle solution qui estimeront avoir été bien outillés pour réaliser leur inscription;
- statistiques d'achalandage de la page d'information de Québec.ca;
- nombre de visionnement du tutoriel de connexion;
- nombre de vues de l'actualité;
- interactions (partage, j'aime et commentaires) sur les publications du LinkedIn MCN;
- teneur des retombées médiatiques des actions de relations publiques.

PUBLICS CIBLES

Internes

- Les **MO consommateurs** qui souhaitent transférer des PES sur le Service d'authentification gouvernementale. Plus précisément, les équipes de projet des neuf MO⁶ qui utilisent déjà clicSÉCUR – Citoyens et regroupées par expertise :
 - affaires;
 - communication et Web;
 - gestion du changement;
 - services à la clientèle;
 - technologies de l'information.
- Les **MO non-consommateurs de clicSÉCUR – Citoyens** :
 - MFA;
 - SAAQ;
 - Les MO qui offrent déjà une solution d'authentification développée à l'interne ou qui élaborent leur dossier d'affaires pour la mise en place de leur PES, et qui souhaitent connaître les modalités du Service d'authentification gouvernementale.
- Les syndicats d'employées et employés.

⁶ Autorité des marchés financiers (AMF) / Conseil des arts et des lettres du Québec (CALQ) / Groupement des assureurs automobiles (GAA) / Ministère de l'Environnement et de la Lutte contre les changements climatiques (MELCC) / Ministère du Travail, de l'Emploi et de la Solidarité sociale (MTESS) / Office de la protection du consommateur (OPC) / Régie de l'assurance maladie du Québec (RAMQ) / Retraite Québec / Revenu Québec (RQ)

- Les organismes de surveillance et de protection des intérêts des citoyens (ex. Commission d'accès à l'information, Protecteur du citoyen).

Externes

Les citoyens souhaitant transiger en ligne avec l'État, plus spécifiquement :

- Les **utilisateurs, actuels et futurs, des PES susceptibles de recourir au Service d'authentification gouvernementale.**
 - Ce public cible sera segmenté par les MO pour que chacun puisse atteindre sa cible dans ses communications respectives. Une diversité de PES répond à une diversité de besoins et de profils d'utilisateurs.
- Les **utilisateurs de clicSÉCUR** qui ont créé plus de 2,5 millions de comptes et ceux qui en créeront un d'ici les déploiements dans les MO. Ceux-ci pourraient être à la fois utilisateurs des deux solutions.

STRATÉGIE

Puisque l'implantation de la nouvelle solution doit se faire graduellement par MO, selon un calendrier de PES, et considérant les spécificités de chaque PES, la stratégie de communication sera ponctuelle et ciblée auprès des utilisateurs concernés.

La diffusion de l'information se fera à deux niveaux, de façon à accompagner les utilisateurs au moment opportun dans leur démarche de transaction avec l'État :

- une information gouvernementale sur le service en général;
- une information sectorielle pour chaque PES.

L'information gouvernementale sera prise en compte dans les plans de communication propres à chacun des MO qui planteront une PES utilisant le Service d'authentification gouvernementale. Cela comprendra notamment l'information sur le processus de connexion et l'accompagnement pour les utilisateurs, par Services Québec ou le MO concerné.

Cette approche d'intégration de l'information gouvernementale dans les communications sectorielles favorisera une communication de proximité avec l'utilisateur, au bon moment, en cohérence avec la démarche de celui-ci, qui est d'abord motivée par le besoin d'obtenir un service d'un MO. L'authentification de l'utilisateur étant une étape à franchir pour obtenir le service.

Orientations spécifiques pour la communication interne

Information – Mobilisation – Adhésion

- Communiquer régulièrement l'avancement des travaux et ses différents jalons.
- Tenir compte de l'opinion du personnel impliqué lors de l'évaluation des implantations et la recherche d'améliorations.
- Faire du personnel des MO consommateurs des ambassadeurs de la nouvelle solution. Les équipes des MO devront pouvoir s'approprier les nouveautés au moment opportun afin de les communiquer auprès de leurs clientèles.
- Transmettre des communications aux MO non-consommateurs sur les résultats des deux premiers déploiements en vue de susciter leur adhésion au Service d'authentification gouvernementale.

Orientations spécifiques pour la communication externe

Information – Accompagnement – Adhésion

- Diffuser l'information gouvernementale sur la nouvelle solution sur Québec.ca.
- Expliquer les modalités d'utilisation des deux solutions pendant la transition.
- Profiter des canaux de communication des MO consommateurs avec leurs clientèles à des moments clés pour le recours aux PES.
- Prévoir des canaux de communication pour rejoindre l'ensemble des utilisateurs potentiels.
- Profiter des communications aux utilisateurs de la solution actuelle clicSÉCUR pour communiquer sur le Service d'authentification gouvernementale.
- Véhiculer l'image d'une plateforme sécuritaire qui permet d'augmenter la rapidité de traitement lors de démarches administratives avec le gouvernement (une fois le compte créé), en éliminant notamment les délais postaux.
- Mettre en place des procédures de communication pour chaque MO afin de faire face aux risques de panne de la plateforme (gestion de crise pour les situations de dysfonctionnement).

AXE DE COMMUNICATION

Le Service d'authentification gouvernementale est une solution moderne, évolutive, accessible et sécuritaire, qui facilite la communication entre l'État et le citoyen.

MESSAGES

Messages généraux

- L'accès aux différents services en ligne du gouvernement sera simplifié grâce au nouveau Service d'authentification gouvernementale.
- Le Service d'authentification gouvernementale assure une évolution technologique afin de réaliser la transformation numérique gouvernementale.
- Le Service d'authentification gouvernementale offre plus de possibilités pour tenir compte des habitudes de navigation des citoyens.

Pour les publics internes

- Le Service d'authentification gouvernementale contribue à augmenter la cohérence des systèmes et l'accès aux services en ligne gouvernementaux.
- Le Service d'authentification gouvernementale offre des avantages non négligeables pour votre clientèle concernant la sécurité de leurs données et une rapidité de traitement lors de démarches administratives.
- Le gouvernement du Québec prend en considération les spécificités des MO pour proposer une solution optimale pour tous.
- De la formation est disponible pour le personnel afin que tous puissent communiquer de façon juste sur le Service d'authentification gouvernementale.

Pour les publics externes :

- Le Service d'authentification gouvernementale est plus performant quant à son accessibilité technologique (mobile, tablette et ordinateur).
- Le gouvernement du Québec met toute son expertise au service de la sécurité numérique des citoyens par l'intermédiaire du nouveau Service d'authentification gouvernementale.
- La solution clicSÉCUR reste opérationnelle et entretenue pour garantir un niveau conforme de sécurité.

MOYENS DE COMMUNICATION

Différents moyens de communication seront utilisés selon les publics cibles, la nature de l'information à transmettre et les étapes du projet. Ces moyens sont détaillés à l'annexe 2.

BUDGET

À venir en fonction de la stratégie et des moyens retenus.

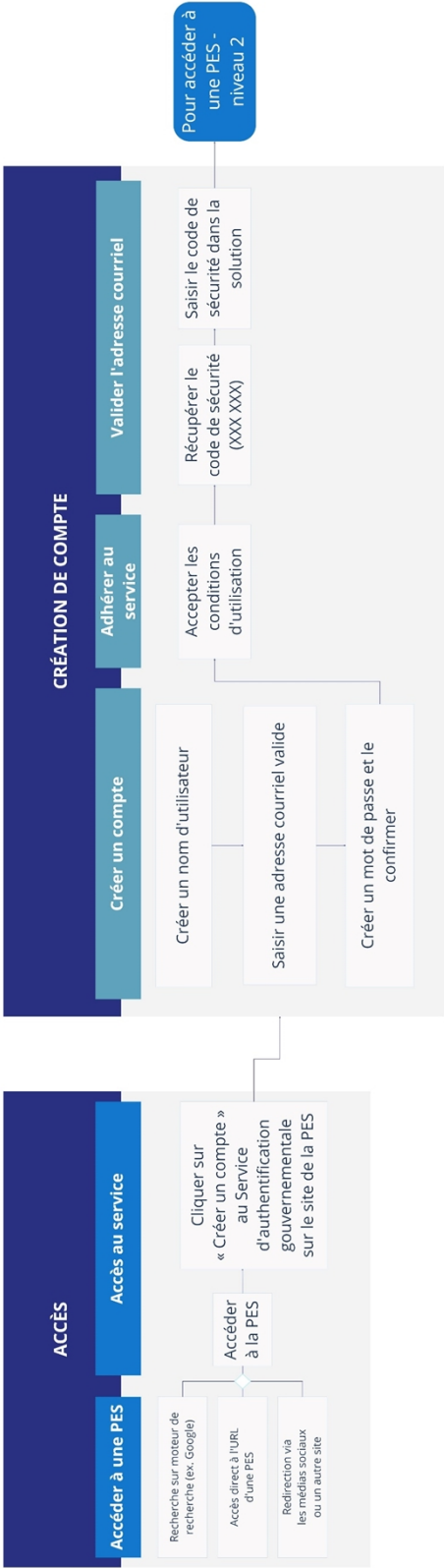
RECHERCHE ET ÉVALUATION

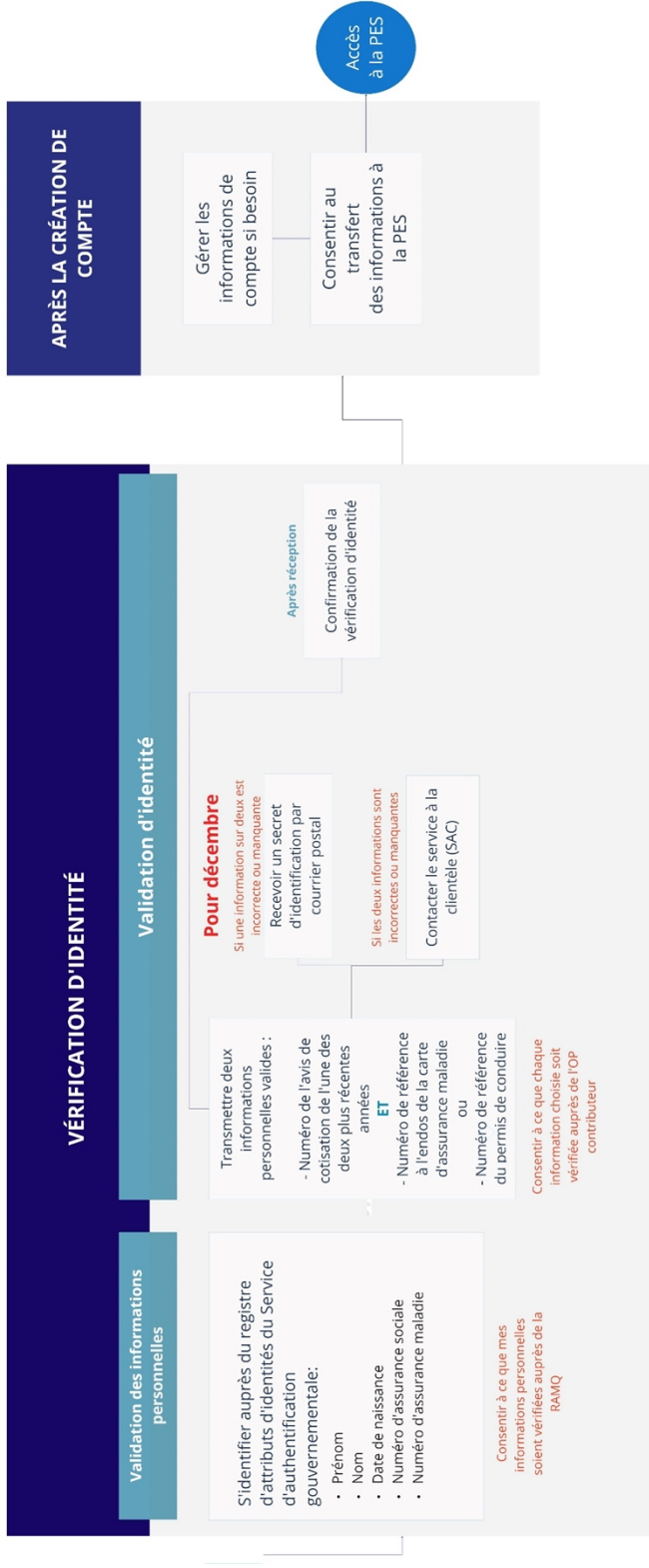
À venir dans la phase subséquente des travaux.

SÉQUENCE DE COMMUNICATION

Voir l'annexe 3.

Annexe 1 – Parcours utilisateur





ANNEXE 2 – MOYENS DE COMMUNICATION

Outils/Moyens		Détails	Porteur/ collaborateur	Publics cibles	Échéancier
Web/numérique	Site Québec.ca. - Fil d'actualités du MCN. - Page sur le Service d'authentification gouvernementale. - Tutoriel pas à pas, une version pour les citoyens.	Objectif : Accompagner les utilisateurs du Service d'authentification gouvernementale.	DCOM du MCN avec GdC du MCN	Citoyens susceptibles d'utiliser le Service d'authentification gouvernementale	En cours et en continu, selon les phases de la stratégie de gestion du changement, avant le déploiement au MFA.
	Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs). Une trousse de communication sera fournie aux MO. Des propositions de messages accompagnés de visuels seront remis. Il s'agira de moyens numériques.	En fonction du calendrier de déploiement, une communication identique sera soumise aux MO. Objectif : Informer les citoyens qu'ils doivent procéder à une nouvelle authentification selon le calendrier de déploiement par MO et par PES	DCOM du MCN	Utilisateurs de la nouvelle solution	Selon le calendrier de déploiement Note : Le MFA utilisera ces outils à compter de novembre 2022
	Message sur les sites Web des MO au moment où le Service d'authentification gouvernementale sera disponible dans le cadre du déploiement d'une PES dans leur organisation respective (une page de contenu avec hyperlien menant à la page de connexion de la nouvelle solution) avec visuel.	Objectifs : Informer les citoyens qu'ils doivent procéder à une nouvelle authentification dès maintenant. Préciser la nature de l'information qui sera demandée et comment l'obtenir. Bon à savoir : Revenu Québec demandera un consentement aux citoyens lors de la production de leur déclaration fiscale dès le printemps 2022,	DCOM du MCN, par l'entremise de chaque DCOM des MO	Clientèles du MO utilisatrices du Service d'authentification gouvernementale	Selon le calendrier de déploiement. Note : Le MFA utilisera ces outils à compter de novembre 2022

		afin qu'il soit rendu accessible en ligne. Une promotion de cette demande de consentement s'accentuera.				Déembre 2022
	Message sur la page de connexion de clicSÉQUR avec hyperlien vers la page d'information sur le Service d'authentification gouvernementale sur Québec.ca.	Objectifs : Informer les citoyens de l'évolution de clicSÉQUR et qu'ils devront procéder à une nouvelle authentification au cours des prochains mois, ainsi que de la coexistence de clicSÉQUR et du Service d'authentification gouvernementale. Préciser la nature de l'information qui sera demandée et comment l'obtenir.	DCOM du MCN, par l'entremise de Services Québec (MTESS)	Utilisateurs de clicSÉQUR		
Médias sociaux	Une publication sur la page LinkedIn du MCN. Une publication sur la page Facebook et le Twitter du gouvernement du Québec.	Objectif : Annoncer l'utilisation de la nouvelle solution dans le déploiement de l'offre de services en ligne du gouvernement du Québec, de façon progressive. Demande de partages aux MO visés	DCOM du MCN DCOM des M	Grand public	2023 (à préciser) Suivant le déploiement de la SAAQ	

	Comptes de médias sociaux des MO visés.	Stratégie de publication de contenus à déterminer en collaboration avec les DCOM visées et la DCNG	DCOM du MCN DCOM des MO DCN		
Outils de communication à l'intention des MO	Plateforme collaborative SharePoint du MCN à l'usage exclusif des ministères et organismes (MO) – équipes de gestion du changement (pour partage avec les équipes internes tel que les services à la clientèle, relations d'affaires et communications : Pour diffusion aux équipes internes : • Foire aux questions. • Aide-mémoire. • Documents de formation (PowerPoint). • Série de webinaires. Pour diffusion externe : • Modèle de papillon avec texte et image pour insertion dans des communications en format papier. Pour diffusion dans les intranets : • Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels).	Objectifs : • Accompagner le personnel impliqué dans le déploiement du Service d'authentification gouvernementale. • Présenter l'état d'avancement des travaux. • Annoncer la disponibilité des outils.	GdC du MCN avec DCOM du MCN	Pour les équipes des MO consommateurs et non-consommateurs	En cours et en continu

Forum des sous-ministres	- Présentation sur les déploiements prévus - Stratégie de gestion du changement - Stratégie de communication	Objectif : Renseigner et rassurer les sous-ministres à l'égard du déploiement du Service d'authentification gouvernementale.	DCOM et BSM du MCN	Sous-ministres	Novembre 2022 ou après
Relations publiques	Lignes de presse au plan gouvernemental Document de type « questions-réponses »	Objectifs : unifier le message et gérer le risque médiatique.	DCOM du MCN	Grand public	1 mois avant le premier déploiement, soit fin septembre 2022
	- Brefpage technique (<i>à la discrétion du cabinet du ministre du MCN</i>) - Point de presse (<i>à la discrétion du cabinet du ministre du MCN</i>) <i>Voir à informer le cabinet du MFA</i>	Objectif : Positionner le projet du Service d'authentification gouvernementale dans l'espace public, annoncer le déploiement et expliquer le projet	DCOM du MCN	Grand public	Fin-octobre
	Communiqué de presse (<i>à la discrétion du cabinet du ministre du MCN</i>) <i>Voir à s'arrimer avec le cabinet du MFA et du MTQ</i>	Objectif : Faire le bilan des premiers déploiement	DCOMS du MCN, du MFA et de la SAAQ	Grand public	Novembre 2022 (MFA) Février 2022 (SAAQ)

Annexe 3 - Séquence de communication

	Septembre 2022	Déploiement MFA	Novembre	Décembre	Déploiement SAAQ	Février
Site Québec.ca	- Actualité pour annoncer le début du déploiement - Mise en ligne d'une page d'information sur le Service d'authentification gouvernemental - Diffusion d'un tutoriel de connexion pour les citoyens		Actualité pour faire le bilan du 1 ^{er} déploiement au MFA.	Actualité pour annoncer le prochain déploiement		- Actualité pour faire le bilan 2^e déploiement à la SAAQ. <i>Calendrier de déploiement pour la poursuite du projet</i>
Site du MO		MFA : Diffuser le tutoriel et les moyens pour communiquer avec le service à la clientèle	Actualité pour faire le bilan du 1 ^{er} déploiement au MFA.		SAAQ : Diffuser le tutoriel et les moyens pour communiquer avec le service à la clientèle	Actualité pour faire le bilan du 2^e déploiement à la SAAQ.
Médias sociaux	Une publication pour annoncer la page d'information sur Québec.ca et le tutoriel de connexion sur la page LinkedIn du MCN et demande de partage sur les comptes des MO visés <i>Stratégie de publication de contenu à déterminer en collaboration avec les DCOM visées et la DCNG</i>	Veille et gestion des commentaires sur le sujet	Pertinence d'une publication sur le bilan du 1 ^{er} déploiement?		Veille et gestion des commentaires sur le sujet	Une publication pour annoncer la séquence de déploiement sur la page LinkedIn du MCN et demande de partage sur les comptes des MO visés <i>Stratégie de publication de contenu à déterminer en collaboration avec les DCOM visées et la DCNG</i>
Plateforme collaborative SharePoint du MCN	Annoncer la disponibilité des outils :		Ajustements en vue du prochain	Diffusion des documents		Ajustements en vue du prochain

à l'usage exclusif des MO	- Foire aux questions. - Aide-mémoire. - Documents de formation. - Série de webinaires. - Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels). - Modèle de papillon avec texte et image pour insertion dans des communications en format papier.		déploiement (solution, approche, matériel pour le service à la clientèle)	ajustés, au besoin.		déploiement (solution, approche, matériel pour le service à la clientèle) <i>Calendrier de déploiement pour la poursuite du projet</i>
Relations publiques	- Lignes de presse au plan gouvernemental - Document de type « questions-réponses »	- Brefpage technique - Point de presse	- Communiqué de presse (bilan du déploiement) - Bonification des documents (lignes de presse et Questions-Réponses) selon l'expérience vécue avec le 1^{er} déploiement			- Communiqué de presse (bilan du déploiement) - Bonification des documents (lignes de presse et Questions-Réponses) selon l'expérience vécue avec le 2^e déploiement <i>Annonce du calendrier de déploiement pour la poursuite du projet</i>
Forum des sous-ministres			- Présentation sur les déploiements prévus - Stratégie de gestion du changement - Stratégie de communication			
Page de connexion de clicSÉCUR				Diffusion d'un bandeau d'information qui réfère à la page sur le Service d'authentification gouvernementale (expliquer la cohabitation des deux solutions)		

Communications administratives de l'organisation visée	MFA : Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, papillon, etc.).		SAAQ : Communication personnalisée (notification par courriel ou texto ou autre mode de communication par les MO consommateurs, papillon, etc.). <i>*Selon la fréquence des communications établie avec la clientèle cible.</i>		À établir avec le prochain MO visé, selon le calendrier de déploiement.
--	---	--	--	--	---

Annexe 3 - Séquence de communication

		Déploiement MFA ^{1 2}		Déploiements MFA ³ et SAAQ	
	Octobre	Novembre	Décembre	Janvier 2023	Février
Site Québec.ca	Mise en ligne d’une page d’information sur le Service d’authentification gouvernementale		Diffuser le tutoriel et les moyens pour communiquer avec le service à la clientèle ⁴	Actualité pour annoncer les deux premiers déploiements (MFA et SAAQ).	- Actualité pour faire le bilan des deux premiers déploiements (MFA et SAAQ). - Calendrier de déploiement pour la poursuite du projet
Site du MO		Diffuser un message sur la page Web de la PES menant à la page de connexion du Service d’authentification gouvernementale		Fin décembre-janvier : Diffuser un message sur la page Web de la PES menant à la page de connexion du Service d’authentification gouvernementale	
Médias sociaux			- Une publication pour annoncer la page d’information sur Québec.ca incluant le tutoriel de connexion sur la page LinkedIn du MCN Stratégie de publication de contenu à déterminer en collaboration avec les DCOM visées et la DCNG - Veille et gestion des commentaires sur le sujet	- Publication pour annoncer les deux premiers déploiements - Veille et gestion des commentaires sur le sujet	Publication pour faire le bilan des deux premiers déploiements (MFA et SAAQ). Une publication pour annoncer la séquence de déploiement sur la page LinkedIn du MCN et demande de partage sur les comptes des MO visés Stratégie de publication de contenu à déterminer en collaboration avec les DCOM visées et la DCNG
Plateforme collaborative SharePoint du MCN à l’usage exclusif des MO	Annoncer la disponibilité des outils : - Foire aux questions. - Plateforme de formation (documents PDF en appui) - Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels).		Ajustements en vue du prochain déploiement (solution, approche, matériel pour le service à la clientèle) Diffusion des documents ajustés, au besoin.		- Ajustements en vue du prochain déploiement (solution, approche, matériel pour le service à la clientèle) - Calendrier de déploiement pour la poursuite du projet
Relations publiques	- Lignes de presse au plan gouvernemental - Document de type « questions-réponses »	Fin-novembre – début décembre (à la discrétion des cabinets) : - Breffage technique - Point de presse	Bonification des documents (lignes de presse et questions-réponses) selon l’expérience vécue avec le groupe restreint du MFA		MFA et SAAQ : - Communiqué de presse conjoint : bilan des 2 premiers lancements – arrimer avec le MFA et la SAAQ selon le moment de leur annonce du lancement de leur prestation électronique des services) - Bonification des documents (lignes de presse et questions-réponses) selon les expériences vécues - Annonce du calendrier de déploiement pour la poursuite du projet

¹ Le MFA ne souhaite pas faire de promotion pour le déploiement de sa PES et le déploiement du Service d’authentification gouvernementale de l’automne (31 octobre ou semaine du 14 novembre) pour éviter de semer la confusion (groupe restreint). Le MFA souhaite faire de la promotion lorsque leur PES sera proposée à un bassin de clientèles plus large, soit en janvier 2023.

² Sous réserve de la prise du décret sur l’évaluation des facteurs relatifs à la vie privée et les règles de sécurité.

³ Lorsque la prestation électronique de services sera rendue disponible à un bassin de clientèles plus large.

⁴ Un guide de connexion pour le groupe restreint d’utilisateurs de la prestation électronique de services du ministère de la Famille (MFA) sera diffusé par des envois personnalisés.

Forum des sous-ministres		À confirmer après la formation du nouveau conseil des ministres : • Présentation sur les déploiements prévus • Stratégie de gestion du changement • Stratégie de communication			
Page de connexion de clicSÉCUR			Diffusion d'un bandeau d'information qui réfère à la page sur le Service d'authentification gouvernementale (expliquer la cohabitation des deux solutions).		
Communications administratives de l'organisation visée			MFA et SAAQ : Communication personnalisée (lettre qui sera déposée dans Mon dossier pour les citoyens qui ont déjà créé un compte avec le MO - notification par courriel ou texto ou autre mode de communication par les MO consommateurs). Insertion d'un papillon dans les envois postaux, si déjà prévu par le MO. etc.).*Selon la fréquence des communications établie avec la clientèle cible.		À établir avec le prochain MO visé, selon le calendrier de déploiement.

Service québécois d'identité numérique (SQIN)

Comité stratégique

2022-11-08



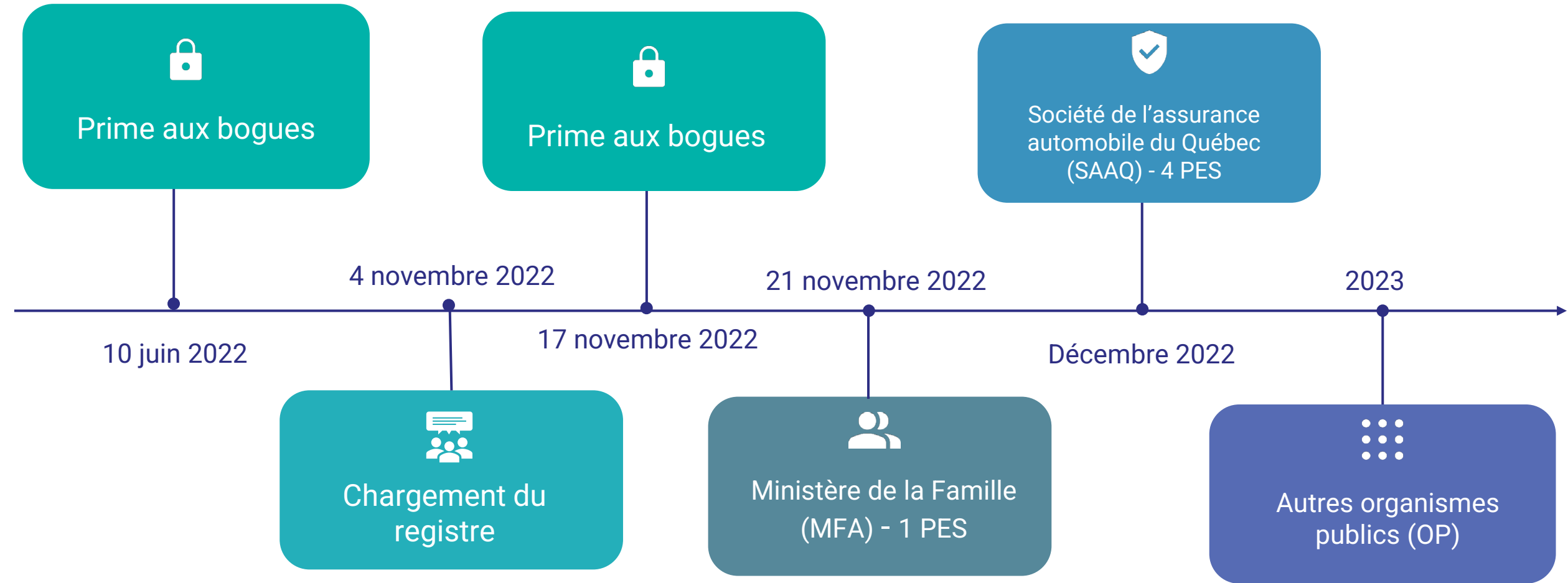
3. États de situation

- Rappel des priorités
- Grands jalons
- Activités juridiques
- Collaboration pancanadienne – SQIN 2
- SCT Canada – SQIN 1

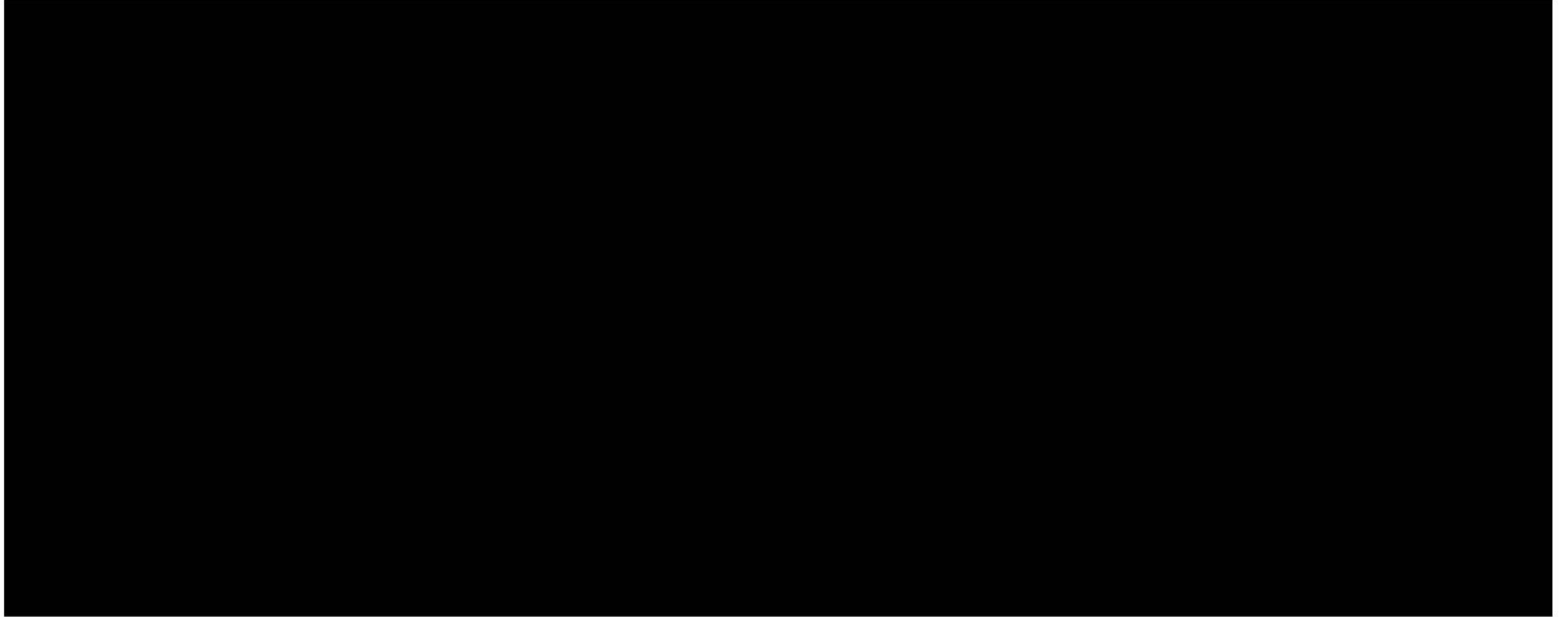
3.1 Programme SQIN - Les priorités

1. Les livraisons du MFA et de la SAAQ – SQIN 1
2. Les travaux prioritaires de 2023 – SQIN 1
3. Les travaux relatifs à SQIN 2
4. La collaboration pancanadienne – SQIN 2
5. L'intégration du SAG aux PES du fédéral – SQIN 1

3.2 Grands jalons



3.3 Activités juridiques





3.4 Présentation d'un projet en identité numérique de la Colombie-Britannique (C.-B.)

3.5 SCT Canada - SQIN 1 - Rencontres de l'automne 2022

Travaux: évaluation du SAG en vertu du Cadre de Confiance Pancanadien (CCP)

- 22 septembre - Présentation par SCT Canada ayant pour objectifs de:
 - présenter le mandat et les membres du comité de travail
 - convenir d'un horaire pour les séances du comité et donner un aperçu du plan de travail (fréquence: 1 rencontre hebdomadaire si possible)
- 6 octobre: Rencontre pour présenter le processus d'évaluation et les documents afférents
- 13 octobre: Présentation par le MCN du programme SQIN et du SAG
- 20 octobre: Période de questions concernant les cahiers de preuves à remplir

Prochaines étapes:

- Poursuivre les travaux visant à déposer le premier cahier de preuves concernant les politiques, directives, etc. de l'organisation et du projet (date de dépôt à confirmer)
- Participer aux prochaines rencontres et prendre connaissance des prochains cahiers



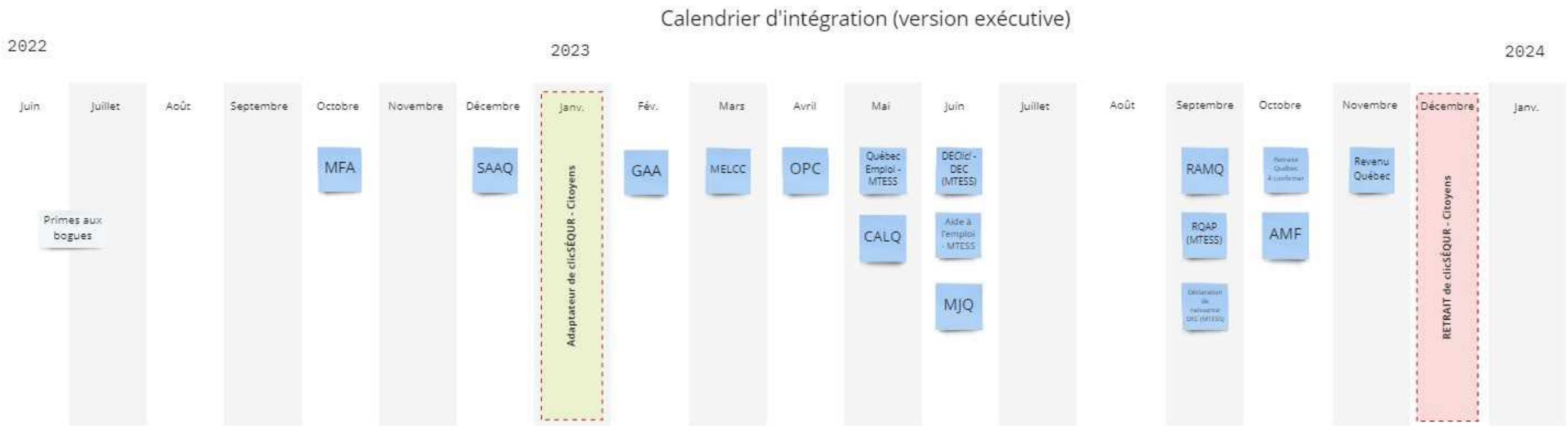
Intégration des OP

- Calendrier de déploiement

Orientations d'intégration - rappel

1. ClicSÉQUR sera décommissionné en décembre 2023 mais, pour Revenu Québec (RQ), cette cible pourrait être ajustée en fonction de la date de disponibilité de la source de confiance RQ requise pour ses PES.
2. Les migrations au SAG des PES utilisant actuellement clicSÉQUR sont prioritaires.
3. Toute demande d'intégration du SAG à de nouvelles PES doit être présentée au comité stratégique.
4. La planification des intégrations du SAG est établie de façon à répartir la charge de travail du service à la clientèle de manière équilibrée, en fonction de la volumétrie anticipée de demandes de soutien pour chacune des PES des OP.

Calendrier d'intégration officiel du 27 septembre



Activités en septembre - octobre 2022

- Rencontrer chaque OP consommateur de CSC afin de leur proposer le nouveau calendrier de déploiement
- Convenir avec eux qu'ils seront au rendez-vous!

Calendrier d'intégration de travail

Calendrier d'intégration pour approbation

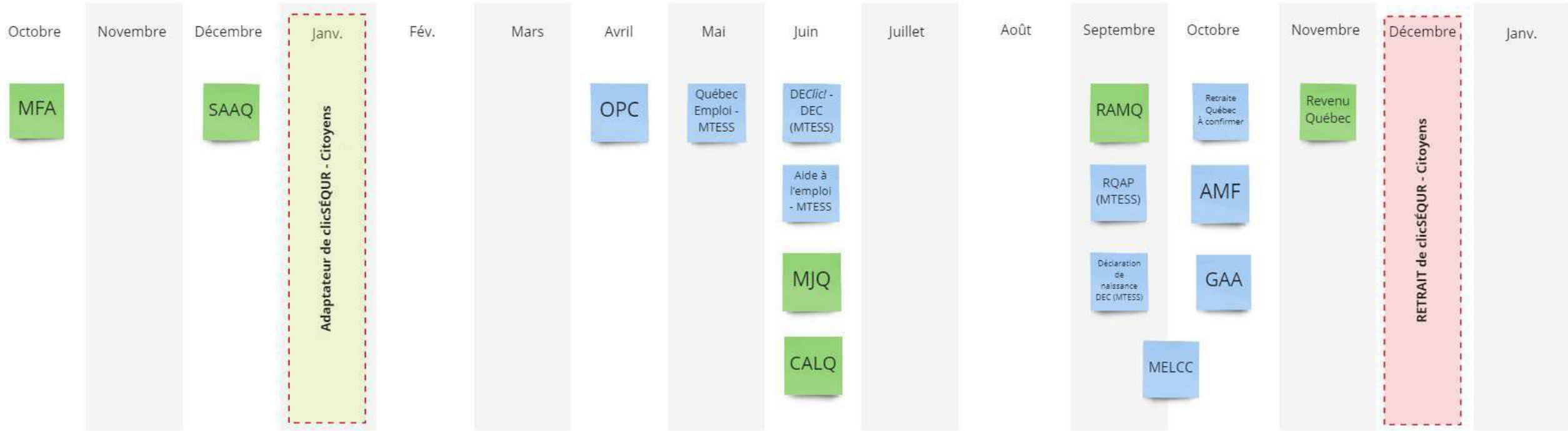
Légende

En bleu: Dates à reconfirmer

En vert: Dates confirmées

2023

2024



Constats



13

- Accumulation d'OP à l'automne 2023
- Planification de 6 mois d'intégration avant la mise en ligne
- Prérequis : PL 95

Plan d'action

14

- Effectuer le calcul de nos capacités basé sur notre nouvelle expérience avec MFA
- Confirmer les périodes favorables à leur intégration en fonction des capacités des SAC et des équipes d'intégration du MCN
- Impliquer les équipes du MESS lors des rencontres avec les OP
- Présenter les résultats et scénarios possibles au prochain comité stratégique



Service à la clientèle

- Besoins supplémentaires en heures rémunérées – état de situation

Besoins en effectifs supplémentaires – état de situation

20-21 octobre 2022

- Rencontre avec les représentants de la Direction principale des programmes sociaux et de santé du Sous-secrétariat aux politiques budgétaires et aux programmes du Secrétariat du Conseil du trésor pour répondre à leurs questions
- Transmission de la dernière version de travail du CT au SCT pour analyse

Novembre 2022

- Préparation d'une note de décision pour accompagner le CT
- Réception et intégration des commentaires du SCT
- Dépôt officiel du CT au SIG

Prochaine étape

- Obtention de l'approbation du SCT



Stratégie de communication

Présentations auprès des organismes publics

1. Début décembre 2022 : présentation du Service d'authentification gouvernementale au Forum des gestionnaires en technologie de l'information (FGTI).
2. À planifier : consultation auprès des DI afin de connaître les contacts pour présenter le SAG aux secteurs d'affaires détenteur des PES.

Merci!



Annexes

Portée Livraison Novembre et Janvier

Phases de l'intégration du Service d'authentification gouvernementale

Portée des livraisons

Fonctionnalités	Portée	Commentaires
Création du compte (inscription)	✓	Livraison Novembre
Connexion (déjà inscrit)	✓	Livraison Novembre
Vérification d'identité niveau 2		
Saisie des attributs d'identité	✓	Livraison Novembre
Acceptation des conditions d'utilisation	✓	Livraison Novembre
Consentements	✓	Livraison Novembre
Secrets RAMQ et RQ	✓	Livraison Novembre
Secret SAAQ		
Bulle technologique	✓	Livraison Novembre
Solution via CASA	✗	Remplacement de la bulle technologique (était prévu en janvier 2023)
Secret à usage unique par la poste	✓	Terminé à 80% / Dépendance avec Revenu Québec pour l'envoi par la poste – En développement
Registre d'attributs d'identité	✓	Livraison Novembre

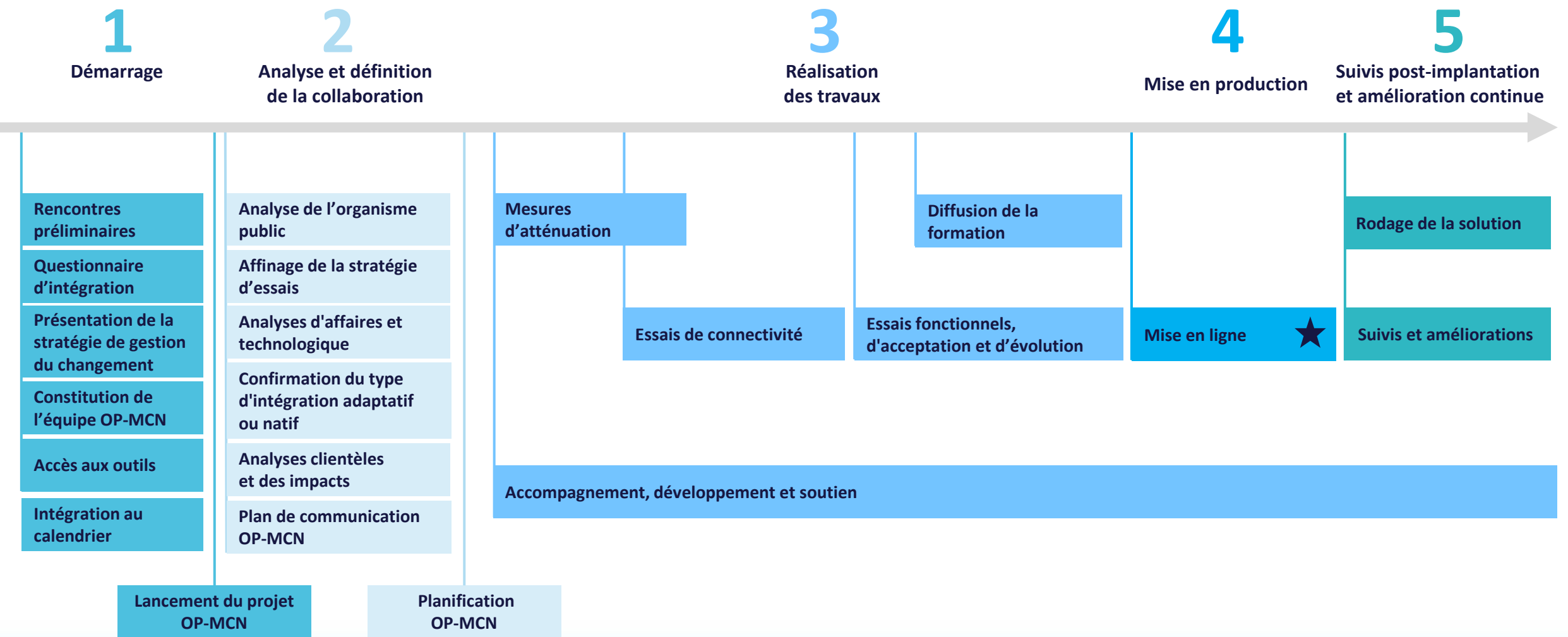
Portée des livraisons

Fonctionnalités	Portée	Commentaires
Infrastructure		
Environnements de production haute disponibilité	✓	Livraison Novembre/ Incluant la mise à l'échelle automatique en fonction de la charge
Environnements de développement (pipeline)	✓	Livraison Novembre/ Copie de sécurité selon les exigences de reprises après sinistre
Reprise en cas de sinistre (fondation)	✓	Délai de reprise de [redacted] dépendamment de quand arrive le sinistre relativement aux travaux d'automatisation réalisé.
Reprise en cas de sinistre (optimale)	🕒	Délai [redacted]
Copies de sécurités (Code, données, config. etc.)	✓	Livraison Novembre / Copie de sécurité [redacted]
Processus d'exploitation		
Gestion des incidents	✓	Livraison Novembre [redacted]
Processus manuels (ex: alerte, surveillance)	✓	Livraison Novembre [redacted]
Automatisation des environnements de développement et de production partenaires	✓	Livraison Novembre
Automatisation des processus (ex: alerte, surveillance)	🕒	Ex: Guide d'exploitation complet et recettes / T1 2023
Automatisation du déploiement des infrastructures	🕒	T1 2023
Essais de charge	✗	Surveillance [redacted]

Portée des livraisons

Fonctionnalités	Portée	Commentaires
Gestion de compte		
Modification du mot de passe	✓	Livraison Novembre
Suppression d'un compte, modification du courriel et consultation de l'historique d'activité par le citoyen	🕒	Livraison Mars – Avril 2023 (analyse impact et scénario alternatif et préparation des outils pour soutenir le SAC – arrimage avec le MESS)
Service à la clientèle		
Processus, procédures, matériel de formation, outil d'aide à la navigation	✓	Livraison Novembre
Envoi de l'adresse courriel à la SAAQ	✓	Validation [REDACTED] en cours
Journalisation (événements citoyen et pilotage)	✓	Livraison Novembre
Détection des menaces	✓	Livraison Novembre
Version mobile	✓	Site web accessible sur un appareil mobile – Expérience WEB dégradée sur appareil mobile
Traduction en anglais	🕒	Nouvelle Loi applicable à partir de juin 2023 / Analyse d'impact à faire - Les consentements seront traduits pour la livraison SAAQ

Phases de l'intégration du Service d'authentification gouvernementale



RENCONTRE DU COMITÉ STRATÉGIQUE DU PROJET « Accès bonifié aux PES citoyen et entreprise »		
COMPTE RENDU		
DATE : Le 27 septembre 2022 HEURE : De 8h00 à 9h00 LIEU : Teams		Ordre du jour 1. Adoption de l'ordre du jour – 5 min. 2. Approbation du point de décision de la rencontre du 16 août 2022 2.1 Points de suivi du compte rendu du 16 août 2022 3. États de situation – 10 min. 3.1 Programme SQIN – les priorités 3.2 Activités juridiques 3.3 Collaboration pancanadienne 3.4 SCT Canada 4. Intégration des organismes publics – 15 min. 4.1 Orientations d'intégration 4.2 Activités en septembre 2022 4.3 Calendrier de déploiement 4.4 Activités en octobre 2022 5. Service à la clientèle – 10 min. 5.1 Besoins supplémentaires en heures rémunérées - état de situation 6. Séquence de communication – 20 min. 7. Varia 8. Prochaine rencontre : 8 novembre 2022, 8h Annexe - Tableau de bord stratégique du 15 septembre 2022
PRÉSENCES M. Jean-François Ayotte (MCN) M. Jean-Philippe Beausoleil (RQ) Mme Carole Bédard (MCN) Mme Julie Bélanger (MCN) M. Martin Boucher (MCE) M. François Boulanger (RAMQ) Mme Catherine Boutin (MCE) Mme Caroline Foldes-Busque (SAAQ) M. Philippe Cayer (MFA) M. Jean-François Cloutier (RQ) – en remplacement de Carole Gagnon Mme Nathalie Croteau (RAMQ) Mme Odile Darbouze (RQ) Mme Caroline Drouin (MTESS) Mme Isabelle Guillemette (MCN) M. Jonathan Kelly (MCN) Mme Isabelle Laterreur (MCN) Mme Sonia Marceau (RAMQ) Mme Marie-Chantal Mbengue (MCN) Mme Marie-Pier Sauvé (MCE) Mme Mélanie Savard (MCN) Mme Nelly Savard (MCN) M. Steeve Tremblay (MCN)	ABSENCES M. Stéphane Asselin (MCN) M. Bernard Beaulieu (RQ) Mme Nicole Bourget (RQ) Mme Heather Dearborn (MCN) M. Alain Dumas (RQ) Mme Carole Gagnon (RQ) M. Patrick Gingras (MJQ) M. Pierre Lafleur (RAMQ) M. Yvan Latour (RAMQ) M. Stéphane Leclerc (MCN) M. Karl Malenfant (SAAQ) M. Vincent Métivier (MCN) Mme Claude Rochette (MCN) M. Gael Segal (RAMQ) M. Steeve Waterhouse (MCN) INVITÉ Mme Karine Morin Mme Nathalie Demers (MCN) Mme Sophie Perron (MCN)	

POINT	SUJET	DISCUSSION – ORIENTATION – DÉCISION
1.	Adoption de l'ordre du jour	L'ordre du jour a été présenté par Julie Bélanger et adopté à l'unanimité.
2.	Approbation du point de décision de la rencontre du 16 août 2022 2.1 Point de suivi du compte rendu du 16 août 2022	Le compte rendu ainsi que les points de suivi ont été approuvés par les membres du comité. M. Jean-Philippe Beausoleil mentionne que, dans le compte rendu de la rencontre du 16 août, M. Bernard Beaulieu doit être inscrit présent en tant que représentant de RQ (et non de RAMQ). Mme Julie Bélanger propose de faire la correction et de retourner le compte rendu aux membres du comité.
3.	États de situation 3.1 Programme SQIN – les priorités 3.2 Activités juridiques 3.3 Collaboration pancanadienne 3.4 SCT Canada	3.1 Mme Bélanger présente l'ordre de priorité des dossiers en cours du programme SQIN. Elle précise que la 3e priorité – les travaux relatifs à SQIN 2 – comprend les activités en lien avec le portefeuille numérique. 3.2 Mme Bélanger souligne qu'il reste les collègues de RQ à rencontrer pour leur présenter l'état de situation concernant le décret en préparation relativement au chargement du registre d'identité. La rencontre est prévue le 27 septembre en après-midi. Le décret serait déposé pour le prochain conseil des ministres. M. Jonathan Kelly précise qu'il s'agit de mettre de l'avant une mesure transitoire en parallèle des travaux requis en lien avec les règles de gouvernance pour répondre aux exigences de la CAI. Cette mesure permettrait d'y aller de l'avant avec la livraison au MFA. 3.3 M. Kelly mentionne qu'il rencontre ses homologues des autres provinces régulièrement au sujet de la collaboration pancanadienne en matière d'identité numérique. Les travaux de développement des composantes communes permettant l'interopérabilité entre provinces se poursuivent. Ces travaux technologiques se font en amont d'une entente officielle qui devrait se concrétiser une fois la période électorale passée. Lors de la dernière rencontre, il a rappelé que la priorité du Québec actuellement est de faire fonctionner SQIN 1. M. Kelly informe les membres qu'il surveille actuellement un 1^{er} déploiement relatif à l'identité numérique du côté de la Colombie-Britannique (CB). Il s'agit d'un projet pilote, prévu dans quelques semaines, dont les participants sont un nombre restreint d'avocats. En plus de tester l'aspect technologique (à noter qu'il s'agit essentiellement de la même technologie de base qui est utilisée au Québec) le projet a pour objectifs d'observer la réaction des utilisateurs (aspect gestion du changement) ainsi que d'obtenir des commentaires sur le volet juridique. M. Kelly songe à inviter des représentants de la CB à venir présenter ce projet pilote d'ici décembre 2022. 3.4 M. Kelly enchaîne en rappelant que l'équipe SQIN est en pourparlers avec le SCT Canada pour ce qui est de l'intégration éventuelle du SAG à des prestations électroniques de service du gouvernement fédéral.

POINT	SUJET	DISCUSSION – ORIENTATION – DÉCISION
	Intégration des organismes publics 4.1 Orientations d'intégration 4.2 Activités en septembre 2022 4.3 Calendrier de déploiement 4.4 Activités en octobre 2022	4.1 Mme Julie Bélanger rappelle les orientations d'intégration qui ont été entérinées par les membres du comité. Elle souligne que la 3^{ème} orientation vise à consulter les membres pour déterminer les impacts d'une nouvelle demande d'intégration sur le calendrier de déploiement. Elle mentionne également que la 4^{ème} vise à s'assurer que l'intégration dans deux grands organismes ne se déroulent pas en même temps afin de ne pas perturber les activités de service à la clientèle. Mme Caroline Drouin précise qu'il faut également considérer qu'il n'y aura pas de nouvelles intégrations de PES à clicSÉCUR. Elle demande que ceci soit mentionné dans la communication qui sera faite à la communauté des dirigeants de l'information pour les informer des orientations d'intégration. 4.2 et 4.3 Mme Bélanger présente les activités d'intégration prévues pour septembre 2022 de même que le calendrier de déploiement qui a été convenu lors des rencontres avec les organismes publics consommateurs, utilisateurs actuels de ClicSÉCUR. 4.4 Mme Bélanger présente les activités d'intégration prévues pour octobre 2022. Elle précise que celles-ci visent à s'assurer que le plan de déploiement est viable, qu'il tient la route pour la prochaine année. À ce stade-ci de la rencontre, M. Martin Boucher demande à Mme Drouin s'il serait pertinent de mettre en place un plan de contingence qui tiendrait compte de l'arrivée de nouvelles PES de même que des mouvements d'intégration des OP à Québec.ca. Mme Drouin précise que les demandes d'adhésion à clicSÉCUR sont tout de même peu nombreuses pour le moment et que la gestion des demandes devra se faire cas par cas. M. Kelly mentionne que, à partir de 2023, s'il y avait des collisions dans les séquences de déploiement, la pertinence d'élaborer un plan de contingence pourrait être revue. Il y aurait lieu alors soit de revoir le séquençement ou d'envisager du parallélisme en ajoutant des effectifs.
5.	Service à la clientèle 5.1 Besoins supplémentaires en heures rémunérées – état de situation	5.1 Mme Isabelle Laterreur présente un état de situation pour la demande rehaussement d'effectifs en lien avec le service à la clientèle. Elle mentionne que la rédaction d'un CT consolidé sera complétée pour le début d'octobre 2022. Mme Bélanger précise qu'un retour aux partenaires sera fait pour s'assurer d'une image commune de ce qui doit apparaître dans le CT en termes de nombre d'heures rémunérées et de financement associé. M. Kelly mentionne qu'il est important de souligner, lors de nos interventions auprès de nos autorités, que ce rehaussement d'effectifs pour le service à la clientèle du SAG est un besoin temporaire. Le grand volume d'appels de soutien étant dû, en grande partie, au fait qu'il n'y a pas de registre d'identité unique pour le moment au Québec et que des incohérences d'attributs entre les bases de données peuvent survenir pour certains citoyens.
6.	Séquence de communication	Mme Karine Morin introduit le sujet des communications en lien avec le déploiement du SAG, plus précisément pour les livraisons du MFA et de la SAAQ. Elle précise que les équipes de communication des partenaires ont été impliquées et que leurs commentaires ont été intégrés aux documents concernant le plan de communication. Elle mentionne que c'est l'équipe des communications du MCN, avec l'équipe du programme SQIN, qui produit l'information générale qui sera diffusée concernant le SAG. L'équipe du MCN sera en appui aux équipes de communication des OP pour ce qui est de la préparation de l'information spécifique s'adressant à leurs clientèles. Mme Morin précise que les documents relatifs aux communications seront transmis aux membres. Mme Nathalie Demers, responsable du volet communication du projet SQIN 1, présente un document concernant les moyens de communication. Elle informe les membres qu'une trousse de communication sera partagée avec les équipes de communications des partenaires et des organismes qui

POINT	SUJET	DISCUSSION – ORIENTATION – DÉCISION
		intégreront le SAQ à leurs PES. Mme Caroline Drouin veut s'assurer que le citoyen qui veut consommer une PES aura été avisé à l'avance de l'étape de création de compte obligatoire. Mme Morin mentionne que le tableau de séquence de communication est plus explicite à cet égard. Par exemple, elle explique qu'un message à l'intérieur d'un bandeau d'alerte est prévu dans la page d'accueil de clicSÉCUR pour répondre à ce besoin. Ce message pointera vers la page de Québec.ca qui explique ce qu'est le Service d'authentification gouvernementale. Un tutoriel de connexion sera également disponible. Mme Demers précise également que, par l'entremise des divers outils de communication, les citoyens seront renseignés à l'avance sur les informations dont ils auront besoin pour pouvoir se connecter à une PES gouvernementale via le SAG. Mme Caroline Foldes-Busque, à ce moment, rappelle qu'un citoyen ne peut créer un compte SAG au cas où il en aurait besoin. Il pourra le faire seulement lorsqu'il voudra se connecter à une PES.
7.	Varia	Mme Julie Bélanger rappelle aux membres qu'ils peuvent toujours lui faire part de préoccupations ou d'éléments dont ils voudraient discuter lors des rencontres du comité. Les membres n'ont qu'à lui transmettre des sujets qu'ils souhaiteraient voir inclure dans l'ordre du jour. Mme Foldes-Busque souligne qu'il serait souhaitable qu'une rencontre du comité se tienne au moins une semaine avant la date d'implantation au MFA pour voir si tous les paramètres favorables sont rencontrés afin de réussir l'implantation. Mme Bélanger réitère que, lorsque le décret sera approuvé, le calendrier de déploiement sera confirmé, une rencontre pourra être organisée pour présenter les prochaines étapes.
8.	Prochaine rencontre	8 novembre 2022, 8h
	ANNEXE	Tableau de bord stratégique du 15 septembre 2022

POINT	SUJETS – POINTS DE SUIVI	SUIVI	DATE D'INSCRIPTION DU POINT	RESPONSABLES	ÉTAT
6.	Orientations d'intégration des PES	Préciser les orientations d'intégration pour obtenir l'adhésion des membres du comité stratégique.	2022-08-16	MCN-SQIN	Terminé
		Transmettre une communication à la communauté TI lorsque les orientations seront définies et approuvées. 2022-09-27 : Ajouter dans cette communication qu'il ne peut plus y avoir d'intégration de ClicSÉCUR lors de nouvelles PES.	2022-08-16	MCN-SQIN : Isabelle Guillemette	À faire
7.	Correction au compte rendu de la rencontre du 16 août 2022	Retourner aux membres le compte rendu corrigé de la rencontre du 16 août. M. Bernard Beaulieu est représentant de RQ (et non de RAMQ). 2022-10-31 : Le compte rendu de la dernière rencontre a été corrigé et une nouvelle version transmise aux membres.	2022-09-27	MCN-SQIN	Terminé
8.	Présentation d'un projet en identité numérique de la Colombie-Britannique (C.-B.)	Vérifier la possibilité pour des représentants du gouvernement de la C.-B de présenter aux membres du comité leur projet pilote d'ici décembre 2022.	2022-09-27	MCN-SQIN	À faire
9.	Documents relatifs aux communications concernant le SAG	Transmettre aux membres du comité les documents de communication dont il a été question lors de la rencontre.	2022-09-27	MCN-SQIN	À faire
10.	Rencontre d'information à la suite de l'approbation du décret	Organiser une rencontre d'information pour les membres du comité lorsque le décret aura été approuvé et que le calendrier de déploiement pourra être officialisé.	2022-09-27	MCN-SQIN	À faire

POINT	SUJETS – POINTS DE DÉCISION	SUIVI	DATE D'INSCRIPTION DU POINT
1.	Implantation de la première livraison du SAG	Recommandation du scénario 3 pour l'implantation de la première livraison du SAG. Selon ce scénario, le lancement de la prime aux bogues aurait lieu le 10 juin et une mise en ligne de la solution SAG pour le MFA à la mi-août.	2022-04-22
2.	Orientations d'intégration du SAG au PES	La version des orientations intégrant les commentaires des membres a été transmise par courriel par Julie Bélanger le 22 août 2022. Aucun nouveau commentaire n'a été reçu. Les orientations ont été rappelées et confirmées lors de la rencontre du 27 septembre 2022.	2022-09-27

RENCONTRE COMITÉ STRATÉGIQUE PROGRAMME SERVICE QUÉBÉCOIS D’IDENTITÉ NUMÉRIQUE (SQIN)	
DATE : 8 NOVEMBRE 2022 HEURE : 8 H À 9 H ENDROIT : VISIOCONFÉRENCE – TEAMS	
Participants : • M. Jonathan Kelly (MCN) • M^{me} Julie Bélanger (MCN) • M. Steeve Waterhouse (MCN) • M^{me} Nelly Savard (MCN) • M^{me} Isabelle Guillemette (MCN) • M. Steeve Tremblay (MCN) • M. Stéphane Leclerc (MCN) • M. Jean-François Ayotte (MCN) • M^{me} Mélanie Savard (MCN) • M^{me} Heather Dearborn (MCN) • M^{me} Carole Bédard (MCN) • M. Martin Boucher (MCE) • M. Patrick Gingras (MJQ) • M^{me} Caroline Drouin (MESS) • M. Gaël Segal (RAMQ) • Mme Carole Gagnon (Revenu Québec) • M^{me} Nicole Bourget (Revenu Québec) • M. Karl Malenfant (SAAQ) • M^{me} Sonia Marceau (RAMQ) • M^{me} Nathalie Croteau (RAMQ) • M. Jean-Philippe Beausoleil (RQ) • M. Philippe Cayer (MFA) • M. Yvan Latour (RAMQ) • M^{me} Odile Darbouze (Revenu Québec)	
ORDRE DU JOUR	
1.	Adoption de l’ordre du jour – 5 min.
2.	Approbation du compte rendu de la rencontre du 27 septembre 2022 – 5 min
	2.1 Points de suivi du compte rendu du 27 septembre 2022
3.	États de situation – 30 min.
	3.1 Rappel des priorités
	3.2 Grands jalons
	3.3 Activités juridiques
	3.4 Collaboration pancanadienne
	3.5 SCT-Canada
4.	Intégration des organismes publics – 10 min.
5.	Service à la clientèle – 5 min.
6.	Stratégie de communication – 5 min.
7.	Varia
8.	Prochaine rencontre : 20 décembre 2022, 8h00
	Annexe : - Tableau de bord stratégique du 17 octobre 2022



Service d'authentification gouvernementale

Moyens de communication

Le 6 octobre 2022

Service d'authentification gouvernementale

Moyens de communication

Québec.ca

- Mise en ligne d'une page d'information spécifique
- Diffusion d'un tutoriel – À noter : Pour le groupe restreint d'utilisateurs de la prestation électronique de services du ministère de la Famille (MFA) cet automne, un guide de connexion leur sera transmis par des envois personnalisés
- Actualité pour annoncer les 2 premiers déploiements (MFA et SAAQ)
- Actualité pour faire le bilan des deux premiers déploiements



Service d'authentification gouvernementale

Moyens de communication

Site Web du MO

- Diffusion d'un message sur la page Web de la PES menant à la page de connexion du Service d'authentification gouvernementale

Médias sociaux (page LinkedIn du MCN, page Facebook et Twitter du gouvernement du Québec)

- Publication pour annoncer la page d'information incluant le tutoriel sur Québec.ca
- Publication pour annoncer les deux premiers déploiements
- Publication pour faire le bilan des deux premiers déploiements
- Veille et gestion des commentaires sur le sujet



Service d'authentification gouvernementale

Moyens de communication

Plateforme collaborative SharePoint du MCN à l'usage exclusif des MO (GdC)

- Foire aux questions
- Plateforme de formation (documents PDF en appui)
- Trousse du MCN pour alimenter les sections dédiées des intranets des MO (textes et visuels)



Service d'authentification gouvernementale

Moyens de communication

Relations publiques

- Lignes de presse au plan gouvernemental
- Document de type questions et réponses
- Breffage technique
- Point de presse
- Bonification des documents selon les expériences vécues
- Communiqué de presse (bilan, etc. – arrimage avec les MO)



Service d'authentification gouvernementale

Moyens de communication

Forum des sous-ministres

À confirmer après la formation du nouveau Conseil des ministres

- Présentation sur les déploiements prévus
- Stratégie de gestion du changement
- Stratégie de communication



Service d'authentification gouvernementale

Moyens de communication

Page de connexion de clicSÉQUR

- Diffusion d'un bandeau d'information qui réfère à la page sur le Service d'authentification gouvernementale de Québec.ca (mentionnant la coexistence des 2 solutions)

Communications administratives de l'organisation visée

- Communication personnalisée (lettre qui sera déposée dans Mon dossier pour les citoyens qui ont déjà créé un compte avec le MO - notification par courriel ou texto ou autre mode de communication par les MO consommateurs).