

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

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).

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.

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

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 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.

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

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'efficience 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 :
 - o affaires;
 - o communication et Web;
 - o gestion du changement;
 - o services à la clientèle;
 - o technologies de l'information.

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 **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.
- 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.

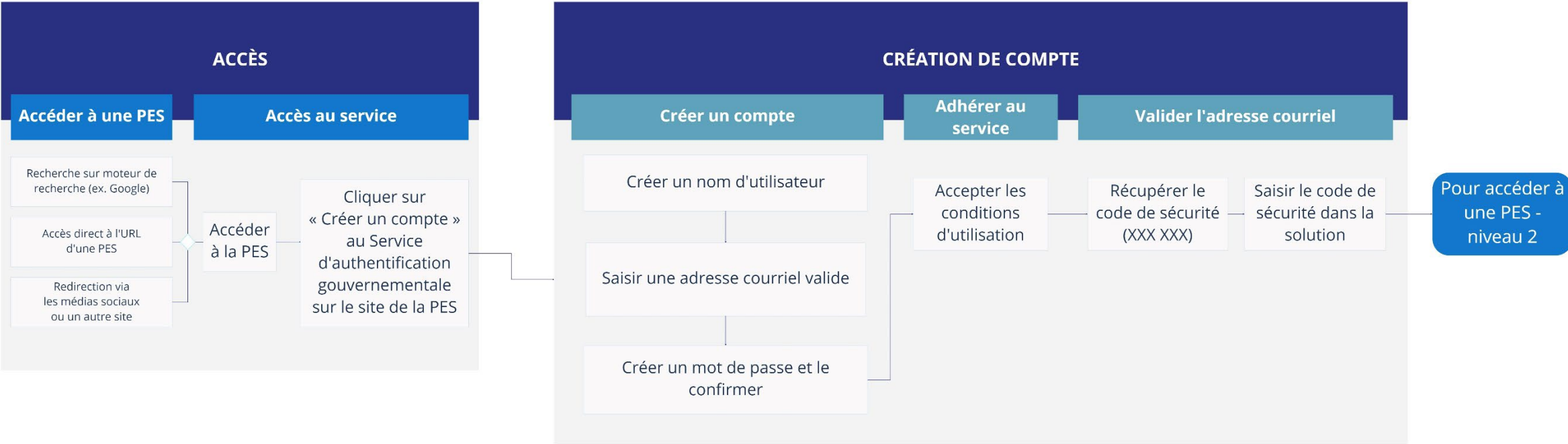
RECHERCHE ET ÉVALUATION

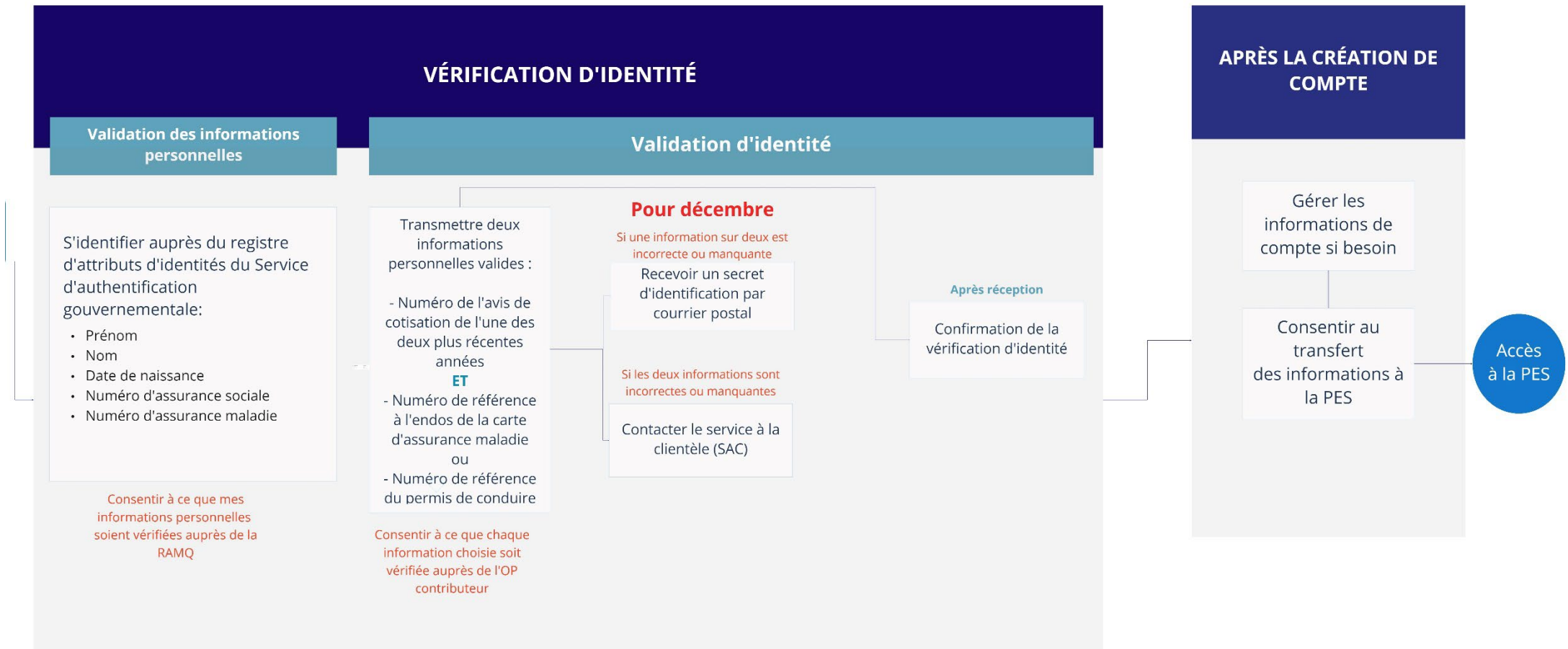
À venir dans la phase subséquente des travaux.

SÉQUENCE DE COMMUNICATION

Voir l'annexe 3.

Annexe 1 – Parcours utilisateur





Annexe 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.