

A hand holding a smartphone with a city skyline in the background.

POLITIQUES publiques

Priorité des conseils mixtes canadiens en matière d'identité numérique

Recommandations de politiques publiques

Préparé par le Groupe de travail sur les politiques publiques,
septembre 2018

Table des matières

1.	Contexte et objectifs	3
2.	Contexte	3
3.	Définitions clés.....	4
4.	Renseignements généraux sur le Groupe de travail.....	7
	Portée.....	7
	Membres du Groupe de travail	7
	Principaux documents	8
	Approche.....	8
	Principes directeurs	8
5.	Thèmes généraux en matière de responsabilisation	8
	Exigences en matière de protection des renseignements personnels et de sécurité.....	8
	Établissement et utilisation de l'identité numérique.....	9
	Preuve de l'identité essentielle	9
6.	Assurance de l'identité (ID)	10
	Discussion	10
	Rôles et responsabilités recommandés	10
7.	Assurance des justificatifs	11
	Discussion	11
	Rôles et responsabilités recommandés	11
8.	Enregistrement de l'identité (ID).....	12
	Discussion	12
	Rôles et responsabilités recommandés	13
9.	Accès aux services	13
	Discussion	14
	Rôles et responsabilités recommandés	14
10.	Avis et consentement	14
	Discussion	15
	Rôles et responsabilités recommandés	15
11.	Conclusion	16

Aux membres des conseils mixtes canadiens

À titre de coresponsables du volet des priorités en matière d'identité numérique, nous sommes heureux de présenter les recommandations suivantes en vue d'adopter une position stratégique pancanadienne sur la question des rôles et des responsabilités des secteurs public et privé en matière d'identité numérique. Nous estimons que cela nous rapproche de la transformation des services gouvernementaux, en permettant au gouvernement de transcender les frontières et en permettant aux Canadiens de participer à la société numérique en pleine croissance, avec confiance et en toute sécurité.

À l'issue de l'approbation des conseils mixtes de mettre sur pied un Groupe de travail sur les politiques publiques, nous avons lancé un appel de participants à tous les membres du Sous-comité sur la gestion de l'identité (SCGI) et des conseils mixtes. Le Groupe de travail a été créé en mai 2018; il est formé de 17 représentants des niveaux municipal, provincial et fédéral. Le groupe s'est réuni au cours de l'été 2018, et le présent rapport est le résultat de ses délibérations.

Misant sur les travaux actuels du Cadre de confiance pancanadien (CCP) et du SCGI, le Groupe de travail a établi trois principes directeurs :

- le droit d'une personne à une identité ne doit pas être compromis;
- la protection des renseignements personnels et la sécurité sont des éléments essentiels pour permettre aux Canadiens de participer avec confiance à la société numérique;

- la commodité et le choix sont des facteurs clés pour les citoyens.

En se fondant sur ces principes, trois thèmes généraux au chapitre de la responsabilisation ont été recommandés :

- la protection des renseignements personnels et la sécurité : le secteur public doit demeurer responsable de l'établissement des exigences juridiques et de la surveillance de la conformité;
- établissement et utilisation d'une identité numérique : pour répondre aux exigences en matière de commodité et de choix, les secteurs public et privé ont des rôles à jouer dans la prestation, la gestion et l'utilisation de l'identité numérique;
- preuve de l'identité essentielle (certificat de naissance et dossier d'arrivée dans le pays) : le secteur public doit maintenir la responsabilité de la délivrance d'une identité numérique.

Dans ce contexte, les recommandations détaillées reconnaissent l'importance du rôle du secteur privé. Nous sommes impatients de voir ce que la croissance et la collaboration futures dans ce domaine signifieront pour les Canadiens.

Nous remercions sincèrement le Groupe de travail pour son dévouement et sa volonté de s'attaquer à la question particulièrement importante de la pertinence des rôles des secteurs public et privé au chapitre de l'identité numérique.

Jackie Stankey

Directrice administrative par intérim, Province de l'Alberta, Service Alberta

Sophia Howse

Directrice administrative, Province de la Colombie-Britannique, Programme provincial de gestion de l'information sur l'identité

1. Contexte et objectifs

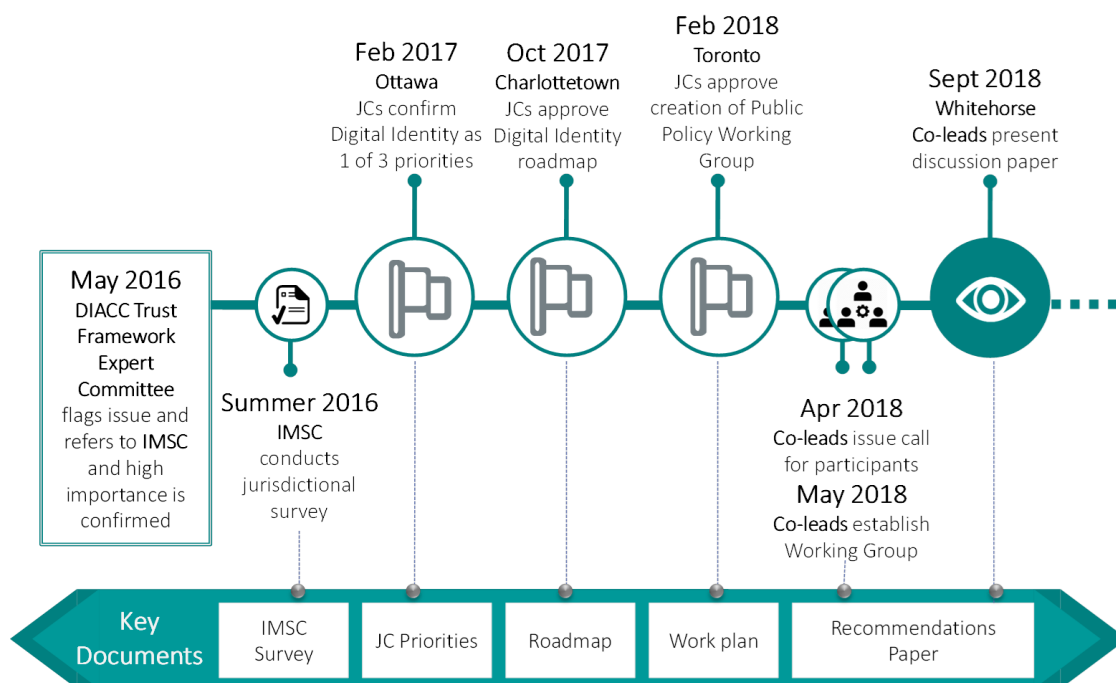
L'environnement de l'identité numérique évolue rapidement et, à mesure que l'identité passe du papier au monde numérique, les lignes de démarcation entre les secteurs public et privé s'estompent :

- les technologies perturbatrices changent le paysage identitaire et agissent dans l'environnement de l'identité;
- les gouvernements prennent des mesures pour corriger les défaillances et les lacunes du marché en fournissant des biens là où le secteur privé est peu enclin à en fournir;
- les nouvelles technologies donnent souvent lieu à de nouveaux biens et services.

Les objectifs du Groupe de travail sur les politiques publiques (GTPP) sont les suivants :

- évaluer et formuler des recommandations sur les rôles et les responsabilités appropriés des secteurs public et privé en matière de gestion de l'identité numérique;
- formuler des commentaires stratégiques sur la façon de faire progresser le cadre de fiabilité pancanadien.

2. Contexte



En mai 2016, la question des rôles appropriés des secteurs public et privé dans la gestion de l'identité a été soulevée par le Comité d'experts du cadre de confiance du DIACC. La question a été renvoyée au Sous-comité de la gestion de l'identité (SCGI), et les discussions subséquentes ont confirmé qu'il s'agissait là d'un domaine important qui nécessitait des recherches plus poussées.

À l'été 2016, avant la création du GTPP, le SCGI a effectué un examen intergouvernemental afin de clarifier sa position concernant les rôles et les responsabilités des secteurs public et privé, et de justifier les décisions. Les résultats ont été présentés dans le « document de travail : Rôles et responsabilités des secteurs public et privé ».

En février 2017, les conseils mixtes ont approuvé trois domaines prioritaires devant être traités diligemment, dont l'identité numérique. Deux coresponsables, soit celui de l'Alberta et celui de la Colombie-Britannique, ont été désignés pour planifier et coordonner les travaux dans ce domaine. En octobre 2017, les coresponsables ont présenté une feuille de route sur l'identité numérique et ont obtenu l'approbation des conseils mixtes pour aller de l'avant. L'un des volets de travail de la feuille de route était les « politiques publiques », et, à la réunion des conseils mixtes de février 2018, les coresponsables ont obtenu l'approbation d'entreprendre le travail dans ce domaine et ont établi le GTPP. La vision des conseils mixtes était que ce Groupe de travail mènerait des recherches, animerait des discussions et élaborerait des recommandations en vue d'adopter une politique pancanadienne sur la question du rôle des secteurs public et privé dans l'identité numérique. En avril 2018, un appel à participants au GTPP a été envoyé par courriel à tous les membres du SCGI et des conseils mixtes, et le groupe a été créé en mai 2018.

Le présent rapport, qui est le résultat des délibérations du GTPP, est présenté aux conseils mixtes en septembre 2018 pour examen, avec l'intention d'en demander l'approbation après la présentation des commentaires.

3. Définitions clés

La gestion de l'identité et de l'identité numérique sont des sujets complexes et en constante évolution. Un certain nombre de nouveaux termes sont entrés dans notre lexique; il existe des définitions largement acceptées pour certains termes, tandis que d'autres définitions sont moins normalisées. Les définitions adoptées par le SCGI en avril 2016 ont été utilisées aux fins du présent document. Le tableau ci-dessous présente les termes clés.

<i>Assurance</i>	Mesure du degré de certitude qui indique qu'une déclaration ou un fait est vrai.
<i>Authentification</i>	Processus d'établissement de la vérité ou de l'authenticité pour obtenir une assurance.
<i>Justificatif d'identité</i>	Objet physique ou électronique unique (ou identificateur) délivré à une personne ou à une organisation ou associé à un appareil (p. ex., clé, jeton, document, identificateur de programme).

<i>Assurance du justificatif</i>	L'assurance qu'une personne, une organisation ou un appareil a conservé le contrôle des justificatifs d'identité qui lui ont été confiés (p. ex., clé, jeton, document, identifiant) et que ces justificatifs d'identité n'ont pas été compromis (altérés, corrompus, modifiés, etc.).
<i>Preuve de l'identité essentielle</i>	Délivrée par une institution fédérale relativement à l'enregistrement d'un événement vital ou majeur, la preuve de l'identité essentielle sert à établir des renseignements d'identité de base comme le prénom, le nom de famille, la date de naissance et le lieu de naissance. Les certificats de naissance, les cartes de résident permanent et les certificats de citoyenneté sont des exemples de preuve de l'identité essentielle.
<i>Identité</i>	Une référence ou une désignation utilisée pour distinguer une personne, un organisme ou un appareil.
<i>Assurance de l'identité</i>	Une mesure du degré de certitude qu'une personne, une organisation ou un appareil est bien ce qu'il ou elle prétend être.
<i>Enregistrement de l'identité</i>	Relie une identité à un justificatif, c'est-à-dire relie la vraie personne au justificatif.
<i>Établissement de l'identité</i>	La création d'un dossier d'identité faisant autorité sur lequel d'autres peuvent compter pour les activités, les programmes et les services subséquents du gouvernement.
<i>Délivrance d'identité</i>	La création d'une preuve d'identité qui est émise à une personne et sur laquelle d'autres peuvent compter pour les activités, les programmes et les services subséquents du gouvernement.
<i>Vérification de l'identité</i>	La confirmation que les renseignements sur l'identité présentés concernent bien la personne qui fait la demande.
<i>Identité numérique de confiance</i>	La représentation électronique d'une personne, utilisée exclusivement par cette personne, pour recevoir divers services et effectuer des transactions en toute confiance. Une personne peut être une « personne physique » (p. ex., un particulier) ou une « personne morale », ce qui comprend les sociétés et autres organisations.

Personne vérifiée

Connaître (ou avoir un certain degré de certitude) le fait qu'une personne est réelle et identifiable, et qu'elle est vraiment la personne qu'elle prétend être.

4. Renseignements généraux sur le Groupe de travail

Portée

Le GTPP a été chargé d'évaluer les rôles et les responsabilités appropriés en ce qui a trait à l'identité numérique de confiance. Si l'on se réfère à la définition ci-dessus, il s'agit de la représentation électronique d'une personne, utilisée exclusivement par cette personne pour recevoir divers services et effectuer des transactions importantes en toute confiance.

Le GTPP a établi les cinq composantes suivantes d'une identité numérique de confiance, et les a utilisées pour l'analyse stratégique :

- **Créer une identité**

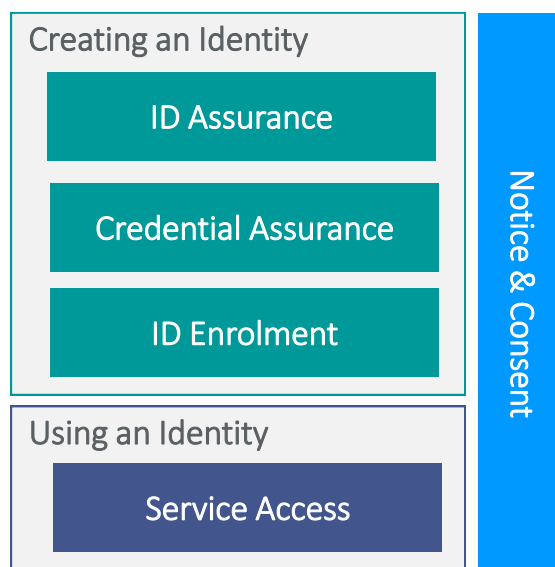
- *Assurance de l'identité (ID)* : vérification de l'identité de la personne qu'elle prétend être aux fins de l'établissement d'une identité numérique.
- *Assurance du justificatif* : les règles et les normes associées à un justificatif, afin qu'il soit sécurisé et fiable lors d'événements d'authentification futurs.
- *Enregistrement de l'identité (ID)* : la liaison d'une identité à un justificatif.

- **Utilisation d'une identité**

- *Accès aux services* : authentification d'une personne à un point de service, afin de veiller à ce que la personne est bien celle qu'elle prétend être et qu'elle peut avoir accès aux services.

- **Avis et consentement**

- *Avis et consentement* : déclenchés à de multiples moments lors de la création ou de l'utilisation d'une identité, informant une personne des pouvoirs en vertu desquels des renseignements personnels sont recueillis, de la façon dont les renseignements personnels seront communiqués, et demandant le consentement approprié pour procéder.



Membres du Groupe de travail

Le Groupe de travail comptait 17 participants, dont des représentants municipaux, provinciaux et fédéraux :

- 2 chefs d'équipe en Colombie-Britannique;
- 1 représentant d'une municipalité de l'Ontario;
- 5 représentants des 3 provinces suivantes : Alberta, Nouveau-Brunswick et Nouvelle-Écosse;

- 9 représentants fédéraux des ministères suivants : Emploi et Développement social Canada, Immigration, Réfugiés et Citoyenneté Canada et Secrétariat du Conseil du Trésor du Canada.

La participation au Groupe de travail était volontaire, et s'est déroulée au cours de l'été 2018.

Principaux documents

Le GTPP a tiré parti du document de travail du Sous-comité sur la gestion de l'identité (SCGI) ainsi que du Cadre de confiance pancanadien pour déterminer les composantes clés de la gestion de l'identité, là où il fallait fournir des éclaircissements sur les rôles et les responsabilités. (Voir le schéma à l'annexe I.)

Approche

Le GTPP a tiré parti du document de travail du SCGI pour mettre en évidence les points clés qui méritaient d'être examinés plus à fond. La matrice économique des biens publics par rapport aux biens privés, élaborée par V. Ostrom et E. Ostrom, a été utilisée lors des discussions comme moyen d'évaluer où se situent les cinq composantes de l'identité numérique et de déterminer quels sont les rôles appropriés pour les secteurs public et privé. (Voir l'annexe III pour plus de détails sur la matrice des biens publics par rapport aux biens privés.)

Principes directeurs

Les trois principes clés qui ont émergé des discussions du GTPP ont été appliqués pour définir les rôles appropriés des secteurs public et privé :

- les droits internationaux de la personne stipulent que le droit d'une personne à une identité ne peut être compromis;
- il est essentiel de répondre aux attentes des citoyens et de respecter les exigences législatives en matière de protection des renseignements personnels et de sécurité si l'on veut que les Canadiens puissent interagir avec le gouvernement en toute confiance et participer à la société numérique;
- la commodité et le choix en matière d'accès aux services sont des facteurs clés pour les citoyens, et les modèles de prestation de services doivent répondre à ces exigences.

5. Thèmes généraux en matière de responsabilisation

En se fondant sur les principes directeurs, le GTPP a élaboré quatre thèmes généraux en matière de responsabilisation qui s'appliquent à tous les éléments d'une identité numérique de confiance. Résumés ci-dessous, ils sont repris dans l'analyse plus détaillée de chaque composante.

Exigences en matière de protection des renseignements personnels et de sécurité

Compte tenu de l'importance d'assurer un niveau élevé de confiance dans les protocoles de protection des renseignements personnels et de sécurité et des risques importants de violation

de ces protocoles, le GTPP a jugé que le secteur public devait demeurer responsable de l'établissement des exigences juridiques ainsi que de la surveillance de la conformité.

Tous les services d'identité numérique, qu'ils soient offerts par le secteur public ou privé, devront se conformer à ces exigences.

Établissement et utilisation de l'identité numérique

Satisfaire les deux éléments de « de commodité et de choix pour les citoyens » exige que les secteurs public et privé jouent tous deux un rôle important dans la prestation des services. Ces services doivent être conformes au cadre réglementaire décrit ci-dessus.

Il est important que le secteur public continue de jouer un rôle dans l'établissement d'une identité numérique afin de veiller à ce qu'elles soient largement disponibles. Cependant, lorsqu'il n'y a pas de droit légal au service, le secteur privé peut jouer un rôle important dans la prestation et la gestion de l'identité numérique.

Preuve de l'identité essentielle

Au cours des discussions, il est devenu évident que les preuves de l'identité essentielles (certificats de naissance et dossier d'arrivée dans le pays) jouent un rôle distinct et spécial dans la création d'une identité, et qu'elles méritent d'être traitées séparément.

Les articles 6 et 16 de la Déclaration universelle des droits de l'homme stipulent que « Chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique. » Ainsi, toute personne a droit à une identité, et l'établissement de cette identité doit être considéré comme un bien public. Le maintien de la responsabilité à l'égard des documents de base (p. ex., certificats de naissance, d'immigration et de citoyenneté) dans le domaine public garantit que toute personne est en mesure d'obtenir une preuve de l'identité essentielle.

De plus, les conséquences d'une violation des données associées aux documents de base constituent une menace importante et peuvent entraîner une perte de la confiance du public dans la gestion gouvernementale des renseignements personnels. Encore une fois, cela milite en faveur du maintien par le secteur public de la responsabilité juridique et fiduciaire de l'établissement et de la protection de ces justificatifs de base.

Le fait de conserver les documents de base dans le domaine public permet de veiller à ce qu'il y ait un seul registre et que l'accès ne soit pas limité à certains groupes ou clients. Le fait d'avoir un seul registre dans chaque administration contribue à préserver l'intégrité de ce registre et limite les risques de fraude ou d'abus. De plus, si une identité fictive était découverte, il y aurait moins de sources faisant autorité à devoir être rapprochées.

Le GTPP a conclu que la responsabilité de la délivrance des justificatifs d'identité fondamentaux doit continuer d'incomber au secteur public et ne peut être déléguée au secteur privé. Cependant, il a été reconnu que le secteur privé pouvait ajouter de la valeur dans ce domaine en fournissant des services de gestion des justificatifs d'identité fondamentaux à la demande et au nom des

citoyens. Les cinq composantes ci-dessous ne tiennent pas compte de la discussion plus poussée sur les documents de base.

6. Assurance de l'identité (ID)

L'assurance de l'identité est une mesure du degré de certitude qu'une personne, une organisation ou un appareil est bien ce qu'il ou elle prétend être. La vérification de l'identité d'une personne pour savoir si elle est bien ce qu'elle prétend être est une première étape essentielle de l'établissement d'une identité numérique.

L'assurance de l'identité comprend la détermination des règles de vérification de l'identité d'une personne et l'établissement de son identité; p. ex., quels sont les types de documents requis, si une contre-vérification est nécessaire, etc. La rigueur requise varie selon le niveau d'assurance visé; p. ex., à des niveaux d'assurance inférieurs, l'autosurveillance peut être suffisante, tandis qu'à des niveaux plus élevés, il faut des preuves d'identité originales et possiblement une vérification en personne.

À la suite de la vérification, la personne est maintenant reconnue, et une identité numérique peut être créée, tout en offrant un niveau d'assurance clair.

Discussion

L'établissement d'une identité numérique fondée sur des preuves d'identité peut être la responsabilité du secteur public ou du secteur privé; p. ex., les banques qui établissent l'identité numérique d'un client ou les écoles qui établissent l'identité d'un élève. L'organisation pertinente serait chargée d'établir les normes relatives à l'événement de vérification et de se conformer aux exigences juridiques en matière de protection des renseignements personnels, de protection des données et d'avis et de consentement.

Rôles et responsabilités recommandés

Secteur public	<ul style="list-style-type: none">• Établir les lois, les normes et les politiques relatives aux justificatifs d'identité.• Veiller à ce que toutes les parties se conforment aux lois, aux normes et aux politiques.• Fournir, s'il y a lieu, des services de vérification.• Veiller à la gestion des normes du processus de vérification de leurs propres justificatifs d'identité.• Veiller à ce que les services d'assurance de l'identité soient conformes aux lois, aux règlements, aux politiques et aux normes.
Secteur privé	<ul style="list-style-type: none">• Peut fournir des services de vérification de l'assurance de l'identité à la demande du secteur public et au nom de ce dernier pour (à l'exception de l'assurance de l'identité de base).

-
- Veiller à la gestion des normes du processus de vérification de leurs propres justificatifs d'identité.
 - Veiller à ce que les services d'assurance de l'identité soient conformes aux lois, aux règlements, aux politiques et aux normes.
-

7. Assurance des justificatifs

L'assurance des justificatifs permet de confirmer qu'une personne, une organisation ou un appareil a conservé le contrôle des justificatifs d'identité qui lui ont été confiés (p. ex., clé, jeton, document, identifiant) et que ces justificatifs d'identité n'ont pas été compromis (altérés, corrompus, modifiés, etc.).

L'assurance des justificatifs a pour but de veiller à ce que les événements d'authentification futurs soient sûrs, sécurisés et difficiles à recréer. L'établissement des normes minimales qui régissent la vigueur du justificatif rendent cette confiance possible (p. ex., caractéristiques de sécurité pour un justificatif physique, normes relatives aux mots de passe).

Discussion

Aujourd'hui, les secteurs public et privé délivrent des justificatifs d'identité et établissent des normes pour l'assurance de ces justificatifs. En effet, le secteur privé est un acteur plus important dans ce domaine. En général, l'organisation émettrice établit les normes d'assurance de l'identité et veille à ce qu'elles soient respectées. Cependant, la délivrance de justificatifs ne se fait pas en vase clos, et le secteur public doit conserver la responsabilité de maintenir le cadre réglementaire qui protège les données d'identité des citoyens. Par exemple, il est recommandé que le secteur public établisse les règles et les règlements sur l'utilisation possible de l'information sur les justificatifs (p. ex., ce qui peut et ne peut pas être échangé) et que toutes les organisations émettrices reconnaissent et respectent ces règles. Les citoyens pourront ainsi avoir une bonne confiance à cet égard.

Dans ce contexte réglementaire, l'assurance des justificatifs d'identité demeurera probablement un domaine d'activité autant du secteur public que privé. En effet, l'écosystème doit fournir un éventail de justificatifs d'identité afin d'offrir aux citoyens des choix et une sécurité.

Rôles et responsabilités recommandés

Secteur public	<ul style="list-style-type: none">• Établir des lois, des normes et des politiques relativement aux justificatifs qui protègent la sécurité et les renseignements personnels.• Veiller à ce que toutes les parties se conforment aux lois, aux normes et aux politiques.• Établir des normes pour l'assurance des justificatifs d'identité délivrés par le gouvernement.
----------------	--

	<ul style="list-style-type: none"> • Se conformer aux exigences législatives, aux normes et aux politiques relativement aux justificatifs délivrés par le gouvernement.
Secteur privé	<ul style="list-style-type: none"> • Peut fournir des services d'assurance des justificatifs à la demande du secteur public et en son nom. Élaborer des normes d'assurance des justificatifs d'identité délivrés au nom de leur propre organisation. • Se conformer aux exigences législatives, aux normes et aux politiques relativement aux justificatifs d'identité.

8. Enregistrement de l'identité (ID)

L'enregistrement de l'identité relie une identité à un justificatif, ce qui relie la personne réelle au justificatif. Ce processus d'enregistrement peut désigner la liaison d'une nouvelle identité à un justificatif existant ou la délivrance d'un nouveau justificatif; par exemple, le service de l'Agence du revenu du Canada (ARC) du gouvernement fédéral lie l'identité d'une personne à un client authentifié existant au moyen de sa carte bancaire (aucune information d'identité n'est fournie par la banque); la British Columbia Services Card lie une nouvelle identité à un nouveau justificatif d'identité (la carte).

Discussion

Dans le contexte du cadre défini, dont il a été question dans la section sur l'assurance des justificatifs, les organisations des secteurs public et privé peuvent établir une identité numérique et procéder à l'enregistrement de l'identité. Cette organisation sera responsable de ce qui suit :

- déterminer si un justificatif existant répond aux exigences établies et peut être utilisé ou si un nouveau justificatif doit être délivré;
- veiller à ce que les nouveaux justificatifs d'identité répondent aux exigences établies;
- la liaison subséquente de l'identité avec le justificatif, comme précurseur de l'authentification et de l'accès aux services.

L'écosystème de l'identité numérique ouvre aussi des possibilités de partenariats public-privé. Par exemple, l'ARC utilise actuellement un modèle mixte d'une prestation de services offerte par les secteurs public et privé. Les clients peuvent ouvrir une session dans le site de l'ARC ou utiliser SecureKey Concierge, un service offert par une entreprise privée et qui leur permet d'utiliser leurs justificatifs d'identité délivrés par la banque. L'ARC termine le processus d'enregistrement de l'identité en demandant au client certains renseignements personnels (p. ex., le numéro d'assurance sociale, la date de naissance, le code postal et un montant tiré de la dernière déclaration de revenus). Une fois ces renseignements validés par l'ARC, un code de sécurité est envoyé par la poste pour terminer le processus d'enregistrement de l'identité qui lie le client à son justificatif d'identité préféré. En offrant un choix d'ouverture de session à l'aide des justificatifs d'identité, le gouvernement fédéral accroît la commodité de ses services en ligne pour les clients. De nombreuses personnes utilisent régulièrement leurs justificatifs d'identité en ligne pour effectuer des transactions opérations bancaires ou payer des factures; par conséquent, le fait

d'utiliser les mêmes justificatifs pour accéder aux services gouvernementaux en ligne permet aux clients de ne pas avoir à choisir un nom d'utilisateur et un mot de passe supplémentaires.

Cependant, le Groupe de travail a déterminé qu'il y a des secteurs précis où, selon lui, le secteur public devrait conserver la responsabilité :

- des services publics et de nature délicate (p. ex., services de santé, d'éducation et sociaux);
- lorsque le justificatif peut être utilisé pour modifier des données de base et que les effets en chaîne peuvent être importants.

Que l'identité soit établie par le secteur public ou privé, la responsabilité de lier l'identité à un justificatif et, éventuellement, d'émettre un nouveau justificatif peut être déléguée à un tiers, étant entendu que les exigences réglementaires continuent d'être respectées.

Rôles et responsabilités recommandés

Secteur public	<ul style="list-style-type: none">• Veiller à établir des lois, des normes et des politiques sur l'enregistrement de l'identité qui protègent la sécurité et les renseignements personnels.• Veiller à ce que les exigences réglementaires relatives à l'enregistrement de l'identité soient respectées.• Veiller à la gestion et à l'intégrité des processus de délivrance et de liaison des justificatifs d'identité délivrés par le secteur public.• Veiller à ce que les exigences réglementaires relatives à l'enregistrement de l'identité soient respectées.
Secteur privé	<ul style="list-style-type: none">• Veiller à ce que les exigences réglementaires relatives à l'enregistrement de l'identité soient respectées.• Veiller à la gestion des processus de liaison et de délivrance des justificatifs d'identité délivrés par le secteur privé.

9. Accès aux services

L'accès aux services désigne une situation où une personne présente un justificatif dans le but d'avoir accès à un service. Lorsque le fournisseur de services (ou la partie qui se fie au justificatif) reçoit l'information sur les justificatifs, il détermine s'il est fiable ou non afin de confirmer que la personne qui demande le service est bien celle qu'elle prétend être. Cette détermination sera fondée sur le niveau connu d'assurance de l'identité et du justificatif ainsi que sur la tolérance au risque du fournisseur de services. Si l'identité est authentifiée avec succès, le fournisseur de services confirme ensuite que l'accès est autorisé.

L'accès aux services peut être un événement ponctuel ou déclencher un enregistrement aux services plus constant.

Discussion

Dans ce cas-ci, le fournisseur de services est propriétaire du service et des règles qui régissent les justificatifs auxquels on doit faire confiance. La détermination des justificatifs devant être acceptés sera fondée sur l'évaluation, par les propriétaires de services, du niveau d'assurance requis pour le service en question. Par exemple, un accès à des dossiers médicaux exigerait probablement un niveau d'assurance très élevé, alors que l'inscription à un bulletin électronique pourrait ne pas en exiger.

Les fournisseurs de services peuvent provenir du secteur public ou privé, et il n'y a pas de différence dans leurs rôles; il incombe à chaque partie qui se fie à un justificatif d'établir des normes d'accès et de veiller à ce que les justificatifs présentés par la personne satisfassent à ces règles

Rôles et responsabilités recommandés

Secteur public	<ul style="list-style-type: none">• Déterminer les niveaux d'assurance requis pour les services gouvernementaux et veiller à ce que les exigences relatives à l'enregistrement aux services soient respectées.• Veiller à ce que la bonne identité numérique corresponde au bon destinataire des services gouvernementaux ou y soit reliée.
Secteur privé	<ul style="list-style-type: none">• Déterminer les niveaux d'assurance requis pour des services donnés et veiller à ce que les exigences relatives à l'enregistrement aux services soient respectées.• Veiller à ce que la bonne identité numérique corresponde au bon destinataire du service.

10. Avis et consentement

Les termes « avis et consentement » font référence à la façon dont les personnes sont informées de la manière dont leurs renseignements sont recueillis, utilisés et communiqués ainsi qu'aux choix qui leur sont offerts à cet égard. Dans un avis, les contrôleurs des renseignements personnels doivent fournir des énoncés clairs et facilement accessibles au sujet de leurs pratiques et de leurs politiques. Le secteur public doit émettre un avis (bien que ce dernier doive aussi demander le consentement) et le secteur privé doit demander le consentement. Pour que le consentement soit valable, l'utilisateur doit comprendre quels renseignements sont utilisés et à quelles fins. Autrement dit, la personne doit comprendre ce à quoi elle consent. En vertu de la législation fédérale, les organisations du secteur privé sont tenues d'obtenir le consentement des particuliers pour recueillir, utiliser et divulguer légalement des renseignements personnels dans le cadre d'activités commerciales, conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) fédérale et des lois sur la protection des renseignements personnels (*Personal Information Protection Act*) de la Colombie-Britannique et de l'Alberta, pour n'en nommer que quelques-unes. Sans consentement, les organisations ne sont autorisées à traiter des renseignements personnels que dans des circonstances limitées.

L'avis et le consentement peuvent être requis à de multiples points du processus d'identification numérique : vérification, authentification et enregistrement.

Discussion

La responsabilité de prévoir des processus adéquats concernant les avis et les consentements incombe à l'organisation qui recueille, stocke et échange des données. Aujourd'hui, ces processus sont régis par un cadre juridique. Même si le secteur public pourrait fournir davantage de conseils sur le consentement valable et ses conséquences, au bout du compte, si un citoyen est conscient des risques, comprend les répercussions et les accepte, c'est son droit de le donner.

Il est important de noter qu'il existe des règlements qui limitent, entre autres, l'utilisation par des tiers des renseignements relatifs à l'identité. Il existe des exemples dans d'autres industries où le secteur privé respecte les cadres juridiques et les exigences relatives à la façon dont les renseignements relatifs à l'identité sont traités, comme la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, qui est supervisée par le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE).

Par ailleurs, le public s'inquiète de plus en plus des violations à la sécurité. Il incombe à l'organisation qui recueille des renseignements d'aviser les sources de ces renseignements et leur propriétaire. À l'heure actuelle, en vertu de l'article 10 du projet de loi S-4, intitulé la *Loi sur la protection des renseignements personnels numériques*, des règlements visant les organisations sont élaborés, pour ce qui est du contenu de l'avis et de la divulgation sans consentement.

Rôles et responsabilités recommandés

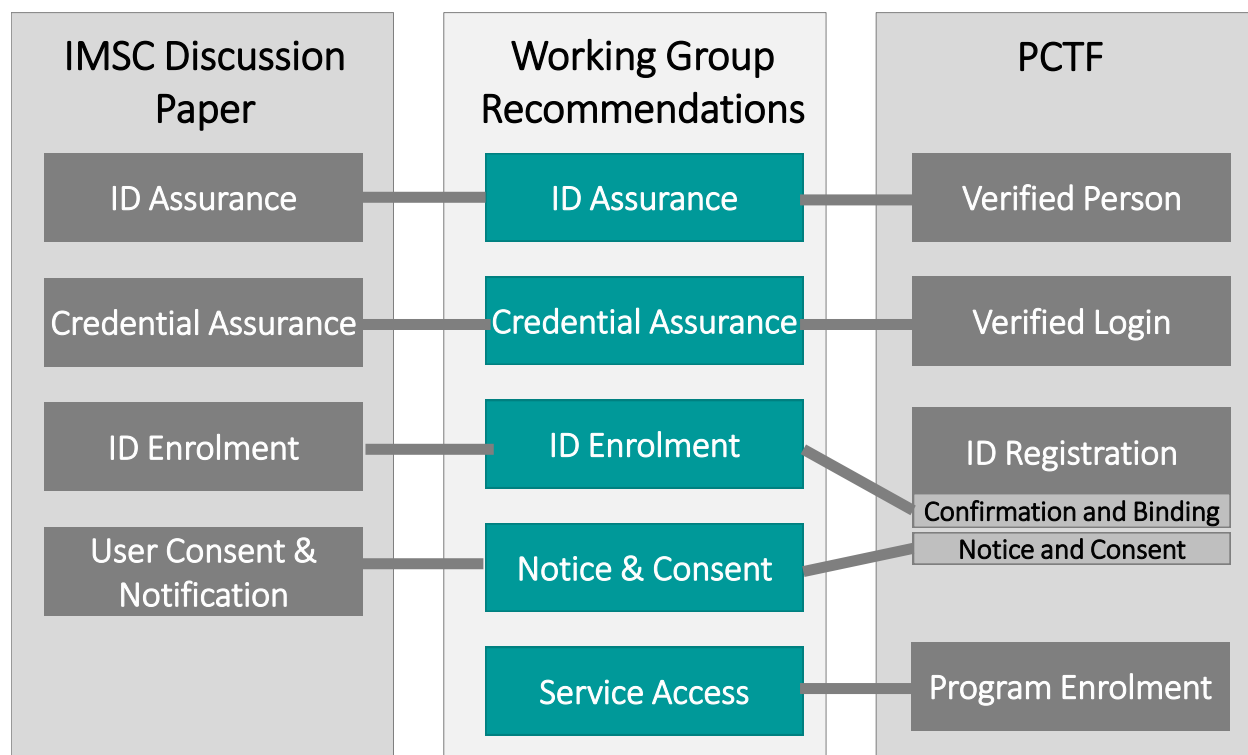
En particulier, les rôles et les responsabilités en matière d'avis et de consentement relèvent de la sphère de la protection des renseignements personnels et sont déjà bien définis dans la législation. S'appliquent les lois actuelles sur la protection des renseignements personnels numériques et la protection des renseignements personnels, ainsi que la LPRPDE (au niveau fédéral) et les lois sur la protection des renseignements personnels et la sécurité à l'échelle provinciale.

Secteur public	<ul style="list-style-type: none">• Veiller à établir le cadre réglementaire pour ce qui est des avis et des consentements.• Veiller au respect des règlements.• Veiller à mettre en place une tribune où les citoyens pourront exprimer leurs préoccupations.• Veiller à ce que le processus d'avis et de consentement soit conforme aux règlements.
Secteur privé	<ul style="list-style-type: none">• Veiller à fonctionner conformément aux lois pertinentes.

11. Conclusion

Être reconnu par son pays devant la loi et avoir une identité dans son pays sont des droits de la personne. Par conséquent, fondamentalement, l'identité numérique est un bien public. Au Canada, en établissant votre identité, vous êtes automatiquement inscrit aux programmes et services offerts par le gouvernement. Il y a aussi d'autres services comme l'éducation et les banques qui ne sont pas des droits, mais des privilèges, et qui, par conséquent, peuvent aller au-delà du domaine public et faire appel au secteur privé. Tout au long de la discussion, un thème surgissait constamment : la responsabilisation. Le fournisseur de services doit être tenu responsable en cas de violations à la confiance ou à la protection des renseignements personnels. Pour répondre aux demandes et aux attentes des citoyens en matière d'accès aux services et de participation à la société numérique, les fournisseurs de services doivent respecter une norme en matière d'identité numérique bien définie. La confiance et l'inclusion doivent faire partie d'une norme établie par le secteur public pour toutes les organisations qui délivrent, gèrent ou utilisent une identité numérique au Canada.

Annexe I – Mise en correspondance avec le document de travail du Sous-comité sur la gestion de l'identité (SCGI) et le Cadre de confiance pancanadien



Le processus de mise en correspondance a permis de cerner une lacune dans les composantes énoncées dans le document de travail du SCGI : l'accès aux services ou l'inscription aux programmes. Bien que le document du SCGI comprenne l'« enregistrement de l'ID », on estime qu'il y a une différence suffisamment importante entre le fait de lier une identité à un justificatif et l'utilisation subséquente du justificatif pour accéder aux services de manière à ce que les deux composantes soient séparées. (La personne X a un certificat de naissance de l'Ontario et peut donc créer un permis de conduire.) Une personne dont l'identité a été vérifiée peut accéder à un service. (La personne X, qui a plus de 19 ans, a maintenant un permis de conduire. Elle est en mesure de conduire un véhicule et de l'alcool peut lui être servi.)

Le terme « accès aux services » a été choisi à des fins de clarification et pour le distinguer des composantes préliminaires de l'établissement de l'identité.

Annexe II – Matrice des biens publics et privés

Un bien privé est un produit qui doit être acheté pour être consommé, et la consommation par une personne empêche une autre personne de le consommer. En d'autres termes, un bien est considéré comme un bien privé s'il y a concurrence entre des personnes pour obtenir le bien en question et si la consommation du bien empêche quelqu'un d'autre de le consommer. Un bien privé est le contraire d'un bien public. Les biens publics sont généralement accessibles à tous, et la consommation par une partie ne dissuade pas une autre partie de l'utiliser. De plus, il ne peut pas être exclu de la consommation; il est impossible d'exclure quiconque de la consommation de ce bien. De nombreux biens publics peuvent être consommés gratuitement.

	Excludable	Non-Excludable
Rival	Private Goods <i>"Typical Goods"</i> (Clothes, Food, Flowers, etc.)	Common Goods <i>"Common Pool Resources"</i> (Mines, Fisheries, Forests, etc.)
Non-Rival	Club Goods <i>"Artificially Scarce Goods"</i> (Cable TV, Private Parks, Cinemas, etc.)	Public Goods <i>"Collective Goods"</i> (Air, News, Sunshine, etc.)

Dans le contexte de cette matrice, les services d'identité numérique sécurisés entrent dans le quadrant des « biens publics ». Presque tous les biens publics sont considérés comme des biens non rivaux et ne pouvant pas être exclus de la consommation. La caractéristique « non rivale » signifie que la disponibilité d'un produit ou d'un service n'est pas réduite au fur et à mesure que les gens le consomment. Quand un produit ou un service ne peut pas être exclu de la consommation, cela signifie qu'il est impossible de le fournir sans le rendre disponible à de nombreuses personnes. Par conséquent, un bien public doit être disponible pour tout le monde, et sa quantité ne doit pas être limitée. Cependant, l'identité numérique n'est pas de même mesure d'une identité à l'autre et, selon le degré d'assurance, elle peut ou non être jugée suffisante pour permettre l'accès à un service particulier. Par exemple, le fait d'être né au Canada vous donne droit à certains droits et à certains services, mais il incombe à la personne de fournir des preuves au moyen d'un certificat de naissance ou de documents d'immigration. Pour conclure, l'on peut dire que l'identité numérique entre dans la catégorie d'un bien semi-public, tout comme les bibliothèques, les musées et les services éducatifs, puisqu'elle n'est pas rivale et qu'en quelque sorte elle ne peut pas être exclue de la consommation.

Annexe III – Liste des participants au Groupe de travail

Coprésident du Groupe de travail sur l'identité numérique

Jackie Stankey, gouvernement de l'Alberta

Sophia Howse, gouvernement de la Colombie-Britannique

Chefs d'équipe

Roxanna Dehghan, gouvernement de la Colombie-Britannique

Sharon McLean, gouvernement de la Colombie-Britannique

Gouvernement fédéral

Caroline Cossette, Service Canada

Elizabeth Dussault, Service Canada

Adam Hayes, Immigration, Réfugiés et Citoyenneté Canada

Allison Littlefortin, Immigration, Réfugiés et Citoyenneté Canada

Michelle Richardson, Immigration, Réfugiés et Citoyenneté Canada

Teresa Reeve, Immigration, Réfugiés et Citoyenneté Canada

Marie-Christine Rousseau, Immigration, Réfugiés et Citoyenneté Canada

Lieu Yen, Immigration, Réfugiés et Citoyenneté Canada

Tim Bouma, Secrétariat du Conseil du Trésor du Canada

Ken McMillan, Secrétariat du Conseil du Trésor du Canada

Gouvernements provinciaux

Chantal Ritcey (également responsable des communications), gouvernement de l'Alberta

Scott Duff, gouvernement de la Nouvelle-Écosse

Roxana Azad, gouvernement de la Nouvelle-Écosse

Laura Offman, gouvernement de la Nouvelle-Écosse

Liane MacFarlane, gouvernement du Nouveau-Brunswick

Municipalités

Norm Synnott, Municipalité de Windsor