

Conseils mixtes du Canada  
Volet des priorités de l'identité  
numérique

Cadre  
de gouvernance  
de l'identité numérique

Version 1.0

Recommandations issues de l'atelier en  
personne

des 23 et 24 juillet 2019

# Table des matières

---

1. Contexte.....	3
2. Termes clés .....	4
3. Principes de conception du cadre de gouvernance .....	5
4. Résumé des principaux thèmes .....	6
5. Cadre de gouvernance pour les identités numériques au Canada .....	6
Thème 1 : Établissement des “règles” .....	8
Cadre de confiance pancanadien (CCP) .....	8
Législation fondamentale : Loi sur la protection des renseignements personnels .....	8
Hypothèses clés .....	8
Thème 2 : Reconnaissance des entités de confiance.....	9
Hypothèses clés .....	9
Thème 3 : Gouvernance des processus opérationnels.....	9
Hypothèses clés .....	9
6. Recommandations sur la responsabilisation .....	11
Thème 1 : Établissement des “règles” .....	11
Thème 2 : Reconnaissance des entités de confiance.....	12
Thème 3 : Gouvernance des processus opérationnels.....	12
Sommaire des responsabilités recommandées .....	14
7. Mise en correspondance avec les structures de gouvernance existantes .....	15
Forum mixte public-privé : Un CIANC actualisé .....	15
Responsable de l’identité numérique du secteur public de chaque administration : nouveau .....	15
Forum du secteur public : un SCGI restructuré.....	16
8. Autres recommandations .....	17
Identités juridiques .....	17
Évaluation réalisée par les administrations sur leur état de préparation quant à l’émission d’identités numériques .....	17
Rôle continu de l’ISAC .....	17

Déclaration des Conseils mixtes en matière d'identités numériques .....	18
Poursuite des ateliers en personne à ce niveau .....	18
9. Prochaines étapes .....	18
Immédiatement .....	18
Lorsque les responsables de l'IN sont désignés.....	18
Lorsque les responsables de l'IN et le CIANC recadré sont en place.....	18
Distribution .....	21
Répondants : .....	21
Introduction au sondage.....	22
DÉLAI : Veuillez retourner à Sharon.McLean@gov.bc.ca avant le 30 juin 2019.....	23
QUESTION 1 .....	23
QUESTION 2 .....	23
QUESTION 3 .....	24
QUESTION 4 .....	24
QUESTION 5 .....	24
QUESTION 6 .....	24
QUESTION 7 .....	24
COORDONNÉES (FACULTATIF) .....	24

## Aux membres des conseils mixtes canadiens

À titre de coresponsables pour le volet des priorités de l'identité numérique (IN), nous sommes heureux de présenter les recommandations suivantes pour un cadre de gouvernance de l'identité numérique au Canada.

Conformément à l'orientation des Conseils mixtes en février 2019, nous avons diffusé un sondage auprès des organismes publics et privés afin de recueillir des commentaires sur les questions essentielles suivantes :

- « **ce qui** » devrait être gouverné;
- « **comment** » il devrait être gouverné;
- « **qui** » devrait responsable de la gouvernance.

Nous avons reçu vingt-six réponses détaillées et trouvé trois grands thèmes de **ce qui** devrait être gouverné :

- **Établissement des règles d'intégration** : établir des critères clairs en vue d'obtenir une plus grande participation au paysage pancanadien de l'identité numérique.
- **Reconnaissance des entités de confiance** : les processus par lesquels les entités prouvent le respect des règles établies et sont, par conséquent, considérées comme fiables.
- **Gouvernance des processus opérationnels** : surveillance des services quotidiens de création, d'utilisation et de gestion des identités numériques.

### Recommandations sur la responsabilisation

Les trois thèmes ont encadré les discussions lors de l'atelier en personne d'une journée et demie en juillet et ancré les recommandations en matière de responsabilisation :

#### *Établissement des règles :*

- Secteur public : les lois habilitantes qui peuvent être nécessaires pour

permettre aux administrations d'émettre des IN;

- Forum mixte des secteurs public et privé : établir des critères de conformité au moyen du Cadre de confiance pancanadien

#### *Reconnaissance des entités de confiance :*

Il s'agit d'un domaine très complexe et les responsabilités peuvent être différentes et dépendantes, par exemple, si les entités sont du secteur public ou privé. Il était impossible d'examiner chacun de ces cas d'utilisation et on recommande ce qui suit :

- Forum mixte des secteurs public et privé : définir les exigences pour reconnaître les entités de confiance.

#### *Gouvernance des processus opérationnels :*

- Chaque entité de confiance (secteur public ou privé) : élaborer des politiques internes, concevoir leur programme et prendre des décisions en matière de technologie et d'architecture.

### Recommandations de structure

*Forum mixte public-privé : Un Conseil de l'identification et de l'authentification numériques du Canada (CIANC) actualisé*

- Le CIANC deviendra le forum mixte des secteurs public et privé, à condition qu'il n'y ait pas d'obstacles financiers à la participation de toutes les administrations.

*Responsable de l'IN : Une nouvelle orientation*

- Chaque administration devrait désigner un responsable de l'IN ayant l'autorité de représenter l'administration sur l'identité numérique et se concentrer sur la manière dont elle deviendra un émetteur d'IN.

*Forum du secteur public : Un Sous-comité de gestion de l'identité (SCGI) recadré*

- Il faudrait recadrer le SCGI pour l'harmoniser avec le rôle du forum mixte, en mettant l'accent sur l'état de préparation de l'administration à émettre des IN.

Nous remercions sincèrement tous ceux qui ont répondu au sondage ou participé à l'atelier. Nous croyons que les recommandations permettront d'accélérer les progrès vers l'ouverture de l'économie numérique croissante du Canada aux citoyens.

*Sophia Howse*

Directrice exécutif, Programme provincial de gestion de l'identité, Province de la Colombie-Britannique

*Alexandre Bourque*

Directeur de la mobilisation et de la surveillance, Cybersécurité, Secrétariat du Conseil du Trésor du Canada, gouvernement du Canada

# Cadre de gouvernance de l'identité numérique

Recommandations issues de l'atelier en personne des 23 et

24 juillet 2019

---

## 1. CONTEXTE

L'identité numérique (IN) est une priorité élevée pour les Conseils mixtes (CM) du Canada. En février 2019, les CM ont reconnu que des progrès importants ont été réalisés dans le volet de travail prioritaire sur l'identité numérique. Ils reconnaissent aussi que, pour réussir, il faudra ultimement établir un cadre de gouvernance robuste pour l'identité numérique au Canada. Les CM ont demandé aux coresponsables du volet de travail prioritaire sur l'identité numérique d'organiser un atelier en personne, avec les représentants de tous les intervenants clés, afin d'élaborer des recommandations pour un cadre de gouvernance des identités numériques au Canada. (Voir l'annexe I pour la liste des invités et des participants.)

Il a été déterminé que le cadre de gouvernance doit répondre aux trois questions clés ci-dessous :

- **QUELS** domaines devraient faire l'objet de gouvernance?
- **COMMENT** devraient-ils faire l'objet de gouvernance?
- **QUI** devrait en être responsable?

En reconnaissant que de nombreuses personnes et organisations ont eu d'importants commentaires, un sondage a été largement diffusé auprès des organismes publics et privés avant l'atelier en personne. Vingt-six réponses ont été reçues des gouvernements fédéral et provinciaux, du secteur privé et des organismes sans but lucratif. (Voir l'annexe II pour la distribution, les répondants et une copie du sondage.)

Les réponses ont permis d'encadrer les discussions à l'atelier et ont porté sur trois grands thèmes de ce qui devrait être gouverné dans le paysage canadien de l'identité numérique :

- les règles que devront suivre les organisations en vue de se joindre au secteur pancanadien de l'identité numérique;
- la reconnaissance des entités de confiance (diffuseur d'identité, fournisseur de réseau et fournisseur de service);
- les processus opérationnels liés à l'émission, l'usage et la gestion des identités numériques.

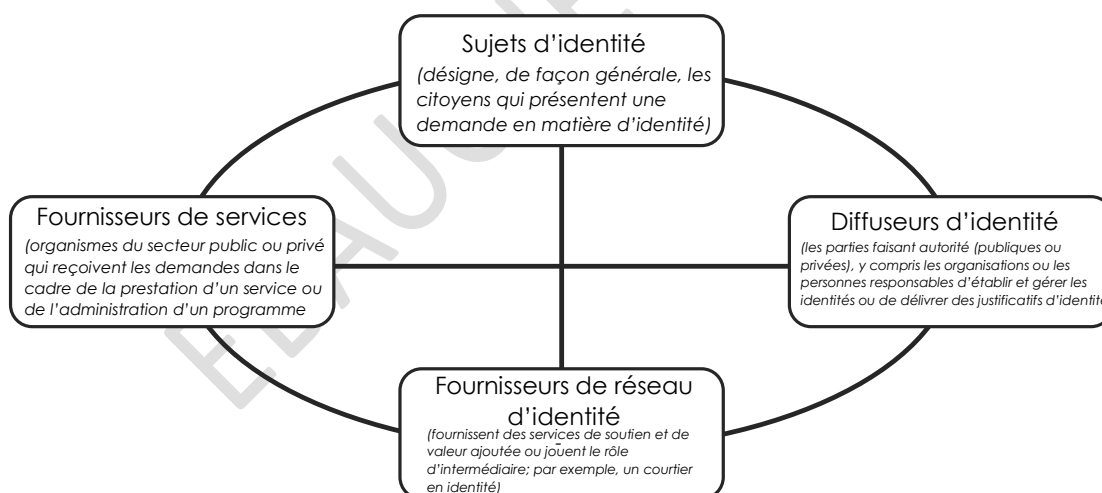
L'atelier en personne a eu lieu les 23 et 24 juillet 2019 à Toronto. Il fut dirigé par un animateur externe indépendant et soutenu par les coresponsables du volet de travail prioritaire sur l'identité numérique. Conformément aux directives des CM, des invitations ont été envoyées au gouvernement fédéral (Conseil du Trésor du Canada; Emploi et Développement social Canada; Immigration, Réfugiés et Citoyenneté Canada), à toutes les provinces, à deux territoires, aux municipalités, aux registres d'entreprises, au coprésident du groupe de travail opérationnel des CM, aux coprésidents du SCGI, aux organismes de délivrance de permis de conduire, aux entités de statistiques de l'état civil, à l'Institut des services axés sur les citoyens (ISAC), le Conseil de l'identification et de l'authentification numériques du Canada (CIANC), et aux représentants d'organismes du secteur privé des banques, des finances et de la technologie.

L'atelier a fait l'objet d'une grande ouverture et d'une grande participation dans son ensemble, ce qui a permis d'arriver à un consensus sur une série de recommandations ayant été réunies dans le présent rapport. Celles-ci seront présentées aux CM lors de la réunion du mois de septembre 2019.

## 2. TERMES CLÉS

Les termes suivants sont utilisés pour décrire les principaux acteurs :

- **Sujets d'identité** : désigne, de façon générale, les citoyens qui présentent une demande en matière d'identité, que ce soit à titre de particulier ou d'entreprise.
- **Diffuseurs d'identité** : les parties faisant autorité (publiques ou privées), y compris les organisations ou les personnes responsables d'établir et gérer les identités ou de délivrer des justificatifs d'identité. Également appelés fournisseurs de demandes, ils peuvent délivrer des demandes de sujets d'identité (le responsable de la demande ou son délégué) ou des parties utilisatrices qui dépendent de l'écosystème où ils participent.
- **Fournisseurs de services** : organismes du secteur public ou privé qui reçoivent les demandes dans le cadre de la prestation d'un service ou de l'administration d'un programme. (Aussi appelés clients des demandes d'identité ou parties utilisatrices.)
- **Fournisseurs de réseau d'identité** : les organismes qui fournissent des services de soutien et de valeur ajoutée ou jouent le rôle d'intermédiaire; par exemple, un courtier en identité.



- « **Entités** » est un autre terme utilisé dans le présent document. Il est utilisé comme un terme collectif pour les fournisseurs de services, les émetteurs d'identité et les fournisseurs de réseau d'identité. Une entité devient une « **entité de confiance** » lorsqu'elle a été reconnue comme confirmant les normes et critères qui régissent l'écosystème de l'identité numérique.

### 3. PRINCIPES DE CONCEPTION DU CADRE DE GOUVERNANCE

Le sondage proposait un certain nombre de principes pour orienter la conception du cadre de gouvernance. À l'atelier, on a également examiné des principes possibles tirés d'autres sources, comme la Déclaration sur les identités numériques des Conseils mixtes, le Document sur les politiques publiques, le profil du secteur public du CCP et du CIANC.

Les principaux principes de conception abordés pendant l'atelier sont décrits ci-dessous. Ces principes ont explicitement été élaborés en vue de déterminer comment concevoir le cadre de gouvernance. On a reconnu lors de l'atelier qu'il existait d'autres principes valides qui coexistent et s'appliquent à d'autres aspects des identités numériques, notamment l'élaboration de normes technologiquement agnostiques et la conception de services fournissant un accès pratique et sécuritaire aux citoyens.

On y reconnaît également que la responsabilité d'émettre les identités fondamentales (les actes de naissance et les attestations d'immigration) doit continuer d'incomber aux organismes responsables des données de l'état civil et à Immigration, Réfugiés et Citoyenneté Canada.

#### **Le cadre de gouvernance doit...**

- *suffire à préserver l'intégrité des identités numériques.* Le cadre de gouvernance doit veiller à la protection appropriée des données d'identité, sans être trop restrictif. Le cadre doit être assez souple pour favoriser l'innovation qui permettra au Canada d'être un chef de file. Plutôt que de mettre l'accent sur les règles, le cadre devrait viser à maximiser la collaboration;
- *être une coalition des partenaires consentants faisant autorité sur ceux qui l'adoptent.* Le cadre de gouvernance doit reconnaître l'importance de la collaboration dans l'ensemble du secteur de l'identité numérique. Une collaboration où l'on reconnaît les responsabilités partagées et où l'on travaille en vue d'établir des structures et des processus justes et appropriés. Les organismes qui choisissent de participer au secteur de l'IN doivent respecter les limites convenues;
- *mettre à profit les cadres existants en vue de permettre une véritable interopérabilité.* Le cadre de gouvernance doit mettre à profit les organismes, les normes et les cadres existants et réduire autant que possible le dédoublement des efforts. En mettant à profit les normes et les critères existants, la réalisation et le maintien d'une véritable interopérabilité deviennent plus réalistes;
- *veiller à ce que les particuliers aient le contrôle de leurs propres données, dans les limites de la loi.* Le cadre de gouvernance doit respecter les composantes essentielles de notification et de consentement afin de veiller à ce que les citoyens et les entreprises gardent le contrôle de leurs propres données, et qu'ils déterminent eux-mêmes comment les partager et les utiliser;
- *permettre aux fournisseurs de services de choisir à qui ils font confiance.* Le cadre de gouvernance doit promouvoir un langage uniforme et une compréhension commune des différents niveaux d'assurance. Toutefois, il doit également respecter le fait que les fournisseurs de services seront responsables de déterminer le niveau d'assurance dont ils ont besoin pour leur service et les entités dont ils doivent accepter des données.
- *être capable d'évoluer et de s'adapter.* Le cadre de gouvernance établi aujourd'hui doit également être viable dans l'environnement numérique de demain, qui est sur le point d'augmenter considérablement.



- *utiliser des mesures incitatives claires pour influencer le comportement des utilisateurs.* Le cadre de gouvernance devrait tenir compte des intérêts des diverses parties et mettre en place des mesures d'incitation pour accélérer l'adoption et l'acceptation à grande échelle.

## 4. RÉSUMÉ DES PRINCIPAUX THÈMES

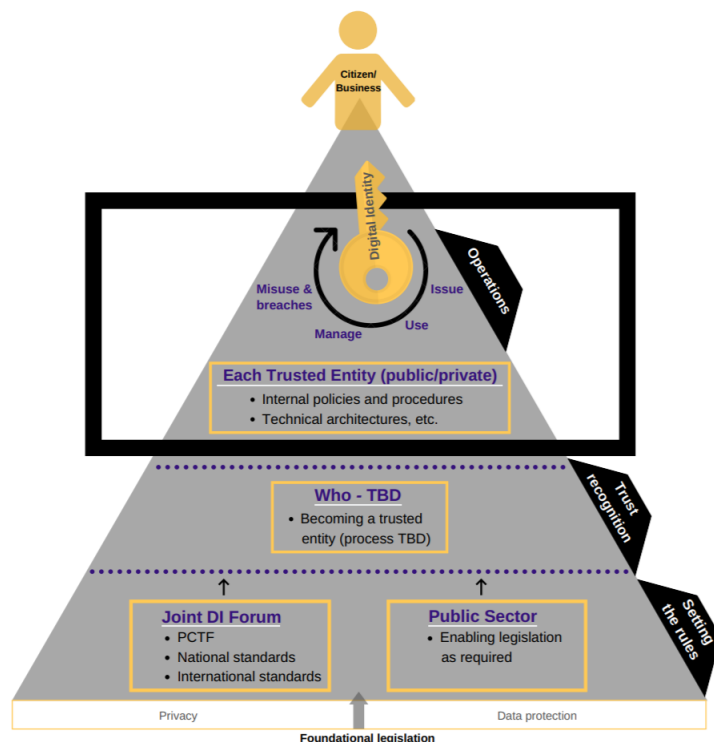
Les réponses au sondage ont permis de déterminer trois grands thèmes, dont huit sous-thèmes connexes, de **ce qui** doit être gouverné (voir le diagramme ci-dessous). Ces thèmes ont été utilisés pour encadrer les discussions durant l'atelier. La séparation des discussions en fonction de ces thèmes s'est prouvée utile. Les trois thèmes permettent d'ancrer les recommandations dans le présent document.

1. Setting the rules for onboarding	
Overarching standards & conformance criteria	core standards and criteria for Canadian digital identities
Privacy, notice & consent	authority to collect, record keeping, sharing data
Data management & protection	collecting, compiling, aggregating, storage & retention
2. Recognizing trusted entities	
Being an issuer, network provider or service provider	how organizations are recognized as trusted entities
3. Governing the operational processes	
Creating a digital identity	Issuance, enrollment and ensuring equal access for all
Using a digital identity	authentication, authorization, attribute exchange, propagation
Managing digital identities	managing the digital identity lifecycle, complaints & revocation
Misuse & breaches	notification, remediation and penalties

## 5. CADRE DE GOUVERNANCE POUR LES IDENTITÉS NUMÉRIQUES AU CANADA

Le cadre de gouvernance ci-après est fondé sur les discussions de l'atelier portant sur les trois grands thèmes suivants : « établir les règles », « reconnaître les entités de confiance »; et « les processus opérationnels ». Les propositions découlant du sondage ont été utilisées pour alimenter les discussions. Les participants à l'atelier se sont penchés sur la meilleure manière de gouverner et ont déterminé à qui incombent les responsabilités.

Dans le diagramme ci-dessous, ces trois thèmes sont présentés sous forme de niveaux distincts et illustrent la portée de **CE QUI** doit être gouverné. Dans chaque niveau, le **QUI** et le **COMMENT** sont indiqués dans les cases à bordures jaunes.



- Les lois en vigueur, notamment les lois sur la protection des données et la protection des renseignements personnels, déterminent les exigences relatives aux identités numériques. Ces lois existent cependant à l'extérieur de la portée du cadre de gouvernance sur l'identité numérique. Aucune modification n'est proposée aux responsabilités, mais le cadre de gouvernance tient compte des lois comme des éléments fondamentaux de l'environnement d'IN.
- Le secteur public devrait être responsable de déterminer et de créer toutes les lois habilitantes nécessaires.
- Un forum mixte des secteurs public et privé sur l'IN devrait être chargé d'établir et de maintenir les critères permettant de devenir une entité de confiance dans l'écosystème pancanadien de l'identité numérique et de collaborer avec les organismes accrédités en vue d'établir des normes d'identité numérique pour le Canada.
- Le forum mixte public privé doit déterminer le processus visant à devenir une entité de confiance. Les responsabilités et les détails associés à ce processus devront être élaborés et pourraient inclure une sorte d'autoattestation ou un processus d'accréditation officiel.
- Dans ce cadre législatif, les entités de confiance devraient être responsables des activités quotidiennes liées à l'émission, à l'utilisation et à la gestion des identités numériques. Dans des circonstances exceptionnelles, comme les plaintes, l'utilisation abusive et les atteintes, un forum mixte public-privé aura des responsabilités précises.

## Thème 1 : Établissement des « règles »

Le premier thème principal consistait à établir des règles générales pour les IN au Canada. On reconnaît dans les réponses au sondage et dans l'atelier l'importance d'établir des critères clairs en vue d'obtenir une plus grande participation au paysage pancanadien de l'identité numérique. Les exigences législatives, les politiques, les normes et les critères de conformité ont été assimilés à une notion de « porte d'entrée robuste ».

### Cadre de confiance pancanadien (CCP)

Le Cadre de confiance pancanadien (CCP) a été cerné à titre de mécanisme de gouvernance clé. On recommande à l'issue de l'atelier deux ajouts au CCP :

- des directives sur les types de transactions et les attributs pouvant être demandés;
- des définitions pour les niveaux d'assurance.

Les participants à l'atelier ont également déterminé qu'il est nécessaire d'établir des normes nationales. Il fut plus précisément question d'établir une échelle de fiabilité, accompagnée des définitions, schémas, autorisations, rôles et responsabilités sous-jacentes. Ces normes seraient utilisées pour évaluer les différentes entités et établir des niveaux de fiabilité de l'identité clairs et faciles à comprendre qui pourraient être diffusés dans l'ensemble du secteur de l'identité numérique. Les participants à l'atelier se sont penchés sur le fait que, à plus long terme, le CCP pourrait évoluer de sorte à ne pas se limiter aux critères de conformité et inclure des normes plus robustes et explicites, comme une approche normalisée à la définition des niveaux d'assurances entre les différentes administrations. En ce qui concerne le court terme, toutefois, on recommande d'élaborer des normes nationales qui existeront en parallèle avec le CCP, mais en dehors de celui-ci.

### Législation fondamentale : Loi sur la protection des renseignements personnels

Deux domaines d'exigences législatives ont été jugés critiques : la protection des renseignements personnels et la protection des données (ce qui recouvre les cas d'utilisation abusive ou d'atteinte à la protection des renseignements). Dans ces deux domaines, on a été noté que les lois en vigueur établissent d'importants paramètres que tous les acteurs du secteur de l'identité numérique doivent respecter. On ne s'attend pas à ce que les responsabilités actuelles soient modifiées, mais les participants de l'atelier ont considéré deux rôles précis pour un forum mixte public-privé sur l'identité numérique :

- évaluer et surveiller les obstacles législatifs et formuler des recommandations en vue d'apporter des changements aux organismes de gouvernance existants en matière de protection des renseignements personnels et des données;
- interpréter les lois et les politiques centrales en lien avec les exigences relatives aux identités numériques.

### Hypothèses clés

- Les organisations qui souhaitent faire affaire dans les pays de l'UE seront responsables de se conformer au Règlement général sur la protection des données (RGPD).
- Le Canada ne prévoit pas appliquer de règlement semblable au RGPD pour l'instant.

## *Thème 2 : Reconnaissance des entités de confiance*

Le deuxième thème, « Reconnaissance des entités de confiance », est axé sur la manière de permettre aux entités de l'écosystème pancanadien de l'identité numérique de reconnaître les entités de confiance. On a entre autres examiné la possibilité d'imposer des autoattestations, l'atteinte des normes nationales et des critères du CCP publiés, ou encore l'établissement d'un processus d'évaluation et d'accréditation générant une marque de confiance. On a reconnu qu'il s'agit d'un domaine très complexe qui comporte plusieurs cas d'utilisation : les diffuseurs d'identité des secteurs public et privé; les identités numériques fondamentales par rapport aux identités numériques dérivées; l'autosouveraineté par rapport au fournisseur de services, et le fournisseur de services par rapport à l'émetteur d'identité.

Compte tenu du temps accordé à l'atelier, il était impossible d'examiner chacun de ces cas d'utilisation et d'élaborer des recommandations. Néanmoins, les entités du secteur privé trouvent bien utile l'idée d'émettre une marque de confiance à titre de processus d'accréditation officiel. Un examen plus approfondi sera nécessaire :

- Le forum mixte public privé sur l'IN déterminera et évaluera les différents cas d'utilisation et définir les exigences de reconnaissance des entités de confiance.

### *Hypothèses clés*

- Les fournisseurs de service choisissent à qui faire confiance.

## *Thème 3 : Gouvernance des processus opérationnels*

Le dernier thème se penche sur la gouvernance requise pour les activités quotidiennes relatives à l'émission, l'utilisation et la gestion des identités numériques. Vu le contexte des thèmes mentionnés précédemment et l'harmonisation avec les principes clés concernant l'application de la gouvernance seulement lorsque celle-ci est requise afin de garder un minimum de règles, les participants à l'atelier ont recommandé d'appliquer une gouvernance supplémentaire uniquement dans le cadre des processus exceptionnels concernant les plaintes, les révocations, l'utilisation abusive et les atteintes à la protection des renseignements.

En reconnaissant les identités numériques dynamiques, les participants à l'atelier ont également recommandé que le forum mixte public-privé sur les IN soit responsable de :

- communiquer les résultats des mises à l'essai et des projets pilotes, ainsi que les pratiques exemplaires qui en découlent;
- gérer le changement, de manière générale, jouer un rôle central en veillant à ce que tous les changements soient communiqués à tous les groupes d'intervenants principaux.

### *Hypothèses clés*

- Les lois, les politiques, les normes et les critères de conformité sont en place, et les entités œuvrant dans le paysage sont connues et fiables.
- Les décisions internes des entités de confiance liées aux processus, aux politiques, aux technologies et à l'architecture doivent être perçues comme une « boîte noire » dans le cadre de gouvernance.
- Les diffuseurs d'identité seront responsables de produire les premières réponses aux plaintes.

- Les diffuseurs d'identité seront responsables de révoquer des identités et des demandes.
- Il existe des modèles de responsabilité s'appliquant au secteur privé.
- Les lois existantes couvrent les responsabilités du secteur privé et précisent les pénalités qui pourraient leur incomber.
- Les services de police continueront de mener des enquêtes lorsque des activités criminelles sont soupçonnées.

ÉBAUCHE - ne pas diffuser

## 6. RECOMMANDATIONS SUR LA RESPONSABILISATION

Les huit sous-thèmes ont été étudiés durant l'atelier. Il en découle des recommandations précises en matière de responsabilités. Ces recommandations figurent dans les tableaux ci-dessous.

### Thème 1 : Établissement des « règles »

QUOI	Secteur de l'identité numérique (QUI)
<b>Normes et critères de conformité généraux</b>	
Cadre de confiance pancanadien	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Élaborer, élargir et maintenir le Cadre de confiance pancanadien, dans le but de garantir l'interopérabilité.</li> </ul> </li> </ul>
Normes nationales	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Établir une échelle de fiabilité, ainsi que les schémas et les règles permettant d'évaluer les entités en fonction de celle-ci.</li> <li>• Définir les normes essentielles en matière d'infrastructure afin de veiller à la cybersécurité, notamment en assurant la liaison avec le Centre canadien pour la cybersécurité et les organismes de normalisation accrédités.</li> </ul> </li> </ul>
Normes internationales	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• S'assurer de mettre à profit les normes internationales dans les cadres canadiens et veiller à ce que le Canada influence adéquatement les normes internationales émergentes.</li> </ul> </li> </ul>
<b>Protection des renseignements personnels, avis et consentement</b>	
Lois (lois gouvernées par les structures existantes)	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Évaluer et surveiller les obstacles législatifs et faire des recommandations en vue d'apporter des changements.</li> <li>• Interpréter les lois et les politiques centrales.</li> <li>• Définir la notion de « diffuseur » et déterminer s'il faut l'inclure dans la législation.</li> </ul> </li> </ul>
Politiques	<ul style="list-style-type: none"> <li>• <b>Toutes les entités de confiance du secteur de l'IN :</b> <ul style="list-style-type: none"> <li>• Élaborer des programmes de protection des renseignements personnels et des politiques internes connexes.</li> </ul> </li> </ul>
Éducation et sensibilisation	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Sensibiliser les sujets d'identité (les citoyens) sur les pratiques exemplaires et les risques.</li> </ul> </li> </ul>
<b>Gestion et protection des données</b>	
Lois (lois gouvernées par les structures existantes)	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Évaluer et surveiller les obstacles législatifs et faire des recommandations en vue d'apporter des changements.</li> <li>• Interpréter les lois et les politiques centrales.</li> </ul> </li> </ul>
Initiatives menées par l'industrie	<ul style="list-style-type: none"> <li>• <b>Toutes les entités de confiance du secteur de l'IN :</b> <ul style="list-style-type: none"> <li>• Lancer des initiatives précises dans le but d'étudier les tendances émergentes ou les problèmes perçus.</li> </ul> </li> </ul>

QUOI	Secteur de l'identité numérique (QUI)
Éducation et sensibilisation	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Sensibiliser les sujets d'identité (les citoyens) sur les pratiques exemplaires et les risques.</li> </ul> </li> </ul>

## Thème 2 : Reconnaissance des entités de confiance

QUOI	Secteur de l'identité numérique (QUI)
<b>Être un diffuseur d'identité, un fournisseur de réseau ou un fournisseur de services</b>	
Des discussions plus approfondies seront requises	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Tenir à jour un registre central des entités de confiance, ainsi que leurs rôles, leurs profils, leurs contrôles compensatoires, entre autres.</li> </ul> </li> </ul>

## Thème 3 : Gouvernance des processus opérationnels

QUOI	Secteur de l'identité numérique (QUI)
<b>Créer une identité numérique</b>	
<p><i>Aucune gouvernance supplémentaire n'est requise au-delà des règles, des critères et du processus de reconnaissance établis dans les thèmes 1 et 2. Une fois qu'une entité est jugée fiable, le processus opérationnel de création d'une identité numérique est géré par l'entité précise.</i></p> <p><i>(Veuillez noter que la responsabilité actuelle d'émettre les identités fondamentales doit continuer d'incomber aux organismes responsables des données de l'état civil et à Immigration, Réfugiés et Citoyenneté Canada)</i></p>	
<b>Utiliser une identité numérique</b>	
<p><i>Aucune gouvernance supplémentaire n'est requise au-delà des règles, des critères et du processus de reconnaissance établis dans les thèmes 1 et 2.</i></p>	
<b>Gérer des identités numériques</b>	
<p>Supposons que chaque entité sera responsable de produire les premières réponses aux plaintes.</p> <p>Supposons que chaque entité sera responsable de gérer la révocation des IN et des demandes.</p>	
Examen collaboratif	<ul style="list-style-type: none"> <li>• <b>Forum mixte public-privé sur l'IN :</b> <ul style="list-style-type: none"> <li>• Examiner les plaintes acheminées et veiller à ce que les sujets d'identité vivent une expérience sans heurts (doit comprendre les ORDEC et les registraires).</li> </ul> </li> </ul>
Rapports de transparence	<ul style="list-style-type: none"> <li>• <b>Les organisations qui reçoivent ou répondent aux demandes :</b> <ul style="list-style-type: none"> <li>• Préparer des rapports de transparence.</li> </ul> </li> </ul>
<b>Utilisations abusives et atteintes à la protection des renseignements</b>	
Politique	<ul style="list-style-type: none"> <li>• <b>Toutes les entités de confiance</b> <ul style="list-style-type: none"> <li>• Établir des politiques internes qui sont conformes aux lois</li> </ul> </li> <li>• <b>Forum mixte public-privé sur l'IN :</b></li> </ul>

QUOI	Secteur de l'identité numérique (QUI)
	<ul style="list-style-type: none"> <li>• Établir un réseau permettant d'envoyer des avis éclair à l'ensemble de l'écosystème.</li> </ul>
Examens d'assurance et enquêtes	<ul style="list-style-type: none"> <li>• <b>Toutes les entités de confiance</b> <ul style="list-style-type: none"> <li>• Enregistrer et signaler les atteintes possibles, mener des évaluations et analyser les réponses.</li> </ul> </li> <li>• <b>Fournisseurs de réseau</b> <ul style="list-style-type: none"> <li>• Sensibiliser et éduquer sur les possibilités d'améliorer la sécurité et la protection des renseignements personnels.</li> </ul> </li> <li>• <i>Remarques :</i> <ul style="list-style-type: none"> <li>• <i>Tiers : Les services de tiers peuvent être sollicités en vue de mener des examens d'assurance et des enquêtes, à la discrétion du diffuseur d'identité, du fournisseur de réseau ou du fournisseur de services.</i></li> <li>• <i>En supposant que les entités de confiance devront prouver qu'elles respectent les normes consignées dans le cadre du processus de reconnaissance.</i></li> </ul> </li> </ul>



## Sommaire des responsabilités recommandées

Le tableau ci-après résume la répartition recommandée des responsabilités entre les entités de confiance, le forum mixte public privé sur l'IN et le secteur public.

Entités de confiance du secteur de l'IN (public et privé)	Forum mixte sur l'IN (public et privé)	Secteur public
<ul style="list-style-type: none"> <li>Décisions relatives aux politiques internes, aux programmes de protection des renseignements personnels, à la technologie et à l'architecture</li> <li>Initiatives menées par l'industrie, le cas échéant</li> <li>Rapports de transparence</li> <li>Enregistrer et signaler les atteintes potentielles, mener des évaluations et analyser les réponses</li> <li>Les fournisseurs de réseau doivent étudier les possibilités d'améliorer la sécurité et la protection des données</li> </ul>	<ul style="list-style-type: none"> <li>Évaluer et surveiller les obstacles législatifs</li> <li>Interpréter les lois et les politiques</li> <li>Cadre de confiance pancanadien</li> <li>Registre central des entités de confiance</li> <li>Normes essentielles en matière d'infrastructure pour veiller à la cybersécurité et à l'interopérabilité</li> <li>Liaison pour les normes internationales</li> <li>Gérer un réseau permettant d'envoyer des avis éclair concernant l'utilisation abusive ou les atteintes à la protection des renseignements.</li> <li>Examiner les plaintes acheminées</li> <li>Communiquer les résultats des mises à l'essai et des projets pilotes</li> <li>Gérer le changement, de manière générale, pour veiller à ce que tous les changements soient communiqués aux intervenants principaux</li> </ul> <p><b>Tâches préparatoires</b></p> <ul style="list-style-type: none"> <li>Établir une échelle de fiabilité, ainsi que les schémas et les règles permettant d'évaluer les acteurs en fonction de celle-ci</li> </ul>	<ul style="list-style-type: none"> <li>Évaluer si des lois habilitantes sont nécessaires pour donner aux administrations le pouvoir d'émettre des identités numériques et de déclencher un suivi, au besoin</li> <li>Établir une liaison avec les structures existantes de gouvernance législative et politique, afin de veiller à ce que les obstacles à l'IN soient communiqués et fassent l'objet de discussions</li> <li>Les ORDEC et IRCC continuent d'émettre les identités fondamentales</li> </ul>

	<ul style="list-style-type: none"> <li>• Définir la notion de « diffuseur » et déterminer s'il faut l'inclure dans les lois</li> <li>• Définir les exigences permettant de reconnaître les entités de confiance</li> </ul>	
--	--	--

## 7. MISE EN CORRESPONDANCE AVEC LES STRUCTURES DE GOUVERNANCE EXISTANTES

L'examen des structures de gouvernance existante révèle que deux organismes seront touchés par les changements recommandés : le CIANC et le SCGI.

### *Forum mixte public-privé : Un CIANC actualisé*

Les participants de l'atelier ont considéré le CIANC comme l'organisme le mieux placé pour assumer les responsabilités prévues pour le forum mixte public-privé sur l'IN, indiquées dans la section précédente. Les obstacles suivants ont été discernés :

- Toutes les administrations doivent être représentées et il ne doit pas y avoir d'obstacle financier à la participation. Il est entendu que le conseil d'administration du CIANC en discute actuellement.
- Les représentants du secteur public doivent aussi représenter le ORDEC et les responsables du permis de conduire de leur administration. Il pourrait être nécessaire d'établir de nouvelles structures ou de nouveaux canaux de communications dans l'ensemble des administrations.

### *Responsable de l'identité numérique du secteur public de chaque administration : nouveau*

Les participants à l'atelier ont reconnu que, pour veiller aux progrès continus vers la délivrance d'identités numériques au Canada, il sera important d'avoir un responsable désigné dans chaque administration. On recommande que cette seule personne ait le pouvoir de représenter l'administration en matière d'identité numérique couvrant, au moins, l'identité numérique des clients des services de santé, de délivrance de permis de conduire et du Bureau de l'état civil.

La personne désignée doit :

- entreprendre un examen des politiques et des lois pour comprendre comment l'administration peut devenir un diffuseur d'ID numérique;
- être en mesure de représenter l'administration avec la confiance des membres des conseils mixtes des administrations, ainsi que des sous-ministres adjoints et des directeurs exécutifs des services de santé, de la délivrance de permis de conduire, du Bureau de l'état civil et des registres ministériels;
- être capable d'aborder des sujets comme les modèles d'exécution de programmes, les modèles de prestation de services, leur habilitation dans les lois, les politiques et la

logistique dans l'administration qui seraient liés aux progrès en vue d'être diffuseur d'ID numérique.

### *Forum du secteur public : un SCGI restructuré*

Il fut reconnu lors de l'atelier qu'il sera nécessaire d'établir un forum réservé au secteur public. On y trouve un rôle continu pour le SCGI. Si le CIANC pouvait éliminer les obstacles mentionnés ci-dessus, son mandat actualisé et élargi entraînerait une restructuration du SCGI pour veiller à ce qu'il y ait une représentation appropriée de toutes les administrations. On recommande que le SCGI soit restructuré pour inclure les responsables de l'IN recommandés ci-dessus et que le mandat soit mis à jour pour s'harmoniser avec le rôle du forum mixte public privé, en mettant l'accent sur les défis associés à la préparation des administrations et à leur capacité d'être des diffuseurs d'ID numérique.

## 8. AUTRES RECOMMANDATIONS

### *Identités juridiques*

Les participants à l'atelier ont reconnu la différence entre les identités juridiques (fondamentales) et les identités dérivées (celles qui se fondent sur les identités fondamentales pour une preuve d'identité) et ont recommandé que la responsabilité de délivrer des identités juridiques continue d'incomber au Bureau de l'état civil et à IRCC.

Les participants à l'atelier ont noté que les identités fondamentales existantes sur papier sont susceptibles d'être utilisées à mauvais escient (lorsqu'une personne peut se voir attribuer plusieurs identités qui sont ensuite utilisées par d'autres). On a reconnu que plus l'identité numérique est proche de la source fondamentale, moins il y a de risques que cela se produise. On recommande ce qui suit :

- Les ORDEC et IRCC continuent de délivrer des certificats de naissance et des documents d'immigration numériques et s'assurent que chaque personne n'a qu'une seule identité.

### *Évaluation réalisée par les administrations sur leur état de préparation quant à l'émission d'identités numériques*

On reconnaît dans les recommandations ci-dessus que les lois portant sur la protection des renseignements personnels et des données diffèrent selon l'administration. Il pourrait être nécessaire de mettre à jour les lois existantes ou d'établir de nouvelles lois habilitantes, afin de permettre l'émission d'identités numériques. Conformément à la Déclaration récente des conseils mixtes sur l'ID numérique, on recommande ce qui suit :

- chaque administration effectue une évaluation de son état de préparation pour émettre des identités numériques, y compris la détermination pour savoir si elle a actuellement le pouvoir législatif d'agir à titre de diffuseur conformément à la composante des personnes dont l'identité a été vérifiée du profil du secteur public du Cadre de confiance pancanadien.

### *Rôle continu de l'ISAC*

Les participants à l'atelier ont compris que l'Institut des services axés sur les citoyens (ISAC) a été créé pour appuyer, faire progresser et favoriser les efforts intergouvernementaux visant à améliorer la satisfaction des citoyens à l'égard des services du secteur public. On a reconnu que l'ISAC offre une plateforme neutre pour l'échange de renseignements et la collaboration et qu'il est bien approprié pour mener et entreprendre des travaux de collaboration interjuridictionnels à l'appui de l'intégration des services numériques.

Comme nous l'avons déjà mentionné, les participants à l'atelier ont appuyé l'exploitation du CIANC afin d'établir le forum mixte public-privé nécessaire. Pour que cela devienne une réalité, on a demandé au CIANC d'examiner la structure des droits d'adhésion pour favoriser la participation active de toutes les administrations sans obstacle. Il sera important de suivre les progrès et de travailler ensemble pour apporter les changements nécessaires. Étant donné que l'ISAC est la manifestation juridique des Conseils, on recommande ce qui suit :

- L'ISAC est chargé de mener des discussions avec le CIANC et de négocier des changements à la structure des coûts au nom des conseils.

## *Déclaration des Conseils mixtes en matière d'identités numériques*

Les participants à l'atelier estiment que des progrès importants ont été réalisés. Ils recommandent d'examiner et mettre à jour la Déclaration des CM à la lumière de ces progrès.

## *Poursuite des ateliers en personne à ce niveau*

Les participants ont largement indiqué que l'atelier avait permis de susciter des discussions très ouvertes sur des questions de grande envergure. On recommande de continuer cela :

- un atelier en personne mixte sera organisé tous les trimestres.

## 9. PROCHAINES ÉTAPES

Avec l'approbation des recommandations du présent document, les prochaines étapes consisteront à poursuivre la mise en œuvre des recommandations susmentionnées comme suit :

### *Immédiatement*

- Demander à l'ISAC de négocier avec le CIANC en vue d'établir une structure de frais d'adhésion qui soit un forum mixte public-privé sans obstacle
- Encourager chaque administration à nommer un responsable désigné de l'IN
- Demander à ORDEC et IRCC d'entreprendre des travaux afin de délivrer des identités numériques fondamentales
- Demander aux coresponsables des priorités de l'IN d'organiser un atelier en personne avec les responsables de l'IN pour élaborer un plan de mise en œuvre et appuyer les évaluations, afin d'en rendre compte à la réunion en personne des Conseils mixtes en février
  - mettre en place une équipe spéciale chargée d'élaborer et de gérer un plan détaillé;
  - élaborer une stratégie de mobilisation et de communication;
  - rencontrer les pairs et les présidents appartenant à des organismes de gouvernance pancanadiens semblables, comme le Conseil canadien des administrateurs en transport motorisé et le consortium sur les systèmes bancaires ouverts;
  - organiser des ateliers multipartites de suivi pour établir un consensus majoritaire sur les priorités et le modèle de gouvernance.

### *Lorsque les responsables de l'IN sont désignés*

- Encourager chaque administration à effectuer des évaluations de l'état de préparation

### *Lorsque les responsables de l'IN et le CIANC recadré sont en place*

- Demander aux coprésidents du SCGI et aux coresponsables des priorités de l'IN de mettre à jour le mandat du SCGI

## Annexe I – Invités et participants à l’atelier

	Nom	Secteur	Rôle	Notes
	Sophia Howse	Provincial (C.-B.)	Corresponsable du volet de l'identité numérique	Coanimation
	Alexandre Bourque	Fédéral (SCT – DPT/BDPI)	Corresponsable du volet de l'identité numérique	Coanimation
	Marc Brouillard	Fédéral (SCT – DPT)	Coprésident du SCGI	Membre au Conseil du CIANC
	Rob Devries	Provincial (ON)	Coprésident du SCGI	Membre au Conseil du CIANC
	Colleen Boldon	Provincial (N.-B.)		Membre au Conseil du CIANC
	Igor Solesa	Provincial (ON)		
	Peter Watkins	Provincial (C.-B.)		
	Sherry McCourt	Provincial (Î.-P.-É.)	Registraire également représenté	
	Arlene Williams	Provincial (N.-É.)		
	Mark Healey	Provincial (T.-N.-L.)		
	Omar Subhani	Fédéral (IRCC)		IN pour l'immigration
N'a pas participé	Sean McLeish	Territorial (YK)		
	Imraan Bashir	Fédéral (SCT)		Politique d'entreprise sur l'IN et surveillance pour le GC
Remplaçante envoyée	Rob Frelich Remplaçante : Janice Lobodale	Fédéral (Service Canada/EDSC)		IN pour la prestation d'avantages
	Pirth Singh	Fédéral (ISDE)		IN pour les entreprises
	Joni Brennan	Présidente du CIANC		
	Franklin Garrigues	Secteur privé : Banque TD		Membre au Conseil du CIANC
	Neil Butters	Secteur privé : Interac		Membre au Conseil du CIANC
	Andre Boyson	Secteur privé : Secure Key		Membre au Conseil du CIANC
	Dan Batista	Représentant de l'ISAC		

	Nom	Secteur	Rôle	Notes
	Jack Shewchuk	Représentant du Conseil de la statistique de l'état civil du Canada		Réponse envoyée par la C.-B.
N'a pas participé	Wynmann Rose	Représentante des responsables pour les permis de conduire		De l'Ontario
	Sharon McLean	S.O.	Animatrice principale	
	Maria Luisa Willen	ISAC (Observatrice)		
	Cathy Kealey	ISAC (Observatrice)		
	Suezan Le Breton	Provincial (C.-B.) (Observatrice)		
Absents	Chantal Ritcey	Provincial (AB)		
Absents	Cosanna Preston	Provincial (SK)		
Absents	Manitoba	Provincial (MB)		
Absents	Québec	Provincial (QC)		
Absents	Territoires du Nord-Ouest	Territorial (T.N-O.)		

## Annexe II – Distribution, répondants et contenu du sondage

### *Distribution*

- Tous les membres du CPSSP et du CDPISP
- CIANC

On demande dans le courriel d'accompagnement de distribuer le sondage dans toutes les organisations.

### *Répondants :*

Gouvernement fédéral	
• Secrétariat du Conseil du Trésor du Canada	• Commission de l'immigration et du statut de réfugié du Canada
• Innovation, Sciences et Développement économique	• Services publics et Approvisionnement Canada
• Emploi et Développement social Canada	• Agence du revenu du Canada
• Immigration, Réfugiés et Citoyenneté Canada	
Secteur privé	
• CIANC	• PricewaterhouseCoopers
• Biometric Signature ID	• 2Keys
• Vancouver City Savings Credit Union (Vancity)	• Manulife
• Interac	
Provinces et territoires	
• Ontario * 2	• Nouvelle-Écosse
• Colombie-Britannique	• Nouveau-Brunswick
• Alberta	• Territoires du Nord-Ouest
• Saskatchewan	• Québec
• Terre-Neuve-et-Labrador	
Bureau de l'état civil	
• ORDEC – C.-B.	
Organisme à but non lucratif	
• Inforoute Santé du Canada	



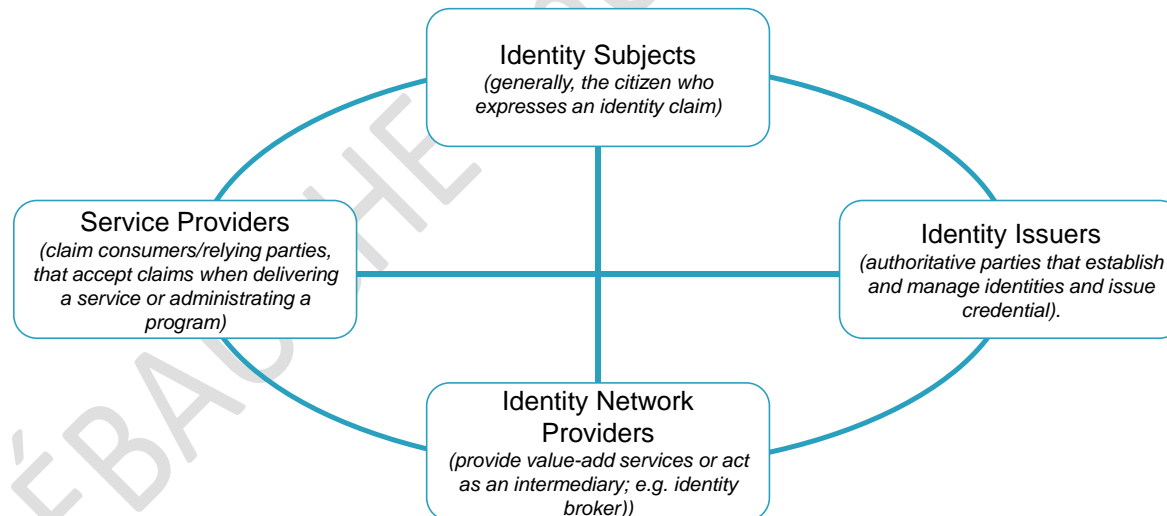
# Sondage sur la gouvernance de l'identité numérique au Canada, juin 2019

---

## Introduction au sondage

Le cœur du sondage est structuré autour des interactions entre les quatre groupes d'intervenants clés dans l'écosystème de l'identité numérique :

- **Sujets d'identité** : Désigne, de façon générale, les citoyens qui présentent une demande en matière d'identité, que ce soit à titre de particulier ou d'entreprise.
- **Diffuseurs d'identité** : Les parties faisant autorité (publiques ou privées), y compris les organisations ou les personnes responsables d'établir et gérer les identités ou de délivrer des justificatifs d'identité. Parfois connus sous l'appellation fournisseurs de demandes, ils peuvent transmettre des demandes aux parties de confiance.
- **Fournisseurs de services** : organismes du secteur public ou privé qui reçoivent les demandes dans le cadre de la prestation d'un service ou de l'administration d'un programme. (Aussi appelés clients des demandes d'identité ou parties utilisatrices.)
- **Fournisseurs de réseau d'identité** : les organismes qui fournissent des services de soutien et de valeur ajoutée ou jouent le rôle d'intermédiaire; par exemple, un courtier en identité.



DÉLAI : Veuillez retourner à [Sharon.McLean@gov.bc.ca](mailto:Sharon.McLean@gov.bc.ca) avant le 30 juin 2019

Pour toute question, veuillez communiquer avec Sharon à l'adresse indiquée ci-dessus.

## QUESTION 1

Quel(s) groupe(s) d'intervenants représentez-vous? (Sujet d'identité, diffuseur d'identité, fournisseur de services, fournisseur d'un réseau d'identité)

## QUESTION 2

Veuillez nous faire part de vos commentaires sur ce qui devrait faire l'objet de gouvernance et nous faire part de vos suggestions quant à la façon d'y parvenir. Il pourrait être utile de tenir compte des fonctions et des services des quatre groupes d'intervenants et des interactions entre eux afin de déterminer quels domaines devraient faire l'objet de gouvernance. Veuillez fournir des commentaires sur les questions suivantes :

- **QUELS domaines devraient faire l'objet de gouvernance?** Ces domaines devraient appartenir à un niveau relativement élevé. Par exemple, « l'émission de l'identité », soit une interaction entre le sujet d'identité et le diffuseur d'identité, est un domaine que vous pourriez prendre en considération.
- **COMMENT devraient-ils faire l'objet de gouvernance?** (Par exemple, lois, politiques, CCP, audits, évaluations, certifications)
- **QUI devrait en être responsable?** (Par exemple, les gouvernements fédéral, provinciaux ou territoriaux, le secteur privé, des tiers indépendants ou une responsabilité conjointe.) Veuillez déterminer si le modèle de gouvernance varie entre les organisations du secteur public et du secteur privé. Par exemple, si le fournisseur d'identité est un gouvernement provincial et que la demande est envoyée à un autre gouvernement provincial, le modèle de gouvernance est-il différent de celui où le fournisseur d'identité est une banque et le fournisseur de service est une autre organisation du secteur privé.

(Veuillez ajouter des lignes supplémentaires, au besoin)

Sujet ou domaine devant faire l'objet de gouvernance (Quoi?)	Option de gouvernance (Qui et comment?)


### QUESTION 3

Y a-t-il des aspects de l'émission et de la gestion des identités numériques qui, selon vous, ne devraient PAS faire l'objet de gouvernance?

### QUESTION 4

Y a-t-il des leçons clés que nous devrions tirer de la manière dont les identités numériques sont administrées au Canada aujourd'hui?

### QUESTION 5

Existe-t-il des cadres de gouvernance comparables dans d'autres industries (par exemple, les finances ou l'assurance) ou dans d'autres pays desquels on pourrait, selon vous, tirer des enseignements utiles?

### QUESTION 6

Y a-t-il des influences externes dont il faut tenir compte dans l'évaluation des options de gouvernance, maintenant ou à l'avenir?

### QUESTION 7

Avez-vous d'autres commentaires?

### COORDONNÉES (FACULTATIF)

Il s'agit d'un sujet complexe. Nous pourrions avoir des questions de suivi à vous poser à la lumière de votre réponse. Si vous n'avez aucune objection, veuillez nous fournir votre nom ainsi que l'adresse électronique au moyen desquels Sharon McLean pourra communiquer avec vous pour obtenir des précisions ou discuter de réponses précises. Ces renseignements ne seront pas utilisés pour nommer les gens qui ont fourni des commentaires dans la publication des résultats.

Nom :

Courriel :