Rapport | juin 2024

Un plan d'action pour le progrès :

Perspectives stratégiques pour un accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens

Parrainé par :
Gouvernement du Yukon,
Ministère de la Voirie et des Travaux publics

Écrit par :
Hadrien Seymour-Provencher
et Cosanna Preston-Idedia
du Laboratoire de la confiance numérique du Canada

LABORATOIRE DE
confiance numérique

Table des matières

Avis de droit d'auteur et licence **3**
Résumé **4**
INTRODUCTION **6**
Faire progresser la fourniture de services numériques sûr, convivial et sécuritaire 8
Approche 11
CONCLUSIONS, ANALYSE ET RECOMMANDATIONS **12**
Systèmes de gestion de l'accès aux services numériques pour les citoyens et progression de NA1 à NA3 **13**
Constatations relatives aux gouvernements et au marché 15
Analyse 20
Recommandations 22
Les plateformes SSO comme courtiers en données **25**
Constatations relatives aux gouvernements et au marché 26
Analyse 29
Recommandations 30
Fédération **32**
Constatations relatives aux gouvernements et au marché 32
Analyse 34
Recommandations 35
Comment travailler efficacement avec les commissaires à la protection de la vie privée **37**
Constatations relatives aux gouvernements 37
Commissaires à la protection de la vie privée 38
Analyse 39
Recommandations 40
Vers des justificatifs numériques **41**
Constatations relatives aux gouvernements et au marché 41
Analyse 45
Recommandations 47
RECOMMANDATIONS GÉNÉRALES **48**
CONCLUSION **54**
Prêt à passer à la prochaine étape en vue des justificatifs numériques? 55
ANNEXE **56**

Avis de droit d'auteur et licence

Écrit par :

Hadrien Seymour-Provencher

et Cosanna Preston-Idedia

du **Laboratoire de la confiance numérique du Canada (LabCN)**

Résumé

De nombreuses administrations au Canada, du gouvernement fédéral aux provinces et territoires en passant par les municipalités, cherchent à améliorer l'accès aux services numériques destinés aux citoyens de manière sécurisée, pratique et abordable, tout en protégeant la vie privée. Avec plus de 3 500 gouvernements au Canada, y compris les gouvernements municipaux, il y a beaucoup d'occasions de tirer des leçons des pratiques émergentes plutôt que de recommencer à zéro encore et encore. Ce rapport, rédigé par le Laboratoire de la confiance numérique du Canada (LabCN) et parrainé par le gouvernement du Yukon, vise précisément à atteindre cet objectif en offrant un aperçu stratégique de la gestion de l'accès aux services numériques pour les citoyens à tous les niveaux de gouvernement au Canada, à leurs parties prenantes et à leurs partenaires d'exécution.

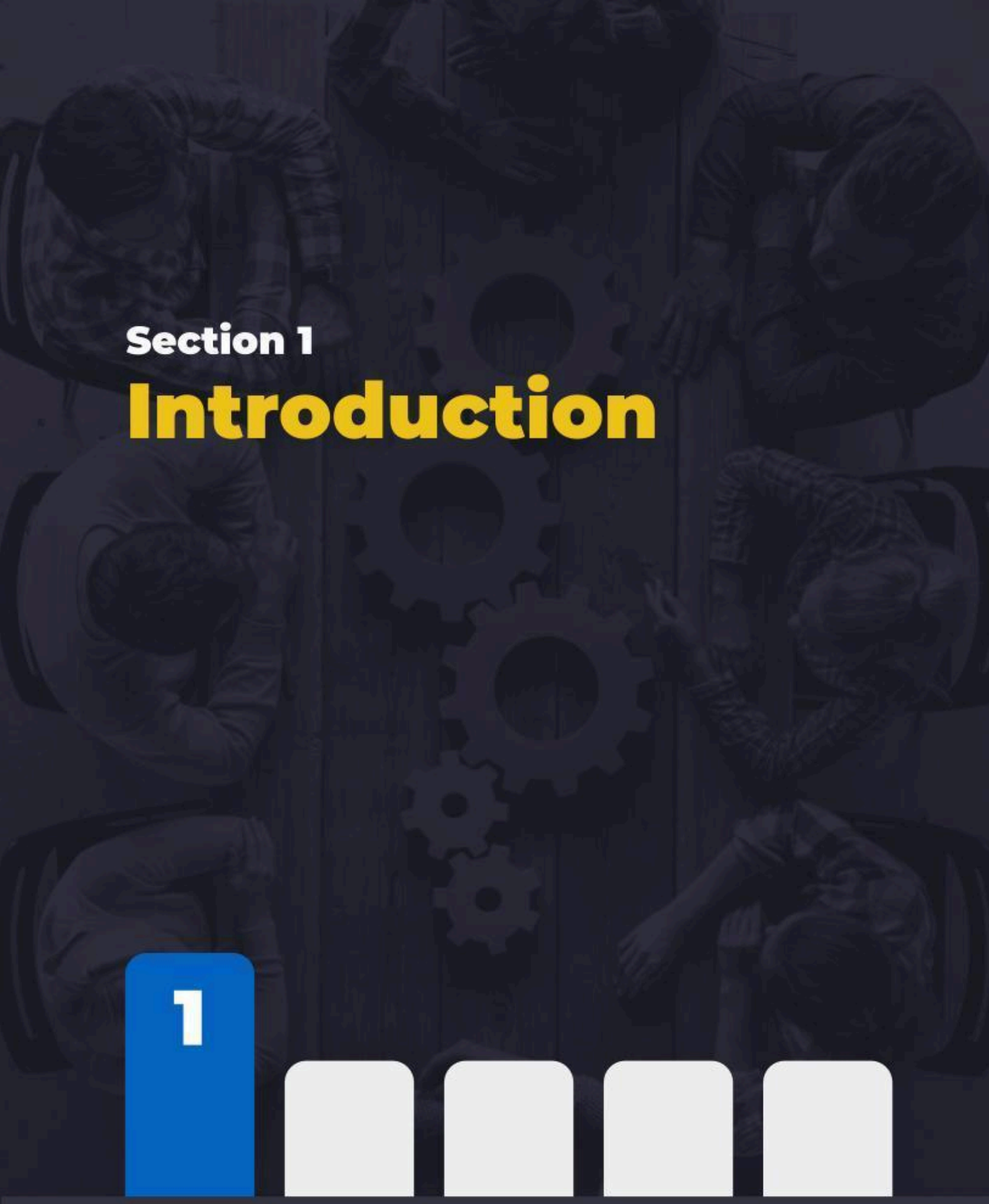
L'approche adoptée pour ce rapport a consisté en une analyse juridictionnelle et une étude de marché comprenant des recherches secondaires et des entretiens avec des représentants gouvernementaux, des commissaires à la protection de la vie privée et des fournisseurs de solutions. Ces entretiens ont porté sur les sujets suivants : progression de NA1 à NA3, courtage de données, fédération avec les gouvernements fédéral et provinciaux/territoriaux, collaboration avec les commissaires à la protection de la vie privée et adoption de justificatifs numériques.

Le rapport met l'accent sur l'alignement des niveaux d'assurance de l'identité (NA) pour l'accès aux services numériques des citoyens sur les normes fédérales, et sur la priorité donnée à l'expérience utilisateur en offrant de multiples options d'authentification et de vérification de l'identité. En outre, ce rapport souligne l'importance de travailler efficacement avec les commissaires à la protection de la vie privée en s'engageant dès le début et en collaborant tout au long des phases de conception, de mise en œuvre et d'amélioration continue afin de garantir la transparence et le consentement des utilisateurs.

Les recommandations générales sont les suivantes

1. Adopter une approche programmatique pour garantir un accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens
2. Élaborer une stratégie de programme à long terme
3. Élaborer un cadre de protection de la vie privée
4. Centrer l'utilisateur dans le développement et les opérations
5. Adopter une approche collaborative de l'approvisionnement
6. Communiquer avec précision et instaurer la confiance
7. Rester engagé dans la communauté

En s'appuyant sur une approche collaborative et axée sur la recherche, LabCN a élaboré un plan détaillé qui offre des perspectives intéressantes et des orientations stratégiques pour soutenir la progression continue d'un accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens.



Section 1

Introduction

1

Introduction

De nombreuses administrations à travers le Canada, du gouvernement fédéral aux provinces et territoires en passant par les municipalités, s'interrogent sur la manière d'améliorer l'accès aux services numériques pour les citoyens d'une manière sécuritaire, respectueuse de la vie privée, pratique et abordable. Alors que l'accent est actuellement mis sur une approche centralisée par le biais de plateformes d'authentification unique (SSO), les modèles décentralisés commencent à gagner du terrain au Canada. Ces initiatives pourraient ouvrir la voie à une approche pancanadienne visant à offrir aux Canadiens des justificatifs numériques, non seulement pour leur pièce d'identité avec photo émise par le gouvernement, comme le permis de conduire, mais aussi des justificatifs individuels pour tous leurs documents importants tels que les licences d'affaires, les certifications professionnelles, les pièces d'identité des employés, les permis, etc.

Avec plus de 3 500 gouvernements au Canada, y compris les gouvernements municipaux, il y a de nombreuses opportunités de tirer des leçons des pratiques émergentes plutôt que de tout inventer à partir de zéro, encore et encore. Ce rapport, rédigé par le Laboratoire de la confiance numérique du Canada (LabCN) et parrainé par le gouvernement du Yukon, vise précisément à atteindre cet objectif en offrant un aperçu stratégique de la gestion de l'accès aux services numériques pour les citoyens à tous les niveaux de gouvernement au Canada, à leurs parties prenantes et à leurs partenaires d'exécution.

Pour ce faire, le Laboratoire de la confiance numérique du Canada (LabCN) a été guidé par les questions principales énumérées ci-dessous.

Principales questions à étudier :

1. Comment une administration augmente-t-elle le niveau d'assurance associé à l'accès aux services numériques destinés aux citoyens et aux entreprises?
2. Les plateformes d'authentification unique pour la prestation de services numériques gouvernementaux devraient-elles prendre en charge le courtage de données pour les parties utilisatrices au sein de l'administration, et éventuellement entre les programmes gouvernementaux? Dans un tel cas, comment cela devrait-il se faire?
3. Comment les plateformes d'authentification unique utilisées au niveau provincial et territorial peuvent-elles accéder aux services du gouvernement fédéral par le mécanisme de la fédération?

4. Comment une équipe de services numériques destinés aux citoyens peut-elle collaborer de façon optimale avec son commissaire à la protection de la vie privée pour garantir un accès sûr, convivial et sécuritaire aux services numériques destinés?

5. Comment une équipe de services numériques destinés aux citoyens peut-elle se préparer à un avenir avec des justificatifs numériques?

Réaliser un accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens.

La valeur de l'offre de services en ligne aux citoyens n'est plus à démontrer. La prestation de services numériques, lorsqu'elle est bien réalisée, est moins coûteuse pour les gouvernements, avec la possibilité d'être 20 fois moins chère que le téléphone, 30 fois moins chère que le courrier et 50 fois moins chère que la prestation de services en personne.[1] La prestation de services numériques est également plus pratique et plus inclusive pour les citoyens, car elle offre un accès 24 heures sur 24 et 7 jours sur 7 à l'administration, permettant aux citoyens d'accomplir leurs tâches à tout moment et en tout lieu.

Cependant, parallèlement à cette augmentation de l'accès pratique aux services gouvernementaux, le Canada a également constaté une augmentation des violations de la vie privée et des cas de fraude d'identité. L'usurpation d'identité est le premier type de fraude au Canada et les cybermenaces montent en flèche, les pertes financières dues à la fraude au Canada ayant plus que triplé, passant de 165 millions de dollars en 2020 à 554 millions de dollars en 2023.[2] Pendant la même période, 27 milliards d'enregistrements de données canadiennes ont été exposés en raison d'atteintes à la vie privée.[3] La prévalence de la fraude et les atteintes à la vie privée ont démontré que tous les systèmes ne sont pas égaux en matière de sécurité et de protection des données personnelles.

S'il n'existe pas de solution miracle pour prévenir la fraude et les cyberattaques contre les systèmes de gestion de l'accès aux services numériques destinés aux citoyens, il est essentiel de s'assurer qu'ils fonctionnent avec un niveau d'assurance

[1] Central Digital and Data Office, Cabinet Office. 2012. "Digital Efficiency Report. Gov.UK. https://www.gov.uk/government/publications/digital-efficiency-report
[2] Centre antifraude du Canada. 2024. "Bulletin du Centre antifraude du Canada". https://x.com/canantifraud/status/1747656665334165965/photo/1
[3] Statista. 2023. “Number of data records exposed due to data breaches in Canada from 1st quarter 2020 to 1st quarter 2023”. https://www.statista.com/statistics/1324220/canada-number-of-leaked-records/

suffisamment élevé - généralement le niveau d'assurance 3 (NA3) - pour protéger les informations personnelles les plus sensibles ou les informations de grande valeur. (Voir Progression de NA1 à NA3 pour plus de détails sur les niveaux d'assurance).

Plus important encore, NA3 offre une bien meilleure garantie que la bonne personne accède aux bons services. Toutefois, deux problèmes au moins subsistent :

1. Aujourd'hui, la plupart des authentifications NA3 sont encore proposées par des systèmes centralisés, ce qui signifie que cette forme sécurisée de preuve d'identité ne peut être utilisée qu'avec le niveau spécifique de gouvernement qui propose l'authentification ou les services auxquels ils ont accès par le biais de la fédération. Les citoyens ne peuvent pas utiliser cette preuve numérique de leur identité pour effectuer d'autres transactions numériques, par exemple auprès d'une banque, lors de la location ou de l'achat d'un logement, de la location d'une voiture ou de l'achat de biens soumis à des restrictions d'âge. Cependant, ils peuvent utiliser leur carte d'identité physique avec photo délivrée par le gouvernement (par exemple, un permis de conduire) pour prouver qu'ils sont bien qui ils prétendent être à qui ils veulent.
2. Les identifiants de connexion basés sur NA3 ne traitent qu'un seul élément de la fraude à l'identité, à savoir que vous êtes bien celui que vous prétendez être. Ils n'abordent pas les autres éléments de la fraude à l'identité, comme la production frauduleuse d'un permis, d'un document financier ou d'une licence au nom de quelqu'un d'autre, ce qui peut facilement être fait avec un document délivré sur un morceau de papier ou sous forme de PDF.

Pour résoudre ces deux problèmes, les équipes chargées des services numériques aux citoyens doivent faire un pas de plus dans leur feuille de route numérique et mettre en place des justificatifs numériques.

La valeur des justificatifs numériques

Les justificatifs numériques représentent une approche transformatrice de la vérification de l'identité. Les gouvernements et les organisations du monde entier explorent le potentiel des justificatifs numériques pour renforcer la sécurité, tout en donnant aux individus un plus grand contrôle sur leurs données personnelles.

En termes simples, les justificatifs numériques peuvent être définis par trois points principaux :

1. **Un justificatif numérique est une représentation numérique des informations contenues dans son équivalent physique,** tel qu'une carte

d'identité avec photo délivrée par le gouvernement, un permis, un badge d'employé, un état financier ou une preuve d'enregistrement d'une entreprise.

    - Un justificatif numérique peut également représenter des informations qui ne sont pas facilement disponibles dans un justificatif physique aujourd'hui, comme une preuve d'adresse.
    - C'est plus qu'un simple accès à l'information. C'est l'information.

2. **Les justificatifs numériques (aspirent à être) compatibles** (également appelés interopérables). Cela signifie que les justificatifs numériques ne sont pas liés à un seul système technologique ou à une seule organisation. Tout comme nous pouvons aujourd'hui utiliser n'importe quelle carte de crédit avec n'importe quel terminal de point de vente, l'objectif pour les justificatifs numériques est que n'importe quel justificatif puisse être utilisé avec n'importe quelle technologie de vérification. Les travaux en cours sur les cadres de confiance et les tests d'interopérabilité, entre autres initiatives, continuent de pousser la communauté des justificatifs numériques à concrétiser cette vision.
3. **Les justificatifs numériques sont signés cryptographiquement et vérifiables.** La signature cryptographique signifie que vous pouvez automatiquement savoir si l'une des données contenues dans le justificatif a été altérée. Cela permet au destinataire de faire confiance aux données fournies.

Les justificatifs numériques présentent un certain nombre d'avantages. Nous en soulignons trois parmi les plus importants :

1. **Il s'agit d'une solution au risque de falsification des documents délivrés sur papier ou en format PDF.**
   Si un permis, une licence ou une carte d'identité avec photo délivrée par le gouvernement est délivré sous forme de justificatif numérique, cela signifie qu'un citoyen peut porter ce justificatif sur lui dans un portefeuille numérique, tout comme il porterait ses cartes importantes dans un portefeuille ou rangerait ses dossiers importants dans un tiroir. La différence est qu'un permis imprimé ou en format PDF, comme nous l'avons établi, peut être facilement falsifié. Grâce aux justificatifs numériques, le risque de falsification est considérablement réduit.
2. **Il renforce la protection de la vie privée et des données.**
   De nombreux types de justificatifs numériques ont la capacité de divulguer des informations de manière sélective. Ainsi, lorsqu'un citoyen choisit de partager son permis de conduire ou une pièce d'identité avec photo délivrée

par le gouvernement avec quelqu'un, par exemple en partageant un formulaire de taxe sur les carburants avec une institution financière pour démontrer la conformité dans le cadre d'une demande de prêt, l'institution financière peut avoir besoin de savoir seulement que le formulaire a été déposé, et non les détails du formulaire. La personne qui partage l'information peut choisir de ne partager que cet attribut de données.

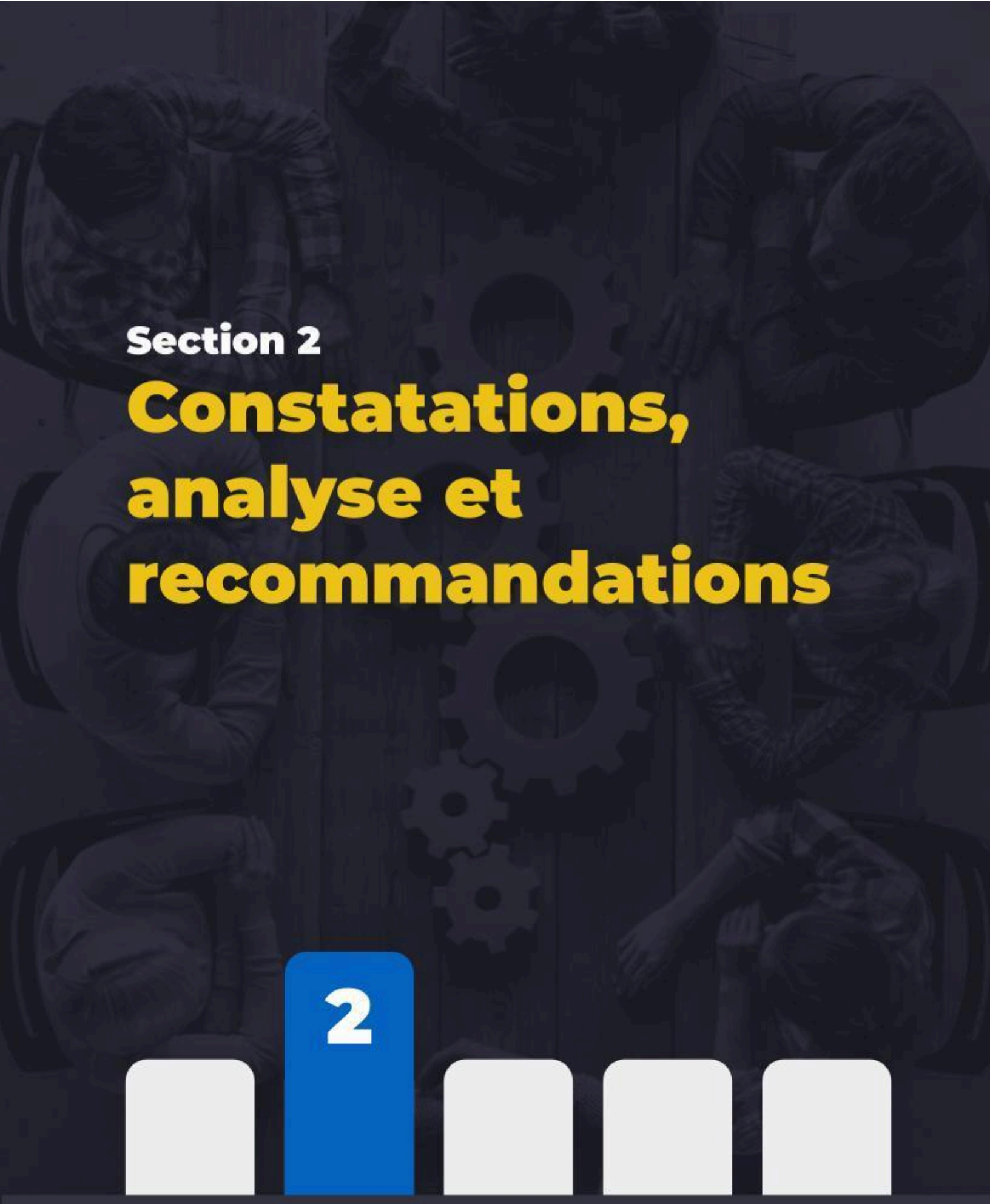
3. **Plus de commodité et de sécurité**
   Un justificatif numérique équivalent à une carte d'identité avec photo délivrée par l'État peut remplacer le nom d'utilisateur et le mot de passe comme clé d'accès aux services de l'État et à tout autre service du secteur privé qui choisit d'accepter cette forme d'authentification. C'est un peu comme si l'on glissait une carte d'employé pour accéder à un bâtiment. Cela élimine le processus frustrant et souvent fastidieux de réinitialisation des mots de passe. Le remplacement des noms d'utilisateur et des mots de passe par des justificatifs numériques contribue également à limiter les fraudes à l'identité et les atteintes à la vie privée.

Cela ne signifie pas que les systèmes de gestion de l'accès aux services numériques destinés aux citoyens doivent immédiatement passer aux justificatifs numériques. Bien qu'il s'agisse d'une option, elle n'est probablement pas abordable pour les petites administrations.

Approche

L'approche adoptée pour ce rapport a consisté en **une étude de marché et analyse des administrations.** LabCN a mené des entretiens avec des personnes appartenant aux groupes d'intervenants suivants : Administrations (7), commissaires à la protection de la vie privée (4), fournisseurs de solutions (5) et un expert du gouvernement pancanadien. Ces entretiens ont eu lieu entre décembre 2023 et février 2024.

En plus de la recherche, LabCN a ajouté sa propre analyse pour élaborer ce rapport public comprenant des conclusions et des recommandations.



Section 2

Constatations, analyse et recommandations

2

Systèmes de gestion de l'accès aux services numériques pour les citoyens et progression de NA1 à NA3

La question principale de cette section était la suivante :

Comment une administration augmente-t-elle le niveau d'assurance associé à l'accès aux services numériques destinés aux citoyens et aux entreprises ?

Deux des décisions clés en matière de gestion des accès pour une équipe de services numériques aux citoyens consistent à déterminer le degré de rigueur nécessaire au moment de l'attribution d'un compte (ou d'un justificatif numérique) à une personne et à déterminer le degré de rigueur nécessaire au moment de l'authentification (lorsque la personne se connecte) ou de la vérification (lorsque la personne utilise son justificatif numérique). Par exemple, il est plus confortable de procéder avec moins d'assurance que la personne est bien celle qu'elle prétend être lorsqu'elle effectue une transaction sur Kijiji ou Facebook Marketplace que lorsqu'elle accède à des informations classifiées, à des informations confidentielles de l'entreprise ou à un contrat d'une valeur de plusieurs millions de dollars.

Cette rigueur est appelée niveau d'assurance (NA). Selon les lignes directrices du gouvernement fédéral sur la garantie de l'identité, il existe quatre niveaux d'assurance qui vont de NA1 à NA4 :

- NA1 - peu d'inquiétude quant à l'authenticité de la personne ou du justificatif, car l'accès au système ou à l'information n'entraînerait que peu ou pas de dommages.
- NA4 - il est nécessaire d'être extrêmement sûr que la personne et la pièce d'identité présentée sont légitimes, car l'accès au système ou à l'information risque d'entraîner des dommages catastrophiques. En règle générale, la lettre d'intention 4 est réservée aux questions de sécurité nationale.

Le niveau NA3 est généralement considéré comme le plus haut niveau requis pour les services gouvernementaux aux citoyens. Les principales exigences du gouvernement du Canada pour les niveaux NA1 et 3[4] sont les suivantes :

Exigence	Niveau 1	Niveau 3
Unicité	Définir les informations relatives à l'identité Définir le contexte	Définir les informations relatives à l'identité Définir le contexte
Preuve d'identité	Aucune restriction quant aux éléments de preuve fournis	**Deux** exemples de preuves d'identité (Au moins un doit être une preuve d'identité fondamentale)
Exactitude des informations sur l'identité	Acceptation de l'auto-affirmation de l'information sur l'identité par un individu	Les informations relatives à l'identité correspondent de manière acceptable à l'affirmation d'une personne et à toutes les preuves d'identité. **et** Confirmation de la preuve fondamentale de l'identité à l'aide d'une source faisant autorité **et** Confirmation que les preuves d'identité proviennent d'une autorité appropriée, en

[4] Gouvernement du Canada. Mars 2016. "Guideline on Identity Assurance". https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30678&section=html#:~:text=Table%202.%20Minimum%20Requirements%20to%20Establish%20an%20Identity%20Assurance%20Level

		utilisant une source faisant autorité ou inspection par un examinateur qualifié
Lien entre les informations relatives à l'identité et l'individu	Aucune exigence	Au moins **un des** éléments suivants i. Confirmation basée sur la connaissance ii. Confirmation d'une caractéristique biologique ou comportementale iii. Confirmation d'un arbitre de confiance iv. Confirmation de la possession physique

Le modèle de mise en œuvre de la NA3 évolue et varie d'un programme de services numériques aux citoyens à l'autre. Il comprend des options asynchrones et synchrones et va de la validation en personne à la validation par téléconférence, en passant par l'expérimentation d'une validation à distance entièrement automatisée par vérification faciale.

Constatations relatives aux gouvernements et au marché

Gouvernements

Approche générale de la vérification de l'identité et de l'accueil des nouveaux arrivants

À l'heure actuelle, il n'existe pas de méthode uniforme de gestion de la vérification de l'identité pour l'ensemble des gouvernements du Canada, et souvent pas non plus au sein d'une même administration. Il n'est pas rare que chaque service au sein d'un gouvernement interprète et mette en œuvre les procédures d'authentification dans le contexte de son service spécifique. Cette approche fragmentée a conduit à des défis tels que des processus de vérification répétitifs entraînant une expérience fragmentée pour l'utilisateur.

Si les mesures de sécurité sont essentielles, il est tout aussi important de veiller à ce que les processus d'authentification soient transparents et conviviaux afin d'éviter la frustration et l'abandon des utilisateurs. Certaines provinces et certains territoires proposent des plateformes d'authentification unique (SSO) qui permettent aux utilisateurs de s'authentifier et de se connecter en toute sécurité à un compte géré de manière centralisée afin d'accéder aux services gouvernementaux intégrés en

aval. Les fonctionnalités de la plateforme peuvent inclure la création de comptes, l'authentification, l'autorisation, la révocation, la déconnexion globale, la gestion des profils, la gestion des notifications, etc.

Certains programmes proposent deux niveaux : un compte "de base" au niveau NA1 (courriel, nom et prénom) et un compte "vérifié" au niveau NA2 ou NA3, l'accent étant mis sur ce dernier en raison de sa pertinence dans les scénarios impliquant des transactions financières ou l'échange d'informations sensibles telles que des dossiers médicaux.

Pour les plateformes d'authentification unique qui commencent au niveau NA1 (parfois avec des étapes supplémentaires qui pourraient être appelées NA1.5), le processus d'accueil comprend généralement un nom et un mot de passe autodéclarés ou une vérification par rapport à une autre source, telle que les informations d'identification bancaires en ligne. Les services en aval peuvent nécessiter des informations ou des vérifications supplémentaires, comme le fait de se rendre dans un point de service pour immatriculer un premier véhicule. Les processus d'accueil de NA1 ne gèrent généralement pas les doubles comptes. Dans ce cas, le client peut créer autant de comptes qu'il le souhaite. Il peut souhaiter disposer de comptes distincts pour différents services, ce qui lui offre une certaine souplesse. En général, la seule exigence est que chaque compte ait une adresse électronique unique. En ce qui concerne les doubles demandes ou l'accès aux services, l'unicité est déterminée par d'autres mécanismes, et l'équipe des services numériques aux citoyens peut travailler avec le ministère ou le département sur leurs exigences spécifiques

Mise en évidence

BC Services Card - un exemple canadien de LOA3

Pour obtenir la **BC Services Card** émise par le gouvernement, une carte physique vérifiée conformément à LOA3, l'identité d'un résident doit être vérifiée à un bureau de service physique, ou par un agent du gouvernement dans les zones rurales. L'identité est vérifiée en présentant deux pièces d'identité. Il s'agit généralement d'un permis de conduire, qui peut être recoupé pour garantir l'unicité de la carte. La BC Services Card a remplacé la carte provinciale de soins de santé et peut également être combinée avec le permis de conduire de la Colombie-Britannique.

La **BC Services Card** peut être utilisée pour créer et accéder à un compte BC Services Card, qui est la principale plateforme d'authentification unique du gouvernement de la Colombie-Britannique. La configuration du compte se fait à l'aide d'une application mobile ou d'un nom d'utilisateur et d'un mot de passe. Ce processus nécessite une nouvelle vérification de l'identité de la personne, à l'aide de sa BC Services Card. Une fois vérifiée, elle peut accéder à son compte en ligne en enregistrant une adresse électronique et en définissant un nom d'utilisateur et un mot de passe. Il en résulte un compte LOA3 pour l'accès aux services en ligne.

en matière de services. Soit les ministères/départements peuvent gérer les doublons dans leur service en aval, soit les exigences d'accueil sont configurées de manière à garantir un lien univoque entre les enregistrements des comptes.

Si la base de la plateforme d'authentification unique est NA3, la norme reste la vérification par un agent dans un point de service. Les personnes se présentent avec des pièces d'identité acceptables pour une vérification en personne, qui peut impliquer une interrogation d'une base de données juridictionnelle, telle qu'un registre des véhicules à moteur, avant qu'un compte NA3 ne leur soit accordé. Il y a généralement des limites à la vérification des personnes qui ne sont pas originaires de la province ou du territoire et qui n'ont pas de pièce d'identité de la province ou du territoire. Les doublons sont évités en raison des exigences d'unicité de l'enregistrement.

Les cadres de confiance dans le contexte gouvernemental

Ces programmes de NA plus élevés tendent également à s'aligner sur le Profile du secteur public du cadre de confiance pancanadien (CCP-PSP)[5], un ensemble de lignes directrices conçues pour faciliter les interactions numériques sécurisées et fiables au sein du secteur public canadien.

Les feuilles de route et les visions peuvent inclure un objectif visant à atteindre le NA3, conformément aux lignes directrices énoncées dans le CCP-PSP. Toutefois, pour atteindre ce niveau, des mesures supplémentaires seraient nécessaires, notamment en ce qui concerne la collecte et la validation des documents d'identité fondamentaux, tels que l'acte de naissance d'une personne. Le problème est que les certificats de naissance posent leurs propres problèmes de sécurité et que les provinces et territoires ne peuvent vérifier les certificats de naissance que pour les personnes nées dans leur juridiction, ce qui pose un problème pour atteindre le niveau NA3. Pour remédier à cette limitation et accroître le niveau de confiance dans les processus de vérification de l'identité, les gouvernements explorent des stratégies visant à demander des informations supplémentaires qui peuvent être vérifiées en ligne, à distance ou de manière asymétrique. Cette approche vise à améliorer les procédures d'authentification et à progresser vers une NA plus élevée dans le cadre des contraintes posées par les méthodes de vérification actuelles. En conséquence, très peu de gouvernements ont été en mesure de mettre en œuvre la NA3 à ce jour, et cela reste un défi.

[5] Profile du secteur public du Cadre de confiance pancanadien | Pan-Canadian Trust Framework . https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_4

Commissaires à la protection de la vie privée

Les commissaires à la protection de la vie privée préconisent une approche de la gestion de l'accès aux services numériques destinés aux citoyens qui soit axée sur la protection de la vie privée, en soulignant la nécessité de trouver un équilibre entre les exigences en matière de sécurité et d'authentification, tout en sauvegardant le droit à la vie privée des personnes. Un NA plus élevé peut renforcer la sécurité et la fiabilité de la vérification de l'identité, mais il pose également des problèmes liés à la collecte et à la gestion des informations personnelles. Cela s'applique à la fois à l'augmentation de la collecte de données personnelles et à la compréhensibilité et à la transparence du consentement.

Pour répondre aux préoccupations en matière de protection de la vie privée associées à des NA plus élevées, les commissaires à la protection de la vie privée ont toujours dit que les gouvernements devraient impliquer leur commissaire à la protection de la vie privée dès le début du processus et mener des évaluations des facteurs relatifs à la vie privée (EFVP) tout au long du projet (au lieu d'une seule à la fin). Cela permet d'identifier et d'atténuer les risques potentiels liés à la collecte, à l'utilisation, à la conservation et à la divulgation des informations personnelles. Les commissaires à la protection de la vie privée recommandent d'appliquer les principes de consentement et de contrôle de l'utilisateur d'une manière claire et conviviale. Le fait de ne collecter que la quantité nécessaire de renseignements personnels aux fins prévues, autorisées et spécifiées permet aux administrations de remplir leurs obligations et de respecter les lois et règlements pertinents en matière de protection de la vie privée, tant au niveau fédéral qu'au niveau provincial ou territorial.

Biométrie et technologies émergentes

Les inquiétudes concernant les violations de données, en particulier avec l'introduction de l'intelligence artificielle (IA) et des technologies biométriques, soulignent la nécessité de mesures de sécurité strictes et d'une évaluation continue des plateformes de SSO. Cependant, les commissaires à la protection de la vie privée de tout le pays débattent de la manière précise d'y parvenir, notamment en ce qui concerne l'utilisation de la biométrie. Un commissaire à la protection de la vie privée a déclaré que "chaque fois que les données biométriques d'une personne se trouvent quelque part dans le nuage ou ailleurs que sur votre téléphone, c'est un problème parce que vous ne pouvez pas changer vos données biométriques comme

vous pouvez le faire pour un mot de passe, et avec l'IA [les utilisations rudimentaires de certaines données biométriques] pourraient être truquées". [6]

D'un autre côté, une autre personne a une vision plus positive de la question. Considérant la tendance comme inévitable, ils ont déclaré qu'"il y a des risques et que c'est un peu une pente glissante. Je pense qu'il est inévitable que nous utilisions ces technologies et que plus nous utilisons de points de données, plus la vérification devient fiable".[7] En résumé, la technologie biométrique est un bon moyen d'authentification, mais la récompense doit être à la hauteur de la justification.

Fournisseurs de solutions

Comment aborder l'obtention d'un NA3

En ce qui concerne l'obtention de NA plus élevées, les fournisseurs de solutions ont fait part de leurs réflexions sur les niveaux cibles, les considérations transfrontalières et l'importance d'une bonne technologie et de processus opérationnels. Certains fournisseurs de solutions ont suggéré que les gouvernements puissent sauter le niveau d'assurance 2 et se concentrer directement sur l'obtention du niveau d'assurance 3 afin d'avoir la certitude de s'adresser à la bonne personne. Les fournisseurs de solutions ont également souligné que les normes NA (Niveau d'assurance ou Level of Assurance - Canadien) et IAL (Identity Assurance Level - Américain) sont relativement similaires dans l'ensemble et qu'il s'agit en fin de compte de déterminer le niveau de confiance nécessaire pour vérifier l'identité d'une personne. En conséquence, le fait de commencer par les orientations canadiennes en matière de NA permet aux administrations d'envisager avec succès des utilisations transfrontalières si elles le souhaitent. Enfin, les fournisseurs de solutions ont souligné que la technologie elle-même n'est pas le principal obstacle à l'obtention d'une plus grande confiance dans les transactions en ligne. Si les solutions technologiques avancées peuvent faciliter la mise en œuvre des cadres de la NA, les défis les plus difficiles à relever consistent à adapter les processus opérationnels et à s'aligner sur les exigences réglementaires établies.

Vérification en personne ou à distance

Les fournisseurs de solutions se sont également prononcés sur la question de la vérification en personne par rapport à la vérification à distance. Ils reconnaissent que la vérification en personne reste cruciale pour certaines transactions et qu'elle devrait

[6] Citation tirée des entretiens avec les commissaires à la protection de la vie privée menés par LabCN en janvier et février 2024.
[7] Citation tirée des entretiens avec les commissaires à la protection de la vie privée menés par LabCN en janvier et février 2024.

être intégrée dans les solutions de gestion de l'identité et de l'accès lorsque cela est nécessaire. Mais ils ont également souligné que cela peut prendre du temps et poser des problèmes dans les zones rurales ou éloignées où l'accès aux services gouvernementaux peut être limité. La vérification à distance permet aux individus de vérifier leur identité en ligne et peut offrir plus de commodité et d'accessibilité. La vérification à distance peut s'appuyer sur des technologies telles que l'authentification biométrique, la numérisation de documents et les signatures électroniques pour vérifier l'identité. Cependant, ces deux méthodes présentent des inconvénients. Si la vérification à distance est pratique, elle peut soulever des inquiétudes quant à la sécurité et à la prévention de la fraude.

Analyse

Chacune des juridictions provinciales et territoriales interrogées dispose de sa propre plateforme SSO, avec des offres variées de lettres d'intention et de méthodes d'authentification. Différentes approches existent pour la vérification de l'identité dans les gouvernements, avec des gammes en termes d'inscription et d'authentification numériques. Bien que les équipes chargées des services numériques aux citoyens dans les administrations manifestent l'intention de fournir une vérification NA3 pour les services gouvernementaux connectés, il reste des défis à relever pour se conformer pleinement à la Directive sur la gestion de l'identité du gouvernement fédéral, en particulier en ce qui concerne l'utilisation de l'identité fondatrice.

Autres méthodes de vérification

La norme fédérale sur l'assurance de l'identité et des justificatifs pour le NA3 comprend des exigences telles qu'une instance fondamentale de preuve de l'identité, le recoupement des affirmations d'une personne avec un registre de dossiers tenu par une autorité reconnue, l'inspection des pièces d'identité par des examinateurs formés, et fait allusion à l'utilisation de la technologie biométrique comme méthode pour relier les informations sur l'identité.

Cela a ouvert la voie à la réalisation de NA3 par des moyens non conventionnels qui permettraient d'élargir l'éventail des options offertes aux citoyens souhaitant une vérification en ligne, et d'accroître l'accessibilité et l'inclusion. Les exemples incluent des options asynchrones et synchrones telles que les approches basées sur la vidéoconférence, et l'expérimentation d'une validation à distance entièrement automatisée via la reconnaissance faciale et la détection de l'authenticité. Pour les personnes ayant des problèmes de mobilité ou résidant dans des zones rurales, cela

pourrait s'avérer exceptionnellement accommodant et accroître considérablement l'accessibilité et l'inclusion des groupes disparates et défavorisés.

Toutefois, la prudence est de mise lorsqu'il s'agit de procéder à une vérification à distance. Les téléconférences sont de plus en plus risquées avec l'augmentation des "deep fakes" et d'autres formes de technologie d'intelligence artificielle. Les préoccupations éthiques et législatives entourant l'utilisation de la technologie biométrique pour la vérification de l'identité n'ont pas non plus été entièrement examinées, et la résolution sur le développement d'un cadre rigoureux est encore en cours d'évolution.[8] L'impact de ces technologies émergentes sur la vie privée, la sécurité et la sûreté reste à déterminer et façonnera leur intégration dans les approches actuelles de la vérification de l'identité pour la prestation de services gouvernementaux en ligne.

Susciter l'adhésion

Il n'est pas facile de faire passer les gouvernements à une plateforme SSO et à la NA3 le cas échéant. De nombreuses administrations ont cherché à obtenir un mandat d'entreprise pour faire avancer les choses, mais même celles qui en ont reçu un doivent encore prouver la valeur de la plateforme pour les services de première ligne. Il semble qu'aucun gouvernement n'ait trouvé la solution miracle : un mandat est utile mais pas suffisant. Les équipes ont discuté de l'importance de démontrer la valeur de la plateforme, certaines soulignant également l'importance de versions rapides et d'itérations continues. L'offre de la vérification d'identité NA3 a été un attrait plutôt qu'un facteur de dissuasion pour certains, soulignant la valeur d'une protection accrue de la vie privée et la possibilité de réduire les charges de validation pour les services de première ligne.

Approche flexible au NAs

Bien que la réalisation de la NA3 soit considérée comme un objectif souhaitable, il est essentiel de reconnaître que le cheminement vers ce niveau d'assurance plus élevé peut varier en fonction des priorités et des contraintes de l'organisation. Il faut comprendre que le choix de NA à appliquer dans un contexte donné doit trouver un équilibre entre le risque et l'accessibilité pour l'utilisateur et peut exiger qu'un secteur de programme accepte un risque plus élevé en raison de préoccupations liées à l'accessibilité.

---

[8] Le Commissariat à la protection de la vie privée du Canada. 2024. "Consultation sur la biométrie — Appel aux observations". https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-bio/

Par exemple, il y a des programmes qui devraient être NA3 du point de vue de la gestion des risques, comme l'assistance financière. Cependant, en raison de contraintes d'infrastructure ou d'accessibilité, les programmes peuvent être rétrogradés à une NA inférieure. Pour reprendre l'exemple de l'aide financière, si la NA a été rétrogradée au moment de la demande, un justificatif d'identité supplémentaire peut être exigé au moment de l'octroi de l'aide financière.

Des efforts visant à rendre la NA2 plus fiable au lieu de viser la NA3 de manière générale pourraient contribuer à relever ces défis. Certains programmes de services numériques aux citoyens visent un niveau d'assurance plus élevé alors que ce n'est pas vraiment nécessaire. Une solution pour rendre la vérification et l'inscription plus accessibles pourrait consister à renforcer les processus d'authentification existants en exigeant plusieurs pièces d'identité ou en mettant en œuvre des modèles d'authentification adaptatifs basés sur le niveau de risque associé à chaque transaction.

Renforcement des processus, de l'expérience utilisateur et de la gestion des risques

Il est important que la gestion de l'accès aux services numériques pour les citoyens ne se limite pas à l'obtention d'un NA plus élevée. Il existe des moyens complémentaires de renforcer l'accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens qui méritent également une attention particulière. Il s'agit notamment de s'attaquer aux systèmes existants qui entravent l'efficacité des mesures de sécurité, de surveiller le comportement des utilisateurs pour identifier les domaines à améliorer, de donner la priorité à l'expérience en alignant le parcours de l'utilisateur sur le niveau de risque attendu, ou de réduire la complexité en normalisant les processus et en rationalisant les accords pour garantir l'évolutivité de la prestation de services. Cela peut conduire à améliorer les méthodes d'authentification, à renforcer les procédures de vérification de l'identité et à minimiser la dette technique.

Recommandations

1. **Adopter une approche fondée sur le risque :** Adopter une approche fondée sur les risques pour déterminer l'exigence de NA appropriée pour chaque service. Comprendre que tous les services peuvent ne pas nécessiter de NA3 et/ou que les préoccupations relatives à l'accessibilité des citoyens à un service peuvent l'emporter sur les risques associés (par exemple, en termes d'accès à des formes d'aide financière). Impliquer les services en aval et collaborer avec

eux pour déterminer leurs exigences en matière de NA sur la base d'une évaluation des risques.

2. **S'aligner sur les normes fédérales :** Aligner les NAs pour l'accès aux services numériques destinés aux citoyens sur la Directive fédérale relative à la gestion de l'identité et sur les Ligne directrice sur l'assurance de l'identité. Déterminer la nécessité des NA 1 à 3 en fonction des contraintes d'accès des citoyens, de la sensibilité des informations auxquelles on accède et du risque de préjudice en cas de violation.

   Note : Le NA4 est généralement considéré comme hors du champ d'application des services aux citoyens.

3. **Choisissez un processus de vérification de l'identité centré sur l'utilisateur, à voies multiples et abordable :**

   Choisir des processus de vérification de l'identité qui répondent aux exigences de le NA souhaitée tout en tirant parti de l'infrastructure existante, comme les agents provinciaux/territoriaux/municipaux ou l'infrastructure de vérification existante d'une autre administration.

   - **Éviter les approches de vérification à voie unique.** Privilégier l'expérience de l'utilisateur en offrant aux citoyens de multiples options de vérification de l'identité et d'authentification. Veiller à ce que les processus soient accessibles tant du point de vue du handicap que du point de vue socio-économique, et à ce qu'ils soient faciles à utiliser sur différents appareils et plateformes.
   - **Suivre les progrès de la vérification à distance.** Étudier la possibilité de tirer parti de la vérification faciale et de la détection de la présence, et suivre l'évolution du Document d'orientation provisoire à l'intention des institutions publiques sur le traitement des données biométriques du Commissaire à la protection de la vie privée du Canada.
   - **Équilibrer le risque et l'accès** De nombreux processus NA3 peuvent limiter la plateforme SSO à la vérification des personnes résidant dans la province ou le territoire. Il se peut qu'un programme doive accepter un niveau d'assurance inférieur pour les personnes résidant en dehors de la province ou du territoire concerné, rechercher des fédérations et/ou explorer d'autres méthodes de vérification, telles que les vérifications des bureaux de crédit.

4. **Engagement des parties prenantes du gouvernement :** Renforcer le mandat des services numériques aux citoyens pour une gestion de l'accès sûre, conviviale et sécuritaire afin de placer tous les services en ligne destinés aux citoyens derrière une plateforme SSO. Cependant, il faut reconnaître que même les mandats les plus forts n'éliminent pas la nécessité d'obtenir et de maintenir l'adhésion des ministères par l'éducation et l'établissement de relations. Démontrer les avantages des services numériques améliorés pour les citoyens, tels que l'augmentation de la sécurité, de l'efficacité et de l'expérience utilisateur.

Les plateformes SSO comme courtiers en données

Alors que tous les niveaux de gouvernement au Canada continuent de moderniser leur infrastructure numérique pour améliorer les services aux citoyens, le concept de courtage de données joue un rôle important pour faciliter l'accès à ces services. Le courtage de données implique l'échange d'informations entre différentes entités afin de permettre une prestation de services personnalisée et efficace.

La question principale de cette section était la suivante :

Les plateformes d'authentification unique pour la prestation de services numériques gouvernementaux devraient-elles prendre en charge le courtage de données pour les parties utilisatrices au sein de l'administration, et éventuellement entre les programmes gouvernementaux? Dans un tel cas, comment cela devrait-il se faire?

Dans le contexte des services numériques destinés aux citoyens et des plateformes SSO, la gestion du consentement et le respect des lois sur la protection de la vie privée sont essentiels pour maintenir la confiance des citoyens et garantir la conformité aux exigences réglementaires. Deux scénarios sont couramment envisagés :

1. Partager ce que l'on appelle généralement les "données de l'annuaire" (par exemple, le nom, l'adresse électronique, parfois l'adresse et/ou la date de naissance, ainsi que tout enregistrement de validation de l'identité) d'une plateforme d'authentification unique vers un service en aval afin de garantir la vérification des informations et d'éviter à l'utilisateur d'avoir à saisir les mêmes informations à plusieurs endroits.
2. Partage d'informations entre deux services de première ligne, par exemple partage d'informations fiscales provinciales/territoriales ou municipales dans le cadre d'une demande de subvention.

En explorant le courtage de données, nous avons abordé ces deux scénarios.

Constatations relatives aux gouvernements et au marché

Gouvernements

Les plateformes de SSO de certaines provinces partagent des informations avec les services gouvernementaux connectés après l'authentification, y compris des attributs tels que le nom, la date de naissance, le sexe documenté et l'adresse pour la vérification de l'identité. Cependant, la sensibilité de chaque attribut varie et le partage de ces attributs doit être justifié en fonction des exigences du programme et de l'autorité de collecte. Certains programmes n'utilisent pas explicitement le terme "courtage de données", mais reconnaissent l'existence d'accords de partage de données.

Dites-le nous une fois

Le modèle "Dites-le nous une fois" dans la prestation de services gouvernementaux vise à simplifier le processus de mise à jour des informations personnelles. Il permet aux citoyens de fournir leurs coordonnées une seule fois à une autorité ou une agence centrale, ce qui évite de devoir répéter les mêmes informations dans plusieurs départements ou services gouvernementaux. Il n'existe pas d'approche uniforme au sein des services gouvernementaux, et les pratiques de courtage de données varient d'un service à l'autre et d'un département à l'autre. Chaque administration met en œuvre des protocoles basés sur ses accords de partenariat spécifiques et son autorité de collecte. Grâce à des approches fondées sur les risques, à l'engagement des parties prenantes et à l'utilisation responsable des technologies disponibles, les gouvernements s'efforcent de trouver un équilibre entre le confort des citoyens et le droit à la vie privée lorsqu'ils facilitent des échanges de données sûrs et efficaces pour les services aux citoyens.

Par exemple, un programme de services numériques pour les citoyens pourrait appliquer les lignes directrices suivantes :

- Pour le NA1, les services gouvernementaux connectés sont fournis avec des champs de données de base non vérifiés tels que le prénom/nom préféré, le nom de famille, l'adresse électronique, ainsi que l'identifiant du compte.
- Pour les services connectés NA2 et NA3, les attributs sont généralement vérifiés avant d'être envoyés. Il peut s'agir d'un nom, d'une adresse et d'une date de naissance vérifiés sur un permis de conduire ou une carte de santé, ou dans la base de données source de la carte concernée, par exemple, en plus des champs de données de base.

Liaison des comptes

L'interconnexion des comptes est un élément clé pour les services publics qui offraient des services en ligne avant d'utiliser une plateforme d'authentification unique. Dans la plupart des cas, les équipes de services numériques aux citoyens ne se chargent pas de la migration des anciens comptes vers la plateforme d'authentification unique. Au lieu de cela, elles peuvent utiliser un processus de liaison de compte, permettant aux citoyens de lier leur nouveau compte à un dossier existant auprès d'un service connecté. Par exemple, un programme de prêts étudiants aurait eu son propre identifiant avant d'utiliser une plateforme d'authentification unique pour les services numériques aux citoyens. Plutôt que de migrer l'ancien compte, la plateforme SSO relie le compte en posant à l'étudiant quelques questions sur sa demande de prêt étudiant (comme son nom, son numéro de matricule et son numéro d'assurance sociale), puis l'organisme de prêt étudiant est en mesure de relier le compte SSO au compte existant dans la base de données des prêts étudiants. Cela permet d'assurer la continuité sans avoir à s'exposer aux risques liés à la migration des données. Les étudiants doivent accepter les nouvelles conditions d'utilisation.

Commissaires à la protection de la vie privée

Les commissaires à la protection de la vie privée convergent vers une approche prudente du courtage de données pour les services numériques destinés aux citoyens. Il est également reconnu que la pratique consistant à demander de manière répétée les mêmes informations aux individus dans différents services gouvernementaux est considérée comme inefficace, inutile et frustrante pour les citoyens.

Premièrement, elle implique la collecte d'attributs personnels par des entités gouvernementales dans le but d'administrer des programmes spécifiques. Cette collecte doit être justifiée par la nécessité de l'information pour le fonctionnement du programme, elle ne doit être entreprise qu'avec le consentement de l'individu et elle doit faire l'objet d'un examen minutieux. Par exemple, si certaines informations peuvent être légitimement partagées avec d'autres agences gouvernementales à des fins spécifiques, comme les déclarations fiscales à l'Agence du revenu du Canada (ARC), il y a lieu de s'inquiéter lorsque les données sont partagées sans justification claire ou sans le consentement de l'individu. Les commissaires à la protection de la vie privée sont également préoccupés par le courtage de données lorsqu'il implique que le gouvernement partage des données avec des tiers externes. Il est intéressant de noter qu'aucune équipe de services numériques aux citoyens n'a déclaré partager avec des tiers les informations collectées via sa plateforme SSO.

Les sentiments des commissaires à la protection de la vie privée peuvent être résumés comme suit : "le risque de perdre la confiance des citoyens est trop grand. Faites attention aux services qui s'intègrent dans le [système SSO]. Mettez en place des accords de partage d'informations, des consentements et des normes raisonnables. Il doit être clair que le gouvernement est autorisé à collecter les données en question".[9]

Il a également été mentionné que "s'il s'agit d'une relation de gouvernement à gouvernement et qu'elle implique une entreprise technologique engagée [pour exécuter le courtage], le contrat [entre le gouvernement et l'entreprise technologique] doit être rédigé de manière à ce que les informations ne puissent être utilisées que pour des opérations gouvernementales et qu'à l'expiration du contrat, tout soit effacé et une preuve soit fournie".[10]

Délégation d'autorité dans le cadre du partage des données

En outre, les commissaires à la protection de la vie privée ont évoqué des scénarios dans lesquels les données doivent être partagées avec une personne agissant au nom d'une autre personne. Bien que la délégation de pouvoir ne soit pas ce qui vient généralement à l'esprit lorsqu'on envisage le courtage de données, les commissaires à la protection de la vie privée l'ont constamment soulevée et il vaut donc la peine d'en tenir compte dans le présent rapport. Les commissaires ont encouragé les gouvernements à collaborer avec leurs commissariats à la protection de la vie privée lorsqu'ils envisagent de déléguer des pouvoirs et de partager des informations avec un délégué (par exemple, un parent, un tuteur ou une procuration).

Par exemple, pour une personne telle qu'un tuteur agissant au nom d'un enfant, des mécanismes clairs doivent être mis en place pour vérifier l'autorité de la personne agissant au nom d'une autre, afin de s'assurer que les données sont partagées avec la bonne personne. Cela peut impliquer de prouver la tutelle légale ou d'obtenir une autorisation explicite et documentée de la personne en question (par exemple, une délégation de pouvoir dans le cas d'un parent âgé), en fonction du contexte et des exigences légales. En outre, une fois établie la nécessité pour une personne d'agir au nom d'une autre, des dispositions doivent être prises pour transférer la propriété ou le contrôle à la personne d'origine, le cas échéant. Il peut s'agir de procédures claires de révocation de l'autorisation ou de transfert des droits d'accès, garantissant la protection de l'identité et du droit à la vie privée de la personne concernée tout au long du processus.

[9] Citation tirée des entretiens avec les commissaires à la protection de la vie privée menés par LabCN entre janvier et février 2024.
[10] Ibid.

Fournisseurs de solutions

Le point de vue des fournisseurs de solutions a souligné l'importance de l'autorité, du consentement et des considérations relatives à la protection de la vie privée dans le cadre du courtage de données. Bien que les fournisseurs de solutions ne puissent pas couvrir toutes les exigences potentielles et imprévues en matière de consentement, ils ont fait écho aux commissaires à la protection de la vie privée en soulignant qu'un engagement précoce du bureau respectif du commissaire à la protection de la vie privée aiderait à garantir l'intégration des préoccupations de conception avant le développement et la mise en œuvre du système.

Techniques de courtage de données

Les fournisseurs de solutions ont souligné l'importance du contrôle de la qualité et de l'audit des activités de courtage de données, en évoquant des mécanismes tels que le stockage temporaire des données et la limitation de la portée de la collecte d'informations.

Ils ont également souligné que si les fournisseurs de solutions proposent des solutions technologiques et une expertise pour soutenir ces efforts, la responsabilité d'assurer la conformité avec les exigences réglementaires dans la manière dont les informations sont partagées entre les services incombe en fin de compte aux programmes.

Enfin, les fournisseurs de solutions ont mentionné que les justificatifs numériques peuvent permettre aux citoyens de contrôler la manière dont les données sont partagées, offrant ainsi une touche innovante au courtage de données traditionnel. Parmi les exemples, on peut citer le partage des carnets de vaccination, des habilitations de sécurité et des certificats d'études. Ceux-ci pourraient être présentés aux services gouvernementaux connectés avec une divulgation sélective appliquée de sorte que le service gouvernemental ne reçoive que ce dont il a exactement besoin.

Analyse

D'une manière générale, les pratiques de courtage de données doivent impliquer la protection de la vie privée, l'obtention du consentement, la prise en compte de scénarios complexes et la mise en place de mécanismes appropriés pour gérer ces situations de manière efficace et éthique.

Alors que certaines provinces, territoires et municipalités progressent dans des domaines tels que les solutions SSO à l'échelle de l'entreprise qui facilitent le courtage de données, d'autres sont à la traîne, aux prises avec des défis fondamentaux en matière de cybersécurité et de gestion de l'accès aux services numériques. Si le recours à des processus de passation de marchés à grande échelle s'avère lent ou difficile, il pourrait être plus durable de se concentrer sur des progrès progressifs et sur l'engagement des parties prenantes afin de parvenir à un courtage de données fiable et respectueux de la vie privée dans l'ensemble des services publics.

Gestion des consentements et autorité de recouvrement

Il est essentiel de donner la priorité au consentement et d'adhérer à une norme raisonnable. Les citoyens doivent comprendre clairement pourquoi et comment leurs informations sont collectées, utilisées, stockées et partagées, et dans quelle mesure ils peuvent contrôler et révoquer leur consentement. En outre, il doit être transparent que le gouvernement a l'autorité légale de collecter et de partager les informations en question.

En outre, bien que la mise en œuvre des pratiques de courtage de données puisse nécessiter plus de temps et d'efforts, une approche méticuleuse est essentielle pour garantir que les données des citoyens sont traitées de manière sûre et éthique. Se lancer dans des initiatives de courtage de données sans une réflexion et une mise en œuvre approfondies risquerait de compromettre la vie privée et la confiance.

Recommandations

5. **Adopter un modèle "Dites-le nous une fois" :** Aspirer à mettre en œuvre une approche "Dites-le nous une fois" dans laquelle les citoyens ne doivent fournir et vérifier qu'une seule fois les informations personnelles de leur annuaire téléphonique, qui sont ensuite partagées en toute sécurité entre la plateforme de gestion des services numériques et les départements et services gouvernementaux qui en dépendent. Cette approche permet de rationaliser les processus pour les citoyens et de réduire la charge que représente la soumission répétée des mêmes informations. Dans la mesure du possible, le stockage doit rester à la source de vérité et n'être accessible qu'à travers la plateforme SSO, conformément à la minimisation des données.
6. **Garantir l'efficacité de la notification, du consentement et de la justification :** Fournir aux citoyens une notification et un consentement clairs, concis et faciles à comprendre sur la manière dont leurs informations

personnelles seront collectées, utilisées, divulguées, stockées et partagées. Veillez à ce que ces informations soient conformes aux exigences légales et réglementaires et respectent le principe de minimisation des données. La plateforme SSO doit fournir :

- Comment les citoyens peuvent exprimer leurs préoccupations, poser des questions ou révoquer leur consentement.
- Des reçus de consentement documentant ce à quoi il y a eu consentement, et à quel moment.
- La possibilité de notifier, et de consentir à nouveau, si les conditions d'utilisation ont été modifiées.

7. **Établir des accords solides de partage des données :** Élaborer des accords de partage de données clairs et complets entre le programme de services numériques aux citoyens et les services connectés. Ces accords doivent préciser les raisons pour lesquelles les données seront partagées, garantir le respect des lois sur la protection de la vie privée et établir des protocoles pour la protection et la suppression des données. Pour les services publics connectés, ces accords devraient être normalisés afin de rationaliser la gestion des accords et d'assurer la cohérence entre les services en aval.
8. **Collaborer avec d'autres administrations :** Tirer parti de l'expérience d'autres administrations dans la mise en œuvre d'initiatives de gestion de l'accès aux services numériques pour les citoyens et de courtage de données.
9. **Garder à l'esprit l'autorité déléguée :** Évaluer et traiter la question de la délégation de pouvoir dans le cadre de la livraison de services numériques, notamment dans les situations où des personnes agissent au nom d'autres personnes (par exemple, dans le cadre d'une tutelle). Développer des processus de vérification pour confirmer l'autorité déléguée, la clarté, la responsabilité et l'alignement sur les processus juridiques existants.

Fédération

La fédération consiste à établir des relations de confiance entre un gestionnaire de services SSO et une ou plusieurs parties utilisatrices afin de permettre une authentification et une autorisation transparentes entre plusieurs systèmes. Dans le contexte de la gestion de l'accès aux services numériques des citoyens, la fédération désigne la possibilité pour les utilisateurs d'utiliser leurs justificatifs provenant d'une source de confiance pour accéder à des services fournis par d'autres entités, sans avoir besoin de justificatifs distincts.

Les plateformes de SSO pour les citoyens sont un exemple de fédération, permettant aux citoyens de s'identifier une seule fois et d'accéder à des services connectés. L'avantage est qu'il n'est pas nécessaire de se souvenir de plusieurs noms d'utilisateur et mots de passe pour accéder aux services provinciaux/territoriaux ou municipaux.

La possibilité de se fédérer aux services du gouvernement du Canada par le biais d'une plateforme de SSO pour les citoyens est un autre exemple. Cette plateforme existe actuellement pour les résidents de la Colombie-Britannique et de l'Alberta, et les considérations relatives aux autres juridictions souhaitant se fédérer avec le gouvernement fédéral font l'objet de la présente section. La question principale de l'enquête était la suivante :

> Comment les plateformes d'authentification unique utilisées au niveau provincial et territorial peuvent-elles accéder aux services du gouvernement fédéral par le mécanisme de la fédération?

La fédération améliore l'expérience de l'utilisateur en permettant un accès sécurisé aux services distribués, en améliorant la sécurité et en facilitant la collaboration entre les différentes juridictions, les programmes et les services.

Constatations relatives aux gouvernements et au marché

Gouvernements

La fédération avec le gouvernement du Canada implique la création d'accords bilatéraux basés sur les évaluations de la province ou du territoire par le gouvernement fédéral, suivies d'une intégration technique. L'évaluation se fait à

l'aide du profil du secteur public (CCP-PSP)[11] , qui permet d'intégrer un service dans le cadre politique du gouvernement du Canada en utilisant une approche commune. Une évaluation réussie donne lieu à une lettre d'acceptation du directeur général de l'information (DSI) du Canada, qui décrit également les résultats et les recommandations. Bien qu'il ne soit pas nécessaire qu'un service réponde à une lettre d'acceptation particulière, le gouvernement fédéral est principalement intéressé par les niveaux 2 et 3 d'assurance de l'identité et des références, conformément à le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3).[12]

Réussites passées et perspectives alternatives

Comme nous l'avons vu, la Colombie-Britannique et l'Alberta ont mis en œuvre avec succès la fédération avec le gouvernement fédéral, permettant à leurs résidents de se connecter aux services du gouvernement fédéral en utilisant leurs informations de connexion uniques provinciales. La fédération s'est appuyée sur une évaluation de la conformité, la collaboration et, bien sûr, la mise en œuvre technique.

D'autres gouvernements ont choisi d'utiliser des solutions de partenaires de SSO, que le gouvernement fédéral soutient également. Les résidents peuvent donc déjà utiliser les mêmes informations d'identification pour se connecter aux services des administrations et aux services du gouvernement du Canada. Cette approche répond aux besoins des résidents et des entreprises sans nécessiter de fédération supplémentaire.

Commissaires à la protection de la vie privée

Les commissaires à la protection de la vie privée ont souligné l'importance de fédérer les plateformes SSO provinciales et territoriales avec le gouvernement fédéral pour accéder aux services de ce dernier. Ils ont également insisté sur la nécessité de protéger la vie privée, d'adopter des mesures de sécurité strictes et d'établir une responsabilité claire grâce à des structures de gouvernance et à la mise en œuvre de processus adéquats.

Un commissaire à la protection de la vie privée a encouragé les gouvernements à poursuivre la fédération avec le gouvernement fédéral, déclarant "quel gâchis ce

[11] Profil du secteur public du Cadre de Confiance pancanadien | Pan-Canadian Trust Framework. https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_4
[12] Gouvernement du Canada. Avril 2018. "Guide d'authentification des utilisateurs pour les systèmes de technologie de l'information (ITSP.30.031 v3)". https://www.cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3

serait si un gouvernement canadien développait cet excellent système de vérification de l'identité et ne l'intégrait pas au gouvernement fédéral pour accéder aux services (en ligne ou autres)".[13]

Il est essentiel de garantir une formation adéquate et des interfaces conviviales pour les citoyens, compte tenu des écarts potentiels entre les générations et des différents niveaux d'accès, en particulier dans les communautés rurales qui disposent souvent d'une connectivité internet limitée. Ils ont également souligné que les programmes gouvernementaux doivent veiller à déterminer qui sera responsable de quoi et à fournir une formation adéquate aux citoyens.

Fournisseurs de solutions

Les fournisseurs de solutions ont souligné l'importance des accords de service et des interfaces techniques normalisés pour faciliter les processus d'intégration entre les gouvernements. Ils ont noté que les aspects techniques de la fédération sont considérés comme moins compliqués, mais ont souligné les défis posés par les considérations juridiques et commerciales. Ils ont plaidé en faveur d'accords évolutifs qui pourraient s'adapter à de multiples juridictions sans dupliquer les efforts.

En outre, les fournisseurs de solutions ont suggéré que les gouvernements, en particulier les plus petits, se concentrent sur des solutions sur mesure qui s'alignent sur des cas d'utilisation spécifiques et des besoins de gouvernance. Dans l'ensemble, les fournisseurs de solutions ont souligné l'importance de la collaboration, de la normalisation et de l'alignement stratégique pour la réussite des initiatives de fédération.

Analyse

La fédération peut tirer parti des systèmes de SSO existants pour améliorer l'accès aux services gouvernementaux entre les différents gouvernements. Bien qu'elle n'ait pas été explicitement étudiée dans le présent rapport, la fédération entre provinces et territoires (par exemple, une province ou un territoire acceptant le processus d'ouverture de session d'une autre province ou d'un autre territoire) ou entre municipalités et provinces/territoires (par exemple, les municipalités tirant parti des processus d'ouverture de session provinciaux ou territoriaux pour accéder aux services municipaux) pourrait améliorer l'accès aux services gouvernementaux, tels que les permis de chasse, pour les personnes qui se déplacent fréquemment. La

[13] Citation tirée des entretiens avec les commissaires à la protection de la vie privée menés par LabCN entre janvier et février 2024.

fédération pourrait également réduire la charge liée au nom d'utilisateur et au mot de passe et, dans le cas des municipalités utilisant des mécanismes d'authentification provinciaux ou territoriaux, limiter la nécessité pour les municipalités de mettre en place leur propre service de gestion des identités et des accès (NA3).

L'évolution du paysage technologique et son impact sur les stratégies de fédération avec les services gouvernementaux est un sujet d'actualité. Les technologies émergentes, telles que les justificatifs numériques, peuvent offrir des approches alternatives qui pourraient alléger ou compléter les méthodes de fédération traditionnelles. Les justificatifs numériques pourraient être utilisés à la place d'un nom d'utilisateur et d'un mot de passe, ce qui éliminerait ou du moins réduirait la nécessité d'une fédération point à point. Cela souligne l'importance de rester adaptable et réactif aux avancées technologiques dans le domaine de la gestion de l'accès aux services numériques destinés aux citoyens.

Recommandations

Pour les juridictions qui souhaitent se fédérer avec le gouvernement fédéral :

10. **Comprendre les exigences de la fédération du gouvernement fédéral :** Examiner en détail le CCP-PSP ainsi que le dernier manuel publié, car ils constituent la base de l'évaluation du gouvernement fédéral. Travailler avec les membres du gouvernement fédéral pour mieux comprendre le processus formel d'évaluation du gouvernement fédéral et identifier les lacunes. Il se peut que le gouvernement fédéral ait évolué dans son approche et qu'il ait dépassé les derniers documents publiés.

11. **Tirer parti des efforts déployés par les gouvernements dans le passé :** Les gouvernements qui ont déjà suivi le processus de fédération fédérale disposent d'une mine de connaissances. Lorsqu'un programme de services numériques aux citoyens entame la phase de préparation et d'analyse des lacunes pour sa ou ses solutions de gestion des identités et des accès, il est vivement recommandé de faire appel à ces administrations.

Pour les fédérations fédérales et tout autre type de fédération, les éléments suivants sont importants :

12. **Allouer les ressources appropriées :** Allouer les ressources nécessaires, y compris le personnel et le budget, pour soutenir le processus de fédération.

Cette initiative nécessite des efforts ciblés et n'est pas recommandée en tant qu'activité secondaire.

13. **S'assurer que la plateforme SSO et les structures de support sont suffisamment documentées :** Examinez les définitions, les processus, les rôles et les responsabilités actuels du programme et assurez-vous qu'ils sont tous documentés.

    - **Définir et documenter la responsabilité et la gouvernance :** Définir et documenter clairement les structures de responsabilité et les processus de gouvernance au sein du programme. Le fait de les concevoir et de les documenter avec des mécanismes de rapport et de contrôle transparents dès le début contribuera à instaurer la confiance entre les parties fédératrices.

14. **Assurer la transparence et le consentement des utilisateurs :** Maintenir la transparence en ce qui concerne la collecte et l'utilisation des données à caractère personnel. Veiller à ce que les citoyens sachent clairement qui, parmi les partenaires de la fédération, collecte, utilise, stocke ou divulgue des données, et quels sont les attributs de ces données. Obtenir le consentement explicite des utilisateurs pour les activités de traitement des données et communiquer clairement les raisons pour lesquelles leurs informations sont collectées, utilisées, stockées et partagées. Le programme doit également permettre aux utilisateurs d'accéder facilement à leurs préférences en matière de consentement et de les mettre à jour, ce qui favorise la transparence.

Comment travailler efficacement avec les commissaires à la protection de la vie privée

Grâce à un engagement proactif, à une communication transparente et à un engagement en faveur de pratiques respectueuses de la vie privée, les entités gouvernementales peuvent efficacement respecter les normes en matière de protection de la vie privée, protéger les informations des citoyens et garantir le succès des initiatives numériques.

La question principale à étudier dans cette section était la suivante :

Comment une équipe de services numériques destinés aux citoyens peut-elle collaborer de façon optimale avec son commissaire à la protection de la vie privée pour garantir un accès sûr, convivial et sécuritaire aux services numériques destinés?

Sur la base d'entretiens avec des responsables gouvernementaux du Canada et de ses provinces/territoires, voici quelques éléments clés sur les stratégies, les bonnes pratiques et les éléments à prendre en compte pour favoriser la collaboration avec les commissaires à la protection de la vie privée.

Constatations relatives aux gouvernements

Un engagement précoce est encouragé, mais il faut reconnaître que le fait de montrer un travail précoce peut se transformer en enquête. Il est donc important que les programmes soient conçus pour soutenir une enquête ultérieure. Les initiatives réussies en matière de services numériques aux citoyens ont travaillé en étroite collaboration avec leurs commissaires à la protection de la vie privée, équilibrant à la fois l'éducation et la consultation depuis la conception de leur système de SSO jusqu'au lancement et à l'amélioration continue. Une consultation supplémentaire est particulièrement importante en cas de changements architecturaux importants, de modifications de la gestion des consentements, d'implications en matière de courtage de données ou d'expérimentation avec la biométrie.

Intégration des services

Pour qu'un service puisse s'intégrer à une plateforme SSO, il doit généralement prouver qu'il est habilité à collecter des données et réaliser sa propre évaluation des incidences sur la vie privée dans le cadre d'une activité d'intégration. Ces évaluations

présentent souvent un intérêt pour les commissaires à la protection de la vie privée et il est généralement recommandé, même si ce n'est pas obligatoire, d'inclure ces derniers dans le processus d'intégration d'un nouveau service.

Commissaires à la protection de la vie privée

L'avis collectif a mis l'accent sur quelques principes clés autour de trois thèmes : la sensibilisation précoce, l'éducation et l'orientation, et la protection de la vie privée dès la conception avec l'engagement de l'utilisateur.

Sensibilisation précoce

Les commissaires à la protection de la vie privée ont encouragé les contacts précoces en général. Ils ont souligné l'importance d'un engagement précoce avec leurs bureaux, en particulier pour les projets impliquant la collecte de données et d'informations personnelles. Les ministères et les programmes devraient prendre l'initiative de demander des conseils et des consultations, plutôt que d'attendre les dernières étapes du développement. Les commissaires à la protection de la vie privée ont reconnu que, par le passé, ils craignaient d'être exclus pour s'être engagés trop tôt dans un projet. Un commissaire à la protection de la vie privée a déclaré que "plus nous intervenons tôt, plus nous avons de chances d'être sur la bonne voie, en veillant à ce que votre projet soit conforme à la réglementation et aux meilleures pratiques en matière de protection de la vie privée dès le départ" et "n'attendez pas d'être allé trop loin dans le développement. Au lieu, utilisez la protection de la vie privée dès la conception". [14]

L'implication du commissaire peut être "une réflexion après coup qui est entreprise plus tard qu'elle n'aurait pu l'être pour cocher une case dans un court délai".[15] Les commissaires à la protection de la vie privée ont fait remarquer qu'il fallait éviter cette approche. Si les équipes de services numériques aux citoyens ne s'engagent pas suffisamment tôt avec leurs commissaires à la protection de la vie privée, elles n'ont pas le temps d'intégrer ce retour d'information dans leur solution. Des consultations fréquentes permettent également d'instaurer la confiance et de promouvoir la transparence.

[14] Citation tirée des entretiens avec les commissaires à la protection de la vie privée menés par LabCN entre janvier et février 2024.
[15] Ibid.

Éducation et orientation

Certains commissaires à la protection de la vie privée proposent du matériel pédagogique, des ateliers et des conférences pour aider les administrations à comprendre les exigences et les meilleures pratiques en matière de protection de la vie privée. Cela permet de dissiper les craintes concernant les relations avec le commissaire à la protection de la vie privée et d'encourager une collaboration proactive.

Certains commissariats à la protection de la vie privée proposent sur leur site web des conseils sur la manière de réaliser une EIPD ou de consulter le commissariat. D'autres ont adopté une approche plus proactive, axée sur l'établissement de relations et l'adoption de modèles de portefeuille avec des équipes désignées pour certains types de projets. Il est important que les secteurs de programmes gouvernementaux apprennent comment leur commissariat à la protection de la vie privée respectif est structuré et quelle est la meilleure façon de s'engager.

Protection de la vie privée dès la conception et engagement du public

Enfin, les commissaires à la protection de la vie privée ont souligné l'importance du respect des principes de protection de la vie privée dès la conception, de la réalisation d'évaluations approfondies des risques, de la mise en œuvre de solides mesures de protection de la vie privée et de la collaboration avec les utilisateurs, autant d'éléments essentiels pour garantir le respect des lois et réglementations en matière de protection de la vie privée. Dans la mesure du possible, les commissaires à la protection de la vie privée ont également encouragé la consultation du public.

Analyse

Ces expériences ont en commun de mettre l'accent sur la sensibilisation et l'engagement précoces auprès des commissariats à la protection de la vie privée. Par exemple, l'examen de chaque service se connectant à une plateforme SSO et les évaluations des incidences sur la vie privée menées tout au long du cycle de vie du projet SSO sont des étapes importantes. Les principes de protection de la vie privée dès la conception sont également importants pour une collaboration efficace avec les commissaires à la protection de la vie privée.

En résumé, pour travailler efficacement avec les commissaires à la protection de la vie privée, il faut une approche proactive, de la formation et des conseils, la compréhension et le respect des méthodologies existantes, ainsi qu'un engagement public significatif. En adoptant ces principes fondamentaux, les initiatives gouvernementales peuvent s'attaquer avec succès aux questions de protection de la vie privée et instaurer un climat de confiance avec les parties prenantes et le public.

Recommandations

15. **S'engager tôt et collaborer :** S'engager très tôt avec le bureau du commissaire à la protection de la vie privée pour garantir l'alignement sur les principes et les réglementations en matière de protection de la vie privée. Tenez-le informé tout au long de la conception, de la mise en œuvre et de l'amélioration continue, et maintenez une étroite collaboration afin de répondre de manière proactive à toute préoccupation ou problème.

16. **Établir des intervalles de rapport réguliers :** Établissez des intervalles de rapport réguliers et déterminez des déclencheurs, tels que l'intégration d'un nouveau service pour programmer des consultations supplémentaires. Cette cohérence contribuera à renforcer la transparence, la confiance et la collaboration.

17. **Travaillez avec votre responsable de la protection de la vie privée :** Faites participer le responsable provincial ou territorial de la protection de la vie privée à l'établissement de la cadence et de l'approche de la collaboration. Il sera important de le tenir au courant des activités de l'équipe des services numériques aux citoyens et c'est lui qui saura le mieux comment collaborer efficacement avec le commissaire à la protection de la vie privée de sa province ou de son territoire.

18. **Travaillez avec votre commissaire à la protection de la vie privée sur le consentement et la transparence :** Lorsqu'une équipe de services numériques aux citoyens donne la priorité au consentement de l'utilisateur et assure la transparence des pratiques de collecte de données, elle doit travailler en étroite collaboration avec son commissaire à la protection de la vie privée pour répondre à toute préoccupation ou hypothèse concernant l'utilisation des données et les implications en matière de protection de la vie privée.

Vers des justificatifs numériques

Comme indiqué dans l'introduction, les justificatifs numériques représentent une approche transformatrice de la vérification de l'identité. Alors que la plupart des programmes gouvernementaux se concentrent sur l'émission d'un justificatif de personne vérifiable - qui est une forme générique de pièce d'identité avec photo émis par le gouvernement - LabCN souhaite attirer l'attention sur la valeur d'un programme de justificatifs numériques qui va au-delà du simple justificatif de personne. Des documents d'enregistrement des entreprises aux permis de chasse en passant par les relevés de notes et les licences, l'investissement dans un programme de justificatifs numériques ouvre un large éventail de possibilités pour les citoyens et les entreprises, tout en réduisant la fraude et en offrant une meilleure protection de la vie privée.

Constatations relatives aux gouvernements et au marché

Gouvernements

Les justificatifs numériques sont envisagés dans la plupart des gouvernements interrogés pour ce rapport, qui en sont à des stades de maturité variables. La Colombie-Britannique est à la pointe avec des justificatifs numériques en cours de production pour les particuliers (personne vérifiée), les avocats (preuve d'être avocat via l'ordre des avocats), l'enregistrement des entreprises et les justificatifs de l'industrie minière tels que les rapports environnementale, sociale et de gouvernance (ESG) et les permis gouvernementaux.

D'autres administations avancent dans leur démarche, explorant activement la mise en œuvre des justificatifs numériques et disposant actuellement de la technologie nécessaire pour les délivrer. Toutefois, avant d'aller de l'avant, elles procèdent à une évaluation juridique complète afin de déterminer le cadre réglementaire entourant l'utilisation des justificatifs numériques. Cette évaluation consiste à examiner la législation existante et à déterminer si des modifications ou de nouvelles lois sont nécessaires pour fournir le soutien juridique nécessaire aux justificatifs numériques.

D'autres encore en sont à divers stades d'expérimentation, explorant des preuves de concept et des projets pilotes, et collaborant à des forums pancanadiens sur les justificatifs numériques et la cybersécurité. Ces administrations peuvent ou non disposer d'une infrastructure d'entreprise. Elles préfèrent commencer par des cas d'utilisation ciblés et de petite envergure, comme les cartes d'employé pour la gestion de groupe et l'exploration des justificatifs liés à l'apprentissage d'un métier.

Une administration s'est lancée dans une série de projets pilotes axés sur les justificatifs numériques, auxquels participent diverses parties prenantes telles que des organismes centraux et des institutions bancaires. Un cas d'utilisation notable concerne la création d'une société en ligne pour ouvrir un compte bancaire commercial et un portefeuille numérique. Toutefois, au moment de la publication du présent rapport, cette initiative n'avait pas abouti à une solution de production.

Au-delà des avancées gouvernementales, il existe également une collaboration intra-gouvernementale sur l'infrastructure de réseau afin de permettre le partage et l'interopérabilité entre les provinces et les territoires. L'objectif est de promouvoir l'adoption de protocoles et de pratiques normalisés pour les justificatifs numériques. Les parties prenantes soulignent l'importance de l'adhésion de toutes les provinces au réseau, ce qui met en évidence la nécessité de normes cohérentes et d'une approche unifiée des justificatifs numériques dans tout le Canada.

Défis

Il ne fait aucun doute que le passage des justificatifs en papier ou les PDF traditionnels aux justificatifs numériques nécessitera une période d'adaptation importante, avec la coexistence probable de plusieurs modes d'authentification pendant la phase de transition. La préparation à une adoption généralisée dépend de l'engagement des parties prenantes, de l'intégration technologique et de l'acceptation dans divers secteurs hautement représentatifs, tels que le domaine de la santé.

Entre-temps, il reste quelques défis à relever. Le travail sur l'infrastructure nationale fondamentale pour soutenir les échanges transfrontaliers de justificatifs reste balbutiant, bien qu'il y ait eu quelques annonces de collaboration pour tenter de faire avancer les choses. [16]

Les piles technologiques sont variées, avec des préférences différentes d'un bout à l'autre du pays, ce qui rend l'interopérabilité plus difficile, et s'il est admis que le pays ne convergera pas vers une pile technologique unique, la complexité dès le départ limite l'évolutivité.

Enfin, la désinformation continue de tronquer les conversations publiques constructives. Le programme du gouvernement de la Saskatchewan a été

[16] Newswire. Janvier 2023. "Avancées importantes en matière d'identité numérique pour le Québec - Rencontre des ministres fédéral, provinciaux et territoriaux sur la confiance numérique et la cybersécurité", https://www.newswire.ca/fr/news-releases/avancees-importantes-en-matiere-d-identite-numerique-pour-le-quebec-rencontre-des-ministres-federal-provinciaux-et-territoriaux-sur-la-confiance-numerique-et-la-cybersecurite-869739478.html

interrompu en raison des pressions exercées par le public[17] et d'autres gouvernements ont également été confrontés à la pression du public en raison de campagnes actives de désinformation et de mésinformation.[18,19]

Enseignements tirés

Les principaux enseignements tirés des initiatives comprennent l'importance de tirer parti des ressources et de l'infrastructure existantes, en particulier grâce à des composants open source. En outre, le partenariat avec des justificatifs numériques réputés permet de rationaliser le processus de mise en œuvre et de réduire les délais et les efforts.

Une juridiction a recommandé de commencer modestement et de se concentrer sur la mise en œuvre d'un produit minimum viable avec des références à faible risque. Elle préconise une approche de croissance progressive, permettant d'affiner et d'étendre les capacités au fil du temps, à mesure que le projet mûrit et prend de l'ampleur.

Dans l'ensemble, il est important d'adopter une approche systématique de l'adoption des justificatifs numériques, en veillant à ce que les considérations juridiques et pratiques soient soigneusement prises en compte avant la mise en œuvre.

Commissaires à la protection de la vie privée

Les principes fondamentaux de la protection de la vie privée restent inchangés malgré l'avènement des justificatifs numériques. Les commissaires à la protection de la vie privée ont souligné l'importance de faire la distinction entre les différents types de justificatifs numériques et de veiller à ce que les considérations relatives à la protection de la vie privée et à la sécurité soient primordiales à chaque étape de leur mise en œuvre. Si des technologies telles que la reconnaissance faciale et la biométrie offrent des possibilités d'authentification, elles doivent être déployées en accordant une attention particulière à la protection de la vie privée.

---

[17] CTV News. 2022. "Plan to introduce digital identification system in Sask. put on hold", https://regina.ctvnews.ca/plan-to-introduce-digital-identification-system-in-sask-put-on-hold-1.5846948

[18] Laboratoire de la confiance numérique du Canada. 2023. "Mésinformation et désinformation en matière d'identité numérique", https://dtlab-labcn.org/mesinformation-et-desinformation-en-matiere-didentite-numerique/

[19] CTV News. 2022 "Ontario government won't comment on progress of digital ID program", https://toronto.ctvnews.ca/ontario-government-won-t-comment-on-progress-of-digital-id-program-1.5852732

En outre, un commissaire a proposé de qualifier ces justificatifs de "vérification", suggérant que "l'étiquette de vérification... passe mieux que celle d'identité numérique ou de justificatif numérique", en référence à la désinformation qui sévit sur le sujet. Un autre a fait court et simple, déclarant que l'émergence de la technologie biométrique n'avait "aucun impact" et que les "mêmes principes s'appliquaient".[20]

Les thèmes récurrents de la protection de la vie privée et de la responsabilité, repris par les commissaires à la protection de la vie privée, sont renforcés par une résolution commune, dans laquelle les commissaires à la protection de la vie privée et les médiateurs de l'ensemble du pays s'alignent sur des sujets clés.[21] La résolution souligne que la participation à un écosystème de justificatifs numériques doit être volontaire et facultative pour les individus. Les personnes doivent pouvoir contrôler leurs informations personnelles et disposer de mécanismes de consentement clairs et éclairés.

La résolution souligne l'importance de la protection de la vie privée, de la transparence et des droits individuels dans la conception et le fonctionnement des systèmes de justificatifs numériques au Canada. Ce document présente les caractéristiques importantes d'un écosystème de justificatifs numériques afin de gagner la confiance et de respecter les principes susmentionnés, à savoir la minimisation et la protection des informations personnelles, la vérifiabilité et l'accès équitable. Il témoigne d'un engagement à faire en sorte que les initiatives en matière de justificatifs numériques profitent aux Canadiens tout en respectant leur droit à la vie privée.

Collectivement, les déclarations des commissaires à la protection de la vie privée soulignent qu'il est impératif de gagner la confiance et de tenir compte de la perception du public en employant et en maintenant des mesures de protection de la vie privée et de sécurité lors de l'élaboration des justificatifs numériques afin de garantir la confiance dans leur utilisation. Les commissaires à la protection de la vie privée reconnaissent les avantages potentiels des justificatifs numériques, mais s'inquiètent également des conséquences sur la vie privée et de la nécessité de disposer de cadres juridiques clairs pour régir leur utilisation. En outre, la vie privée des utilisateurs doit être protégée tout au long du cycle de vie des titres.

---

[20] Citation tirée des entretiens avec les commissaires à la protection de la vie privée menés par LabCN entre janvier et février 2024.
[21] Commissariat à la protection de la vie privée du Canada. Septembre 2022. "Assurer le droit à la vie privée et la transparence dans l'écosystème d'identité numérique au Canada". https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_220921_02/

Fournisseurs de solutions

Les fournisseurs de solutions ont suggéré de commencer modestement, avec des projets de justificatifs numériques gérables, en préconisant la réalisation de tests et de projets pilotes avant une mise en œuvre à grande échelle. Ils conseillent de suivre les normes établies et mettent en garde contre la tentation de tout construire en même temps. Un fournisseur de solutions a suggéré aux administrations de "commencer, de mettre en place des tests et des projets pilotes et d'être prêtes à faire face aux changements. N'essayez pas de tout construire vous-même".[22]

La définition et la mise en œuvre des justificatifs numériques varient selon les parties prenantes, ce qui nécessite la recherche d'un consensus pour aligner la compréhension et les attentes. "Il peut avoir des significations différentes selon les personnes et prendre des formes diverses telles qu'un diplôme ou une licence. Il s'agit simplement d'un justificatif numérique qui peut être vérifié par rapport à une source faisant autorité." Ils expliquent que les organisations doivent "examiner l'objectif commercial et ce qu'elles essaient d'atteindre, puis sélectionner la technologie qui a du sens en termes d'évolutivité et de sécurité, et qui répond à d'autres besoins de l'entreprise".[23]

Les fournisseurs de solutions ont l'expérience de l'intégration avec les portefeuilles numériques et prévoient que les gouvernements deviendront d'importants émetteurs de justificatifs numériques. La collaboration entre les équipes techniques et les équipes de marketing/communication est essentielle à la réussite des projets de justificatifs numériques, car elle garantit la faisabilité technologique et une communication efficace avec les parties prenantes. Bien que des défis existent, les fournisseurs de solutions restent confiants dans la valeur et le potentiel des justificatifs numériques malgré des revers occasionnels ou des détracteurs.

Analyse

Les justificatifs numériques représentent un changement de paradigme potentiel en termes de protection de la vie privée et de surveillance au sein de nos systèmes. Cependant, il est important de comprendre les subtilités des justificatifs numériques. Par exemple, à l'heure où nous écrivons ces lignes, le Verifiable Credential Standard du World Wide Web Consortium (W3C)[24] est plus sûr sur le plan cryptographique,

[22] Une citation tirée des entretiens avec les fournisseurs de solutions menés par LabCN entre janvier et février 2024.
[23] Ibid
[24]Consortium World Wide Web (W3C). Mars 2023. "W3C Verifiable Credential (VC) Data Model V1.1". https://www.w3.org/TR/vc-data-model/

mais protège moins la vie privée que son équivalent Hyperledger, connu sous le nom d'Anoncreds. [25]

Pour naviguer dans cette technologie émergente, une collaboration ouverte et des progrès progressifs sont encouragés, avec de petites équipes travaillant ouvertement, collaborant avec d'autres, et démontrant des preuves tangibles de concept pour favoriser la compréhension et l'adhésion.

Les efforts d'exploration et les projets pilotes actuels peuvent permettre aux petites autorités gouvernementales d'être non seulement plus aptes sur le plan technologique, mais aussi de préparer les entreprises en prévision d'une adoption plus large. Même si certains ne cherchent pas activement à obtenir des justificatifs numériques, il est intéressant d'explorer leurs applications et implications potentielles, notamment en raison des avantages qu'ils présentent en termes de protection de la vie privée et de réduction de la fraude.

Prochaines étapes

Les principaux éléments à prendre en compte sont la définition des cas d'utilisation, la prise en compte des questions de protection de la vie privée et la garantie de l'interopérabilité avec d'autres systèmes. Sur ce dernier point, il convient de souligner qu'une organisation de premier plan dans ce domaine a fourni une feuille de route de haut niveau pour permettre l'interopérabilité à court terme par l'intermédiaire des gouvernements participants qui utilisent tous le même réseau. L'objectif de cette feuille de route est d'accélérer la mise en œuvre à court terme. Elle tient compte du fait que de multiples piles technologiques et fournisseurs, et donc des problèmes d'interopérabilité plus complexes, sont susceptibles d'apparaître au fil du temps.

L'évaluation des progrès des justificatifs numériques dans différentes régions révèle un paysage en évolution rapide, caractérisé par des approches diverses, des niveaux de préparation variables et des avancées technologiques constantes. La mise en place de mécanismes de suivi continu des progrès et des tendances peut permettre aux parties prenantes de rester au fait des technologies émergentes, de l'adoption des normes, de l'évolution des meilleures pratiques et des développements réglementaires. En faisant preuve de souplesse et de réactivité, elles peuvent tirer parti de nouvelles opportunités et s'assurer que leur approche reste pertinente. Adopter une approche proactive du suivi des progrès en participant à des groupes communautaires peut contribuer à intégrer l'innovation et à renforcer la capacité à fournir des justificatifs numériques sécurisés et centrés sur l'utilisateur.

---

[25] Hyperledger AnonCreds. Novembre 2022. "AnonCreds Methods Registry V0.1 Draft". https://hyperledger.github.io/anoncreds-methods-registry/

Recommandations

19. **Commencer par des programmes pilotes :** Commencez par des programmes pilotes à petite échelle pour tester l'efficacité des justificatifs numériques dans des cas d'utilisation spécifiques. Ces programmes pilotes peuvent aider à identifier les défis et les opportunités potentiels tout en minimisant les risques associés à une mise en œuvre plus large, et à accroître les capacités internes pour les projets futurs. Cherchez également des occasions de présenter ces projets pilotes, car cela peut générer un retour d'information important et améliorer les possibilités de collaboration.

20. **Tirer parti des réussites des programmes pilotes :** Exploiter les connaissances et les enseignements tirés des programmes pilotes afin d'éclairer les décisions futures et d'étendre les initiatives réussies. Identifier les domaines d'amélioration et itérer sur les projets pilotes pour affiner les processus, relever les défis et maximiser la valeur dérivée des justificatifs numériques à travers le Canada. Adapter les stratégies de mise en œuvre en fonction des enseignements tirés et élaborer des mécanismes pour mieux recueillir et intégrer les commentaires des participants aux projets pilotes et des parties prenantes, tels que les enquêtes et les groupes de discussion.

21. **Familiariser l'équipe avec les normes et les cadres établis :** Prendre le temps de comprendre les différents cadres, normes et composants techniques et leur évolution au niveau mondial (voir l'annexe). Suivre l'évolution des normes et des cadres pour soutenir l'interopérabilité avec l'industrie. Veillez à ce que ces connaissances soient acquises par l'ensemble de l'équipe et non par une seule personne, car elles ont des implications interfonctionnelles.

22. **Suivre les progrès et les tendances :** Suivre en permanence les progrès et les tendances dans le domaine des justificatifs numériques. Rester informé des technologies émergentes, des meilleures pratiques et des évolutions réglementaires afin d'adapter les stratégies de mise en œuvre en conséquence et de tirer parti des nouvelles opportunités. L'annexe contient une liste de groupes de travail à prendre en considération.

Section 3

Recommandations générales

3

Recommandations générales

Ces recommandations sont le reflet de la recherche effectuée pour ce rapport et de l'expertise existante de LabCN.

1. **Adopter une approche programmatique pour garantir un accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens :** Concevoir la gestion de l'accès aux services numériques destinés aux citoyens comme un programme plutôt que comme un projet informatique. Élaborer une vision du programme qui soit centrée sur le citoyen, axée sur les résultats et qui donne la priorité à la collaboration avec les parties prenantes. Travailler à la mise en place d'une dotation en personnel adéquate et à l'établissement d'un financement pluriannuel.

   En particulier :

   a. **Élaborer une structure de gouvernance du programme :** Pour assurer un contrôle rigoureux et susciter l'adhésion, créer un comité de gouvernance (ou s'appuyer sur un comité existant approprié) qui recevra des mises à jour du programme à intervalles réguliers et sera chargé des décisions présentant les risques les plus élevés ou la valeur stratégique la plus importante. Le comité de gouvernance devrait être composé de représentants des principales parties prenantes dans l'ensemble du gouvernement.

   b. **Constituer une équipe interfonctionnelle :** La composition exacte peut varier, mais pour les petites juridictions, il s'agit généralement d'un mélange de membres de l'équipe de base, d'autres ressources affectées au travail dans le cadre d'un portefeuille de tâches plus large (par exemple, un architecte de solutions, un spécialiste de la sécurité ou de la protection de la vie privée) et d'autres aspects du travail confiés à des contractants ou à des vendeurs. L'équipe doit comprendre un chef de programme, un ou plusieurs gestionnaires de projet ou de produit et un ou plusieurs analystes d'affaires, ainsi que des spécialistes dans des domaines tels que la protection de la vie privée, la sécurité, l'expérience utilisateur/la conception de services, la communication, le droit, l'architecture, l'assistance à la clientèle et des représentants des services en aval.

   c. **Investir dans le renforcement des capacités :** Les talents en matière de gestion des justificatifs numériques et des accès centrés sur les

citoyens sont difficiles à trouver. Par conséquent, les gouvernements se concentrent souvent sur l'amélioration des compétences de leur personnel interne. Renforcer les capacités internes liées à la gestion de l'accès aux services numériques pour les citoyens, y compris la formation de l'équipe du programme général décrite ci-dessus. La formation doit permettre de s'assurer que chaque membre de l'équipe possède les connaissances de base, que l'équipe parle le même langage et qu'elle jette des ponts entre les membres de l'équipe technique et ceux de l'équipe commerciale.

2. **Élaborer une stratégie de programme à long terme :** Élaborer une stratégie à long terme qui s'aligne sur les initiatives plus larges de transformation numérique du gouvernement. Veillez à ce que la stratégie soit suffisamment souple pour tenir compte des progrès technologiques futurs, des modifications de la réglementation et des changements dans le comportement et les attentes des utilisateurs.

   En particulier :

   a. **Donner la priorité à la conception et à l'amélioration d'une solution d'authentification unique (SSO) basée sur le NA3 qui puisse être étendue et pérennisée :** Disposer d'une infrastructure SSO basée sur le NA3 est un élément fondamental d'un programme de services numériques pour les citoyens. Le ciblage du NA3 garantit que le programme dispose d'une solide gestion des risques, ce qui, par le biais d'un SSO, est essentiel pour soutenir les objectifs de fédération, de courtage de données et de justificatifs numériques.

   b. **Piloter et évaluer les justificatifs numériques :** Piloter les solutions, les technologies et les processus liés aux justificatifs numériques dans des environnements contrôlés afin d'évaluer leur efficacité et leur faisabilité. Recueillir les réactions des utilisateurs et des parties prenantes afin d'améliorer et d'affiner les pratiques de manière itérative. Commencez par des cas d'utilisation à faible risque et augmentez progressivement l'échelle en fonction du succès des mises en œuvre initiales et du retour d'information des parties prenantes, afin d'être un suiveur rapide.

   c. **Rester flexible et s'adapter :** Reconnaître que le paysage des services numériques destinés aux citoyens est en constante évolution et rester flexible en réponse aux changements technologiques, aux réglementations et aux besoins des utilisateurs. Examinez et mettez régulièrement à jour la stratégie de gestion de l'accès aux services

numériques destinés aux citoyens afin de l'adapter aux nouvelles tendances et aux nouveaux défis.

3. **Élaborer un cadre de protection de la vie privée qui :**

    - **Il est développé en collaboration** avec le responsable de la protection de la vie privée et le commissaire à la protection de la vie privée de chaque juridiction.
    - **Priorise dès la conception les principes de respect de la vie privée**[26] et à la réalisation d'évaluations de l'impact sur la vie privée tout au long de la conception, du développement, de la mise en œuvre et de l'amélioration continue d'un programme de services numériques pour les citoyens.
    - **Identifie les politiques et procédures internes en matière de protection de la vie privée** qui garantissent le respect de la vie privée dès la conception et assure la conformité avec les lois et règlements qui s'alignent sur les obligations légales et les principes énoncés par un commissaire à la protection de la vie privée.
    - **Intègre des mesures de protection de la vie privée**, telles que le cryptage et la minimisation des données, en mettant en œuvre des contrôles d'accès et en établissant des mécanismes d'audit pour protéger les informations sensibles des utilisateurs et maintenir leur confiance dans le processus d'accréditation.
    - **Désigne un ou plusieurs agents de liaison** chargés de servir de point de contact pour les demandes et les initiatives des citoyens et des parties prenantes en matière de protection de la vie privée, de faciliter la communication et la collaboration avec un commissaire à la protection de la vie privée, ainsi que de contrôler et de rendre compte de la conception, de la mise en œuvre et du fonctionnement du cadre relatif à la protection de la vie privée.

    Envisager de doter l'équipe d'un spécialiste de la protection de la vie privée chargé de concevoir et de mettre en œuvre le cadre de protection de la vie privée et de veiller à ce que les membres de l'équipe connaissent les politiques

[26] Commissaire à l'information et à la protection de la vie privée de l'Ontario. Janvier 2018. « Privacy by Design ». https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf *(disponible en anglais seulement)*

et les procédures qu'il contient et qu'ils comprennent leur rôle dans la conception, la prise de décision et la protection des informations personnelles.

4. **Centrer l'utilisateur dans le développement et les opérations**

    a. **Donner la priorité aux principes et aux éléments de conception centrés sur l'utilisateur,** afin de s'assurer que le système répond aux besoins et aux attentes des résidents. Le gouvernement du Canada dispose d'une bibliothèque d'éléments de conception qui peuvent être adaptés selon les besoins.

    b. **Développement itératif :** Adopter une approche de développement itératif, en publiant fréquemment des mises à jour et des améliorations des systèmes de gestion de l'accès aux services numériques destinés aux citoyens. Utilisez le retour d'information des utilisateurs et des parties prenantes pour affiner et améliorer le système au fil du temps.

    c. **Assurer un soutien centré sur le citoyen** pour votre plateforme SSO du citoyen et le programme complet de services numériques du citoyen. Tirer parti de l'expertise dans la mesure du possible afin de maintenir un bon rapport coût-efficacité.

5. **Adopter une approche collaborative pour l'approvisionnement :** Impliquer les fournisseurs de solutions dans le développement de votre procuration. Alors que l'approche traditionnelle consiste en une demande d'information (RFI) suivie d'une demande de proposition (RFP), une approche consultative de l'élaboration d'un RFP est probablement un meilleur moyen de centrer l'utilisateur (le fournisseur qui répond) dans le processus.

    Évaluez les fournisseurs en fonction de leurs antécédents, de leurs capacités, de leur alignement sur votre stratégie de gestion des identités et des accès pour les services numériques destinés aux citoyens et de leur capacité à suivre le rythme des technologies émergentes dans ce domaine. Il est fortement recommandé de procéder à des démonstrations de concepts dans le cadre du processus d'évaluation.

    Donner la priorité aux solutions qui peuvent être adaptées à des cas d'utilisation spécifiques, à des populations d'utilisateurs et à des environnements réglementaires. Cela signifie également qu'il faut avoir une bonne compréhension de la capacité existante, une base solide de cas d'utilisation et des processus détaillés.

6. **Communiquer avec précision et instaurer la confiance :** Alors que le paysage canadien reste marqué par la désinformation concernant la gestion des identités et des accès aux services numériques destinés aux citoyens, la communication doit être ciblée et intentionnelle. Bien que la meilleure façon de communiquer dans ce contexte reste difficile à cerner, voici deux points de départ utiles :

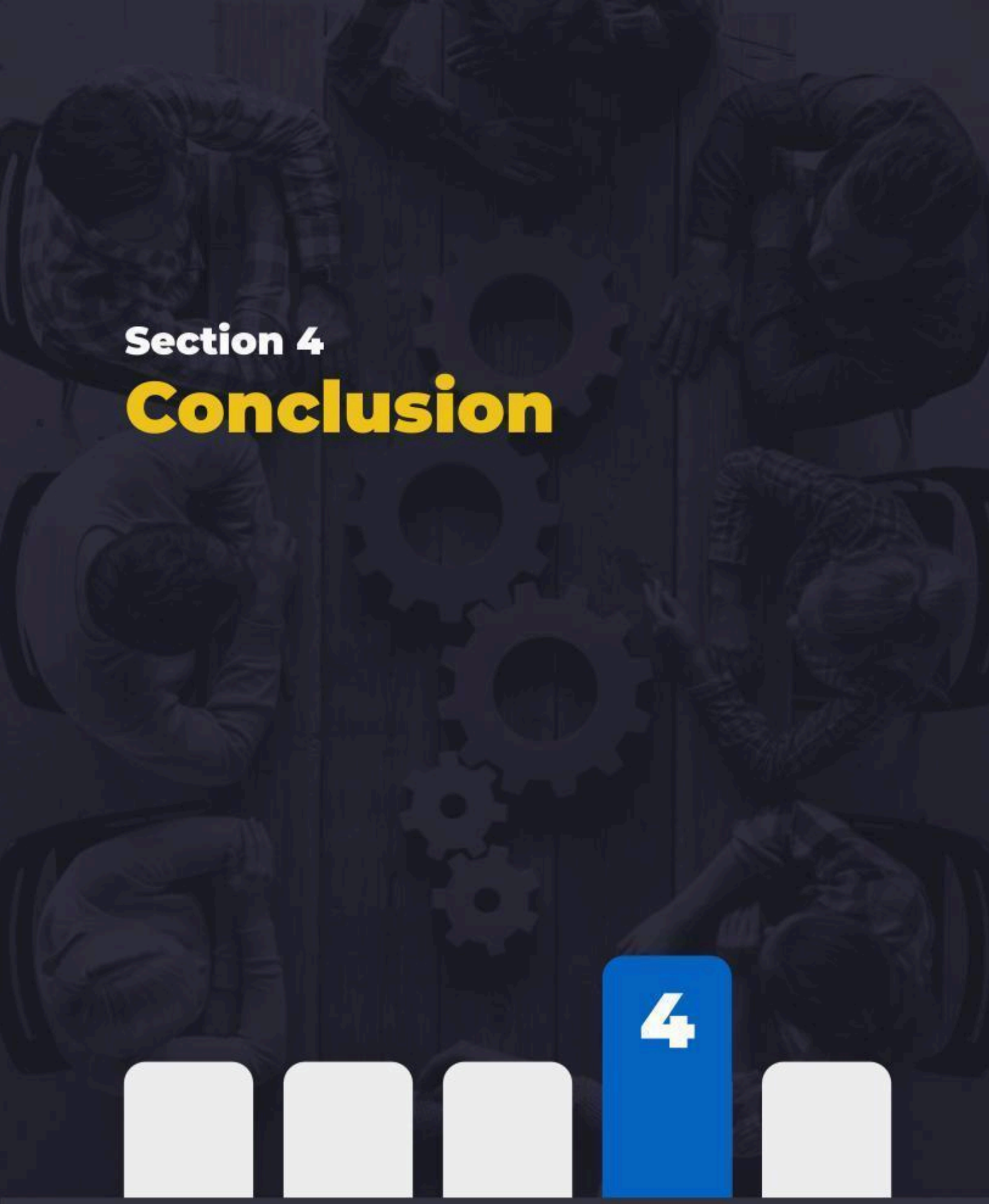
    a. **Obtenir le soutien et la compréhension des personnes d'influence internes et au niveau politique.** Communiquer sur les avantages de services numériques sûrs et transparents pour les citoyens et sur la stratégie à long terme, tout en s'attaquant aux idées fausses ou à la résistance des parties prenantes.

    b. **Donner la priorité à l'engagement du public en se concentrant sur la collecte des besoins des utilisateurs** d'une manière ciblée liée aux cas d'utilisation, plutôt que sur la communication de masse, et maintenir un message clair et démontrable (soutenu par la mise en œuvre du programme) qui met l'accent sur la protection de la vie privée, la sécurité et la commodité.

7. **Rester engagé dans la communauté**

    a. **Travailler en collaboration avec des partenaires externes**, notamment des fournisseurs de solutions de gestion des identités et des accès, d'autres administrations publiques, des organisations à but non lucratif et des associations sectorielles, afin de partager des idées et des bonnes pratiques. Les efforts de collaboration peuvent contribuer à rationaliser et à accélérer les processus et à garantir l'interopérabilité.

    b. **S'engager activement dans les organisations de normalisation et de la communauté technologique** pour accélérer le renforcement des capacités internes tout en contribuant au développement d'un écosystème de justificatifs numériques plus cohérent et interopérable dans l'ensemble du pays.



Section 4

Conclusion

4

Conclusion

De nombreux gouvernements à travers le Canada sont confrontés au défi de promouvoir un accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens. Les recommandations formulées dans le présent rapport fournissent des orientations concrètes aux gouvernements à tous les niveaux au Canada, ainsi qu'à leurs partenaires, qui cherchent à faire progresser l'accès aux services numériques d'une manière structurée et efficace. Les conseils de ce rapport soulignent l'importance d'accorder la priorité à la collaboration entre les parties prenantes, aux approches fondées sur les risques et à l'attention portée aux utilisateurs ultimes.

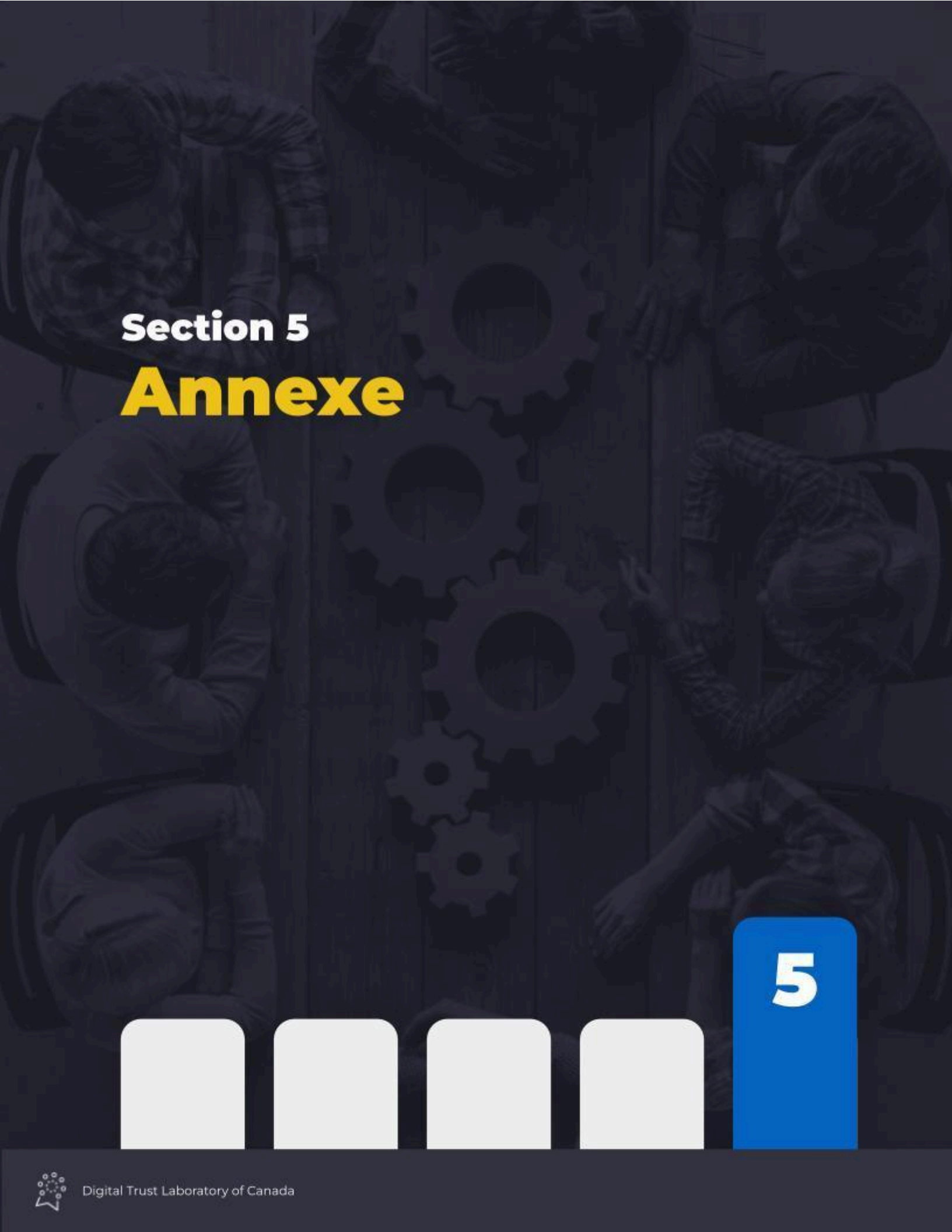
En fin de compte, le rapport recommande d'être prêt à passer aux justificatifs numériques par le biais de programmes pilotes, de tirer parti des réussites des projets pilotes pour éclairer les décisions futures, et de suivre en permanence les progrès et les tendances. Adopter une approche itérative, donner la priorité à la collaboration et instaurer la confiance. Avant tout, il convient d'adopter une approche programmatique pour garantir un accès sûr, convivial et sécuritaire aux services numériques destinés aux citoyens. Il ne s'agit pas d'un simple projet de technologie de l'information. Les gouvernements peuvent alors faire progresser de manière plus efficace et continue leur programme de services numériques aux citoyens et contribuer à un écosystème plus cohésif, fiable et interopérable pour leurs citoyens dans l'ensemble du Canada.

En résumé, en appliquant les recommandations présentées dans ce rapport, les gouvernements à tous les niveaux au Canada peuvent faire en sorte que les programmes de gestion de l'accès aux services numériques pour les citoyens soient prêts sur le plan opérationnel et technologique, à court et à long terme. En suivant les tendances actuelles et émergentes, en étant perçues comme des collaborateurs fiables et en garantissant la sécurité, la confidentialité et la convivialité des services, les équipes des services numériques pour les citoyens des gouvernements canadiens pourront s'adapter et rester à jour tout en répondant à cette évolution.

Prêt à passer à la prochaine étape en vue des justificatifs numériques?

Contactez LabCN pour savoir comment nous pouvons vous aider :

- Renforcement des capacités et formation
- Projets pilotes
- Évaluation des technologies



Section 5

Annexe

5

Annexe - Groupes de travail sur les normes, les cadres et les technologies

Voici une liste non exhaustive, classée par ordre alphabétique, d'organismes de normalisation, de technologie et de cadre que les équipes de services numériques aux citoyens pourraient vouloir suivre pour connaître les avancées en matière de justificatifs numériques et les discussions plus larges sur la gestion des identités et des accès. Il n'est jamais possible de suivre toutes les organisations ou d'y participer, et certaines d'entre elles ne sont ouvertes qu'aux acteurs nationaux. Le cas échéant, LabCN a fourni des notes sur l'organisation à l'intérêt ou à la participation potentielle.

1. Decentralized Identity Foundation (DIF) - DIF est une organisation axée sur l'ingénierie qui se concentre sur le développement des éléments fondamentaux nécessaires pour établir un écosystème ouvert pour l'identité décentralisée et assurer l'interopérabilité entre tous les participants.

2. Institut des normes de gouvernance numérique (DGSI) - L'Institut des normes de gouvernance numérique, qui fait partie du Conseil de la gouvernance numérique, est un organisme accrédité d'élaboration de normes. L'Institut permet d'accroître la confiance dans les systèmes numériques du Canada en élaborant des normes de gouvernance technologique en collaboration avec un large éventail de parties prenantes.

   Note du LabCN : Le Conseil canadien des normes a également délégué à la DGSI le pouvoir d'élaborer des normes d'identité numérique pour le pays.

3. Conseil d'identification et d'authentification numériques du Canada (CCIAN) - Le Conseil d'identification et d'authentification numériques du Canada, connu sous le nom de CCIAN, est une coalition à but non lucratif de dirigeants des secteurs public et privé qui se sont engagés à élaborer un cadre canadien pour l'identification et l'authentification numériques.

   Note du LabCN : Les entreprises canadiennes travaillent désormais activement à la certification de leurs produits en fonction du cadre de confiance pancanadien du CCIAN.

4. Hyperledger Indy Foundation - Hyperledger Foundation promeut l'interopérabilité et la normalisation, ouvrant la voie à l'adoption généralisée de solutions sécurisées et évolutives de chaîne de blocs (blockchain) et de confiance numérique à travers les industries et les secteurs.

Note du LabCN : Hyperledger Indy est le fondement d'un réseau que certains gouvernements canadiens ont exploré comme une option potentielle pour leur écosystème d'émission et de vérification de justificatifs numériques vérifiables.

5. Union internationale des télécommunications - L'UIT est l'agence spécialisée des Nations unies pour les technologies de l'information et de la communication (TIC). Elle facilite la connectivité internationale des réseaux de communication.

   Note du LabCN : L'UIT maintient la recommandation X.509, qui est la base de la majorité des systèmes de gestion basés sur des certificats de clé publique.

6. Internet Engineering Task Force (IETF) - L'IETF est le principal organisme d'élaboration de normes (SDO) pour l'internet. L'IETF élabore des normes volontaires qui sont souvent adoptées par les utilisateurs de l'internet, les opérateurs de réseaux et les vendeurs d'équipements, et contribue ainsi à façonner la trajectoire du développement de l'internet.

   Note du LabCN : l'IETF est responsable du cadre OAuth 2.0, essentiel pour de nombreux services de fédération.

7. IS0 Application permis de conduire sur téléphone mobile (mDL) - établit les spécifications d'interface pour la mise en œuvre d'un permis de conduire en association avec un appareil mobile. Il spécifie également l'interface entre le permis de conduire mobile et le lecteur de permis de conduire mobile, ainsi que l'interface entre le lecteur de permis de conduire mobile et l'infrastructure de l'autorité émettrice.

   Note du LabCN : La norme ISO mDL fait l'objet d'un grand intérêt et d'une certaine adoption aux États-Unis. Elle n'est pas ouverte aux acteurs non-étatiques.

8. The Open Identity Exchange (OIX) - OIX est une communauté permettant à toutes les personnes impliquées dans le secteur de l'identité de se connecter et de collaborer, en développant les orientations nécessaires pour des identités interopérables et fiables. Grâce à notre définition et à notre formation sur les cadres de confiance, nous créons les règles, les outils et la confiance qui permettront à chaque individu de bénéficier d'une identité fiable et universellement acceptée.

Note du LabCN : OIX a récemment publié une analyse des cadres de confiance du monde entier, soulignant les similitudes et les différences. Le cadre du CCIAN a été inclus dans l'analyse.

9. La fondation OpenID est un organisme mondial de normalisation ouverte qui s'engage à aider les gens à affirmer leur identité partout où ils le souhaitent. Il s'agit d'une communauté mondiale dynamique où les pairs et les leaders d'opinion en matière d'identité se réunissent pour créer les écosystèmes d'identité de demain.

   Note du LabCN : le protocole OpenID est un protocole d'authentification qui permet aux utilisateurs de se connecter à un site web tout en déléguant l'authentification à une autorité centrale. Ils sont également responsables de OID4VC - OpenID for Verifiable Credential Issuance and Presentation (OpenID pour l'émission et la présentation de certificats vérifiables).

10. Open Wallet Foundation - L'OWF est un consortium d'entreprises et d'organisations à but non lucratif qui collaborent pour favoriser l'adoption au niveau mondial de solutions de portefeuilles numériques ouvertes, sécurisées et interopérables, ainsi que pour fournir un accès à l'expertise et aux conseils par l'intermédiaire de notre Conseil consultatif gouvernemental.

11. Organisation for the Advancement of Structured Information Standards (OASIS) - OASIS Open offre aux projets - y compris les projets à code source ouvert - une voie vers la normalisation et l'approbation de jure pour référence dans la politique internationale et les marchés publics.

    Note du LabCN : OASIS a contribué à promouvoir SAML (Security Assertion Markup Language), largement utilisé dans les modèles d'authentification fédérée et PKCS 11 : Cryptographic Token Interface Base Specification version.

12. Trust over IP Foundation (ToIP) - ToIP a pour mission de promouvoir des normes mondiales pour les connexions confidentielles et directes entre parties ; de tirer parti des possibilités offertes par les portefeuilles et justificatifs numériques interopérables ; de protéger les identités des citoyens et des entreprises en les ancrant dans des signatures numériques vérifiables ; d'intégrer les éléments techniques de la confiance numérique aux éléments humains - les règles et politiques commerciales qui régissent la collaboration dans un écosystème de confiance numérique performant ; et de favoriser la communication et le partage des connaissances entre les experts en matière de confiance numérique.

13. Groupe de travail du W3C sur les justificatifs vérifiables - La mission du groupe de travail est de faciliter et de sécuriser l'expression et l'échange de références vérifiées par un tiers sur le Web.

    Note du LabCN : Largement acceptée comme l'étalon-or de l'identité et des justificatifs numériques.