Citizen FIRST

OPTIMISÉ PAR
L'Institut des
services axés sur
les citoyens

Confiance et identité numériques : Répondre aux nouvelles attentes en matière de prestation de services publics

- Adoption de l'identité numérique par le gouvernement
- Services de connexion comme point de départ
- Justificatifs d'identité numériques vérifiables pour divers types de données
- Recommandations pour faire progresser la mise en œuvre

Source de l'image : utimaco.com

RAPPORT MENSUEL DES CONSEILS MIXTES À L'INTENTION DES CADRES

Élaboré par le Comité de recherche

Octobre 2021

1. Introduction

Le présent rapport exécutif a été préparé avec l'aide de Peter Watkins, gestionnaire du Programme d'identité numérique de l'Institut des services axés sur les citoyens (ISAC), et des experts des secteurs de compétence en matière d'identité numérique du Conseil mixte. L'**identité numérique est une collection de caractéristiques associées à un individu identifiable de façon unique – stockée et authentifiée dans la sphère numérique – et utilisée pour les transactions, les interactions et les représentations en ligne**[1].

Les organisations gouvernementales du monde entier investissent dans la planification et la mise en œuvre de solutions d'identification numérique. En raison de la croissance continue et rapide de la numérisation, les nouvelles technologies et les nouveaux comportements des utilisateurs transforment la façon dont le gouvernement interagit avec les clients. Ce changement modifie radicalement la portée et les procédures des systèmes de gestion de l'identité du gouvernement[2].

Les organisations gouvernementales commencent à réévaluer leur rôle dans la chaîne d'approvisionnement de l'identité, car la vérification et l'authentification exactes de l'identité d'un client en ligne deviennent essentielles au fonctionnement de la société. Cette capacité d'établir et de vérifier l'identité est considérée comme essentielle au maintien de la confiance des clients et de la sécurité des transactions[3]. Voici un aperçu de l'évolution d'Internet et de la prestation des services du secteur public :

Ère pré-Internet

- Prestation de services sur papier, par la poste, en personne et par téléphone.
- Conservation des renseignements sur les clients au moyen de documents papier et de certificats délivrés par le gouvernement .

Ère numérique

- Étapes préliminaires : Sites Web d'information; les formulaires peuvent être téléchargés. Prestations de services en format papier, par la poste,
en personne et par téléphone.
- Stade actuel : Sites Web de prestation de services, renseignements sur les clients conservés sur papier, via courriel et en format PDF.
- L'identification numérique signifie trouver un moyen pour les clients d'ouvrir une séance sur les sites Web du gouvernement.

Ère d'une économie et d'une société numériques

- Données transmises aux clients sous une forme numérique fiable.
- Les clients peuvent partager leurs données en toute sécurité dans l'économie numérique.
- L'ID numérique est un sous-ensemble de données (sous forme de justificatifs d'identité numériques vérifiables) qui est remis aux clients.

Pourquoi ce rapport est-il important?

- La pandémie de la COVID19 (« la pandémie ») a mis en lumière la nécessité d'avoir plus d'interactions sans contact, ce qui a mené à une accélération de la conception, du développement et du déploiement d'outils d'identité numérique et de solutions sans contact[4].
- L'identification numérique est un facteur clé de la modernisation des services publics (c.-à-d. les certifications et les licences gouvernementales). Elle fournit une authentification fiable et permet aux clients d'accéder à une gamme de services publics (en ligne et en personne) de façon plus rapide, plus sécuritaire et plus pratique[5].
- L'utilisation de systèmes fiables de vérification de l'identité numérique réduit le risque d'erreur humaine dans l'identification et la vérification de l'identité d'un client. Elle peut également améliorer l'efficacité organisationnelle, réduire les coûts et offrir une expérience client plus favorable.

Qu'est-ce qui est couvert dans ce rapport exécutif?

Le présent rapport comprend les éléments suivants :

- Introduction
- Adoption de l'identité numérique par le gouvernement
- Services de connexion comme point de départ
- Justificatifs d'identité numériques vérifiables pour divers types de données
- Conditions pour faire progresser la mise en œuvre

1. The Digital Identity: What It Is + Why It's Valuable
2, 5. How governments can deliver on the promise of digital ID
3. L'identité numérique maintenant : de contrôle de la sécurité à moteur organisationnel
4. Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations

2. Adoption de l'identité numérique par le gouvernement

Les pièces d'identité numériques sont la contrepartie numérique de la pièce d'identification physique (c.-à-d. une carte d'identité physique, un passeport ou un permis de conduire)[6]. Elles fournissent les justificatifs nécessaires pour démontrer qu'une personne est bien celle qu'elle prétend être en ligne. La capacité d'une carte d'identité numérique à simplifier les interactions entre les clients et le gouvernement peut générer des avantages importants. Par exemple[7] :

1. Plus de commodité pour les clients en éliminant les frais de déplacement potentiels.
2. Réduction des temps d'attente grâce à l'authentification en ligne à distance.
3. Amélioration de l'efficacité administrative pour le gouvernement (c.-à-d. en réduisant la paperasse, en accélérant le traitement et en réduisant le risque d'usurpation d'identité).

6. The Benefits of Digital Identity Verification
7. Digital identity, a security imperative for governments
8. Government of Canada Digital Identity (ID)
9. MyAlberta Digital ID: A secure way to verify who you are online
10. Gouvernement de la Colombie-Britannique : Services d'identité et d'authentification
11. ID numérique en Ontario

Exemples de programmes d'identification numérique dans le secteur public

Gouvernement du Canada

Le Secrétariat du Conseil du Trésor du Canada (SCT) travaille avec d'autres ministères et administrations à l'élaboration d'une approche pancanadienne en matière d'identité numérique et à l'acceptation d'une identité numérique digne de confiance dans l'ensemble des administrations et du gouvernement[8]. L'objectif est de permettre aux Canadiens et aux entreprises canadiennes de se connecter avec leur identité numérique provinciale digne de confiance pour accéder aux services du gouvernement fédéral en temps opportun et en toute sécurité.

Alberta

Le gouvernement de l'Alberta offre actuellement à ses clients la carte d'identité numérique My Alberta. MyAlberta Digital ID offre un accès continu à un nombre croissant de sites et de services gouvernementaux, tout en protégeant les renseignements sur les clients et la vie privée[9].

Colombie-Britannique

Le programme provincial de gestion de l'information sur l'identité (IDIM) offre des services d'identité et d'authentification au moyen de la carte de services de la Colombie-Britannique et de BCeID pour appuyer les transactions des clients avec les services gouvernementaux[10]. Ces services d'identité et d'authentification sont disponibles pour aider les clients à accéder aux services en ligne en : vérifiant qu'une personne est bien celle qu'elle prétend être en ligne et en fournissant des renseignements sur son identité, le cas échéant.

Ontario

Le gouvernement de l'Ontario a annoncé le lancement de son nouveau programme d'ID numérique qui sera lancé à la fin de 2021. L'identité numérique remplacera les cartes d'identité matérielles par une version numérique accessible sur les téléphones intelligents et d'autres appareils comme les tablettes ou les ordinateurs portatifs. Pour ce faire, l'Ontario mettra en œuvre une application de Portefeuille numérique. Les clients pourront accéder à leur carte d'identité digne de confiance du gouvernement, laquelle sera protégée par un chiffrement robuste[11].

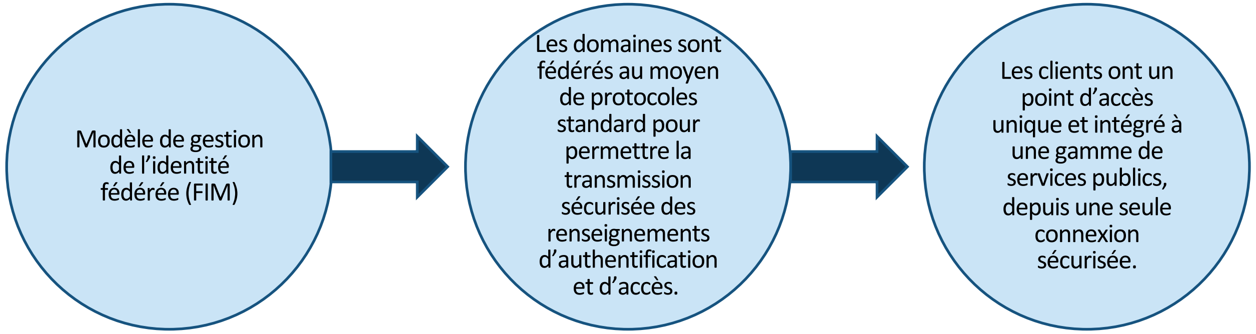
3. Services d’ouverture de séance comme point de départ

Alors que les administrations canadiennes continuent d’investir dans les systèmes d’identification numérique, les experts du domaine soulignent que l’identification numérique et les services gouvernementaux numériques représentent un aspect important de l’avenir au Canada[12]. Certaines administrations sont en avance quant à leur état de préparation en matière d’ID numérique et d’autres tirent parti des leçons apprises à mesure que la demande pour l’adoption de ces services augmente.

Comme point de départ, de nombreuses administrations se concentrent sur l’établissement de services d’ouverture de séance comme composante fondamentale d’une infrastructure d’identification numérique digne de confiance. Avant le passage à l’ID numérique, les identités étaient gérées en silos. Les clients créaient souvent plusieurs comptes sur les sites Web du gouvernement et accumulaient des identifiants et des mots de passe non sécuritaires. Ce modèle de gestion de l’identité compromettait la confidentialité et la sécurité des données des clients et créait une expérience utilisateur peu pratique[13].

À cette fin, les gouvernements mettent en œuvre un modèle de gestion de l’identité fédérée (FIM)[14]. Ce modèle fait référence à l’établissement d’une relation de confiance entre les organisations gouvernementales distinctes et les tiers (comme les fournisseurs d’applications ou les partenaires), ce qui permet le partage d’identités et authentifie les utilisateurs entre les domaines. La FIM permet au gouvernement d’offrir une connexion unique (SSO) pour permettre aux clients d’accéder à de multiples systèmes et portails de services publics en ligne sans avoir à ouvrir une séance dans chacun d’eux.

Services d’identité fédérée



Considérations relatives à la protection des renseignements personnels et des données

En raison de l’augmentation des menaces à la cybersécurité (c.-à-d. les atteintes à la sécurité des données et l’usurpation d’identité) pendant la pandémie, le public est de plus en plus préoccupé par la protection des données et la sécurité des systèmes d’ID numérique. Si elles ne sont pas prises en compte, ces préoccupations constituent un obstacle à l’adoption[15].

Selon Mme Ann Cavoukian, spécialiste de la protection des renseignements personnels, les gouvernements devraient adopter une approche de la « protection de la vie privée dès la conception » pour assurer des protections fondamentales de la vie privée et de la sécurité des données. Cette approche comprend la planification minutieuse de la collecte des données, la création de normes élevées pour le stockage des données afin de se protéger contre les intrusions et l’obligation d’obtenir le consentement de l’utilisateur pour toute utilisation de données personnelles. Les sept principes de la méthodologie de la protection de la vie privée dès la conception comprennent :

1. Prendre des mesures **proactives** et non réactives; des mesures **préventives** et non correctives.
2. Assurer la protection **implicite** de la vie privée.
3. **Enchâsser** la protection de la vie privée dans la conception.
4. Fonctionnalité complète – **Somme positive** et non pas nulle.
5. Sécurité de bout en bout – **Protection pendant toute la période de conservation des renseignements.**
6. **Visibilité** et **transparence** – Maintenir l’**ouverture.**
7. **Respect** de la vie privée des utilisateurs – Rester **centré sur l’utilisateur.**

12. Canadian privacy expert says 2021 could be the year for digital ID projects
13. Digital ID Services Platform - Enabling secure delivery of next gen digital public services
14. Single Sign-on vs. Federated Identity Management: The Complete Guide
15. Façons dont l’ID numérique sécurisera davantage les données des Canadiens : entretien avec Interac et SecureKey
16. Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices

4. Justificatifs d’identité numériques vérifiables pour divers types de données

Un justificatif d’identité est un document qui permet de vérifier qu’une personne possède un attribut, une qualification ou une revendication en particulier (c.-à-d. passeport, permis de conduire ou diplôme universitaire). Dans le monde physique, les justificatifs d’identité peuvent être vérifiés au moyen d’un examen en personne du document. Cependant, en raison de la pandémie, les mesures de distanciation sociale ont accru la nécessité de vérifier numériquement les justificatifs d’identité.

Pour remédier à ce problème, les gouvernements mettent l’accent sur la création de solutions de justificatifs d’identité vérifiables (VC) centrées sur l’utilisateur afin de permettre aux clients d’utiliser leurs justificatifs en ligne d’une manière qui est sécurisée sur le plan cryptographique, qui respecte la vie privée et qui est vérifiable par machine. Il y a trois composantes essentielles des justificatifs d’identité vérifiables[17] :

- Contiennent un mécanisme de validation de la preuve pour assurer la validité de l’émetteur du justificatif et des demandes du sujet.
- Sûrs et à l’épreuve des manipulations.
- Ont été délivrés par une autorité compétente.

Comme les organisations gouvernementales sont des émetteurs faisant autorité pour un large éventail de données importantes sur les clients, elles sont dans une position unique pour mettre en œuvre les justificatifs d’identité vérifiables. Pour être efficace, les implémentations doivent être interopérables et respecter les normes pertinentes, telles que le modèle de données des informations d'identification vérifiables du W3C. Il s’agit d’un ensemble de spécifications et de documents vérifiables qui permettent de vérifier les justificatifs d’identité et de les partager en ligne[18].

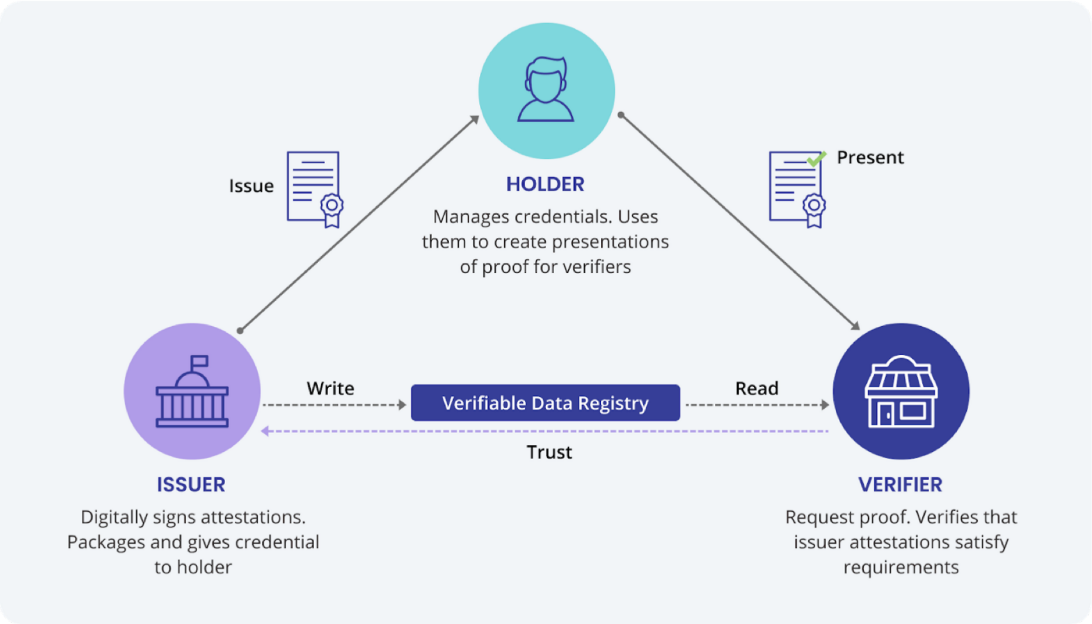
Le virage vers les informations d’identification vérifiables axées sur l’utilisateur donne aux clients un plus grand contrôle sur l’identité et les données. Cela permet aux clients de conserver leurs justificatifs d’identité sous forme numérique et de les présenter aux fournisseurs de services de leur choix. Les clients sont au cœur du triangle de la confiance[19]. Ce triangle est essentiel au fonctionnement des justificatifs d’identité vérifiables.

L’émetteur fait confiance au titulaire → **Le titulaire fait confiance au vérificateur** → **Le vérificateur fait confiance à l’émetteur**

L’écosystème des justificatifs d’identité vérifiables regroupe trois entités[20]

Émetteur	Titulaire	Vérificateur
Entité qui est autorisée à émettre un justificatif d’identité (c.-à-d. des organisations gouvernementales).	Personne ou l’organisation qui détient le justificatif d’identité. Le détenteur a un contrôle complet sur la façon dont le justificatif peut être géré et avec qui il peut être partagé ou révoqué.	Entité qui vérifie le justificatif d’identité et veille à qu’il ait été émis par un émetteur autorisé, qu’il soit inviolable et qu’il soit toujours pertinent (c.-à-d. qu’il n’est pas expiré ou révoqué). Le vérificateur utilise la pièce d’identité vérifiable du détenteur pour en déterminer l’authenticité.

Flux des justificatifs d’identité vérifiables[21]



17, 21. What are Verifiable Credentials (VCs), Demystified.
18. An Introduction to Verifiable Credentials
19, 20. Verifiable Credentials Data Model 1.0

5. Recommandations pour faire progresser la mise en œuvre

La croissance continue des services numériques modifie les attentes des clients concernant leur interaction avec les services gouvernementaux et privés dans l'ensemble de l'économie. Les clients s'attendent maintenant à une expérience simplifiée et centrée sur l'utilisateur dans chaque interaction numérique avec le gouvernement[22].

Afin de répondre aux besoins des clients et d'exceller dans la nouvelle ère numérique, les gouvernements (à tous les niveaux) doivent recadrer l'ID numérique en tant que catalyseur opérationnel essentiel. Pour relever le défi, il faut que les capacités techniques et organisationnelles nécessaires soient en place pour assurer la mise en œuvre et le fonctionnement réussis des solutions de confiance et d'identité numériques.

Des leçons peuvent être tirées de l'expérience de 2021 avec la conception, le développement et la mise en œuvre de solutions numériques de preuve de vaccination dans toutes les administrations. Cet effort a été facilité, en partie, par la priorité des Conseils mixtes pour l'identité numérique.

L'expérience de la mise en œuvre d'une preuve numérique de vaccination a montré la nécessité de cinq conditions essentielles pour faire progresser les solutions de confiance et d'identité numériques.

22. [What Government CIOs Should Know About Digital IDs](#)

Conditions pour faire progresser la mise en œuvre d'une solution de confiance et d'identité numériques

1. **Priorités mandatées :** Les organisations devraient démontrer un engagement clair à améliorer les services numériques. Fournir aux clients leurs données sous une forme numérique fiable devrait être une priorité pour tous les ordres de gouvernements.

2. **Haute direction :** Les organisations devraient attribuer la tâche de produire et de superviser une solution d'identité numérique digne de confiance à un rôle de leadership. Une responsabilité clé de ce rôle devrait consister à mobiliser les dirigeants de toutes les organisations. Il est essentiel de disposer d'une ressource dédiée pour mener à bien ce travail, les solutions en matière d'identité numérique dignes de confiance étant hors de portée d'organisations uniques.

3. **Fonds dédiés :** Permet de veiller à ce que le budget nécessaire ait été alloué pour terminer le travail. Le budget devrait prévoir une marge de manœuvre pour l'expansion au cours de l'exercice financier afin que les équipes puissent être formées.

4. **Équipes de prestation pour la mise en œuvre et les opérations :** Veiller à ce qu'il y ait une équipe interne solide et compétente de fonctionnaires dévoués pour appuyer l'élaboration d'une solution d'identité numérique digne de confiance. Accroître les capacités des entrepreneurs ou des fournisseurs dans des domaines particuliers (c.-à-d. développement de logiciels, conception de services et mise en œuvre).

5. **Collaboration ouverte et harmonisation entre les administrations :** Veiller à ce que toutes les administrations adoptent des méthodes modernes, agiles et numériques pour la conception, l'élaboration et la prestation. Cela réduira les risques et accélérera la mise en œuvre. L'ouverture et la collaboration donneront également des résultats et stimuleront l'harmonisation entre les administrations.

Lectures suggérées

- It’s time to start taking digital identity seriously
- Why A Digital ID For A Digital World Just Makes Sense
- Verifying documents & identity in the public services and beyond
- Digital identity trends – 5 forces that are shaping 2021
- The digital citizen: Improving end-to-end public service delivery via a unique digital identity

Autres articles dignes de mention :

UK AI strategy focused on economic growth, resilience and ethics

Concerns raised over confidentiality and transparency in government data innovation

Plugging in the User Needs For Improved Experiences

All states should become digital societies in post-pandemic era

Ressources de recherche

Accédez aux Ressources de recherche de Citoyens en tête

Contenu récent sur le référentiel de recherche :

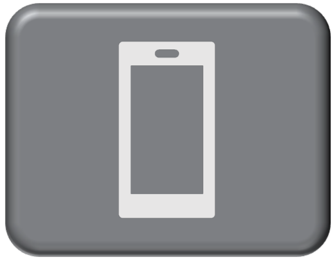
L’intelligence artificielle au gouvernement : Incidences sur la vie privée et les droits de la personne – Rapport des conseils mixtes à l’intention des cadres, septembre 2021

Le présent rapport explore les éléments suivants : Applications gouvernementales, incidences sur la vie privée et les droits de la personne, exemples de défis en matière d’IA, stratégies d’utilisation responsable.

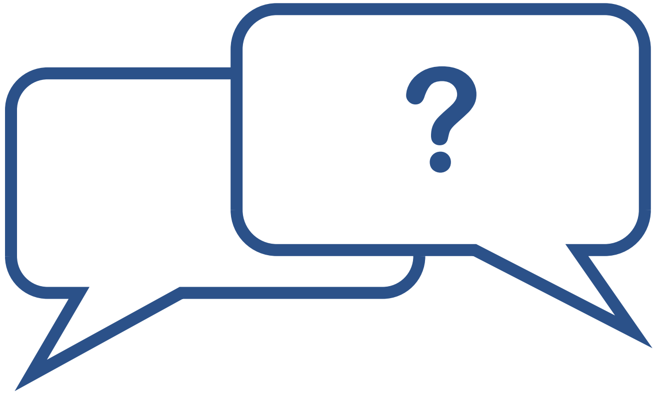
Tendances dans le bulletin quotidien

La COVID19 a accéléré la transition vers les services numériques, de nombreux processus sur papier devant être accessibles en ligne. Plusieurs dirigeants participant à l'événement virtuel [Digital Services Series : Customer Experience] de GovernmentCIO Media & Research ont mentionné la façon dont leur organisation a exploité la puissance de la technologie pour rehausser l'expérience client dans son ensemble. La conception axée sur l'être humain joue un rôle clé dans divers services numériques.

L'évolution des [technologies] de l'informatique en nuage et l'ampleur de ce qu'elles permettent aux différents ordres de gouvernements est difficile à mesurer, qu'il s'agisse de permettre aux premiers intervenants sur le terrain d'intervenir, de distribuer les vaccins et d'en faire le suivi, ou de dispenser de la formation et de travailler à distance. À mesure que les États et les administrations locales poursuivent leurs efforts de modernisation de l'informatique en nuage, ils font face à des défis encore plus complexes en matière de cybersécurité et de conformité. Afin de gérer cette complexité et d'assurer la sécurité, les organisations locales et d'État cherchent de nouvelles approches sécurisées, par exemple Multicloud-as-a-Service (MCaaS).



Selon une récente annonce faite par Justin Trudeau, premier ministre du Canada, les Canadiennes et les Canadiens peuvent maintenant obtenir une preuve de vaccination contre la [COVID19] pour les voyages internationaux. Le formulaire est un document PDF ou autre. La première page contient le nom de la personne, sa date de naissance et son historique de vaccination contre la COVID19. Il comprend également des renseignements sur la province qui délivre la preuve de vaccination, un logo du gouvernement canadien et un code QR.



Nous aimerions connaître votre avis!

Connaissez-vous quelqu'un qui souhaite consulter le rapport exécutif du Conseil mixte? Veuillez partager une copie de ce rapport. Si vous n'êtes pas déjà abonné(e), vous pouvez maintenant vous abonner pour recevoir le [rapport exécutif] en vous inscrivant [ici]. Envoyez vos questions à l'adresse info@iccs-isac.org.

Suivi :