Livre blanc sur l’identité numérique

Vivre à l’ère numérique en toute confiance, c’est possible

Avant-propos

Dans cet ouvrage, des organisations privées au service de millions de personnes et d'entreprises du Québec présentent une vision partagée de l'identité numérique et de son intégration à la vie de tous les jours. Il a pour buts de favoriser l'émergence d'une compréhension commune de l'identité numérique; de répondre à des questions de base que peuvent se poser des citoyens, des consommateurs, des dirigeants d'entreprises; de susciter la collaboration entre les différents acteurs qui seront impliqués dans l'implantation d'une identité numérique; de contribuer à créer un contexte favorable à l'adoption de l'identité numérique au Québec.

Fruit d'une collaboration entre Beneva, le Mouvement Desjardins, KPMG, TELUS et Vidéotron, et réalisé avec l'appui du Laboratoire d'identité numérique du Canada, organisation à but non lucratif vouée à une meilleure cybersécurité grâce aux identités numériques sécuritaires et conviviales, ce livre blanc sur l'identité numérique est diffusé gratuitement par les organisations signataires.

Table des matières

Résumé

- De plus en plus d'organisations et de gouvernements à travers le monde exploitent de nouveaux processus technologiques et mécanismes de vérification de l'identité.
- Plusieurs sondages démontrent toutefois que la confiance des parties concernées demeure à développer.
- Or, c'est l'absence d'une identité numérique véritable qui accroît la vulnérabilité des personnes et des organisations à des fraudes, vols d'identité et autres formes de cyberprédation.
- Actuellement, l'accès aux services en ligne requiert d'utiliser des « identifiants » comme, par exemple, JTREMBLAY, et des « authentifiants » comme des mots de passe.
- Toutefois, les combinaisons identifiants-authentifiants sont complexes à gérer et causent des accumulations et des dispersions de renseignements personnels dans l'espace numérique, en plus de générer du mécontentement et des comportements risqués.
- L'identité numérique n'est pas un identifiant unique, mais un ensemble d'attestations vérifiables propres à une personne (acte de naissance, permis de conduire, carte de membre…) contenues dans le portefeuille numérique de la personne et sous le contrôle exclusif de celle-ci.
- L'identité numérique place la personne au centre de tout et repose sur trois piliers qui sont la capacité d'agir, l'autonomie et l'intégrité des renseignements.
- L'identité numérique décourage également la fraude parce qu'il n'y a plus de « coffre-fort » où s'accumulent les renseignements de millions de personnes, ce sont plutôt ces mêmes personnes qui détiennent et contrôlent leurs renseignements personnels.
- L'identité numérique simplifiera la vie des personnes, accroîtra leur contrôle sur leurs renseignements personnels, améliorera leur sécurité et leur sentiment de sécurité, et contribuera à l'économie en réduisant les pertes liées à la fraude.
- De nombreux pays à travers le monde s'orientent vers l'identité numérique dont plusieurs en Europe sont déjà très actifs.
- L'identité numérique sera mise en place dans le cadre d'une collaboration étroite entre les gouvernements, les entreprises et la population. C'est une évolution nécessaire de la société.

Le contexte

Dans notre vie de tous les jours, l'accès à de nombreux services nécessite que l'on s'identifie. Et chaque fois, l'organisation avec laquelle nous entrons en contact doit pouvoir vérifier notre identité.

Qu'il s'agisse d'obtenir des services publics – éducation, soins de santé, permis – ou de traiter avec une institution financière, un fournisseur de services de télécommunications ou une compagnie d'assurances, il faut d'abord s'identifier et être reconnu comme la personne que l'on dit être.

Le processus d'identification et d'authentification est une composante fondamentale de notre vie économique et citoyenne. Il s'agit toutefois d'un processus qui est long, compliqué et qui peut comporter des failles.

Une étude, réalisée par la firme McKinsey[1] en 2019 concluait que la mise en place d'un processus d'identité numérique permettrait d'ajouter, d'ici 2030, 3 % à 13 % au PIB de sept pays qui ont fait l'objet de l'évaluation (Brésil, Chine, Éthiopie, Inde, Nigeria, Royaume-Uni et États-Unis).

De plus en plus d'organisations et de pays à travers le monde utilisent de nouveaux processus, technologies et mécanismes de vérification de l'identité. Les retombées positives de l'identification et de l'authentification au moyen d'une identité numérique provinciale, voire nationale ou internationale, sont indéniables : amélioration de l'expérience utilisateur en termes de simplicité et d'accessibilité, réduction des risques de fraude et économies en coûts de gestion.

Plusieurs sondages sur le sujet démontrent toutefois que la confiance de la population et d'autres parties prenantes envers les solutions proposées n'est pas toujours présente et freine leur adhésion. Plusieurs raisons expliquent ce constat :

- Les risques inhérents aux technologies numériques déjà utilisées;
- Les incidents répétés de violations de renseignements personnels et de vols d'identité;
- Les préoccupations en lien avec le contrôle et l'utilisation des renseignements personnels ainsi que leur traçabilité pouvant mener à une intrusion dans la vie privée des gens.

Or, dès qu'on s'intéresse un peu au sujet, on réalise rapidement que c'est la situation actuelle qui présente le plus de risques. C'est l'absence d'une identité numérique formelle et véritable qui accroît la vulnérabilité des personnes et des organisations à des fraudes, vols d'identité et autres formes de cyberprédation.

Il y a donc un travail d'éducation populaire et de sensibilisation à la citoyenneté numérique à faire pour susciter une large adhésion à l'identité numérique et réaliser dans les meilleures conditions possibles cette évolution à la fois souhaitable et inévitable d'entrer en relation avec les organisations publiques et privées.

Le présent document y contribue.

[1] McKinsey, Digital identification: A key to inclusive growth, avril 2019.

Qu’est-ce que « l’identité numérique » ?

À la base, l’identité numérique est une représentation numérique d’une personne lui permettant de prouver son identité afin d'effectuer des interactions avec des organisations et d’accéder de façon simple et sécuritaire à des services. Pour bien comprendre ce qu’est l’identité numérique et saisir ses avantages, commençons par voir les limites de la situation actuelle.

Les limites des « identifiants » et « authentifiants »

Tous les jours, dans notre vie numérique, nous utilisons des « identifiants » et des « authentifiants ». Un identifiant est, par exemple, JTREMBLAY. Il me représente auprès d’une organisation. Le mot de passe qui y est associé est l’authentifiant. Je peux partager mon identifiant pour que les gens puissent communiquer avec moi, mais la combinaison identifiant-authentifiant (JTREMBLAY et mot de passe) ne doit être connue que de moi seul et de l’organisation avec laquelle j’interagis afin d’accéder à mon compte bancaire, remplir ma déclaration de revenus, faire des achats en ligne, etc.

La gestion de nos identifiants et authentifiants peut être problématique : leur nombre élevé et la structure de chacun de mes mots de passe devrait être complexe (avec des chiffres, des lettres, des majuscules, des symboles…). Or, les utilisateurs n’ont pas toujours les connaissances, la rigueur ou la discipline pour gérer tous ces authentifiants de façon optimale. Qui plus est, avec les authentifiants, il est difficile, parfois même impossible, pour une organisation d’avoir la certitude que la personne existe vraiment et qu’elle est bien celle qu’elle prétend être.

Ce manque de confiance ou de certitude limite les interactions qu’il nous est possible de faire en ligne, ce qui freine l’adoption des services numériques avec les bénéfices que tous pourraient en tirer.

Pour réduire les risques, de plus en plus d’organisations recourent à des authentifications à double facteur. Par exemple, une personne se connecte à un site transactionnel; elle s’identifie avec JTREMBLAY; elle s’authentifie une première fois avec son mot de passe, et elle s’authentifie une deuxième fois avec un code qui lui aura été envoyé par message texte. C’est certainement un niveau de sécurité supplémentaire, mais la manipulation peut être fastidieuse et ce n’est pas encore la sécurité d’une authentique identité numérique qui est visée.

La réalité qui demeure est que dans l’espace numérique, notre identité est morcelée en une multitude d’identifiants et d’authentifiants qui peuvent constituer des risques de sécurité.

Qu’est-ce que « l’identité numérique » ?

Le triangle de confiance du monde physique

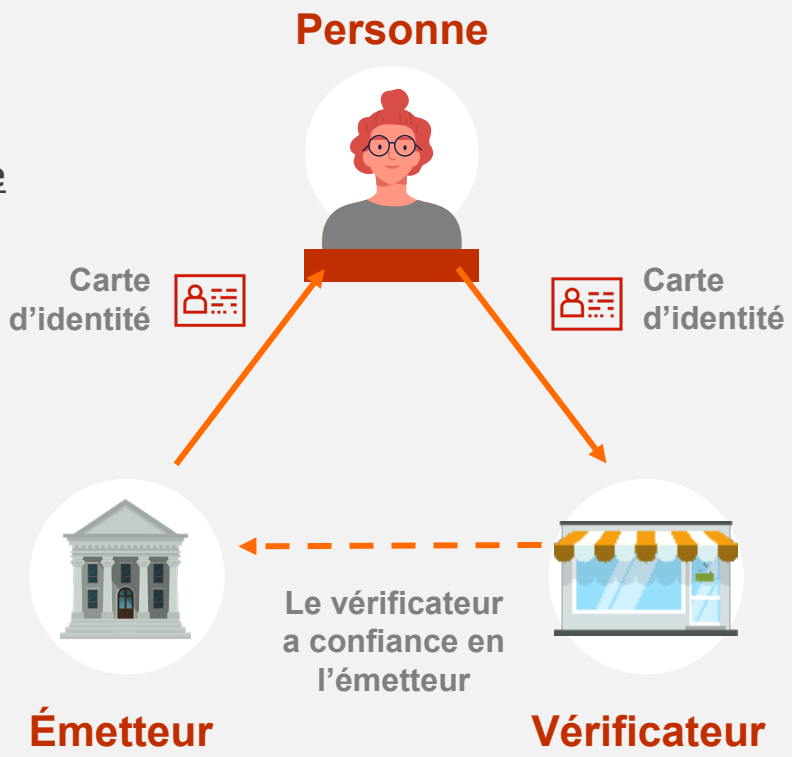
Dans le monde physique, lorsque vient le temps de prouver notre identité, on nous demande de fournir un document avec photo comme notre permis de conduire, notre carte d’assurance maladie ou notre passeport. Ces documents d’identification sont reconnus, parce qu’ils sont émis par des sources crédibles, en l’occurrence des gouvernements, et qu’ils sont pourvus de dispositifs de sécurité dont l’objectif est de limiter la contrefaçon. En général, les gens ont confiance en ces documents.

Dans le monde physique, nous avons **un triangle de confiance** : un émetteur crédible, qui remet à une personne réelle, une « carte d’identité » que le vérificateur (organisation publique ou privée) va accepter comme valide parce qu’il reconnaît la crédibilité de l’émetteur.

L’identité numérique vise à recréer un triangle de confiance dans l’espace numérique. Pour cela, il faut être en mesure de fournir des informations d’identité provenant de documents numériques dont l’exactitude et l’authenticité peuvent être vérifiées et qui sont émises par des organisations de confiance.

FIGURE 1.

Le triangle de confiance dans le monde physique



Qu’est-ce que « l’identité numérique » ?

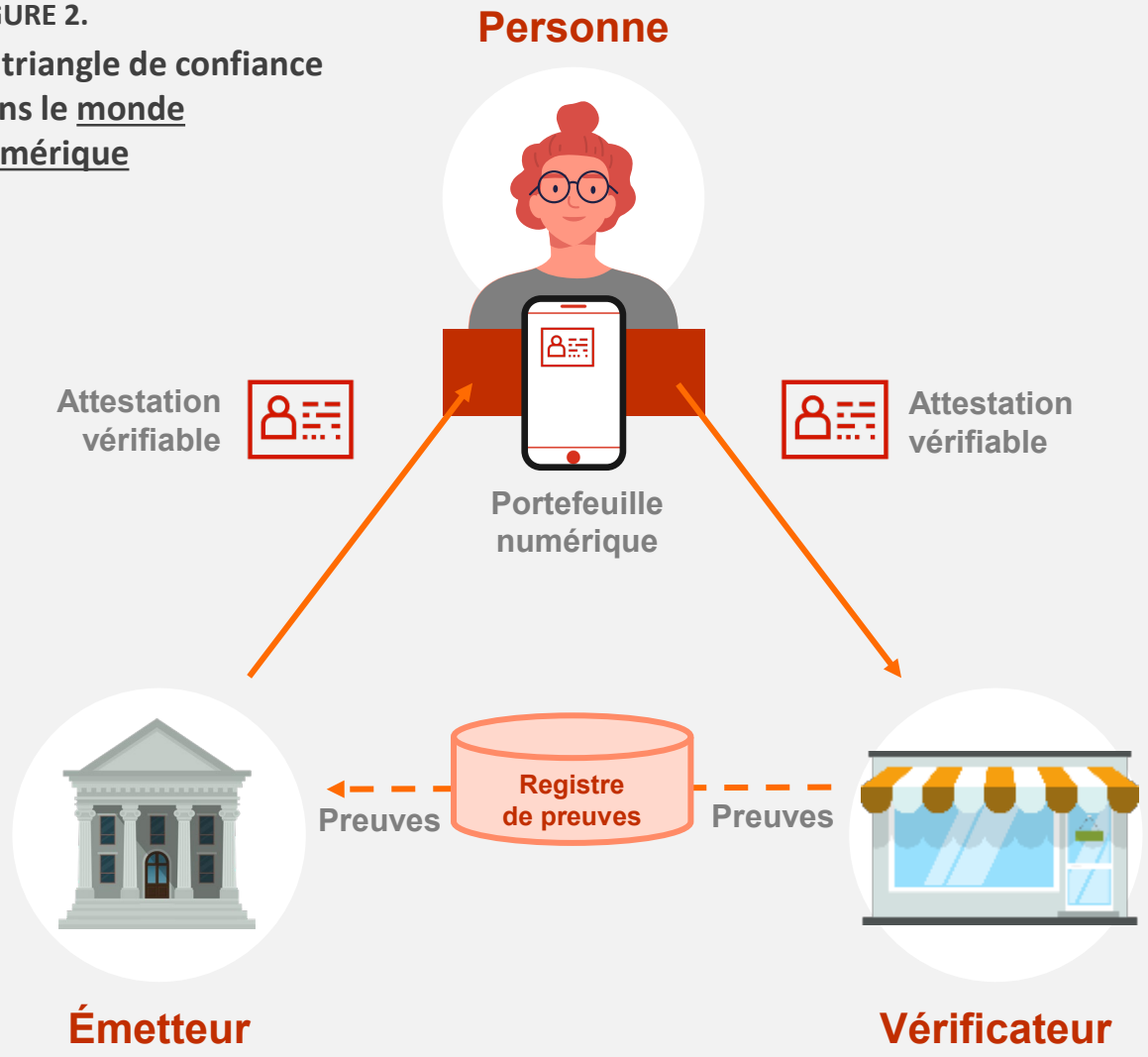
Recréer un triangle de confiance dans l’espace numérique

Pour recréer le **triangle de confiance** et l’introduire dans le monde numérique, les trois mêmes rôles doivent être mis en relation : l’émetteur, la personne et le vérificateur.

Ils doivent respecter certaines conventions, normes et règlements. Les acteurs sont appuyés dans leurs interactions par de nouveaux outils : les attestations vérifiables, le portefeuille numérique et le registre de preuves.

FIGURE 2.

Le triangle de confiance dans le monde numérique



Qu’est-ce que « l’identité numérique » ?

Recréer un triangle de confiance dans l’espace numérique (suite)

Les attestations vérifiables (émises)

Ce sont des documents numériques signés électroniquement par l’émetteur. Ainsi, en tout temps, le vérificateur qui reçoit une information provenant d’une attestation vérifiable est en mesure d’en vérifier l’authenticité et l’intégrité, ce qui rehausse la confiance par rapport aux documents physiques. Ces attestations sont déposées dans un portefeuille numérique détenu par une personne. De cette façon, la personne est en contrôle de ses informations puisque c’est elle qui les détient et doit consentir à ce que ses informations puissent être communiquées à un vérificateur.

Le portefeuille numérique

Il s’agit généralement d’une application mobile installée sur un téléphone intelligent. Il sert de dépôt sécurisé pour les attestations vérifiables et facilite les interactions numériques.

Les attestations vérifiables (présentées)

Ceci permet à une personne de présenter les informations demandées par un vérificateur sans pour autant présenter l’ensemble des informations. Par exemple, si un vérificateur veut obtenir mon nom et mon prénom, il n’est pas nécessaire de transmettre tous mes autres renseignements personnels comme ma date de naissance. De la même façon, il est possible de prouver que je suis en âge d’acheter de l’alcool sans pour autant divulguer ma date de naissance.

Le registre de preuves

Il permet de vérifier qu’une attestation a été émise par un émetteur de confiance et qu’elle n’a pas été révoquée par celui-ci. Aucun renseignement personnel n’est écrit dans le registre de preuves.

L'identité numérique n’est donc pas un identifiant unique comme un numéro d’assurance sociale numérique, mais un ensemble d’attestations vérifiables propres à une personne (acte de naissance, permis de conduire, carte de membre…) contenues dans le portefeuille numérique de la personne et sous le contrôle exclusif de celle-ci.

En quoi l'identité numérique sera-t-elle un progrès ?

Dans l'état actuel des choses, toutes nos interactions numériques laissent des traces. Elles constituent, faute de mieux, notre empreinte numérique qui se trouve ainsi disséminée dans l'espace numérique. Lorsque nous effectuons des achats en ligne, publions un commentaire sur les réseaux sociaux ou consultons simplement un site Internet publicitaire, nous laissons une empreinte qui permet de nous identifier, directement ou indirectement.

Renforcer la protection des renseignements personnels

Mais au-delà des traces numériques dans notre quotidien, il faut réaliser que nous partageons la plupart du temps bien plus de renseignements personnels que nécessaire. Par exemple, nous ne devrions présenter notre permis de conduire qu'aux seuls officiers publics autorisés, mais nous le montrons pourtant à toutes sortes d'occasions. Nous le montrons à l'hôtel, à la bibliothèque, au commis d'un dépanneur… C'est un geste courant. Nous créons également des comptes utilisateurs pour tous nos abonnements Internet : sites de commerce en ligne, réseaux sociaux, sites d'information. À chacune de ces ouvertures de compte, nous consentons à partager plusieurs renseignements nominatifs : nom, prénom, adresse, date de naissance et numéro de téléphone, pour n'en nommer que quelques-uns.

Bref, nos renseignements personnels circulent largement et leur protection est tributaire des dispositifs de sécurité mis en place par les organisations qui les ont collectés et qui les conservent. Malgré les législations qui se resserrent, la qualité des dispositifs de sécurité des organisations demeure très variable.

Pour un tiers mal intentionné, les informations permettant d'accéder aux comptes utilisateurs d'un individu ou même de créer frauduleusement des comptes au nom de quelqu'un d'autre peuvent être parfois trop facilement accessibles.

En quoi l'identité numérique sera-t-elle un progrès ?

Renforcer la protection des renseignements personnels (suite)

Les gouvernements sévissent avec des pénalités de plus en plus sévères pour la mauvaise gestion de renseignements personnels. Mais cette approche punitive ne règle pas le problème de fond : l'accumulation et la dissémination de renseignements personnels dans l'espace numérique représentent un modèle dépassé.

Le mouvement pour l'identité numérique est mondial. Tant les États que les organisations privées militent en sa faveur, notamment pour simplifier la vie des gens et rehausser la sécurité de leurs données. Bien que les modèles d'identité numérique soient encore en développement et diffèrent les uns des autres, ils ont tous pour objectifs de permettre à l'individu d'être en contrôle de ses renseignements personnels et de ne les partager qu'avec des tiers de confiance qui auront préalablement obtenu son consentement formel.

Le Québec et le Canada ne font pas exception et les divers acteurs publics et privés travaillent de concert afin de mettre en place des moyens d'identification qui rehaussent la protection des renseignements personnels et, plus globalement, de la vie privée des individus.

Au cours des dernières années, les fuites de renseignements personnels et les cyberattaques se sont multipliées, tout comme les fraudes liées à l'identité. Collectivement, nous sommes donc arrivés au point où nous devons réinventer nos modes d'identification, et ce, tant dans le monde numérique que physique. C'est dans ce contexte que la mise en place d'une identité numérique s'impose comme la voie à suivre.

En quoi l'identité numérique sera-t-elle un progrès ?

Bâtir la confiance numérique

L'un des plus importants gains qu'apporte l'identité numérique est le degré de contrôle qu'obtient l'individu sur ses renseignements personnels. Dans le monde d'aujourd'hui, nous devons constamment prouver qui nous sommes. Faire cette démonstration nous oblige généralement à fournir une pièce d'identité avec photo délivrée par un gouvernement ou une institution en qui le demandeur a confiance, ce qui à terme nous force à partager beaucoup plus de renseignements personnels que nécessaire. Cette pratique, bien qu'incontournable, n'est pas sécuritaire pour l'individu. Elle représente par ailleurs un actif sensible pour les organisations qui deviennent les gardiens de ces renseignements et qui doivent investir des efforts de plus en plus importants afin d'en assurer la protection. La situation actuelle comporte des risques pour toutes les parties impliquées.

Pour que l'identité numérique soit une solution, elle doit reposer sur la confiance mutuelle. **La notion de confiance est précisément au cœur des efforts de mise en place de l'identité numérique.**

Les acteurs du secteur public et du secteur privé collaborent afin de développer des cadres de confiance visant à baliser les interactions numériques et à mettre en place les bases d'une confiance numérique au pays.

En quoi l'identité numérique sera-t-elle un progrès ?

Bâtir la confiance numérique (suite)

Mondialement, tous les regards sont en effet tournés vers les deux modèles du « Cadre de confiance pancanadien » dont l'un, celui du gouvernement du Canada[2], est orienté vers les organisations publiques et l'autre, celui du Conseil d'identification et d'authentification numérique du Canada (CCIAN)[3] est issu d'une coalition des dirigeants des secteurs public et privé.

Ils visent également à guider la standardisation des écosystèmes d'identité numérique (nationaux et internationaux) en mettant en pratique les politiques, les normes et les technologies requises. En marge de ces travaux, les autorités gouvernementales et certains organismes de certification préparent un cadre réglementaire ainsi que des normes de certification auxquels les divers acteurs de l'écosystème de l'identité numérique devront se soumettre afin d'être considérés comme des émetteurs de confiance. Ainsi, les pièces numériques émises par ces derniers pourront être utilisées en toute confiance par d'autres membres de l'écosystème.

La confiance numérique n'est possible, d'une part, que si des cadres de confiance, plus souvent appelés « cadres de gouvernance », tels que ceux développés au Canada, font l'objet d'un consensus national et, d'autre part, que si les instances gouvernementales concernées leur confèrent la légitimité nécessaire par la mise en place de normes et règlements cohérents. Les piliers et principes de fonctionnement permettront de faire cet arrimage.

---

[2] CIO Strategy Council, Confiance numérique et de l'identité – Partie 1, sept. 2020.

[3] DIACC, Aperçu du Cadre de confiance pancanadien, 2021.

Ces cadres de confiance, comme décrits par le CCIAN, sont : « des ensembles de règles et d'outils conçus pour aider les entreprises et les gouvernements à développer des outils et des services qui permettent de vérifier les informations concernant des interactions numériques. »

Les piliers et principes de l'identité numérique

Nous croyons que l'identité numérique, pour qu'elle suscite une forte adhésion (volontaire), doit être centrée sur la personne. Elle doit d'abord permettre un renforcement de la notion de citoyen, citoyenne. Chaque personne doit se sentir en contrôle de ses renseignements. C'est cette assurance fondamentale qui fera que l'identité numérique sera aussi un bénéfice pour l'ensemble de la société et pour l'économie.

Cela dit, l'identité numérique ne se limite pas aux personnes : une entreprise possédera également une identité numérique. L'enjeu véritable reste humain et, en accord avec plusieurs travaux d'experts[4,5], c'est en étant centrés sur la personne qu'ont été énoncés les principes qui devraient nous guider.

Ces principes révèlent comment nous entrevoyons la mise en place d'un écosystème d'identité numérique de confiance répondant aux attentes et besoins de tous.

Les principes sont regroupés selon trois piliers : **la capacité d'agir, l'autonomie et l'intégrité.**

[4] Sovrin, Principles of SSI v3, septembre 2022. Nous avons adapté la description des principes pour les rendre plus simples à lire et à comprendre.

[5] *Self-sovereign Identity*, Manning publications mai 2021, par Drummond Reed et Alex Preukschat.

Les piliers et principes de l'identité numérique

Piliers	Principes
La capacité d'agir  **La personne est au centre de tout.** **« Je suis en contrôle et j'ai la possibilité d'agir sur mes renseignements personnels et sur mon identité. »**	• Je pourrai choisir les attestations que je déposerai dans mon portefeuille numérique afin de me représenter : ma carte de membre à la bibliothèque municipale, mon permis de conduire, mon passeport, etc. Ces attestations sont des façons différentes de me représenter, en fonction du contexte dans lequel je me trouve. • Je pourrai aussi choisir de déléguer mes attestations à quelqu'un d'autre. Par exemple, je pourrai habiliter une tierce personne à me représenter dans diverses transactions (p. ex. : faire une demande de passeport en mon nom). • J'aurai accès à tous les services et privilèges, sans discrimination, et en ce sens les notions d'égalité et d'inclusion seront mises de l'avant. • Je bénéficierai d'une expérience utilisateur optimale, par les fonctionnalités qui me seront proposées.
L'autonomie  **« Je suis libre de mes choix et à l'abri de toute contrainte dans la gestion de mon identité numérique. »**	• J'ai le choix de participer ou pas à l'écosystème de confiance qui sera mis en place pour l'identité numérique. • Je peux m'assurer qu'une organisation ne soit pas la seule à pouvoir vérifier mes renseignements personnels afin de ne pas être à la merci d'une seule organisation et je préfère que plusieurs organisations puissent le faire, de façon indépendante l'une de l'autre. • Je peux interagir avec plusieurs services, personnes et organisations de façon complètement transparente pour moi. Nous disons alors que les systèmes doivent pouvoir communiquer et échanger entre eux sans que je sois impacté. • Je peux déplacer ou transférer sécuritairement une copie de toutes mes attestations vers un autre portefeuille numérique sans soucis et sans attaches.
L'intégrité  **« J'ai le droit de protéger et de préserver mes renseignements personnels. »**	• Mes renseignements sont en sécurité et je reste en tout temps maître de mes attestations. • Je peux fournir une preuve vérifiable de l'authenticité de mes renseignements personnels. • Je peux conserver mes renseignements personnels confidentiels et divulguer le minimum d'information à qui me le demande : par exemple, prouver que j'ai 18 ans ou plus sans dévoiler ma date de naissance. • Je peux, si je le désire, avoir accès et en toute transparence à l'ensemble des règles, des politiques et des processus qui régissent le système d'identité numérique avec lequel j'interagis.

L’identité numérique dans la vie de tous les jours

L’identité numérique fera partie de la vie de tous les jours des citoyens. Elle sera simple d’utilisation, sécuritaire et permettra à chaque personne qui souhaite l’utiliser d’avoir le contrôle sur ses renseignements personnels. Ces informations seront toujours présentées avec l’autorisation de la personne et, chaque fois, les seuls renseignements présentés seront ceux nécessaires à l’obtention du service désiré, sans plus. L’identité numérique mettra fin à la dissémination des renseignements personnels.

La combinaison du portefeuille numérique et des attestations vérifiables ouvrira la porte à une panoplie d’utilisations touchant autant la vie privée (loisirs, consommation…) ou les relations avec les services publics.

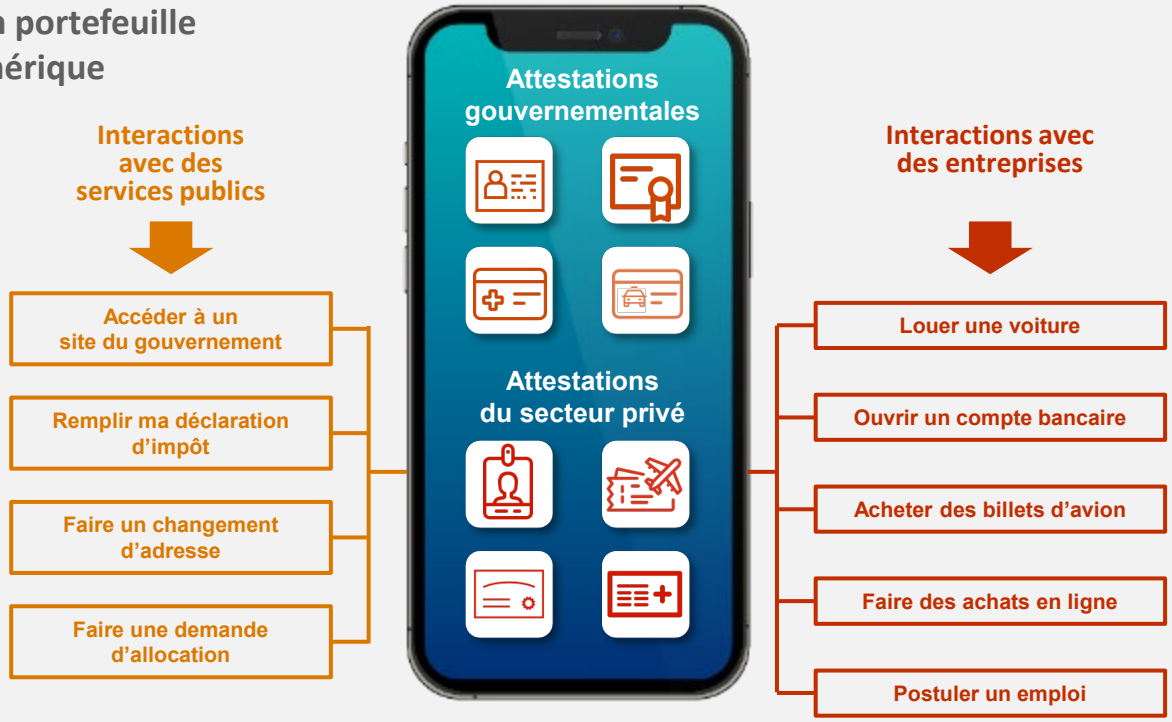
Par exemple, si je dois louer une voiture, je pourrais le faire en ligne en fournissant à l’entreprise de location mes renseignements personnels pertinents, mon droit de conduire et ma preuve d’assurance provenant de trois émetteurs différents.

L’entreprise de location serait en mesure de vérifier que les informations sont intègres et authentiques.

Celles et ceux qui n’ont pas d’appareils intelligents ou qui ne voudraient pas utiliser l'identité numérique pourraient bien sûr continuer d’accéder aux services en utilisant les modes traditionnels actuels.

Dans la section suivante, quelques situations types sont illustrées.

FIGURE 3.
Mon portefeuille numérique

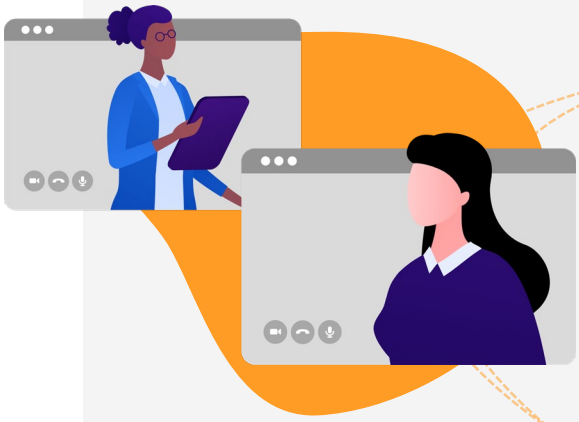


Parcours de l’utilisateur

Nouvel emploi

Étape 1 : Postuler un emploi

Dominique vient tout juste de terminer ses études et s’intéresse à une entreprise de marketing numérique bien connue au Québec. Afin de soumettre sa candidature, l'entreprise lui demande de prouver l’obtention d’un diplôme de premier cycle avant de poursuivre. Dominique utilise son attestation d’études, enregistrée dans son portefeuille numérique et délivrée par son université, pour compléter la demande.



Étape 2 : Entrevue et offre d’emploi

Dominique doit participer à un entretien virtuel, car son profil répond aux exigences du poste. Quelques jours plus tard, une offre décrivant son nouveau poste, son salaire, la structure des primes et les avantages lui est transmise. Heureuse de la nouvelle, Dominique utilise sa signature électronique pour accepter l’offre !

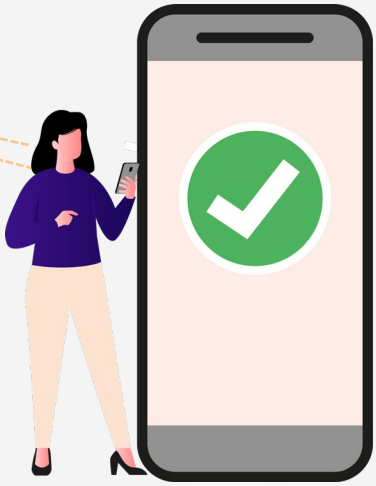
Étape 3 : Partage d’informations

Dominique doit communiquer plusieurs informations permettant à l’entreprise de l’inscrire comme membre du personnel et d’effectuer le dépôt direct toutes les deux semaines. Dominique utilise son portefeuille numérique et sélectionne seulement les attestations vérifiables requises par l’entreprise, lui fournissant une vue détaillée des informations demandées.

L’entreprise confirme l'authenticité des attestations vérifiables reçues, complète l’ouverture du dossier et délivre une attestation indiquant le poste ainsi que le salaire de Dominique.

Exemples d’attestations vérifiables :

- **Informations bancaires;**
- **Identité (NAS, âge, nationalité, etc.);**
- **Adresse;**
- **Permis de travail.**



Étape 4 : Informations supplémentaires

Quelques mois plus tard, son employeur lui délivre son attestation d’emploi, que Dominique ajoute à son portefeuille numérique pour le partager éventuellement avec les gouvernements provincial et fédéral. Dominique sait par ailleurs que les renseignements personnels mis à la disposition de l’employeur pourront être retirés si son emploi se termine.

Parcours de l’utilisateur

Ouverture d’un nouveau compte bancaire[6]

Étape 1 : Ouverture d’un compte bancaire

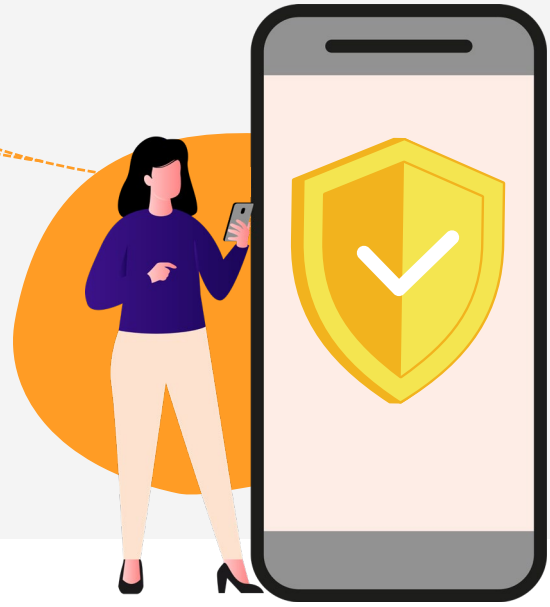
Après avoir décroché son nouveau rôle, Dominique décide d’ouvrir un compte bancaire par l’entremise de l’application mobile de l’institution financière.

Étape 2 : Partage d’informations

Pour valider son identité, l’application mobile propose à Dominique d’utiliser son portefeuille numérique. L’identité numérique lui permet de sélectionner seulement les attestations vérifiables requises par l’institution financière pour les partager en toute sécurité.

Exemples d’attestations vérifiables :

- **Attestation d’emploi;**
- **Identité (NAS, âge, nationalité, etc.) ;**
- **Attestation de domicile.**



Étape 2 : Validation et approbation

L’institution financière confirme l'authenticité des attestations vérifiables reçues et traite la demande de Dominique. Le processus étant très efficace, Dominique reçoit rapidement un courriel confirmant son inscription à sa nouvelle institution financière.

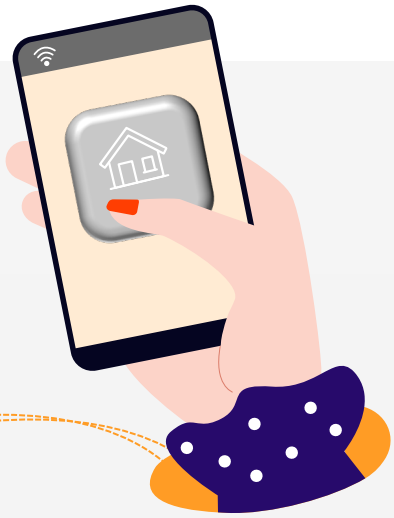
[6] Ontario, ID numérique de l’Ontario : où pourrait-elle être utilisée?, juin 2022.

Parcours de l'utilisateur

Demande de prêt hypothécaire[7]

Étape 1 : **Demande de prêt**

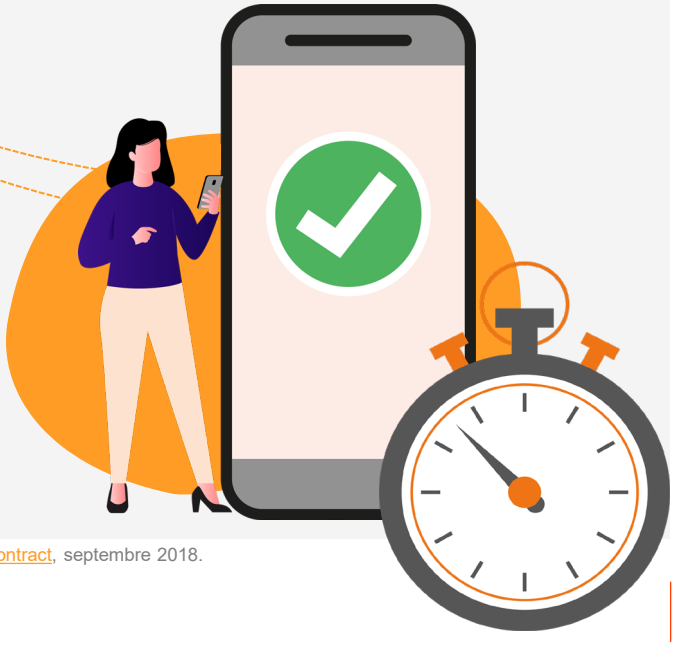
Après quelques années dans son nouveau rôle, Dominique reçoit une promotion et aimerait contracter un prêt hypothécaire pour l'achat d'une propriété. Sa demande est soumise par l'entremise de l'application mobile accessible par son portefeuille numérique.



Toutefois sa demande exige des attestations vérifiables supplémentaires confirmant les réponses fournies par Dominique dans sa demande de prêt au sujet de ses revenus. En utilisant son attestation d'emploi fournie par son employeur et stockée dans son portefeuille numérique, Dominique partage ses informations avec l'institution financière rapidement par l'entremise de l'application mobile.

Étape 2 : **Validation et approbation**

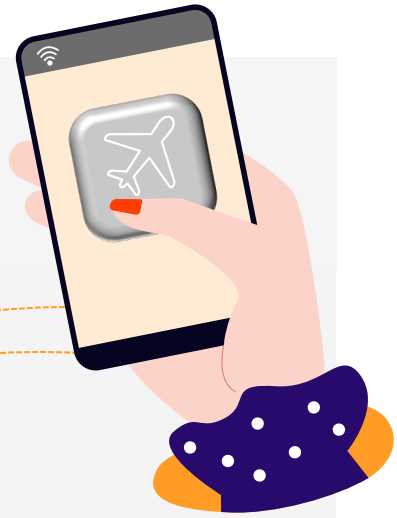
L'institution financière confirme l'authenticité des attestations vérifiables reçues et traite la demande de Dominique. Le prêt est octroyé après approbation.



[7] World Economic Forum, Identity in a Digital World A new chapter in the social contract, septembre 2018.

Parcours de l'utilisateur

Voyage en avion

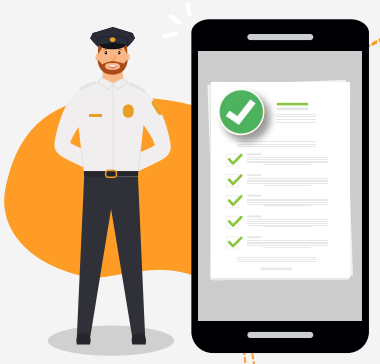


Étape 1 : Enregistrement

Après avoir organisé son voyage de ski en Colombie-Britannique, Dominique arrive à l'aéroport, enregistre ses bagages et se rend au contrôle de sécurité. Dominique ouvre son portefeuille numérique, préparant ses attestations de voyage numériques pour vérification.

Exemples d'attestations vérifiables :

- **Identité ou passeport numérique;**
- **Carte d'embarquement;**
- **Attestation sanitaire (p. ex. : COVID-19).**



Étape 2 : Vérification de l'identité

À cette étape, Dominique doit partager ses informations à l'aide de son portefeuille numérique. Le terminal clignote en vert une fois que son identité a été validée. Après cette vérification, l'échange d'informations est enregistré dans le portefeuille numérique de Dominique qui poursuit son chemin.

Étape 3 : Location de voiture

En attendant son vol, Dominique fait les arrangements pour disposer d'une voiture en Colombie-Britannique. La compagnie de location demande le consentement de Dominique pour accéder à ses attestations vérifiables. Dominique utilise son portefeuille numérique pour sélectionner seulement les attestations vérifiables requises afin de remplir le formulaire de location.

Exemples d'attestations vérifiables :

- **Identité (interprovinciale avec divulgation minimale pour l'âge);**
- **Attestation d'assurance;**
- **Attestation de conduite.**

Étape 4 : Validation et approbation

Rapidement, l'authenticité des attestations vérifiables est confirmée et l'entreprise demande à Dominique de signer électroniquement le contrat afin de l'officialiser. Une fois à destination, Dominique récupère les clés au comptoir de location et quitte l'aéroport.

Quels sont les avantages de l'identité numérique[8] ?

Augmentation de la sécurité et de la confidentialité des renseignements personnels

- Davantage de sécurité et de protection contre le vol d'identité, les fuites de renseignements et la fraude, notamment en raison de la décentralisation des données.
- Protection des renseignements personnels grâce à un niveau de sécurité élevé et, contrairement à votre portefeuille physique, votre identité numérique peut facilement être désactivée en cas de perte ou de vol de votre téléphone.
- Réduction de la quantité de renseignements personnels récoltés et stockés par les organisations.

Meilleur contrôle de vos renseignements personnels

- Consentement plus éclairé : ne dévoilez que les renseignements nécessaires à un moment précis.
- Contrôle complet sur ce que vous souhaitez partager et avec qui vous souhaitez le partager.
- Personne ne peut accéder à vos renseignements personnels sans votre accord.
- Réduction du besoin de gérer de multiples identifiants et mots de passe et moins de risques d'erreur.

Amélioration des services et expérience simplifiée

- Plus grand nombre de services publics et privés disponibles sous forme numérique, ce qui signifie moins d'attente dans les files d'attente physiques.
- Accès à de nouveaux services qui vous étaient inaccessibles ou inconnus auparavant.
- Amélioration générale de l'expérience client en ligne.
- Facile d'utilisation – L'identité numérique est stockée sur votre appareil mobile et est toujours prête à être utilisée quand vous en avez besoin.

[8] McKinsey, Digital identification: A key to inclusive growth, avril 2019. BC Government, BCeID Authentication Service, 2022.

La lutte contre la fraude

La situation actuelle, avec la circulation d'une abondance de renseignements personnels, comporte des risques que l'on tente le mieux possible de mitiger avec de bonnes pratiques de mots de passe et des processus à double authentification, par exemple. Mais malgré les efforts, les investissements et la conscientisation des utilisateurs, le nombre d'incidents, de violations de confidentialité, de vols de renseignements personnels et de fraudes est en hausse. Or, l'un des avantages marqués de l'identité numérique est de lutter plus efficacement contre la fraude. Voyons pourquoi.

On pourrait dire qu'il y a une « économie de la fraude » qui se résume à ceci : avant d'agir, un fraudeur mesure le coût de commettre une fraude par rapport au gain qu'il pourrait en tirer. Si les bénéfices sont plus élevés que les coûts, alors la fraude vaut les efforts.

L'identité numérique vient changer ce rapport coûts-bénéfices de la fraude de la façon suivante : les renseignements personnels des individus, sous forme d'attestations vérifiables, seront stockés dans le portefeuille numérique de chaque personne et non plus dans une base de données centralisée.

Par conséquent, seule la personne qui détient les attestations vérifiables pourra prouver qu'elle est en contrôle de son portefeuille numérique. Pour le fraudeur, au Québec, cela signifie qu'il y aurait 8 millions de portefeuilles numériques à frauder pour avoir l'impact que pourrait avoir le piratage d'une seule base de données centralisée sur la population. De plus, détenir des renseignements personnels ne sera plus suffisant. Le fraudeur devra en plus prouver que c'est bien pour lui que les attestations vérifiables ont été délivrées.

Aujourd'hui, un fraudeur qui détient le numéro d'assurance sociale d'une autre personne peut réussir à se faire passer pour cette autre personne, et ainsi obtenir des services ou des avantages frauduleusement.

Avec l'identité numérique, détenir le numéro d'assurance sociale de quelqu'un d'autre n'est pas suffisant. Il faut démontrer que c'est bien le vôtre. Cela est justement possible grâce à la cryptographie utilisée pour produire les attestations vérifiables que vous aurez dans votre portefeuille numérique.

La lutte contre la fraude

Autrement dit, un numéro d'assurance sociale avec plus de chiffres ou plus sécuritaire qu'actuellement n'est même pas nécessaire. Nous pourrons continuer d'utiliser nos renseignements comme actuellement pour nous identifier, consommer des services ou prouver toutes sortes de choses à notre sujet. Mais il s'agira de produire des attestations vérifiables à partir de ce que nous avons déjà comme information ou document officiel.

Bref, notre attestation vérifiable d'assurance sociale sera une preuve cryptographique de notre numéro d'assurance sociale actuel qui devra être produite, dans ce cas, par Service Canada.

L'identité numérique permet de rendre les renseignements personnels non attrayants et sans valeur pour les fraudeurs.

Les conditions gagnantes d'une démarche d'implantation d'identité numérique

Parmi les conditions gagnantes favorisant la confiance et l'adhésion du plus grand nombre de personnes, d'organisations publiques et d'entreprises privées pour atteindre les retombées escomptées de l'identification numérique, on retrouve principalement :

La mise en place d'une **gouvernance solide et efficace** en termes de lois, politiques, règlements, rôles, responsabilités et processus au sein des écosystèmes de l'identification numérique.

L'appui et l'adoption des **organisations des secteurs public et privé**.

Le **respect de principes de fonctionnement** qui mettent la personne au centre du système selon les piliers Capacité d'agir, Autonomie et Intégrité.

Le rôle des organisations privées

L'identité numérique repose sur un écosystème collaboratif soudé par la confiance mutuelle. Cet écosystème est composé de plusieurs organismes, publics et privés, qui auront, chacun, un rôle important à jouer dans leur secteur d'activité respectif. Toutes les parties prenantes doivent avoir confiance aux processus et aux règles qui auront été mis en place.

Quel serait le rôle des organisations privées ? Trois mots clés : contribution, confiance et adoption.

Contribution

En tant qu'émettrices et vérificatrices de plusieurs attestations, les organisations du secteur privé vont contribuer de manière significative au développement et à l'évolution de l'écosystème de l'identité numérique. Par leur présence essentielle dans la vie économique et sociale de la population, par leur capacité d'investissement, par leur capacité d'innovation et leur savoir-faire technologique, les entreprises privées sont des partenaires incontournables pour construire un écosystème solide. C'est grâce à cette implication continue dans le temps que nous pourrons bâtir la confiance.

Confiance

La contribution du secteur privé, et la qualité de la collaboration entre les gouvernements et le secteur privé seront à la base de la confiance que le système d'identité numérique pourra susciter dans la population. Les entreprises seront, selon les circonstances, des vérificateurs et des émetteurs de confiance dans l'écosystème d'identité numérique.

En travaillant en collaboration avec le secteur public, nous pourrons apporter appui et expertise aux gouvernements afin de s'assurer que les solutions mises en place répondent aux besoins du secteur public et du secteur privé. Les entreprises privées veulent ainsi permettre la création d'une relation de confiance forte pour faciliter son adoption.

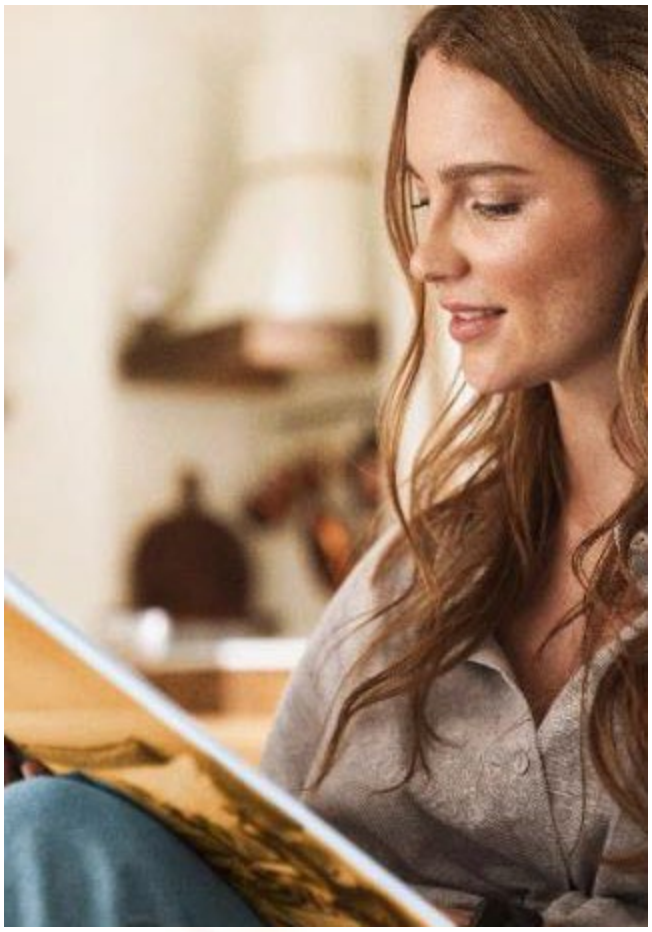
Adoption

Les entreprises privées contribueront à la mise en place de l'identité numérique en collaboration avec les gouvernements; cette collaboration suscitera la confiance de la population et encouragera une adoption massive de l'identité numérique par les citoyens et les citoyennes. Plus encore, comme le secteur privé représente environ 65 %[9] des emplois et du PIB du Québec, c'est d'abord par les entreprises que l'identité numérique entrera dans le quotidien des Québécoises et Québécois. Les entreprises devront être prêtes à faire le passage, elles devront informer et sensibiliser leur clientèle ainsi que faire de l'accompagnement. Les entreprises joueront un rôle clé dans le développement d'une expérience conviviale de l'identité numérique.

[9] Institut de la statistique du Québec, Bilan du marché du travail au Québec en 2022 (quebec.ca), mars 2023.

L’identité numérique ici et ailleurs

Au niveau fédéral, la vision du gouvernement du Canada[10] est de créer un écosystème d’identité numérique où les identités numériques de confiance sont utilisées pour fournir des services du gouvernement canadien de manière transparente sur n’importe quelle plateforme, avec n’importe quel partenaire, sur n’importe quel appareil.



L’identité numérique, une tendance mondiale

La **Banque mondiale** estime que « près de 1 milliard de personnes dans le monde n’ont pas de preuve d’identité élémentaire, ce qui est essentiel pour protéger leurs droits et leur permettre d’avoir un accès égalitaire aux services et aux opportunités[11] » (p. ex. : éducation, soins de santé et emplois).

Aux **Nations unies**, une prise de conscience accrue de la nécessité de systèmes d’identification plus inclusifs et plus robustes a conduit à un appel à l’action mondial, incarné dans la cible 16.9 de leurs objectifs de développement durable : « D’ici 2030, fournir une identité numérique pour tous, incluant les certificats de naissance[12]. »

---

[10] Une vision de l’identité numérique du Canada digne de confiance.

[11] Banque mondiale, Principes sur l'identification pour un développement durable.

[12] Nations unies, Cible de développement durable 16.9.

L’identité numérique ici et ailleurs

L’identité numérique, une tendance mondiale (suite)

L’importance d’impliquer tous les acteurs de l’écosystème et d’avoir des attestations vérifiables utilisables sur l’ensemble des territoires canadiens et à l’international amène les provinces ainsi que le gouvernement fédéral à collaborer entre eux, avec les industries et d’autres pays afin d’explorer les possibilités d’étendre la reconnaissance des justificatifs d’identité au secteur privé, à l’extérieur des provinces, voire à l’extérieur du pays. L’Alberta et la Colombie-Britannique, à titre d’exemple, ont procédé aux premiers examens de leurs justificatifs d’identité numérique pour faire en sorte que ces justificatifs soient acceptés par le gouvernement fédéral.

Voici quelques exemples de collaborations du Canada avec l’international :

- Le Canada et l’Union européenne (UE) travaillent sur des moyens de reconnaître l’utilisation des justificatifs d’identité numérique, y compris les transactions effectuées par l’intermédiaire de portefeuilles numériques, à des fins professionnelles et personnelles.

- Le Canada est l’un des huit pays qui ont formé un groupe de travail sur l’identification numérique en 2020. Le groupe – présidé par l’agence australienne de transformation numérique – comprend également l’Australie, la Finlande, Israël, la Nouvelle-Zélande, Singapour, les Pays-Bas et le Royaume-Uni. Il a rédigé un ensemble de principes de haut niveau pour soutenir le développement de systèmes et d'infrastructures d'identification numérique mutuellement reconnus et vise à renforcer les accords commerciaux dans la poursuite de la reprise économique post-COVID.

À l’extérieur du Canada, les pays suivants se démarquent par leurs initiatives d’identité numérique : la Grèce, l’Allemagne, le Royaume-Uni, l’Australie ainsi que l’UE.

Conclusion

L'identité numérique émerge de façon progressive dans nos sociétés technologiques. Elle n'est ni rupture ni révolution. Elle est une continuité d'évolution et le résultat de perfectionnements technologiques, d'apprentissages communs, de risques mieux maîtrisés. L'identité numérique devient simplement l'outil approprié pour effectuer de façon simple et sécuritaire, dans le contexte des années 2020, le processus d'identification-authentification qui fait partie de la vie citoyenne depuis plusieurs décennies.

L'identité numérique, par sa fonction, s'inscrit ainsi dans une continuité. Mais dans sa manière, elle constitue, il est vrai, un changement important. Elle donne à la personne le plein contrôle sur ses renseignements personnels; elle restreint la dissémination de renseignements personnels dans l'espace numérique; elle libère la personne et les organisations de la gestion complexe de la combinaison identifiants-authentifiants; et avec sa structure décentralisée, l'identité numérique rend la fraude beaucoup plus difficile.

Ces notions peuvent paraître complexes à certains égards. Il est compréhensible que des questions soient posées, qu'une certaine méfiance s'exprime à l'égard des concepts nouveaux qui changent les habitudes et les comportements des citoyens dans un univers de plus en plus numérique.

Il faut prendre le temps de sensibiliser la population, de présenter l'identité numérique, de montrer comment elle s'insérera dans notre quotidien et facilitera notre vie de même que les interactions courantes que nous avons avec les services publics ou des commerces. Ce livre blanc s'inscrit dans cette volonté de nourrir une compréhension commune. **Si son contenu vous a éclairé sur le sujet, n'hésitez pas à le partager.**

beneva

Desjardins

KPMG

TELUS

VIDÉOTRON

LABORATOIRE
d'identité numérique