29-07-2019

SecureKey Technologies inc.

Mémoire dans le cadre des consultations prébudgétaires 2020

SECURE KEY

4101 Yonge Street, Suite 501, Toronto, ON | M2P 1N6

Recommandations

- **Recommandation 1 :** Le gouvernement du Canada doit établir une politique claire qui permettra l'interopérabilité de l'identité numérique et du partage des données entre les entités publiques et privées. La politique doit être conçue de manière à favoriser l'établissement d'un écosystème d'identité et de données numériques axé sur l'utilisateur qui permet de stimuler la croissance de l'économie au Canada, tout en protégeant les données des citoyens, des entreprises et des gouvernements.

- **Recommandation 2 :** Le gouvernement du Canada doit investir pour soutenir la croissance d'un écosystème d'identité numérique et de partage de données axé sur l'utilisateur qui permet de stimuler la croissance de l'économie au Canada et favorise les possibilités d'exportation de l'innovation et de l'expertise canadiennes à l'échelle mondiale.

29-07-2019

Réseaux d'identité numérique et de partage de données : une possibilité inexploitée pour le Canada

Au sujet de SecureKey

SecureKey Technologies (« SecureKey »), une entreprise située à Toronto, est un chef de file canadien novateur qui simplifie l'accès, par les consommateurs, aux services et aux applications en ligne. Utilisant une approche écosystémique et des technologies de pointe, SecureKey permet aux consommateurs de faire appel à des fournisseurs d'identifiants de confiance, comme des institutions financières et des exploitants de réseaux de télécommunication, afin de pouvoir accéder à des services en ligne essentiels. SecureKey est le fournisseur officiel du service d'ouverture de session par l'intermédiaire d'un partenaire du gouvernement du Canada depuis 2012. L'entreprise utilise un système portant le nom de Service Concierge SecureKey. Il est possible d'accéder au Service Concierge SecureKey pour plus de 80 services en ligne offerts par les ministères et organismes du gouvernement du Canada, dont l'Agence du revenu du Canada.

À partir de cette solution, SecureKey s'est associée à sept des principales institutions financières au Canada : BMO, CIBC, Desjardins, Banque Nationale du Canada, RBC, Banque Scotia et TD. Ce consortium intersectoriel d'organisations ayant une optique commune a collaboré pour créer une solution écosystémique globale en matière d'identité numérique qui protégera mieux les citoyens, sans égard aux services en ligne qu'ils choisissent d'utiliser.

À la suite de cette collaboration, SecureKey et ses partenaires ont récemment lancé Vérifiez.Moi, un nouveau service canadien inédit qui aide les citoyens à vérifier leur identité auprès des services numériques de leur choix. Cette technologie de la prochaine génération permettra aux utilisateurs de réaliser leurs activités en ligne, en personne et par téléphone de manière plus sécuritaire, plus privée et comportant moins de risque par rapport aux systèmes de sécurité traditionnels. Vérifiez.Moi aide à confirmer une identité de manière rapide et sécurisée, utilisant des renseignements personnels que les citoyens ont accepté, de façon explicite, de partager avec des connexions de confiance.

Le service Vérifiez.Moi se fonde sur la technologie de chaîne de blocs. Il est protégé par des protocoles de sécurité rigoureux pour éviter que les renseignements personnels des citoyens soient identifiés, utilisés à mauvais escient ou qu'on y ait accès. Le service a été élaboré de manière à ce que des principes de protection de la vie privée Triple Blind^{MC} soient à la base de la solution. Cela signifie qu'aucune partie unique du service, y compris SecureKey, l'exploitant du réseau, ne peut voir l'ensemble des détails d'une transaction. Les destinations et les sources sont inconnues les unes des autres, et le réseau ne peut pas voir les données immobiles ou transmises. Les citoyens demeurent toujours les maîtres du processus en choisissant les données qu'ils veulent partager et les organisations avec qui les partager, ce qui réduit le partage à outrance inutile des renseignements personnels afin d'accéder aux services sélectionnés.

Évolution des services numériques

Avec l'arrivée de l'ère numérique, une panoplie de nouveaux services, de modèles opérationnels et de possibilités de participation à l'économie mondiale a vu le jour. Il n'y a pas si longtemps, il était inimaginable de demander un service de transport partagé depuis un appareil de poche, ou d'accéder, en toute confidentialité, à des services gouvernementaux depuis la maison. Tout ne revient pas aux attentes des citoyens. Les entreprises, les gouvernements et d'autres organisations disposent de fortes motivations pour offrir les services et faire des transactions en ligne, ce qui leur permettra d'améliorer l'expérience des clients, de faire des économies et d'accroître l'intégrité opérationnelle.

Malgré les avantages associés au fait d'offrir les services en ligne, le volume énorme de données requises pour exploiter le système actuel expose des vulnérabilités dont il faut tenir compte. Les coûts et les risques associés au fait que les entreprises conservent des données personnelles sont de plus en plus évidents toutes les fois qu'une brèche de données est massivement médiatisée. Entre-temps, de nombreux consommateurs ne comprennent pas qu'ils produisent un grand volume de données personnelles lorsqu'ils utilisent des services numériques, mais que les données peuvent être utilisées de différentes façons, bonnes ou mauvaises, légalement ou non.

Pour relever ce défi, l'identité numérique fiable sera essentielle pour permettre le développement continu de services numériques. Du commerce électronique à l'économie du partage, un système d'identité numérique robuste et fiable permet d'établir la confiance, d'assurer la sécurité et d'atténuer la fraude. Ainsi, nous affirmons qu'un système d'identité numérique fiable est essentiel pour assurer la croissance de l'économie numérique au Canada, ainsi qu'un aspect important dont le Comité doit tenir compte dans ses travaux. Finalement, il s'agit d'un outil clé pour rendre les services numériques sécuritaires, sécurisés, efficaces et accessibles.
Sans ce système, de nombreux problèmes auxquels les Canadiens font face prendront de l'ampleur en raison de la hausse rapide du nombre de services numériques, ainsi que de la sophistication et de la prévalence croissantes des fraudeurs en ligne.

Le défi que représente l'identité numérique

Aujourd'hui, la capacité d'une organisation de fonctionner au sein d'un environnement numérique relève d'une seule question... « Puis-je faire confiance à la personne, ou à l'identité numérique, qui est l'autre partie de la transaction? ».

Pour reconnaître les clients et fournir un accès de confiance aux services en ligne, les organisations déploient habituellement un ensemble de mesures analogiques et numériques pour confirmer l'identité et atténuer le risque. Cependant, comme nous l'avons vu, ces solutions ont tendance à être complexes et inadéquates. Le niveau de confiance envers celles-ci en a donc souffert.

Habituellement, on demande aux citoyens d'utiliser différentes méthodes d'identification pour respecter les exigences en matière de vérification des organisations auprès desquelles ils souhaitent obtenir des services. Dans le cadre de ces processus, ils ne savent pas où les renseignements vont et comment ils sont utilisés. Ils sont donc naturellement préoccupés par les atteintes à la protection des données et les imposteurs en ligne.
Il est de plus en plus difficile de prouver une identité. Il est peu pratique de le faire en personne. Le processus affiche un potentiel de friction dans le monde numérique, où le risque de fraude et de vol d'identité est supérieur. Les fraudeurs recueillent des renseignements pour en savoir autant que possible sur les citoyens qu'ils imitent. Parfois, ils en savent même plus que les citoyens eux-mêmes. Il est facile de produire de fausses cartes physiques, et il est souvent impossible de vérifier leur validité auprès des sources les ayant délivrées au moment de la transaction. Même les méthodes biométriques, comme les empreintes digitales, qui ont souvent été présentées comme la solution à la fraude numérique, sont ciblées par les pirates, augmentant le risque que les données biométriques soient compromises.

Ces facteurs augmentent la complexité, réduisent la confiance à l'égard du système et ont des répercussions négatives sur la protection de la vie privée. C'est exactement le contraire de ce qui devrait se produire. Notre système de validation de l'identité cloisonné s'avère trop difficile à utiliser pour les consommateurs et trop coûteux à maintenir. Nous devons relever le défi ensemble, et saisir les possibilités qu'offre l'identité numérique.

Les possibilités associées à l'identité numérique

Selon des estimations conservatrices, la valeur potentielle de l'identité numérique fiable pour l'économie canadienne est d'environ 1 % du PIB, ou 15 milliards de dollars[i]. Selon des perspectives encore plus optimistes, « d'ici 2030, la valeur économique de l'utilisation appropriée de l'identité numérique devrait être de 3 à 6 %[ii] ». En fait, à l'échelle de l'économie, l'identité est essentielle pour fournir des services. Les avantages sont particulièrement évidents dans de nombreux secteurs.

On peut observer la nécessité d'utiliser l'identité numérique aujourd'hui avec les services réglementés, comme les services financiers, où les entreprises doivent réaliser de rigoureuses vérifications pour prouver l'identité du client lorsqu'il ouvre un compte, puis faire des vérifications périodiques par après. Ces vérifications sont importantes pour prévenir le blanchiment d'argent et le financement d'activités terroristes. Cependant, elles sont aussi exigeantes en temps, en plus d'être coûteuses et souvent redondantes. Au Canada, des études ont établi que les économies nettes potentielles par institution atteindraient au moins 100 millions de dollars par année, prenant la forme d'efficacité opérationnelle attribuable à la réduction des coûts de traitement manuel et de la fraude[iii].

L'identité numérique fiable est aussi nécessaire dans le cadre d'une vaste gamme de scénarios commerciaux et de commerce de détail en ligne, lorsqu'un paiement est requis. Cela est particulièrement vrai lorsqu'il n'existe pas déjà de relation entre les parties et qu'il faut réduire, d'une certaine manière, le risque que posent les fraudeurs. Dans le monde numérique, les paiements exigent un degré de confiance élevé, puisqu'il est impossible de voir la personne de l'autre côté de la transaction. Souvent, il n'existe aucune façon directe de vérifier numériquement la personne ou l'organisation authentique.

Relever le défi que représente l'identité numérique

Le défi auquel nous faisons face ne revient pas simplement à trouver la meilleure technologie, à avoir les compétences appropriées ou à trouver la somme suffisante pour résoudre le problème. Quiconque est visé par le système doit chercher à résoudre le problème de l'identité numérique à la base de tous les services numériques. Il faut veiller à ce que les données et les renseignements de l'identité relèvent du citoyen.

L'expérience vécue jusqu'à maintenant montre que les méthodes s'appuyant sur un seul facteur ne sont pas à la hauteur. Cela signifie qu'il faut disposer de réseaux de confiance, c'est-à-dire l'écosystème de participants fiables. Tous les participants doivent prendre part à l'établissement de la solution, y compris les citoyens, car le fait qu'ils soient maîtres de leurs données et de la protection de leurs renseignements personnels est à la base de la sécurité.

Ce n'est qu'en réunissant les meilleures forces de chaque acteur de l'écosystème que nous pourrons résoudre le problème de l'identité numérique et regagner la confiance requise des organisations et des citoyens. Imaginez un scénario dans lequel un citoyen peut choisir de partager de manière sécurisée des renseignements au sein d'un réseau constitué d'organisations auxquelles il fait déjà confiance et avec qui il fait des transactions. En utilisant cette approche multidimensionnelle pour prouver l'identité, nous obtenons un degré de confiance beaucoup plus élevé en ce qui concerne l'identité de la personne faisant les transactions. Cependant, il faut trouver une façon de le faire sans devenir un réseau de surveillance ou créer un piège à pirates en ce qui concerne les données. En bref, il faut jeter les bases en ce qui concerne la protection de la vie privée et de la confiance, tout en minimisant le volume de données partagées par les parties.

Parmi les meilleurs moyens servant à vérifier l'identité et à établir et à maintenir la confiance, il y a le fait d'utiliser de multiples sources d'information pouvant être vérifiées et être jumelées, afin d'offrir un degré d'assurance de l'identité beaucoup plus élevé. Un réseau réussi, comme Vérifiez.Moi, réunira ces facteurs de fournisseurs

multiples, par exemple la collaboration d'institutions financières, de fournisseurs de télécommunication et de gouvernements provinciaux, afin d'assurer la robustesse. Un tel système peut se fonder sur trois facteurs : « ce que je sais » (une donnée que seule la personne connaît, comme un mot de passe sécurisé); « ce que j'ai » (un article unique, comme une carte à puce ou un téléphone mobile); « ce que je suis » (comme un identifiant biométrique ou une empreinte faciale). Par exemple, une personne qui utilise un appareil reconnu par son fournisseur de télécommunication ouvre une session pour recevoir des services de sa banque, partageant des renseignements venant directement de sources autorisées (p. ex. le gouvernement), tandis que l'information du fournisseur (comme la banque) est comparée aux renseignements et validée en fonction de ceux-ci. On crée ainsi une expérience sécurisée et transparente pour l'utilisateur.

La collaboration entre le secteur public et le secteur privé est nécessaire

Même si les avantages de l'approche écosystémique en matière d'identité numérique sont reconnus, aucune entreprise ou organisation ne peut, à elle seule, relever le défi. Tous les secteurs de l'économie numérique se fondent sur l'identité numérique. Cela signifie qu'il y a de nombreux intervenants potentiels et besoins différents. Du même coup, puisqu'il est urgent que les consommateurs soient responsables de leur identité numérique, les intervenants ne peuvent plus opter pour leur propre voie à suivre. Les organisations en tout genre, dans les secteurs public et privé, doivent collaborer pour établir des normes et créer un écosystème robuste qui est dans l'intérêt primordial de tous.

Examinant les pratiques exemplaires mondiales, les systèmes les plus réussis englobent les secteurs public et privé, et exigent une coordination importante entre les secteurs fortement réglementés et le gouvernement. Parmi les exemples de réussite, il y a NemID, au Danemark, et BankID, en Suède, où les utilisateurs tirent profit des justificatifs bancaires haute vitesse lors d'interactions exigeant une régularité moindre, comme les soins de santé et le gouvernement. En revanche, les systèmes conçus de manière isolée sont associés à de nombreux problèmes. Il ne s'agit pas d'un modèle pratique que le Canada doit adopter. Il y a notamment UK Verify, dont le taux d'adoption a été faible et dont les coûts de mise en œuvre ont été élevés, et Estonia ID, qui utilise une identité numérique nationale unique délivrée par le gouvernement centralisé et une carte d'identité à puce. Il s'agit d'un modèle qui n'est pas envisagé au Canada.

Avec un système d'industries de base bien réglementées et la collaboration entre le secteur public et le secteur privé, le Canada a l'occasion de résoudre le problème de l'identité numérique et de devenir un modèle pour le monde entier. En montrant la coopération entre les compétences, en déployant des télécommunications avancées sur le plan technologique et en soutenant et en adoptant de nouvelles approches, le Canada peut devenir un chef de file mondial, établissant une norme en matière d'identité numérique. À l'échelle internationale, nous sommes déjà reconnus pour nos idées novatrices, comme l'initiative Global Privacy and Security by Design d'Ann Cavoukian, Ph. D., et le Pan Canadian Trust Framework, soutenu par le Digital Identity and Authentication Council of Canada.

Le cyberrisque touchant l'identité numérique est élevé. Cependant, nous pouvons créer des services qui peuvent valider l'identité à partir de parties multiples lors d'une même transaction, tout en assurant la protection de la vie privée et le contrôle complets du citoyen. Pour assurer la réussite de toute solution, il faut, à la base, protéger la vie privée des citoyens et leur fournir un sentiment de sécurité.

Il est essentiel que l'approche du Canada relie les secteurs fiables de l'économie numérique, comme les finances, les télécommunications, le gouvernement et le commerce. Finalement, toute solution qui n'est pas le fruit d'une collaboration entre le secteur privé et le secteur public aura un succès limité, puisqu'elle maintiendra l'approche cloisonnée qui fait présentement l'objet de pressions.

29-07-2019

Personne-ressource

Eric Swedersky, premier vice-président, prestation et secteur public
Eric.Swedersky@securekey.com

[i] *The Economic Impact of Digital Identity in Canada,* Digital ID & Authentication Council of Canada, 2018.
[ii] *Digital Identification: The Key to Inclusive Growth*, McKinsey and Co, 2019.
[iii] *The Economic Impact of Digital Identity in Canada*, Digital ID & Authentication Council of Canada, 2018.