Identité numérique

Libérer tout le potentiel de l'économie numérique au Canada

Le point de vue de l'Association Interac
et d'Acxsys Corporation

« Les Canadiens doivent pouvoir faire affaire autant avec des organisations canadiennes qu'avec des organisations internationales, et ils doivent pouvoir le faire sans s'inquiéter de leur sécurité. »

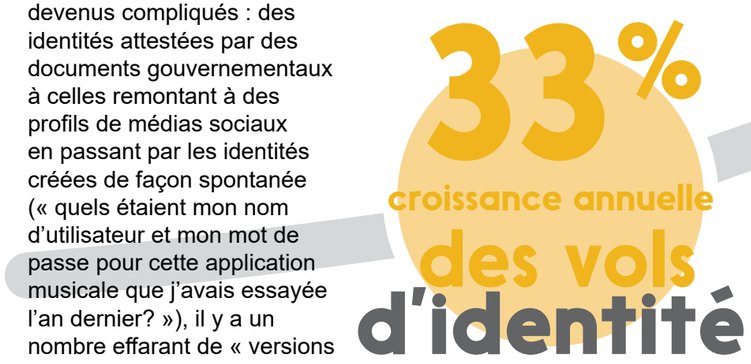
Introduction

La prochaine fois que vous configurerez une nouvelle application mobile et que vous choisirez de vous inscrire à l'aide de l'un de vos comptes de médias sociaux, vous indiquerez qui vous êtes en établissant un lien avec un document d'identité existant (dans ce cas, un document numérique). De même, lorsque vous ouvrez un compte auprès d'une banque la première fois et que l'institution demande à voir votre passeport ou votre permis de conduire, vous certifiez qui vous êtes en établissant un lien avec des pièces d'identité existantes (dans ce cas, des documents physiques) délivrées par un gouvernement.

En tant que consommateurs au XXIe siècle, nous sommes maintenant tellement habitués de décliner notre identité chaque fois que nous nous inscrivons à un autre service en ligne ou à une nouvelle application que nous nous arrêtons rarement pour constater à quel point nos types d'identités personnelles sont devenus compliqués : des identités attestées par des documents gouvernementaux à celles remontant à des profils de médias sociaux en passant par les identités créées de façon spontanée (« quels étaient mon nom d'utilisateur et mon mot de passe pour cette application musicale que j'avais essayée l'an dernier? »), il y a un nombre effarant de « versions » de chacun de nous en circulation.

Les identités numériques basées sur des profils de médias sociaux sont pratiques pour les utilisateurs, mais, comme ces profils sont créés par les utilisateurs justement, ils sont tout à fait insuffisants pour les affaires lorsqu'une valeur ou un risque important est en jeu : vous ne pourrez jamais acheter une maison en utilisant seulement un profil de média social pour vous identifier et prendre possession. Mais les pièces d'identité délivrées par les gouvernements, plus sûres, sont habituellement des documents physiques, ce qui implique que vous devez vous rendre à l'emplacement de la transaction commerciale pour présenter vos pièces d'identité et vous prêter à une identification visuelle – une exigence qui contredit quelque peu la promesse de transactions rapides, transparentes, pratiques et sécurisées pouvant être effectuées sur tous les canaux de l'économie numérique.

Le problème est encore pire, toutefois, parce que les méthodes d'identification non sécurisées ouvrent la porte autant au vol d'identité – dont l'incidence a cru de 33 % par an en moyenne au cours des trois dernières années – qu'à la fraude d'identité, qui coûte maintenant plus de 200 millions de dollars par année aux entreprises canadiennes*.



Les Canadiens doivent pouvoir faire affaire (et s'inscrire à leurs services) autant avec des organisations canadiennes qu'avec des organisations internationales, et ils doivent pouvoir le faire sans s'inquiéter de leur sécurité. Puisqu'une grande part de notre économie dépend des transactions numériques, et que cette part ne cesse de croître, il est essentiel que nous nous attaquions à ces problèmes dès maintenant. Il ne sera possible de profiter de tous les avantages d'une économie du XXIe siècle que si nous mettons au point des méthodes d'identité numérique et d'authentification hautement sécuritaires, omniprésentes et pratiques pour les Canadiens.

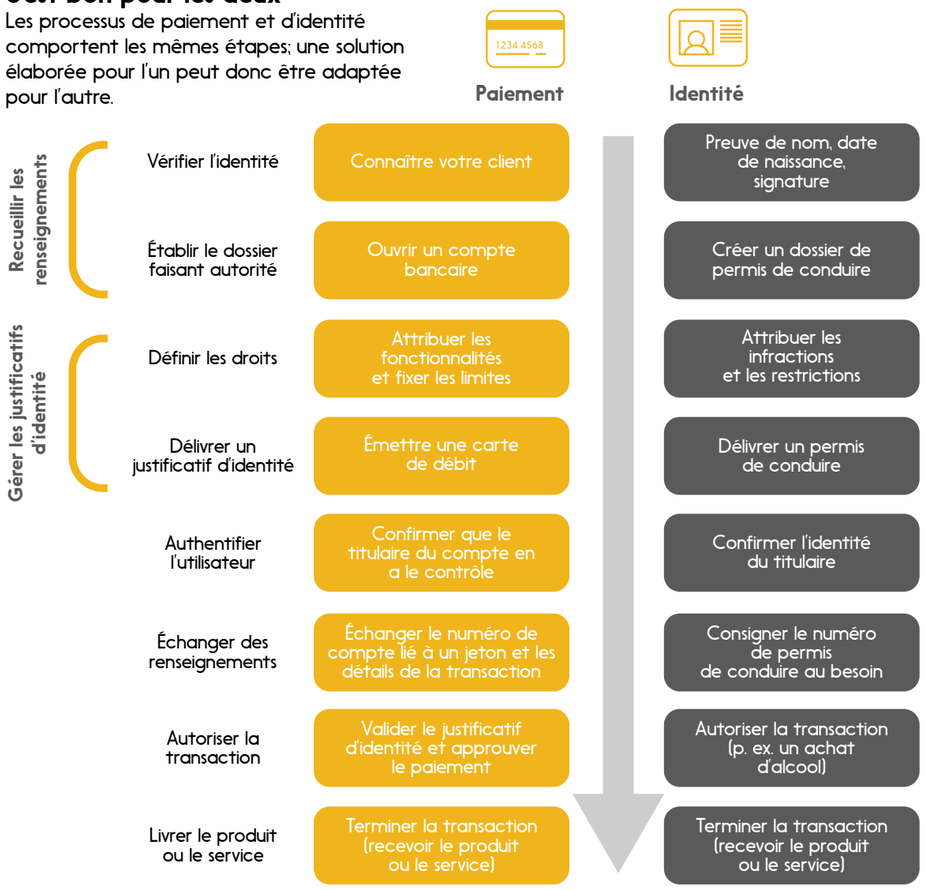
* Source : Centre antifraude du Canada; valeurs déduites des données déclarées et de l'estimation par le CAFC que les données déclarées représentent environ 5 % du total des vols et des fraudes d'identité et des pertes liées à ces fraudes.

Les facteurs de réussite

À l'Association Interac, nous travaillons sur les questions d'identité et d'authentification depuis longtemps, parce que nous avons toujours dû vérifier que les particuliers et les organisations qui font des paiements et qui transfèrent des fonds – comme ceux qui les reçoivent – sont bien ceux qu'ils disent être. Bref, puisque la sécurité est la clé de voûte d'une architecture de paiements fiable, vous pouvez remplacer « faire des paiements » par des activités comme « signer des documents » ou « s'inscrire à des services gouvernementaux », et l'exigence fondamentale d'une identification et d'une authentification numériques à la fois sécuritaires et pratiques reste la même – une exigence que nous avons intégrée à nos processus et à nos technologies il y a des années. La présente section décrit les facteurs qui, selon notre expérience, seront essentiels à toute solution porteuse.

Si c'est bon pour l'un, c'est bon pour les deux

Les processus de paiement et d'identité comportent les mêmes étapes; une solution élaborée pour l'un peut donc être adaptée pour l'autre.



Une marque de confiance

Parce qu'une identité est à la fois éminemment personnelle et essentielle pour des questions importantes telles que le patrimoine et l'accès à des services, l'adoption généralisée par les particuliers et même par les organisations dépendra non seulement des capacités techniques d'une solution donnée, mais aussi (et probablement surtout) du degré de confiance qu'on accorde généralement à un fournisseur de solutions. Une solution d'identité et d'authentification réussie et durable sera vraisemblablement offerte par une marque ayant déjà mérité la confiance des Canadiens en offrant des services sécurisés et fiables dans des domaines connexes pendant une longue période. D'ailleurs, même l'élaboration de la solution y gagnera si elle est dirigée par une marque de confiance, puisque coordonner des partenaires techniques et mobiliser de nombreuses parties prenantes sont des activités qui sont plus facilement accomplies par des organisations qui ont fait leurs preuves et qui ont acquis une réputation de collaborateurs efficaces.

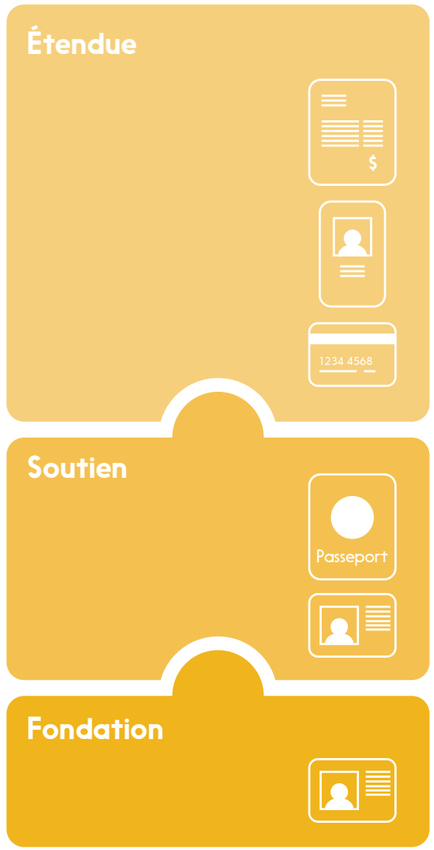
Contrôle par l'utilisateur et commodité

Une bonne solution d'identification et d'authentification doit être fondée sur des valeurs essentielles comme le contrôle par l'utilisateur et le consentement. Les utilisateurs doivent avoir la certitude totale que leurs renseignements personnels leur appartiennent vraiment et qu'une organisation ou un service ne pourra les obtenir, les utiliser ou les stocker qu'avec leur autorisation expresse. De même, une technologie de sécurité difficile à utiliser trouvera peu d'utilisateurs, et il est donc impératif d'intégrer la commodité parmi ses principales caractéristiques. Heureusement, notre travail auprès des institutions financières pour sécuriser les paiements numérique nous a appris qu'un système conçu intelligemment peut être à la fois très sécuritaire et réellement pratique pour les transactions quotidiennes ou horaires. Pendant la conception d'une infrastructure d'identité numérique, il importe de se rappeler que la sécurité et la commodité ne sont pas des conditions opposées qui doivent l'une et l'autre être mises en balance, mais des partenaires dans la création d'un système optimal.

Omniprésence

Comme nous l'avons vu plus haut, nous vivons actuellement dans un univers qui est tout le contraire d'une infrastructure d'identité omniprésente : nos documents physiques sont conservés dans des portefeuilles, des poches, des tiroirs de cuisine ou des coffrets de sûreté; nos identités numériques sont variées, sans lien entre elles et réparties dans des dizaines ou des centaines de bases de données détenues par diverses organisations et entreprises – et chaque fournisseur numérique avec qui nous faisons affaire soit exige de nous de nouveaux identifiants qui ne s'appliquent qu'à son service, ou se fie à des identités de médias sociaux qui ne sont validées par personne et qui ne sont pas valables pour des transactions de grande valeur ou juridiquement contraignantes.

À l'inverse, une infrastructure omniprésente éliminerait cette confusion ainsi que les nombreux espaces d'identité protégés dans lesquels nous devons naviguer (tellement de barrières à franchir et de clés dans nos poches…) tout en offrant un accès uniforme à l'ensemble des services, des transactions et des ententes qui exigent actuellement des pièces d'identité physiques délivrées par des gouvernements. Les organisations n'auraient plus à choisir entre divers moyens de vérifier l'identité des clients ou à en inventer elles-mêmes, et les particuliers n'auraient plus à créer de nouveaux identifiants au pied levé pour chaque nouveau service qu'ils veulent obtenir. Les mêmes méthodes s'appliqueraient à tout ce que les Canadiens utilisent, et à tous ceux avec qui ils font affaire.



La conception par couches

Les justificatifs d'identité délivrés par les gouvernements **servent de fondement à l'écosystème d'identité**; chaque couche de justificatifs d'identité additionnelle dépend de l'authenticité et de la sécurité de la couche qui se trouve en dessous.

Factures de services publics
Preuves d'emploi
Cartes de crédit
Identifiants bancaires

Passeport
Numéro d'assurance sociale (NAS)
Carte santé
Permis de conduire

Carte de résident permanent
Certificat de citoyenneté
Acte de naissance

La sécurité par l'abstraction

Un système omniprésent ne devrait cependant pas exiger des Canadiens qu'ils communiquent des versions numériques de leurs actes de naissance, permis de conduire ou passeports avec toutes les organisations qui ont besoin de les identifier; cela ne ferait qu'accroître la probabilité de vol d'identité et les conséquences qui s'ensuivent puisque ces documents de base (ou leurs codes d'identification uniques) sont transmis, puis sauvegardés maintes fois par de nombreuses parties.

La sécurité devrait plutôt être assurée par l'abstraction de données, en remplaçant les identifiants privés uniques de chaque personne (comme un numéro de permis de conduire) par des identifiants publics uniques qui prouvent son identité sans rien révéler des documents de base qu'elle possède. Ce processus peut être mis en œuvre par la « création de jetons », une méthode que nous utilisons tous les jours pour sécuriser les transactions effectuées sans fil sur les appareils mobiles : le numéro de compte personnel réel d'un utilisateur est converti en jeton, c'est-à-dire qu'il est remplacé par un numéro de compte généré de façon aléatoire qu'un marchand peut utiliser pour recevoir le paiement de son institution financière, mais qui n'a aucune valeur pour un pirate informatique qui intercepterait les données de cette transaction. De même, un particulier devrait pouvoir s'inscrire à un service ou prouver son identité afin de conclure une transaction en utilisant un identifiant lié à un jeton qui serait traité comme s'il s'agissait des documents de base de cette personne, sans l'exposer à un vol d'identité.

Travailler avec des normes

Afin d'assurer l'adoption généralisée d'un cadre d'identité numérique, et son interaction avec les cadres d'identité d'autres territoires, celui-ci devra être compatible avec les normes élaborées conjointement par le secteur et les gouvernements, comme celles établies par l'Organisation de l'aviation civile internationale pour les dispositifs et les puces d'identification des voyageurs ou, dans une perspective plus large, le Pan-Canadian Trust Framework* (cadre de confiance canadien), que nous avons aidé à développer en collaboration avec le Digital ID & Authentication Council of Canada et ses autres membres. De cette façon, les normes font en sorte non seulement que le cadre soit considéré comme étant commun à tous, mais aussi qu'il soit développé pour être une solution complète au problème de l'identité et de l'authentification, d'un bout à l'autre du processus. De plus, en définissant un ensemble d'exigences obligatoires pour un système donné, les normes permettent l'innovation en incitant les divers acteurs à concevoir de nouvelles fonctionnalités; un cadre qui peut être utilisé par tous signifie que de nouvelles offres conçues pour ce cadre peuvent également être utilisées (et possiblement achetées) par tous.

* Consultez le site *https://diacc.ca/pan-canadian-trust-framework/* (en anglais)

Ouverture

Tout comme des normes sont nécessaires pour assurer l'adoption généralisée et favoriser l'innovation, un système qui fonctionne bien devra être ouvert, c'est-à-dire permettre aux entrepreneurs et aux fournisseurs établis de créer de nouvelles fonctions et fonctionnalités pour les particuliers, les entreprises et les gouvernements en sachant qu'ils pourront intégrer leurs offres de manière transparente au cadre d'identification et d'authentification national. Parce que, bien que les normes soient essentielles pour qu'un système puisse satisfaire à ses principales exigences, c'est son ouverture qui permet à la concurrence et à l'innovation de construire sur cette base, de s'adapter à un marché en constante évolution et de découvrir toutes ses possibilités.

Une solution prend forme

Nous croyons qu'une solution d'identité numérique et d'authentification sécuritaire et pratique, fondée sur les principes ci-dessus, est déjà à notre portée. Elle aura trois fonctions essentielles :

1 Création d'une identité numérique de base et des pièces à l'appui

À la naissance ou dans le cadre du processus d'acquisition de la citoyenneté ou d'immigration, les gouvernements continueront de recueillir les principales caractéristiques personnelles et démographiques d'un utilisateur et créeront un dossier numérique sécurisé faisant autorité pour ce qui est de l'identité aux niveaux de base (p. ex., acte de naissance, certificat de citoyenneté).

Des justificatifs d'identité liés à des jetons correspondant au dossier initial faisant autorité seront ensuite émis à l'utilisateur par un fournisseur de service de jetons pour l'utilisation courante aux niveaux de soutien (p. ex., permis de conduire, passeport, carte santé et identifiants bancaires).

2 Ajout de caractéristiques contextuelles et comportementales

Des entités des secteurs public et privé pourront recueillir les caractéristiques des utilisateurs liées à des contextes ou à des comportements précis selon le besoin opérationnel, tandis que des partenaires du secteur privé pourront regrouper ces caractéristiques, puis gérer l'échange de caractéristiques ainsi que les autorisations accordées aux utilisateurs par leurs services seulement en obtenant le consentement exprès de l'utilisateur. Ce principe est essentiel pour garantir que les renseignements personnels sont protégés en tout temps.

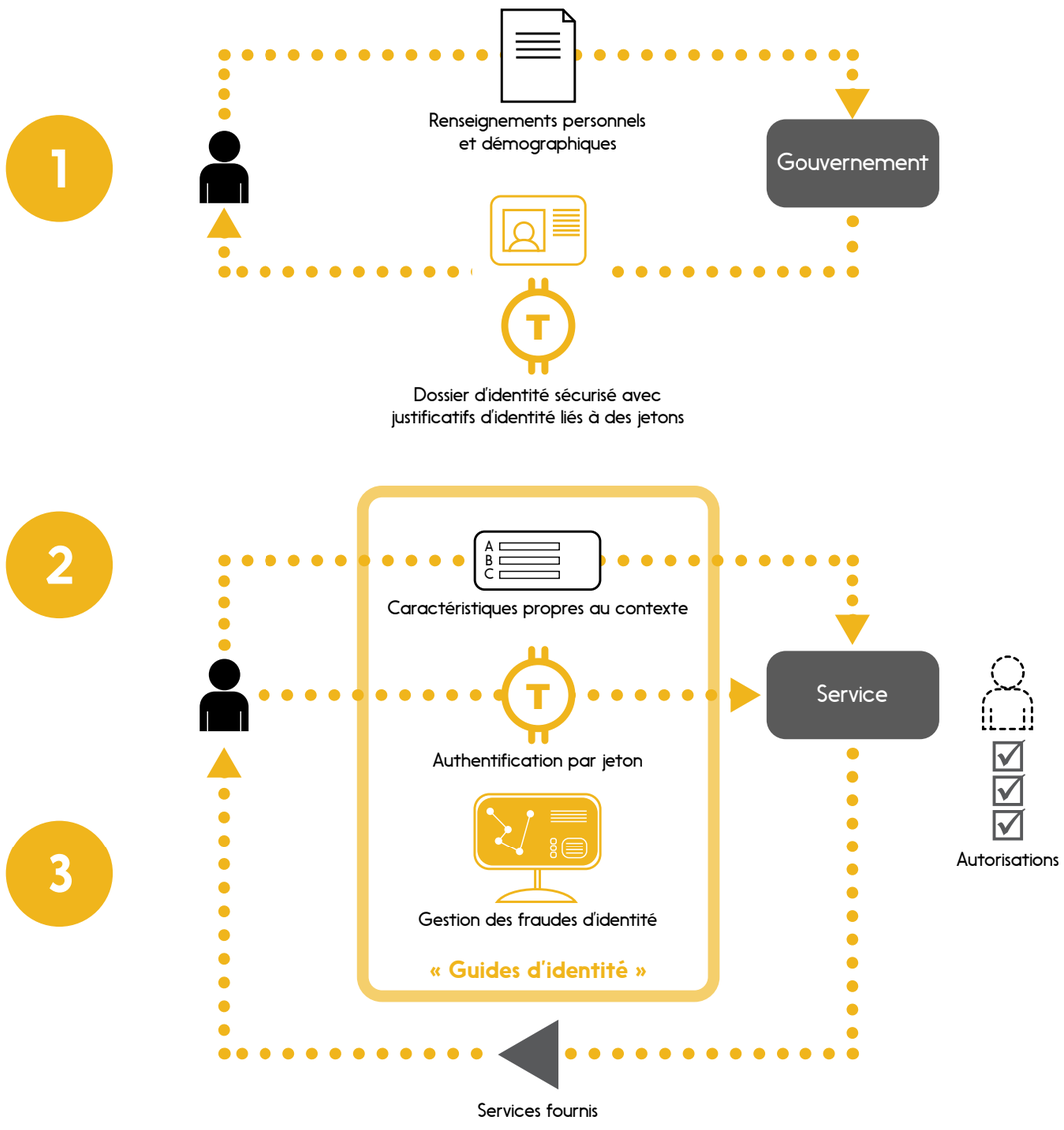
Les parties utilisatrices s'en remettront à la combinaison de justificatifs d'identité liés à des jetons et/ou de caractéristiques approuvée par l'utilisateur pour un service donné. Cette activité s'effectuera par allers et retours entre les utilisateurs et les services sur un ensemble de « guides d'identité » sécurisé, dont l'exploitant fournira également des services tels que des indices de certitude de l'identité et la surveillance et la gestion du risque de fraude d'identité.

3 Authentification et utilisation des identités numériques

L'exploitant des « guides d'identité » authentifiera les utilisateurs pour le compte des fournisseurs d'identité, permettant ainsi des interactions et des transactions numériques sécurisées et dignes de confiance. Les caractéristiques d'identité seront vérifiées au besoin pour un niveau d'assurance donné par les fournisseurs d'identité eux-mêmes, tandis que d'autres partenaires du secteur privé fourniront des produits et des services – comme les données biométriques et l'authentification de documents – qui accroîtront la sécurité.

Fonctions d'un système d'identité et d'authentification

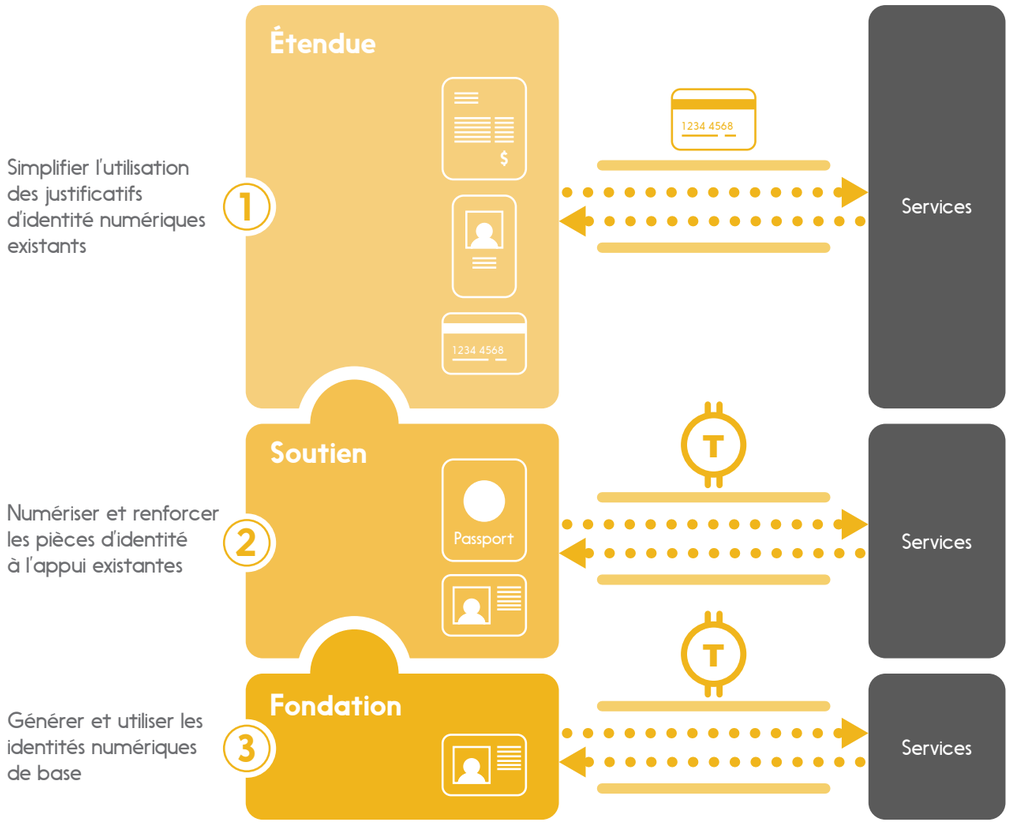
1. Création d'une identité numérique de base et des pièces à l'appui
2. Ajout de caractéristiques contextuelles et comportementales
3. Authentification et utilisation des identités numériques



Bien entendu, la solution complète n'apparaîtra pas du jour au lendemain. Sauf que, en ayant le cadre de confiance canadien pour assise, lequel, rappelons-le, a été développé en collaboration, la migration peut se faire au moyen d'une approche par étapes : d'abord la simplification des processus pour utiliser les identités numériques existantes (comme celles que plusieurs personnes conservent avec leurs institutions financières aujourd'hui), puis la numérisation et le renforcement des pièces d'identité à l'appui existantes (comme des justificatifs d'identité numériques basés sur le permis de conduire) et enfin l'élaboration et l'utilisation d'identités numériques de base (p. ex., un acte de naissance numérique lié à un jeton) pour faciliter et sécuriser les interactions quotidiennes de toute une économie numérique. Et nous entendons jouer un rôle de chef de file dans cette migration.

Migration vers une nouvelle solution d'identité

Le développement par étapes d'une solution permettra aux utilisateurs d'accéder aux services sécurisés publics et privés qu'ils désirent, avec encore plus de sécurité et de commodité.



« Nous croyons qu'une solution d'identité numérique et d'authentification sécuritaire et pratique, fondée sur les principes ci-dessus, est déjà à notre portée. »

Pour en savoir plus sur ce sujet, visitez le site innovation.interac.ca

Publication : Septembre 2017