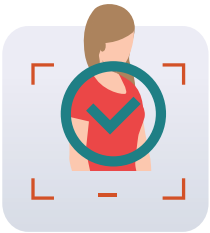
CCIAN

La pertinence des réseaux d'identité en bref

Pourquoi les réseaux d'identité sont importants?

L'identité tient une place importante dans la vie de tous les jours, qu'il s'agisse d'ouvrir un nouveau compte, de prouver son âge ou de voyager à l'étranger.



Aujourd'hui, l'identité est souvent fragmentée; les clients doivent avoir des relations distinctes avec chacune des organisations avec qui ils traitent, lesquelles ont toutes leur propre version électronique (et très probablement différente) du client. Cela crée énormément de friction et de risque. Sans identité numérique fiable et portable, les consommateurs, les gouvernements et les entreprises auront un sérieux manque de confiance dans les interactions en ligne, ce qui empêchera tout le monde de tirer pleinement parti du potentiel des services numériques.

Les réseaux d'identité numérique sont une façon de s'attaquer à ces problèmes, car ils donneront aux personnes plus de contrôle sur leurs données personnelles, permettront aux identités numériques d'être portables, aideront à déceler et à réduire la fraude, et fourniront des mécanismes pour s'assurer que les données sur l'identité sont à jour. Ils créeront des environnements collaboratifs où les besoins de toutes les parties prenantes (pas seulement quelques-unes) sont remplis.

À qui s’adressent les réseaux d’identité?

Utilisateurs de réseaux

Sujet
Personne, organisation ou appareil qui se démarque des autres.

Fournisseur
Personne, organisation ou appareil qui a des renseignements sur le sujet, que celui-ci peut souhaiter partager avec des parties utilisatrices.

Partie utilisatrice
Personne, organisation ou appareil qui veut déterminer l’identité du sujet ou avoir certains renseignements le concernant afin de traiter avec lui d’une manière numérique et de pouvoir faire confiance (ou se fier) aux renseignements reçus.

Quelles fonctions les réseaux d’identité soutiennent-ils?

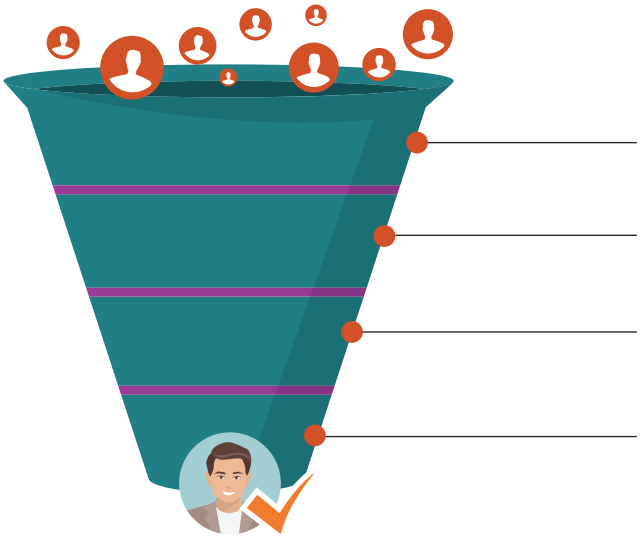
Identification
Processus qui consiste à établir un sujet réel, unique et identifiable.

Authentification
Moyen par lequel un sujet peut affirmer son identité, notamment en montrant qu’il s’agit du sujet déjà vu.

Autorisation
Le fait de donner au sujet le moyen de contrôler les renseignements que les fournisseurs partagent avec les parties utilisatrices. Les renseignements sont divulgués sous la forme d’un justificatif contenant les renseignements (ou « attributs ») partagés avec les métadonnées associées au sujet et décrivent leur provenance.

Comment visualiser les réseaux d’identité?

C’est utile d’utiliser des couches pour décrire les réseaux d’identité. En voici quatre qui aident à comparer d’une manière uniforme les différents aspects des réseaux.



Connexions
Qui est en relation avec qui?

Communications
Comment les parties connectées communiquent-elles?

Justificatifs
Que contiennent les communications entre les parties?

Certifications
Comment les justificatifs sont-ils établis et dans quelle mesure leur faites-vous confiance?

Architectures des réseaux d'identité - Quatre exemples

Ces exemples ne sont pas exhaustifs. Ils visent simplement à illustrer d'une façon générale certaines des approches adoptées afin de montrer que le cadre global peut être appliqué à des solutions ou des mises en œuvre en réseau spécifiques.

Deux types d'interactions

Interactions avec des réseaux d'identité

Interactions entre des parties qui partagent des justificatifs sur le réseau.

Interactions avec des services

Autres interactions pertinentes mais indirectes (p. ex. prestations de services)

Deux types de justificatifs

Justificatifs visibles

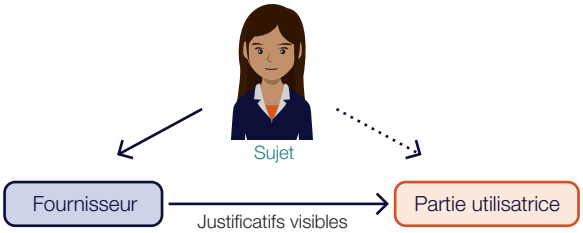
Les parties émettrices et réceptrices peuvent voir le contenu des justificatifs. Les justificatifs sont probablement transmis par une communication sécurisée, mais les parties à chaque extrémité peuvent voir le contenu.

Justificatifs invisibles

Au moins une partie ne peut pas voir le contenu des justificatifs

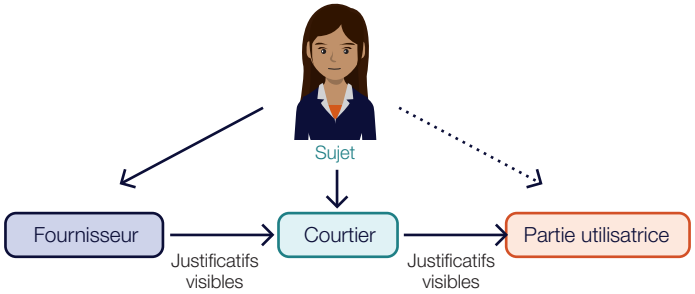
Fédération

La fédération permet à un sujet d'utiliser une identité numérique gérée par une organisation (« fournisseur d'identité ») pour accéder aux services d'une autre organisation (c.-à-d. connexion sociale). Le sujet est en relation avec un seul fournisseur mais peut utiliser plusieurs fournisseurs d'identité, ce qui donne plusieurs identités numériques discrètes.



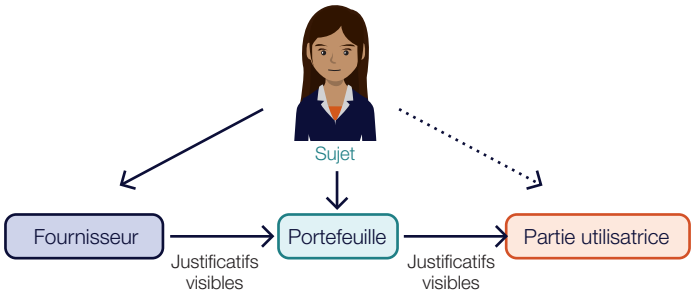
Courtier

Similaire à la fédération, mais avec un « courtier » qui facilite la transmission entre le fournisseur et la ou les parties utilisatrices. Le courtier met le sujet en contact avec le bon fournisseur d'identité. Le sujet est en relation avec un seul fournisseur. Sa portée peut être limitée à l'identification et l'authentification.



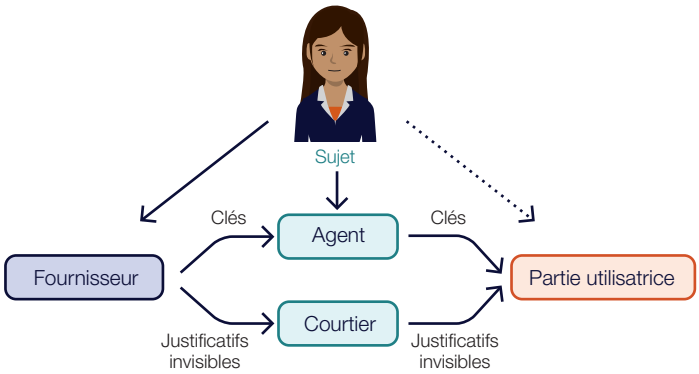
Portefeuille

Le sujet a un portefeuille sécurisé dans lequel il peut entreposer les justificatifs qu'il reçoit des fournisseurs. Lui seul peut voir et contrôler le contenu du portefeuille. Un répertoire ou registre peut aussi être utilisé pour permettre aux parties utilisatrices de vérifier le fournisseur d'un justificatif. L'accent tend à être mis sur le partage de justificatifs (on parle parfois d'échange d'attributs).



Courtier masqué

Similaire à un portefeuille, sauf que le sujet se sert d'un agent utilisateur sécurisé pour contrôler la transmission des justificatifs, et le courtier n'est pas capable de voir les justificatifs transmis. Cela permet aussi au fournisseur et à la partie utilisatrice d'être masqués (c.-à-d. ne pas savoir qui est l'autre partie).



Quelles sont les exigences d'un réseau d'identité?

Gouvernance

Les exigences consistent à établir et appliquer les règles du réseau.

Participation
Il y a des règles précises pour déterminer qui peut être un fournisseur ou une partie utilisatrice, et comment les utilisateurs de réseaux sont vérifiés, les sujets peuvent adhérer et participer, et l'accès pour tous les utilisateurs de réseaux est maintenu à la longue.

Transparence
Elle donne l'assurance que les données personnelles sont traitées en ligne selon les lois qui protègent les données, notamment en obtenant le consentement explicite du sujet. Elle permet de comprendre les processus utilisés pour établir, maintenir et sécuriser des identités numériques.

Responsabilité
Toutes les parties agissent d'une manière responsable tout en remplissant leurs obligations. Quel recours le sujet a-t-il si quelque chose tourne mal? Le fournisseur et la partie utilisatrice ont des arrangements précis en ce qui concerne la responsabilité et l'imputabilité.

Fonctionnement

Les exigences font référence à la mise en œuvre et à l'application des règles du réseau d'identité.

Confidentialité
Elle fait en sort que les justificatifs soient protégés contre une divulgation non autorisée ou inappropriée (c.-à-d. minimisation des données) et partagés uniquement avec un consentement. Elle empêche d'utiliser les justificatifs à des fins de suivi et de surveillance.

Intégrité
Tous les justificatifs sont transmis d'une manière fiable et ne peuvent être altérés d'une façon malveillante. Il faut assurer l'intégrité des données de bout en bout si et quand des justificatifs en sont dérivés. Il doit y avoir des mesures claires pour déceler et prévenir l'activité frauduleuse.

Disponibilité
Les réseaux devraient être conçus de sorte que tous les utilisateurs y aient accès, être disponibles quand c'est nécessaire et s'adresser à tous.

Quels sont les modèles de prestation?

Les réseaux d'identité répondent aux exigences des utilisateurs de réseaux décrites plus haut grâce à une combinaison de confiance et d'agentivité.

Confiance
L'utilisateur de réseau a besoin d'avoir confiance dans le réseau pour s'assurer que ses exigences sont remplies.

Agentivité
L'utilisateur de réseau peut agir d'une façon indépendante et décider librement de la façon dont ses exigences sont remplies.

Tous les réseaux d'identité dépendent d'une combinaison des deux.

Quels facteurs faut-il prendre en compte pour décider de participer ou non à un réseau d'identité?

Secteur

Certains réseaux d'identité sont conçus pour ou dans des secteurs spécifiques (p. ex. gouvernement ou services financiers). Il faut déterminer si le réseau d'identité peut répondre aux besoins de votre secteur.

Portée

Il s'agit du type de transactions pouvant être effectuées entre chaque permutation concevable de personne, d'organisation et d'appareil (p. ex. les appareils branchés ont aussi des identités).

Mode

Les justificatifs seront transférés par les fournisseurs aux parties utilisatrices selon un des modes suivants :

- **En temps réel**
  Actuel; dépend du fournisseur en ligne.
  Il n'y a pas à s'assurer que les justificatifs sont à jour.
- **Entreposage et transfert**
  Plus facile à orchestrer, pas besoin que le fournisseur soit en ligne. Le justificatif est obtenu à l'avance du fournisseur.

Migration de l'identité

Capacité de choisir une organisation différente pour gérer l'identité numérique (y compris les justificatifs).

Interopérabilité

Les réseaux d'identité doivent pouvoir interopérer avec les systèmes dont se servent les utilisateurs du réseau et se conformer de préférence aux normes de l'industrie.

Adoption

Importance d'un réseau d'identité adopté par les sujets, les fournisseurs et les parties utilisatrices.

Gouvernance

Les arrangements en matière de gouvernance sont essentiels pour déterminer comment le réseau est mis en œuvre et quels contrôles sont en place pour qu'il reste sécuritaire et sûr.

Transparence

Plus un système est ouvert au public, plus il est susceptible d'être robuste.

Assurance

Il faut s'assurer que les services sont robustes et vérifiables, notamment les processus pour trouver les attributs, délivrer des justificatifs, se conformer aux normes de sécurité, surveiller et déceler la fraude, et révoquer les justificatifs.

Financement

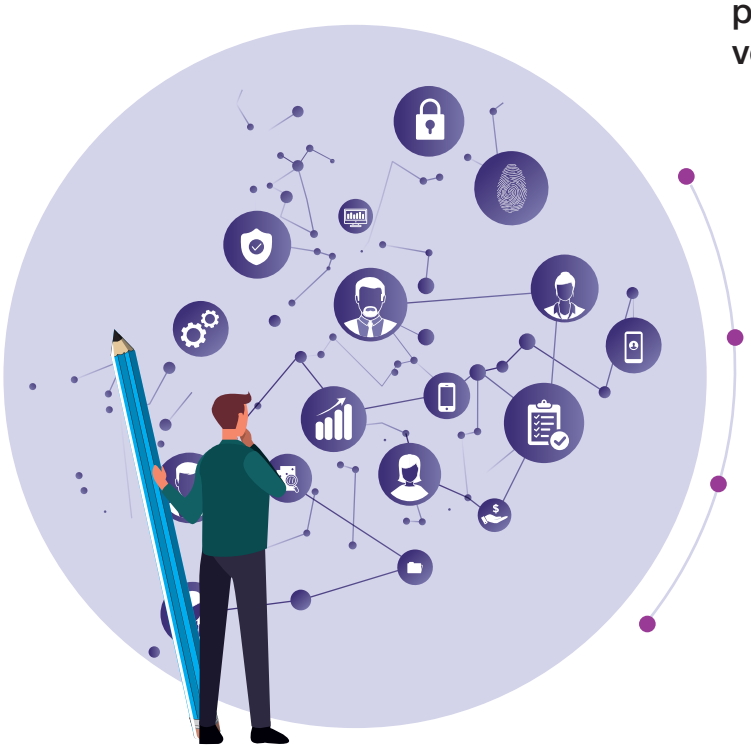
Si le financement du réseau entre en conflit avec les protections qu'il est censé fournir, cela peut soulever des craintes au niveau de la confiance.

Maturité

Le réseau doit être mûr, et pouvoir être testé à l'échelle et atténuer tous les risques qui découlent d'un manque de maturité.

Confidentialité

C'est essentiel que les principes de confidentialité soient respectés; les systèmes sont conçus de la sorte dès la conception. Autres principes importants : choix, protection des données, transparence et responsabilité.



En tant que décideur dans votre organisation, posez-vous ces questions essentielles lorsque vous évaluez un réseau d'identité :

- Est-ce que vous comparez des choses semblables?
- Est-ce que vous vous préparez pour maintenant ou plus tard?
- La mise en œuvre répond-elle à vos besoins spécifiques?
- Quels sont les besoins des utilisateurs du réseau?

Joignez-vous au CCIAN

Faites partie de la communauté qui s'est imposée à l'échelle mondiale grâce aux opportunités économiques et sociales qu'elle procure à tous en bâtissant un écosystème d'identification et d'authentification numériques robuste, sûr et interopérable, qui améliore la confidentialité.

Contact

Conseil canadien de l'identification et de l'authentification numériques

diacc.ca @mydiacc /company/mydiacc /mydiacc