

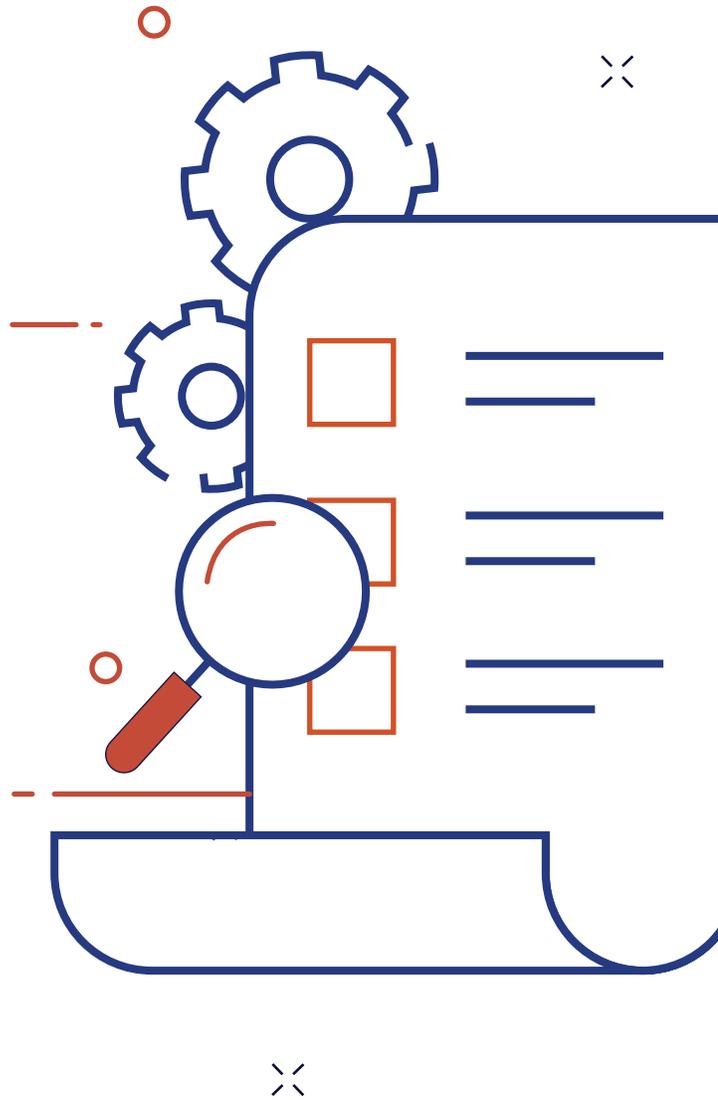


La pertinence des portefeuilles numériques

Lignes directrices pour la conception

Table des matières

Introduction	3
Contexte	3
Qu'est-ce qu'un portefeuille numérique?	4
Pourquoi avons-nous besoin de lignes directrices?	4
Approche adoptée pour l'élaboration des lignes directrices	5
5 lignes directrices essentielles	6
Prochaines étapes	7
Définitions	7
À propos des documents du CCIAN sur l'innovation	8



Introduction

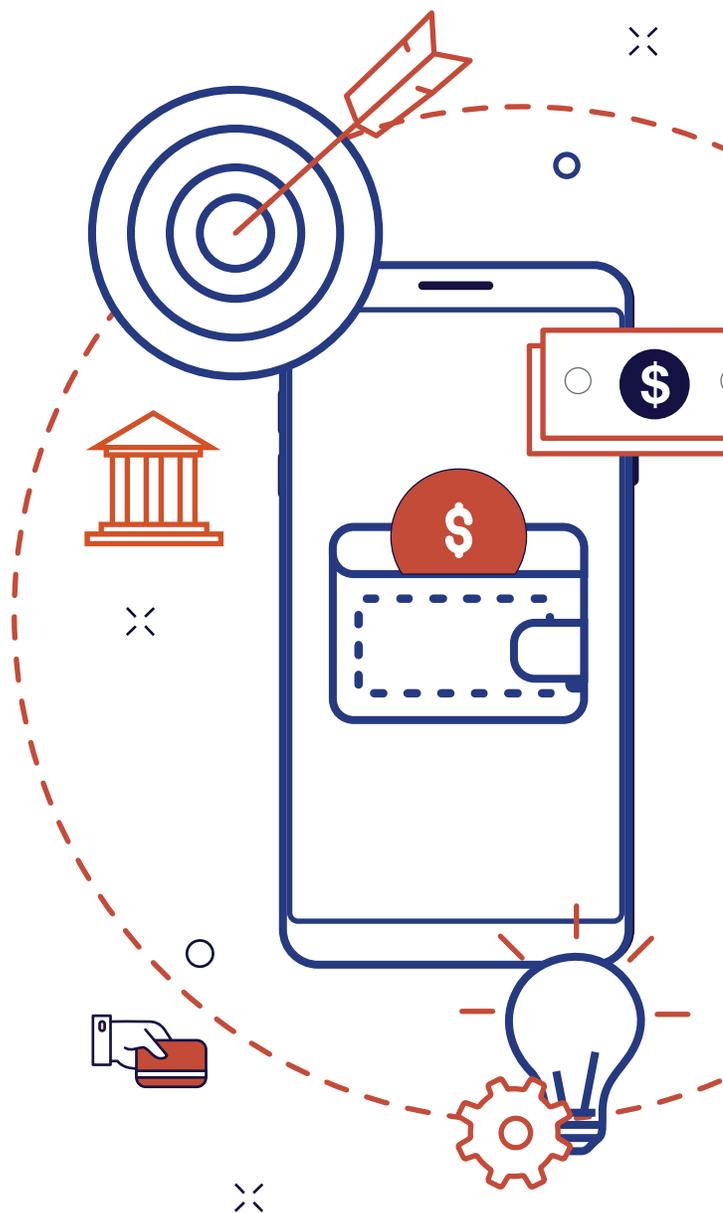
Les progrès récents dans le niveau de perfectionnement des systèmes d'identité numérique redonnent à l'utilisateur le contrôle de ses informations et de sa vie privée. Un élément important de cette avancée est le portefeuille numérique pour les utilisateurs. Ce document présente ce qu'un portefeuille numérique de confiance devrait viser à faire. Sans lui, les développeurs de logiciels sont laissés à eux-mêmes et l'offre du marché sera fragmentée, ce qui retardera ultimement l'adoption d'une solution d'identité numérique centrée sur l'utilisateur.

Contexte

Au cours des 15 dernières années, les gouvernements, les entreprises, les géants des médias sociaux et les compagnies de logiciels ont développé des mécanismes d'identification et d'authentification des utilisateurs afin de fournir à leurs utilisateurs un accès sécurisé aux services électroniques ou numériques. Au cours de cette période, nous avons connu des avancées technologiques en passant de mécanismes simples et faibles employant des codes d'utilisateur et des mots de passe à des techniques d'authentification cryptographique et biométrique fortes, favorisées tout dernièrement par l'adoption quasi universelle des téléphones intelligents.

Nous avons assisté simultanément à l'évolution des solutions d'identité, qui sont passées des systèmes d'authentification à service unique (sur le modèle des solutions conçues pour les systèmes internes des entreprises) à des solutions d'authentification partagée (ou fédérée) utilisant les protocoles Internet standards tels que SAML, OAuth 2.0 et OpenID Connect. De nombreux Canadiens ont l'habitude de se servir de leurs comptes Google et Facebook pour accéder aux services d'autres fournisseurs, ce qui réduit le nombre de codes d'utilisateur et de mots de passe qu'ils doivent gérer. Au Canada, les solutions partagées utilisées par les gouvernements sont notamment l'ouverture de session gouvernementale par Verified.Me (anciennement SecureKey Concierge) adoptée par le gouvernement du Canada, la BC Services Card en Colombie-Britannique et la solution d'identité numérique MyAlberta.

Il y a eu tout dernièrement un développement important des solutions d'identité basées sur la chaîne de blocs qui tirent parti des technologies existantes et promettent d'améliorer l'expérience des utilisateurs, la sécurité, la protection de la vie privée et l'utilité tant pour les fournisseurs de services que pour leurs utilisateurs.



Qu'est-ce qu'un portefeuille numérique?

Un aspect essentiel de ces nouvelles solutions basées sur la chaîne de blocs est la présence d'une application logicielle numérique (parfois appelée agent utilisateur) détenue par l'utilisateur, souvent sur son téléphone intelligent, qui agit comme un conteneur sécurisé pour les informations d'identité de l'utilisateur, fournissant à la fois une solution d'authentification forte et un fournisseur d'informations d'identité vérifiables (ou justificatifs d'identité) aux services qui ont besoin de savoir quelque chose sur un utilisateur. C'est cette application logicielle que plusieurs appellent le « portefeuille numérique ». Un portefeuille permet à l'utilisateur d'accéder à ses informations d'identité et de les contrôler afin de les partager lorsqu'il s'inscrit à un nouveau service ou accède à un service qu'il utilise déjà.

En plus de cette évolution des systèmes d'identité numérique, le secteur des paiements a fait des progrès constants en développant des applications pour téléphones mobiles qui effectuent des transactions sécurisées de paiement sans contact et sur le web. Alors qu'on peut imaginer que les fonctions de paiement et d'identité seront combinées en un seul produit de portefeuille numérique à l'avenir, les présentes lignes directrices portent essentiellement sur la composante identité.

Pourquoi avons-nous besoin de lignes directrices?

Le Conseil canadien de l'identification et de l'authentification numériques (CCIAN) a fait d'excellents progrès pour ce qui est d'élaborer des normes et des pratiques de l'industrie grâce au Cadre de confiance pancanadienMC (CCP). Le CCP décrit les rôles, les services et les exigences visant à assurer l'alignement, l'interopérabilité et la confiance des solutions d'identité numérique, qui sont destinées à fonctionner au-delà des frontières organisationnelles, industrielles et juridictionnelles. Toutefois, le CCP ne traite pas directement des exigences spécifiques pour la mise en œuvre des différentes architectures ou applications de solutions, y compris pour une composante de portefeuille numérique fiable, le cas échéant. Dans cette nouvelle architecture, il est essentiel que le portefeuille numérique soit effectivement digne de confiance et que les Canadiens soient protégés et sachent quels portefeuilles numériques ils peuvent utiliser en toute sécurité. Les fournisseurs de services et les parties dépendantes doivent à leur tour savoir que les informations qu'ils détiennent, envoient et reçoivent sont protégées par des solutions de portefeuille numérique.

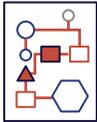
Il est urgent de développer un ensemble de lignes directrices pour souligner le besoin de sécurité, de respect de la vie privée et d'interopérabilité de ces portefeuilles numériques. Sans ces lignes directrices, il y a un grand risque que les fournisseurs de portefeuilles jugent acceptable de sacrifier les sujets de préoccupation visés par les principes au profit de la facilité ou de modèles commerciaux préjudiciables aux détenteurs de portefeuilles. L'absence de ces lignes directrices peut entraîner une fragmentation et une adoption plus lente des réseaux que les portefeuilles soutiennent.

Lors de la réunion du comité d'experts en innovation du CCIAN de juin 2020, le Laboratoire d'identité numérique et d'autres ont proposé, et le CEI a accepté, qu'un groupe de travail élabore un projet de principes relatifs au portefeuille d'identité numérique appelé à être examiné. Il s'agit d'un ensemble de principes durables et de haut niveau pour la sécurité, la protection de la vie privée, l'interopérabilité, l'agencement et d'autres aspects. Ces principes devront être d'un niveau suffisamment élevé pour résister à l'épreuve du temps en soutenant l'innovation et divers modèles commerciaux, mais aussi pour garantir que les besoins des Canadiens, des entreprises canadiennes et du secteur public sont satisfaits. Le groupe de travail a préparé une ébauche de document sur les principes qui vise à compléter ces lignes directrices.

Approche adoptée pour l'élaboration des lignes directrices



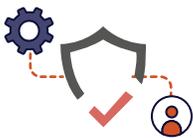
Les lignes directrices se veulent des objectifs ambitieux de haut niveau pour les équipes de développement de logiciels qui conçoivent et construisent des solutions technologiques de portefeuille numérique pour le marché canadien.



Les lignes directrices ne seront pas spécifiques à une technologie ou à un modèle commercial. Le marché numérique comprend plusieurs approches différentes et ces lignes directrices ne devraient pas être intentionnellement préjudiciables à une approche particulière, certaines approches pouvant être plus conformes aux lignes directrices que d'autres.



Les lignes directrices sont destinées à répondre aux intérêts des utilisateurs canadiens, des fournisseurs d'identité (émetteurs), des parties dépendantes (vérificateurs) et des fournisseurs de réseaux.



Les lignes directrices devraient s'appuyer sur les principes du CCP centrés sur l'utilisateur, la confiance, la protection de la vie privée dès la conception et l'intégrité, et s'inspirer de travaux antérieurs tels que [les 7 lois de l'identité](#), [les dix principes de l'identité auto-souveraine](#), [la Charte canadienne du numérique](#), [les principes de l'écosystème de l'identité numérique du CCIAN](#), en utilisant tout particulièrement les travaux du groupe de travail du comité d'experts en innovation du CCIAN.



1

Les portefeuilles devraient avoir une conception centrée sur l'utilisateur

- Travailler dans l'intérêt des utilisateurs
- Soutenir les utilisateurs en cas de problèmes.
- Soutenir les fournisseurs d'identité, les parties dépendantes et les réseaux que les Canadiens veulent et dont ils ont besoin.
- Prouver aux utilisateurs que le portefeuille numérique s'aligne sur ces principes et les normes qui les soutiennent, en tant que marque de confiance reconnue.



2

Les portefeuilles devraient protéger la vie privée de l'utilisateur

- Fournir aux utilisateurs une visibilité et un contrôle sur la divulgation et le stockage des informations d'identité.
- Soutenir les techniques de divulgation minimale des informations sur l'identité.
- Prévenir une éventuelle collusion entre les opérateurs de réseau, les fournisseurs d'identité et les parties dépendantes.
- Fournir une divulgation directe à une partie et empêcher la surveillance par un tiers.

5



Les portefeuilles devraient être accessibles à tous les Canadiens

- Soutenir les normes modernes de l'industrie en matière d'accessibilité.
- Être accessibles à tous les Canadiens, quelle que soit leur capacité financière.
- Fournir une expérience familière, intuitive, simple et informative afin que les utilisateurs puissent faire de bons choix.



4



Les portefeuilles devraient être interopérables

- Utiliser des normes modernes de l'industrie pour l'échange d'informations sur l'identité.
- Soutenir les modèles commerciaux des réseaux en favorisant leurs politiques.

3



Les portefeuilles devraient être sécuritaires

- Fournir aux utilisateurs des informations et des outils pour les aider à gérer, stocker et divulguer des informations d'identité en toute sécurité.
- Identifier et authentifier toutes les parties à une transaction afin que les utilisateurs fassent des choix éclairés.
- Authentifier les utilisateurs en utilisant des méthodes conformes aux normes d'assurance de l'industrie (niveau d'assurance).
- Utiliser les normes de sécurité éprouvées et modernes de l'industrie.
- Utilisez les pratiques exemplaires modernes de l'industrie en matière de développement logiciel.

Prochaines étapes

Ces lignes directrices sont intentionnellement de haut niveau afin de soutenir divers modèles commerciaux et technologies et, espérons-le, de résister également à l'épreuve du temps à mesure que ces modèles et technologies évolueront, ce qu'ils le feront à coup sûr. Mais comme ils sont de haut niveau, les développeurs de logiciels et les organisations qui testent et évaluent les produits auront besoin, pour les mettre en œuvre, de conseils objectifs sous la forme de normes technologiques. Pour cette prochaine étape, le Laboratoire d'identité numérique du Canada propose de collaborer avec les membres du CCIAN et d'autres afin d'élaborer les normes technologiques qui peuvent être utilisées pour s'aligner sur ces lignes directrices.

Un thème commun est ressorti au cours des discussions sur ces lignes directrices, à savoir que des travaux supplémentaires sont nécessaires pour évaluer, mettre à jour et enrichir le CCP avec des lignes directrices similaires qui soutiennent le développement des réseaux, des fournisseurs d'identité et des parties dépendantes dans cette nouvelle architecture.

Definitions

- | | |
|--|--|
| 1. Utilisateur | Personne qui détient un portefeuille numérique, généralement sur son téléphone intelligent. |
| 2. Centré sur l'utilisateur | Système conçu avec les intérêts de l'utilisateur comme principe directeur. |
| 3. Fournisseur d'identité (ou émetteur d'identité) | Service qui envoie des informations d'identité à un portefeuille numérique qui les stocke pour que l'utilisateur puisse en disposer. |
| 4. Partie dépendante (ou vérificateur d'identité) | Service qui reçoit des informations d'identité à partir d'un portefeuille numérique. |
| 5. Réseau | Groupe composé de fournisseurs d'identité et de parties dépendantes, et infrastructure associée qui permet à un portefeuille numérique de recevoir et d'envoyer des informations d'identité en toute sécurité. Le mode de fonctionnement des réseaux est régi par des normes, des politiques et une gouvernance. |
| 6. Divulcation | Transmission d'informations d'identité d'un portefeuille numérique à une partie dépendante. |
| 7. Divulcation directe | Divulcation qui garantit que les informations sur l'identité sont transmises directement d'un portefeuille à une partie dépendante et à aucun autre tiers. |
| 8. Collusion | Processus consistant à lier les informations d'identité de deux ou plusieurs parties dépendantes. |
| 9. Surveillance | Processus d'enregistrement des transactions effectuées entre plusieurs parties dépendantes, fournisseurs d'identité ou un réseau, à l'exclusion du portefeuille numérique lui-même. |

À propos des documents du CCIAN sur l'innovation

Les documents sur l'innovation publiés par le Conseil canadien de l'innovation et de l'authentification numériques (CCIAN) portent sur les enjeux et les débouchés actuels de l'écosystème de l'identité numérique. Ces documents sont guidés par les 10 principes de l'écosystème de l'identification et de l'authentification numériques du CCIAN et par les priorités des membres du CCIAN. Ils fournissent des perspectives sur les auditoires commerciaux, juridiques et techniques au Canada et ailleurs dans le monde. Les documents du CCIAN n'avalisent et ne représentent pas l'opinion d'une organisation compétente du CCIAN. Ils sont pragmatiques et traitent des enjeux du monde réel; ils sont ouverts et transparents; ils envisagent des possibilités futures; ils communiquent les leçons tirées des projets passés; et ils sont rédigés par des experts en la matière qui sont membres du CCIAN et qui connaissent bien le monde réel.

À propos du CCIAN



Fruit du Groupe de travail du gouvernement fédéral sur l'examen du système de paiement, le CCIAN est une coalition sans but lucratif de leaders des secteurs public et privé déterminés à développer un cadre d'identification et d'authentification numériques canadien qui va permettre au Canada de participer pleinement et en toute sécurité à l'économie numérique mondiale.

À propos du Laboratoire d'identité numérique du Canada

Le Laboratoire d'identité numérique du Canada est une entité indépendante sans but lucratif ayant pour vocation d'accélérer l'adoption de solutions d'identité numérique centrées sur les utilisateurs en encourageant la conformité et l'interopérabilité techniques. Le Laboratoire n'est pas un incubateur, et il ne développe et ne vend pas des solutions d'identité numérique. Le Laboratoire, dont le siège social est situé à Gatineau, a été créé en février 2020 avec le soutien du Conseil canadien de l'identification et de l'authentification numériques (<https://diacc.ca>) et de In-Sec-M (<https://insecm.ca>). Pour plus de renseignements, visitez www.digidlab.ca.

Rejoignez-vous au CCIAN

Faites partie de la communauté la plus importante du monde qui ouvre des possibilités économiques et sociales pour tous en bâtissant un écosystème d'identification et d'authentification numériques robuste, sécuritaire, interopérable et plus respectueux de la vie privée.

Contact

Conseil canadien de l'identification et l'authentification numériques

 diacc.ca

 [@mydiacc](https://twitter.com/mydiacc)

 [/company/mydiacc](https://www.linkedin.com/company/mydiacc)

 [/mydiacc](https://www.facebook.com/mydiacc)

