CCIAN

Trousse du gouvernement de la Colombie-Britannique pour les émetteurs de justificatifs vérifiables

Rapport sur la validation de principe

Table des matières

1. À propos du CCIAN 2
2. À propos de l’auteur 2
3. Résumé 3
4. Introduction 3
5. Source d’inspiration de la validation de principe 3
6. Ce qui a été construit 4
7. Réponse de l'industrie 5
8. Principales leçons 9
9. Recommandations 10
10. Conclusion 12
11. Annexe A – Fournisseurs participants 13

À propos du CCIAN

Le Conseil canadien de l'identification et de l'authentification numériques **(**CCIAN**),** qui est le fruit du groupe de travail du gouvernement fédéral chargé d'examiner le système de paiements, est une coalition sans but lucratif de chefs de file des secteurs public et privé déterminés à élaborer un cadre canadien d'identification et d'authentification numériques qui permettra au Canada de participer pleinement et en toute sécurité à l'économie numérique mondiale.

Les rapports du CCIAN traitant des innovations mettent l'accent sur les enjeux et les débouchés actuels de l'écosystème de l'identité numérique. Ils 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. Ces rapports fournissent des perspectives à des auditoires commerciaux, juridiques et techniques au Canada et ailleurs dans le monde. Ils ne sont pas avalisés et ne représentent pas l'opinion d'une organisation compétente du CCIAN. Les rapports du CCIAN portant sur des innovations sont pragmatiques et traitent d'enjeux réels; ils sont ouverts et transparents; ils envisagent des possibilités futures; ils communiquent les leçons retenues de projets antérieurs; et ils sont rédigés par des experts dans le domaine qui sont membres du CCIAN et ont une expertise du monde réel.

À propos de l'auteur

Dave McKay est le coprésident du Comité d'experts en innovation du CCIAN. Il est un architecte de l'identité chez Northern Block spécialisé dans les systèmes décentralisés, professeur au programme de développement de chaînes de blocs au George Brown College, responsable technique du laboratoire de recherche sur la cybersécurité de l'Université Ryerson et directeur général du Canadian Credential Network. Dave a collaboré à la réponse de Northern Block à l'invitation adressée au secteur privé pour participer à ce projet.

Résumé

La validation de principe du CCIAN à l'aide du projet de trousse de la Colombie-Britannique (C.-B.) pour les émetteurs de justificatifs vérifiables a démontré une base de codes sources ouverts comme outil pour soutenir l'adoption d'une identité décentralisée au gouvernement et dans l'industrie partout au Canada et à l'échelle internationale. Les notions abordées dans cette validation de principe ont montré la viabilité actuelle de l'utilisation de l'identité auto-souveraine (IAS) comme moyen de délivrer des documents authentifiés par le gouvernement. L'approche ouverte adoptée par la C.-B. pour cette validation de principe a amené l'industrie à s'impliquer dans le projet.

Introduction

Ce rapport vise à présenter les vecteurs du projet, ce que la validation de principe a démontré, l'expérience et l'apprentissage des participants, et la façon dont les gouvernements pourraient procéder pour instaurer l'identité numérique dans leurs propres programmes. Il utilise une approche narrative pour résumer les résultats de cette validation de principe. Ce rapport fournit des perspectives stratégiques et opérationnelles à propos des résultats de cette validation de principe pour d'autres entités gouvernementales désireuses de bâtir une validation de principe ou un système de production à l'aide de l'IAS. Le rapport a été rédigé à partir d'une série d'entrevues avec des personnes qui ont pris part à l'initiative. Les personnes interrogées comprenaient notamment des fonctionnaires, des fournisseurs ayant accepté de collaborer et des observateurs provenant de l'industrie de la gestion de l'identité.

Source d'inspiration de la validation de principe

Aux États-Unis (É.-U.), le Department of Homeland Security a collaboré avec des fournisseurs pour trouver et mettre en place des réseaux qui suivaient un modèle IAS. La plupart des modèles IAS incluent la notion de portefeuille mobile, d'agent en nuage et de réseau. La recherche et la mise en œuvre initiales ont permis de présenter des justificatifs vérifiables et des identifiants décentralisés à l'aide de normes W3C. Ces travaux ont mis à jour une méthode éventuelle pour en finir avec le problème que pose la centralisation de l'authentification.

La trousse pour les émetteurs de justificatifs vérifiables est une trousse à code source ouvert que le gouvernement de la C.-B. a créé afin de fournir aux gouvernements et autres parties intéressées un outil pour commencer à délivrer des documents officiels qui font autorité. Elle visait à :

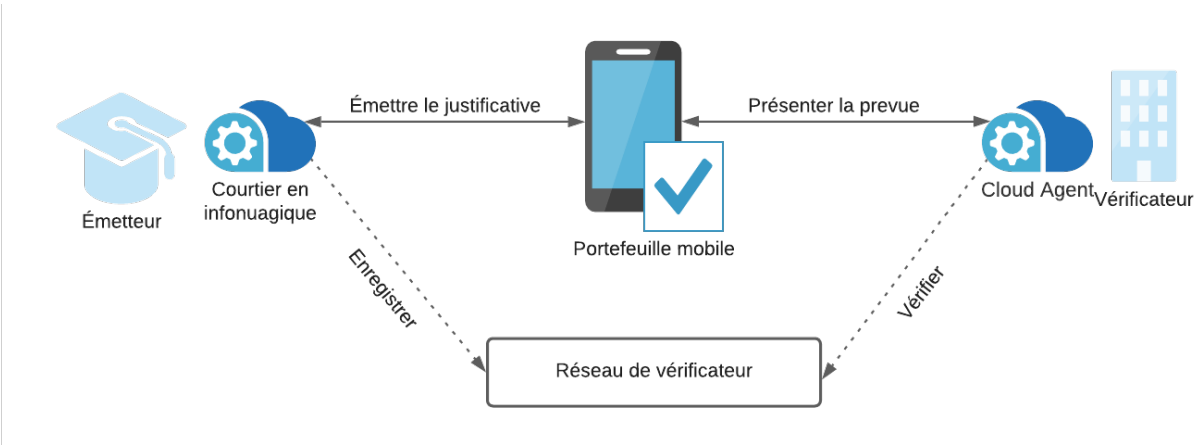
- montrer l'utilité potentielle de la technologie,
- présenter un mécanisme permettant aux résidents d'avoir accès à des données du secteur public faisant autorité à l'aide d'une technologie qui est interopérable dans le monde entier,
- démontrer l'engagement du gouvernement de la C.-B. à résoudre les enjeux connexes,

- obtenir qu'au moins deux fournisseurs acceptent de développer des portefeuilles qui pourraient utiliser les justificatifs émis.

Ce qui a été construit

La validation de principe de la trousse pour les émetteurs de justificatifs vérifiables a donné comme résultat un conteneur de démonstration qui pourrait être installé par des organisations de confiance pour utiliser le service avec leurs propres systèmes ou pour se connecter à un réseau soutenu par le gouvernement de la C.-B. L'approche basée sur les réseaux présentait l'avantage que des organisations de confiance pourraient utiliser des éléments des systèmes IAS de fournisseurs existants pour faire connaître les services que le gouvernement de la C.-B. était en train de développer.

La trousse pour les émetteurs de justificatifs vérifiables couvrait une série de technologies qui peuvent être développées pour émettre un justificatif de personne vérifiée délivré par le gouvernement. Elle a consisté à créer un profil d'utilisateur puis à inviter cet utilisateur par courriel à se connecter et à recevoir son justificatif. Le système était basé sur l'Aries Cloud Agent for Python (ACA-py) que le gouvernement de la C.-B. a aidé à développer. La trousse pour les utilisateurs de justificatifs vérifiables a utilisé diverses technologies émergentes afin que ce soit plus facile pour les participants de bâtir un environnement d'essai et de commencer à émettre leur propre version des justificatifs. Le gouvernement de la C.-B. a étendu le projet pour ajouter d'autres validations de principe en ce qui concerne la façon dont le justificatif de la personne vérifiée pourrait être utilisé avec d'autres systèmes gouvernementaux.



L'approche utilisée pour développer cette validation de principe a été unique. La validation de principe a été menée d'une manière ouverte et transparente en utilisant la bonne gouvernance neutre du CCIAN, au lieu d'élaborer un processus de demandes de propositions propre au secteur public. Il s'agissait dès le départ d'en faire un projet de développement ouvert. Tous les codes ont été développés pour être utilisés avec une licence de code source ouvert et étaient accessibles à partir de Github. Une partie du développement a été financée par des primes grâce au programme BC Code With Us. Des développeurs et des organismes de

développement extérieurs au CCIAN et au gouvernement de la C.-B. ont été invités à prendre part au développement ou à suivre les progrès.

Il s'agissait du premier projet ouvert visant à démontrer l'utilisation des composantes d'un système IAS pour utiliser le triangle de confiance avec un justificatif émis par le gouvernement canadien. Une personne pourrait ainsi se connecter, recevoir un justificatif et le présenter à un autre système de confiance. La mise en place d'un système basé sur un code source ouvert a permis à d'autres parties d'apprendre et de traiter la validation de principe de la trousse pour les émetteurs de justificatifs vérifiables comme un modèle de référence pour bâtir leurs propres systèmes. Un certain nombre de fournisseurs ayant participé à cette validation de principe se sont montrés reconnaissants d'avoir au accès à la trousse pour les émetteurs de justificatifs vérifiables à code source ouvert.

Une fois la validation de principe en place et fonctionnelle, les fournisseurs utilisant le même code de base ont disposé d'un bac à sable d'interopérabilité pouvant servir à imiter la réponse d'un véritable système pour émetteurs de justificatifs vérifiables.

Réponse de l'industrie

Bon nombre des sujets interviewés pour les besoins de ce rapport ont indiqué que la participation à cette validation de principe avait été instructive et révélatrice. Elle les a aidés à mieux comprendre les répercussions et la proposition de valeur que la technologie explorée dans la validation de principe pourrait avoir sur le marché. La validation de principe a démontré les possibilités d'interopérabilité quand les participants tirent parti d'une infrastructure technologique convenue.

L'utilisation de la technologie explorée représente un nouveau paradigme. Il y a eu des défis pour communiquer l'intention de la validation de principe, la façon dont les entreprises pourraient interagir avec et leur raison de le faire. Les fournisseurs ont tout d'abord pris du temps à réagir, mais la communauté de partage d'information basée sur les connaissances facilitée par le CCIAN a été déterminante pour obtenir davantage de réponses. La validation de principe a été développée à partir d'une série de téléconférences régulières organisées par le CCIAN et auxquelles les parties intéressées pouvaient participer. En automne 2020, la réponse à la trousse pour les émetteurs de justificatifs vérifiables a été confirmée et les participants actifs qui partageaient leurs expériences ont pris part à des réunions. Comme une entité gouvernementale était derrière cela et l'utilisait dans un environnement ouvert, la validation de principe a permis d'attirer des fournisseurs; mais elle a encore fait ressortir les défis constants que pose le besoin de définir des modèles commerciaux appropriés pouvant être mis à profit.

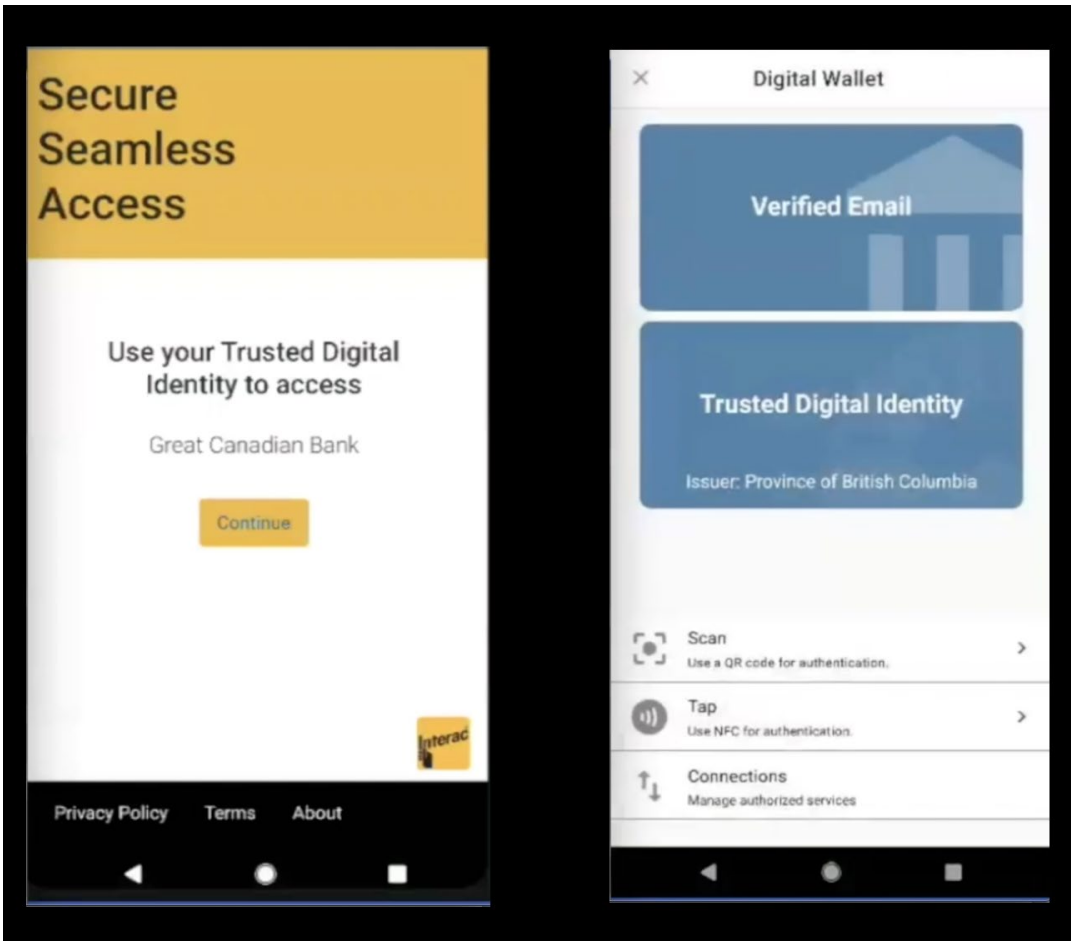
Les fournisseurs suivants ont répondu avec des systèmes qui fonctionnent :

- Northern Block
- Interac/2Keys
- Yoti

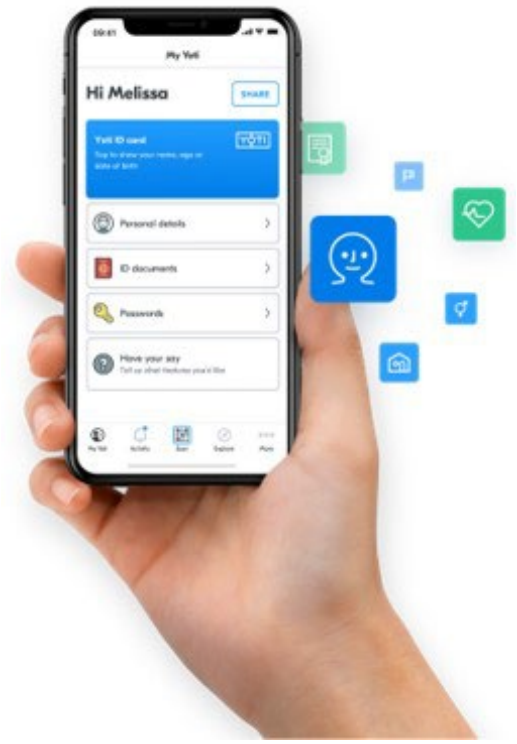
- Applied Recognition
- Vlinder

Chacun de ces fournisseurs a présenté un portefeuille numérique mobile comme validation de principe ou comme version alpha d'une application commercialement exploitable. L'annexe A fournit plus de renseignements sur chaque fournisseur et un lien vers un référentiel de vidéos de chaque système démontré.

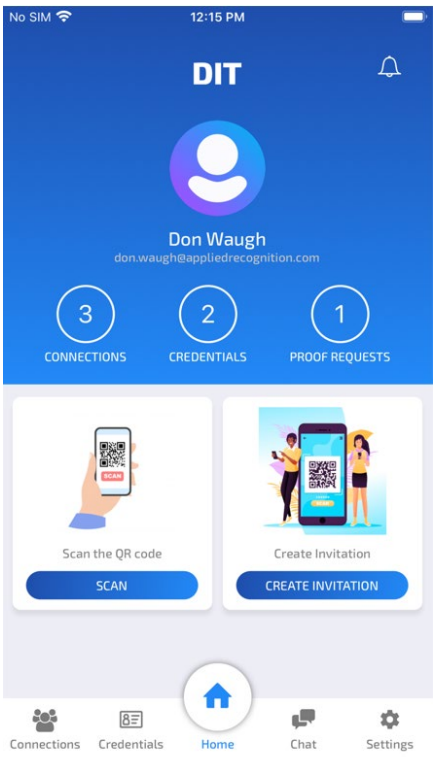
Portefeuille NB Orbit de Northern Block



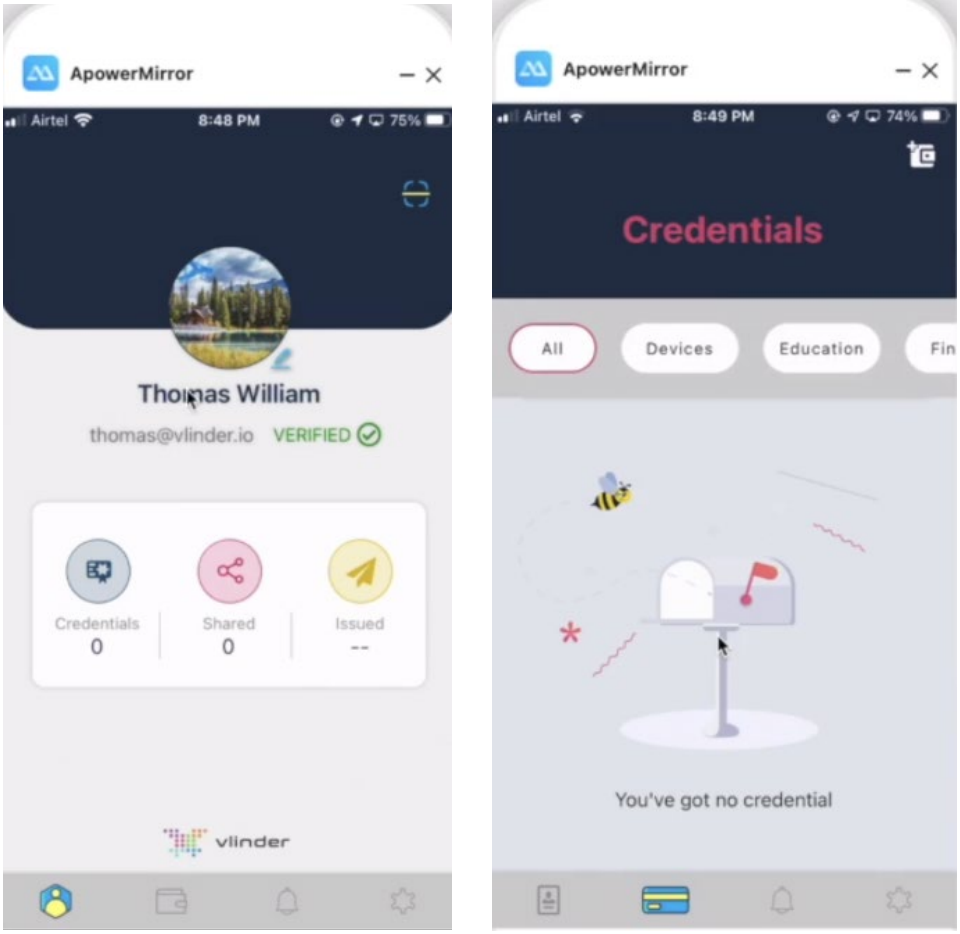
Portefeuille Interac-2Keys



Portefeuille Yoti



Portefeuille Applied Recognition DIT



Portefeuille Vlinder Klefki

Principales leçons

L'équipe du gouvernement de la C.-B. a surtout retenu que la participation et la collaboration ouvertes avec le secteur privé peuvent s'avérer très payantes. Elle a aussi appris à donner aux parties extérieures le temps de se mettre à niveau et d'assimiler l'information qui leur était présentée. Dans ce genre de projet, au lieu de créer d'emblée une énorme demande de propositions, le système peut être bâti en utilisant une approche itérative agile qui nécessite un développement technique une fois identifié. Elle a aussi découvert que certaines organisations de confiance jugeront les choses en fonction de l'apparence de l'interface utilisateur plutôt que de son utilité sous-jacente. Certains répondants potentiels ont été rebutés par les interfaces rudimentaires et le manque de procédure de configuration soignée. Étant donné ce qui a été construit et la réponse, ce sera important à l'avenir que les systèmes IAS soient conçus en fonction des personnes.

L'équipe de la C.-B. a réussi à savoir ce qui peut amener les entreprises à adopter cette technologie. La démonstration d'une maquette de justificatif émis par le gouvernement a été décisive. Pour les participants du secteur privé, c'était une façon de rompre avec le dilemme

inextricable d'un système décentralisé - « si personne n'a de justificatifs à émettre, pourquoi créer alors un portefeuille pour les entreposer? ». Selon eux, si le gouvernement intervient, l'effort en vaut la peine. La validation de principe a bénéficié du cas d'utilisation qu'elle a traité. Le processus selon lequel le gouvernement émet un justificatif à un citoyen qui peut ensuite le faire vérifier par une autre partie (possiblement le secteur privé) a donné des idées aux entreprises impliquées dans la réponse.

Les fournisseurs ont appris ce qu'implique la promotion de leurs offres IAS et comment s'assurer qu'elles sont interopérables. En voyant les systèmes de référence du gouvernement, ils ont été capables de prendre leurs propres décisions architecturales tenant compte des systèmes ouverts fonctionnels existants.

Recommandations

Compte tenu de l'expérience tirée de ce projet, les participants ont quelques recommandations pour d'autres projets du gouvernement et du secteur privé dans la sphère de l'identité décentralisée.

Il n'y a rien comme la collaboration ouverte

Tenez le public au courant des projets que vous entreprenez. Consultez les entreprises publiques et privées, et tenez compte de leur avis. Collaborez à des initiatives à code source ouvert.

Ne restez pas en vase clos, soyez interopérables et fixez-vous une cible d'envergure internationale

À défaut d'une collaboration variée, les solutions seront compartimentées. Les entités devraient déborder de leur région et de leur pays pour s'assurer que les solutions fonctionneront à une échelle internationale.

Les projets ouverts sont une source de motivation pour toutes les parties impliquées

La collaboration favorise des contacts qui peuvent donner un meilleur résultat pour votre projet. L'industrie privée sera ravie d'être écoutée et d'aider à accomplir des tâches.

Trouvez des façons de procéder qui tiennent compte de la dynamique du marché

L'industrie privée doit être agile et tenir compte de ce que le marché veut. Les projets gouvernementaux doivent prendre en considération et cibler des secteurs où ils peuvent soutenir et promouvoir l'innovation, en plus de délivrer des justificatifs qui peuvent servir à améliorer la sécurité et la fiabilité des transactions commerciales.

L’industrie détermine la viabilité et la durabilité commerciales

Les répondants de l’industrie ont désigné les portefeuilles comme composante unique dans un système plus vaste d’émission et de vérification des justificatifs. Le portefeuille semble être durable dans le contexte d’un système plus vaste. Les innovations apportées à l’émission et à la vérification peuvent entraîner des changements dans les opérations liées aux portefeuilles. Le marché des idées est un vecteur essentiel d’innovations qui déterminent les caractéristiques des portefeuilles.

Voici des ressources qui peuvent influencer le choix des portefeuilles dans l’écosystème :

- Une feuille de route précisant quand et comment les justificatifs vérifiables émis par le secteur public deviendraient disponibles.
- Les caractéristiques et fonctionnalités qu’un portefeuille doit comporter pour que le secteur public lui fasse confiance.
- La démonstration de la conformité du cadre de confiance pancanadien, par exemple au moyen du programme de marque de confiance Voilà Vérifié du CCIAN.

La force du gouvernement pour ce qui est d’émettre des justificatifs

La conformité à la loi est essentielle pour avoir un environnement transactionnel qui fonctionne et est stable. Les gouvernements sont des émetteurs naturels de justificatifs vérifiables lisibles à la machine qui représentent des preuves faisant autorité permettant aux entreprises de se conformer aux exigences réglementaires et aux pratiques commerciales.

Le gouvernement peut encourager l’innovation en apportant son soutien

Les gouvernements peuvent jouer un rôle considérable en soutenant l’adoption. Ils doivent participer à des alliances pour guider les normes techniques et la gouvernance des politiques, et investir dans des projets qui s’alignent sur les priorités gouvernementales.

Des systèmes toujours interopérables

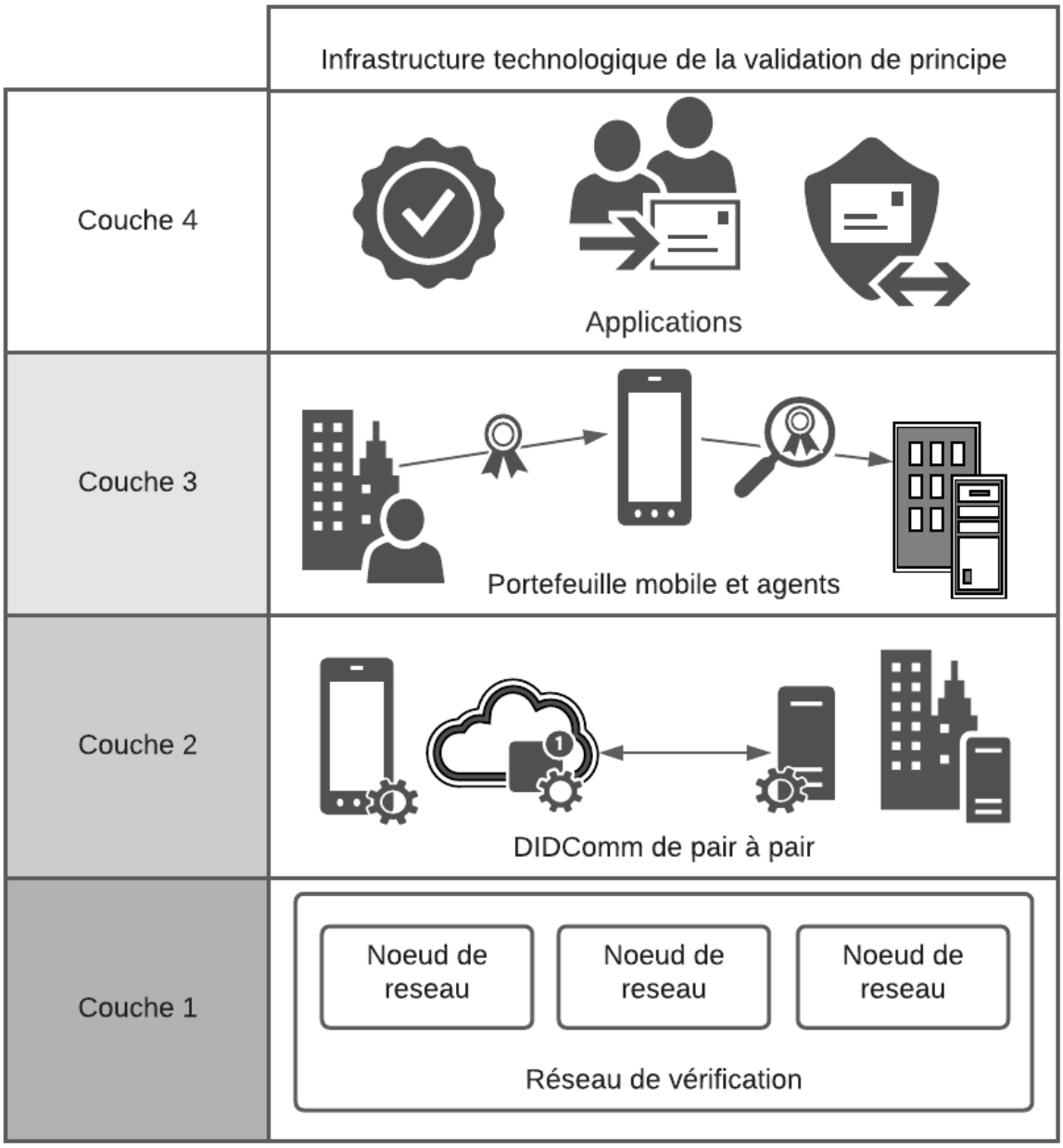
Il faut tout faire pour s’assurer que les systèmes locaux peuvent fonctionner avec ceux d’autres régions et avec l’industrie privée. En plus d’offrir moins de valeur, les systèmes qui ne sont pas interopérables peuvent être ignorés et considérés comme une perte de ressources.

Impliquez-vous dans la gouvernance des réseaux et des registres

Les parties intéressées par le vaste écosystème de l’identité numérique qui utilise l’identité auto-souveraine devraient envisager de participer et de contribuer aux efforts pour bâtir et exploiter ces systèmes et leur gouvernance continue.

1. La gouvernance par couches des services publics nécessite des organisations de confiance destinées à être des intendants et des piliers de confiance pour exploiter le réseau dans un environnement distribué.

2. La couche de gouvernance du fournisseur peut utiliser l'apport des gouvernements pour aider à établir des normes pour le transport et les représentations des justificatifs, et la sélection des signatures cryptographiques à utiliser.
3. Le cadre de gouvernance des justificatifs exige une gouvernance qui établit une conformité en ce qui concerne la confidentialité et la sécurité des justificatifs et des connexions que possèdent les titulaires et les organisations de confiance.
4. Les gouvernements peuvent jouer un très grand rôle dans les cadres de gouvernance des écosystèmes en devenant des registraires de confiance pour les registres fiables des schémas de justificatifs standards et les registres vérifiés des institutions gouvernementales, universitaires, financières et de bienfaisance connues.



Des changements aux lois pourraient être nécessaires pour favoriser les identités numériques et les justificatifs vérifiables

Les gouvernements devraient examiner les lois qui n'accordent pas « la priorité aux personnes et au numérique » afin de favoriser des identités et des justificatifs numériques. La législation qui exige des signatures en personne, des documents papier ou des notaires devrait être revue afin de voir si cette nouvelle technologie peut simplifier ces processus et devenir conforme.

Conclusion

Ce projet a cherché à tester la viabilité de l'adoption des justificatifs vérifiables et de leur interopérabilité dans les secteurs public et privé au Canada. La nature ouverte de ce projet a permis de mener diverses initiatives publiques et privées afin d'obtenir des perspectives stratégiques et opérationnelles de l'interopérabilité grâce à la collaboration. Il existe de nombreuses initiatives privées et à codes sources ouverts. L'annexe A fournit une liste de projets qui ont servi d'inspiration ou ont été inspirés par ce projet.

Pour en savoir davantage sur les sujets discutés dans ce rapport ou vous joindre à la communauté du CCIAN, visitez www.diacc.ca ou écrivez à info@diacc.ca.

Annexe A – Fournisseurs participants

Fournisseur	Northern Block
Personne-ressource	Mathieu Glaude, mathieu@northernblock.io
Offre	Portefeuille NB Orbit : ● https://northernblock.io/products/ssi-digital-wallet/ Plateforme d'émission, de vérification et d'intégration NB Orbit : ● https://northernblock.io/products/ssi-enterprise-cloud/ Northern Block a présenté une version initiale de la suite NB Orbit. Elle consiste en une application pour portefeuille mobile et une plateforme d'émission. La plateforme d'émission, de vérification et d'intégration NB Orbit est actuellement basée sur l'agent ACA-py qui est utilisé dans la trousse pour les émetteurs de justificatifs vérifiables. Le portefeuille et les justificatifs émis sur cette plateforme sont compatibles avec la validation de principe.
Site web	https://northernblock.io/
Vidéo	https://www.youtube.com/watch?v=rI8yt6V3p0U

Fournisseur	Interac et 2Keys
Personne-ressource	Andrew Johnston, ajohnston@2keys.ca
Offre	Interac et 2Keys ont fait une démonstration technologique d'une application mobile pour portefeuilles numériques qui incluait l'acceptation d'un justificatif de personne vérifiée émis par le gouvernement, l'authentification par l'utilisateur final de la présentation du justificatif et une interface ouverte basée sur des normes -- OpenID Connect – pour les parties dépendantes. Interac et 2Keys ont aussi fourni des applications de parties dépendantes pour montrer comment le justificatif de personne vérifiée pourrait être utilisé par les participants à l'écosystème du secteur privé et comment l'authentification biométrique pourrait servir à améliorer la confiance dans l'identité de l'utilisateur final.
Site web	https://www.interac.ca/
Vidéo	https://youtu.be/aso4RPQs5xM

Fournisseur	Yoti
Personne-ressource	Leigh Day, leigh.day@yoti.com
Offre	Yoti a démontré la capacité pour un utilisateur d'intégrer un justificatif créé par le gouvernement à partir de la chaîne de blocs dans l'application Yoti, de le présenter comme un justificatif vérifié et de le partager avec une partie dépendante en « scannant » un code QR.
Site web	www.yoti.com
Vidéo	https://youtu.be/_G2_KDVLVvU

Fournisseur	Applied Recognition Corp.
Personne-ressource	Don Waugh, don.waugh@appliedrecognition.com
Offre	Applied Recognition a présenté une version alpha d'un portefeuille auto-souverain qui intègre la reconnaissance faciale Ver-ID directement dans le portefeuille. Applied Recognition a reconnu les problèmes de sécurité liés à l'utilisation de mots de passe par le portefeuille auto-souverain par rapport à la façon dont les justificatifs et les portefeuilles doivent être sécurisés. L'intégration de la reconnaissance faciale Ver-ID résout plusieurs problèmes

	pour les propriétaires de portefeuilles, les émetteurs de justificatifs et les parties dépendantes, notamment : ● Protection du portefeuille et du titulaire du portefeuille contre le vol d'identité. ● Automatisation et augmentation de la vérification de l'identité pour les émetteurs et les parties dépendantes. ● Biométrie faciale liée à des justificatifs vérifiables assurant que seul le propriétaire véritable peut ouvrir ses justificatifs. ● Assurance pour les parties dépendantes que les justificatifs présentés proviennent du propriétaire véritable et non d'un imposteur. Le portefeuille a été testé avec les sites d'essai du gouvernement de la C.-B. sur les réseaux Sovrin Staging et BCovrin pour démontrer l'interopérabilité entre des réseaux distincts. Applied Recognition a maintenant breveté Ver-ID pour la Digital Identity Trust Foundation, qui va mettre le portefeuille gratuitement à la disposition des consommateurs pour promouvoir et sécuriser les identités numériques et les justificatifs vérifiables.
Site web	www.Appliedrecognition.com/sovrinwallet, https://digitalidentitytrust.org/
Vidéo	https://vimeo.com/548476945

Fournisseur	Vlinder
Personne-ressource	Malini Srinivasan, info@vlinder.io, malini@vlinder.io
Offre	Klefki est une plateforme sécuritaire et sans friction basée sur la chaîne de blocs, qui procure confiance, inclusion et efficacité à l'écosystème des entreprises publiques et privées. Klefki permet aux personnes : 1. De posséder une identité 2. D'accepter les justificatifs des émetteurs et d'entreposer la sécurité dans un portefeuille mobile 3. De partager des justificatifs avec des vérificateurs par consentement et sur demande 4. De divulguer certains détails des justificatifs (preuves) plutôt que des données sensibles réelles Elle permet aux émetteurs : 1. D'émettre des justificatifs directement dans le portefeuille du citoyen

	2. De voir la liste des justificatifs émis dans un tableau de bord Elle permet aux vérificateurs de : 1. Vérifier les justificatifs des citoyens directement auprès de ceux-ci Klefki suit des normes clés, notamment : 1. Normes W3C 2. RGPD 3. Loi sur la protection des données de l'Inde Portefeuille Klefki (iOS) : ● https://apps.apple.com/us/app/klefki/id1546129401 Portefeuille Klefki (Android) : ● https://play.google.com/store/apps/details?id=io.vlinder.klefki Lien vers les produits Klefki : ● https://klefki.io/#product Plateforme Klefki pour les entreprises (écosystème des émetteurs et vérificateurs) : ● https://generic.klefki.io/login
Site web	https://vlinder.io/
Vidéo	Plateforme Klefki : ● https://vlinderdeveloper.wistia.com/medias/3wsjyd0vvu Klefki Real Estate DIACC : ● https://vlinder-uxdeveloper.wistia.com/medias/00poxjn0nk