IDENTITÉ NUMÉRIQUE DES CONSOMMATEURS

TIRER PARTI DE LA TECHNOLOGIE DISTRIBUÉE QUI PROTÈGE DAVANTAGE LA VIE PRIVÉE

Ce document examine les enjeux et les débouchés qui existent actuellement dans les marchés émergents de l'identité, et il décrit les paradigmes rationnels et technologiques pour concevoir un système axé sur le consommateur et plus confidentiel faisant appel à des architectures distribuées modernes. Il vise à accompagner la recherche appliquée qui a été développée par SecureKey dans le cadre d'un programme de recherche appliquée du Digital ID & Authentication Council of Canada (DIACC).

Table des matières

À PROPOS DE CE DOCUMENT **3**

SYNOPSIS **3**

RAISON D'ÊTRE DU SYSTÈME **4**

PRINCIPES DE L'ARCHITECTURE ET DE LA PROTECTION DE LA VIE PRIVÉE **5**

PRINCIPAUX INTÉRESSÉS **6**

FOURNISSEUR DE CASES POSTALES NUMÉRIQUES 6
FOURNISSEUR D'ACTIFS NUMÉRIQUES 6
GARDIEN DES DONNÉES 7
CONSOMMATEUR D'ACTIFS NUMÉRIQUES 7
INTENDANT DE RÉSEAUX 7
UTILISATEUR 7

DÉTAILS DE L'ARCHITECTURE **8**

APPLICATION COMMERCIALE **10**

CONCLUSION : PROPOSITION ROBUSTE POUR LE CONSOMMATEUR **11**

À propos de ce document

Ce document traite des enjeux et des débouchés qui existent actuellement dans les marchés émergents de l'identité, et décrit les paradigmes rationnels et technologiques pour concevoir un système axé sur le consommateur et plus confidentiel faisant appel à des architectures distribuées modernes. Il a été préparé par le Digital ID & Authentication Council of Canada (DIACC) et SecureKey.

Le DIACC est une coalition sans but lucratif d'organismes des secteurs public et privé qui développent un cadre d'identification et d'authentification numériques. Il a été créé dans la foulée du groupe de travail du gouvernement fédéral chargé d'examiner le système de paiements.

SecureKey est un fournisseur de solutions d'identité et d'authentification qui simplifient l'accès des consommateurs aux services et applications en ligne.

Synopsis

La Commission on Enhancing National Cyber Security vient de publier son rapport sur la sécurisation et l'expansion de l'économie numérique (1er décembre 2016). Les impératifs définis dans le rapport consistent à :

1. Protéger, défendre et sécuriser l'infrastructure de l'information et les réseaux numériques actuels;
2. Innover et accélérer les investissements pour sécuriser et développer les réseaux numériques et l'économie numérique;
3. Préparer les consommateurs à s'adapter à l'ère numérique;
4. Bâtir des compétences en cybersécurité chez les travailleurs;
5. Mieux équiper le gouvernement pour fonctionner d'une façon efficace et sécuritaire dans l'ère numérique;
6. Créer une économie numérique mondiale ouverte, équitable, compétitive et sécuritaire.

Le rapport met en outre l'accent sur la nécessité pour l'administration de collaborer avec le secteur privé pour définir, mettre en œuvre et défendre une feuille de route pour i) améliorer la sécurité des réseaux numérique contre le déni de services, la mystification et les autres attaques contre les utilisateurs et l'infrastructure réseau de la nation et ii) accroître le recours à une robuste authentification pour améliorer la gestion de l'identité.

Ce document décrit la façon dont SecureKey a développé un écosystème de l'identité en nuage en utilisant des éléments de la technologie des livres comptables décentralisée (chaîne de blocs) moderne afin de répondre à ces exigences. Le travail initial a été effectué dans le cadre d'un partenariat axé sur la recherche appliquée entre le DIACC et le Command, Control and Interoperability Center for Advanced Analysis (CCICADA) de l'Université Rutgers, et il s'est concentré sur la définition de modèles, l'analyse commerciale et la recherche appliquée.

L'écosystème de l'identité issu de la recherche fournit une authentification robuste, tout en protégeant la vie privée individuelle. Il procure aux utilisateurs ultimes un contrôle et une commodité lorsqu'ils partagent leurs actifs numériques avec d'autres dans l'écosystème.

Le système suit donc les recommandations de la NIST Special Publication 800-63 et les 10 principes canadiens adoptés par le DIACC pour les écosystèmes de l'identité numérique. Il s'aligne aussi sur les lignes directrices de la protection intégrée de la vie privée, qui ont été élaborées conjointement par le Canada et les Pays-Bas.

Raison d’être du système

Un certain nombre d’organismes des secteurs public et privé ont mis sur pied diverses solutions de gestion de l’identité afin de gérer les privilèges d’authentification et d’autorisation de leurs utilisateurs à l’intérieur et en dehors des limites des systèmes et des entreprises. Ces solutions permettent aux utilisateurs ultimes d’authentifier et/ou de fournir leurs données d’identité en utilisant des identifiants numériques tiers qu’ils possèdent déjà et auxquels ils font confiance, notamment ceux de leurs banques.

Ces systèmes de courtage de l’identité actuellement déployés sont très utiles pour les participants, mais on a remarqué que les principes selon lesquels ils sont conçus comportent plusieurs lacunes au niveau de la sécurité et de la protection de la vie privée. Les améliorations visées sont décrites plus en détail dans le livre blanc du National Institute of Standards and Technology (NIST) intitulé « Privacy– Enhanced Identity Brokers » rédigé par Paul Grassi, Naomi Lefkovitz et Kevin Mangold, et dans le livre blanc intitulé « Toward Mending Two Nation-Scale Brokered Identification Systems » de Luis T.A.N Brandõo, Nicolas Christin et George Danezis. L’architecture qui répond aux enjeux indiqués plus haut doit réduire la dépendance à un seul point de confiance et de défaillance, et empêcher une partie de faire le suivi d’une transaction utilisateur, tout en maintenant une piste vérifiable qui ne peut pas être altérée ni utilisée pour l’exploration de données. L’identité du participant devrait aussi être protégée à l’aide de technologies et de protocoles cryptographiques ultramodernes.

Le projet de modèle décentralisé qui est décrit dans ce document utilise également des plateformes et des normes technologiques bien connues, et il est mis à la disposition des participants de l’écosystème grâce à un code base source ouvert dont la licence est facile à obtenir et qui est maintenu par un groupe établi de développeurs. Il est conçu pour faciliter l’adoption et l’intégration avec des composantes dorsales de l’identité enregistrée, et pour se conformer aux exigences de sécurité, de communication réseau et de conception.

Principes de l'architecture et de la protection de la vie privée

Voici les principes directeurs auxquels le système proposé souscrit :

1. Pas d'autorité centralisée
   Les utilisateurs et les membres du consortium interagissent directement avec le marché pour s'assurer qu'il n'y a pas de serveurs intermédiaires agissant comme point de défaillance unique ou en mesure d'interférer avec les transactions.

2. Infrastructure masquée sécurisée
   a. L'identité des participants devrait être garantie et protégée à l'aide de technologies et de protocoles cryptographiques ultramodernes.
   b. Toutes les parties intervenant dans une transaction devraient rester anonymes entre elles.
   c. La transmission des messages entre les participants du réseau et l'utilisateur ultime devrait être sécurisée et l'anonymat de chacun respecté.
   d. L'accès aux données des utilisateurs ne peut se faire à partir de l'infrastructure centrale (sauf lorsque cela est exigé par des ordonnances de tribunaux, des enquêtes légales ou d'autres cas de répudiation).

3. Architecture de données décentralisée, sécurisée et privée
   a. Les règles d'entreposage des données, d'acceptation des transactions, de consignation et de configuration sont réparties entre tous les participants du réseau.
   b. Le propriétaire du réseau tient à jour les activités de vérification financière dans un livre privé avec les preuves d'existence connexes entreposées dans un livre distribué qui est partagé avec tous les participants du réseau.
   c. Chaque actif numérique est chiffré à l'aide d'une clé fractionnée dont le gardien détient une partie et l'utilisateur l'autre partie.

4. Protection de la vie privée et contrôles
   a. Les utilisateurs doivent toujours garder le contrôle. Les données devraient être transmises chiffrées et le consentement devrait être signé à l'aide des clés que l'utilisateur contrôle.
   b. Les données au repos ne doivent pas pouvoir être associées (à moins qu'une enquête n'ait été autorisée).
   c. Les données en transit doivent être consultées par un minimum de systèmes afin de satisfaire la politique d'endos des transactions (l'endos est l'étape où un organisme a vérifié la validité d'une transaction).
   d. Les transactions des utilisateurs (comme le consentement) devraient pouvoir être associées à un utilisateur pendant une enquête autorisée (mais pas autrement). Les enquêtes devraient être autorisées par un plan multiorganisationnel (« en dernier ressort »).
   e. Les transactions devraient être endossées par plusieurs organismes pour être valides (afin de s'assurer qu'aucun organisme ne peut créer des transactions non autorisées).

5. Tenue de livres, audit et facturation
   a. Un historique des transactions doit être tenu et ne peut être modifié.
   b. Il faut avoir une architecture vérifiable et décentralisée où la facturation peut se faire sans que le réseau ne soit actif.

Principales parties prenantes

La solution permet aux utilisateurs de se servir de renseignements vérifiés provenant directement des appareils personnels de parties de confiance bien connues comme les banques, les fournisseurs de services de télécommunication, les gouvernements et les bureaux de crédit.

Pour avoir un marché de l'information numérique à grande échelle, l'écosystème regroupe les organismes partenaires – les membres du consortium – dans un consortium. Ces membres exploitent la plateforme du système, en représentant les organismes auxquels les utilisateurs font déjà confiance, comme leurs banques. **I**s prouvent la validité des renseignements des utilisateurs au marché, tout en donnant accès à ces renseignements.

La solution fournit aux participants du réseau un service de transmission des données masquée et sécurisée qui permet de partager les données à mesure qu'elles sont créées ou mises à jour, mais qui laisse l'utilisateur contrôler le flux de données. Une fois que les renseignements utilisateur sont disponibles sur le marché, ils deviennent un actif numérique.

Chaque membre du consortium est responsable d'émettre des actifs numériques à usage unique ou réutilisables que les utilisateurs peuvent partager avec des services en ligne – les consommateurs d'actifs numériques. Cela permet à un utilisateur de fournir des renseignements fiables provenant de sources multiples et d'authentifier une seule transaction.

Afin de préserver les propriétés du système particulièrement axées sur la protection de la vie privée des utilisateurs, les partenaires qui s'occupent de l'infrastructure du marché ne doivent pas pouvoir inspecter les dossiers des utilisateurs, faire un suivi (ou profilage) de l'activité d'un utilisateur ni se faire passer pour un utilisateur (falsification des transactions).

Les partenaires du système peuvent aussi être des entités concurrentielles dans leur industrie, et ils ne doivent donc pas avoir accès aux connaissances sur les activités d'autres partenaires ou utilisateurs de partenaires dans le réseau.

Fournisseur de cases postales numériques

Les fournisseurs de cases postales numériques sont des organisations hautement qualifiées et fiables, qui ont déjà des relations solides avec les utilisateurs. Ils maintiennent des éléments essentiels de l'écosystème en accomplissant les fonctions suivantes :

- Introduire, éduquer et intégrer les utilisateurs dans l'écosystème
- Authentifier l'utilisateur pendant les transactions dans le réseau
- Maintenir l'intégrité et la stabilité du réseau en faisant fonctionner les composantes essentielles du réseau distribué, notamment la case postale numérique des utilisateurs
- Fournir à l'utilisateur des outils pour soutenir leurs activités réseau, notamment l'authentification, le dépannage et le rétablissement des comptes
- Agir comme le fournisseur principal d'identité ou d'actifs numériques de l'utilisateur dans le réseau

Fournisseur d'actifs numériques

Le fournisseur d'actifs numériques donne de l'information ou des services à propos de ses utilisateurs pa l'intermédiaire du consortium.

Gardien des données

Le gardien des données contrôle l'accès aux données pour le fournisseur d'actifs numériques. Un ensemble de vérificateurs associés peut accéder aux données utilisées pour vérifier les transactions. Mais pour éviter d'avoir un seul point de confiance, plusieurs vérificateurs doivent collaborer pour accéder aux données des transactions à des fins d'audit. En règle générale, le fournisseur de cases postales numériques peut remplir le rôle de gardien des données.

Consommateur d'actifs numériques

Le consommateur d'actifs numériques est une partie utilisatrice qui a besoin de vérifier l'identité de l'utilisateur avant de pouvoir donner accès à une ressource comme un service en ligne.

Intendant de réseaux

Cette partie crée le système, s'occupe de la santé des applications distribuées, et gère l'image de marque, l'attribution des contrats et la facturation. Elle agit aussi comme vérificateur des gardiens.

Utilisateur

L'utilisateur est la personne qui possède les renseignements sur l'identité. Il se sert d'un agent d'utilisateur fiable, généralement une application pour téléphone intelligent, pour contrôler comment et quand les renseignements sur son identité sont fournis au consommateur d'actifs numériques.

Détails de l'architecture

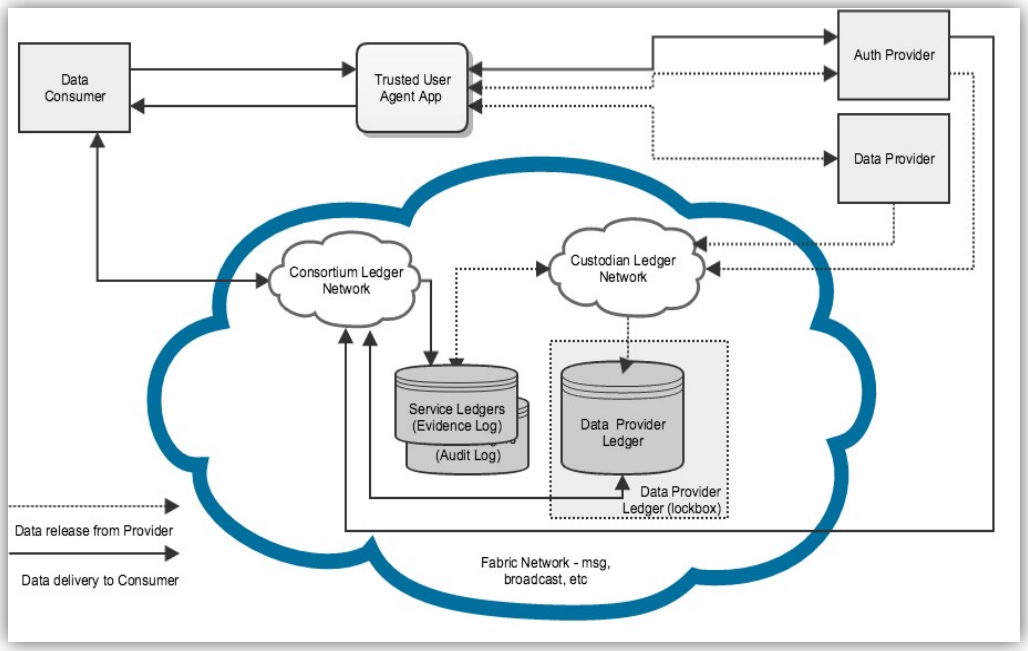
Après avoir examiné les technologies ultramodernes disponibles pour répondre à toutes les exigences énoncées plus haut, SecureKey a décidé que le système serait mieux implanté sur une technologie de livres distribuée qui fournit la preuve des transactions, protège la vie privée des utilisateurs ultimes et fournit à ces derniers le plein contrôle des données associées à leur identité. L'architecture de l'écosystème de l'identité en nuage qui améliore la protection de la vie privée utilise une base de données distribuée constituée de déclarations d'identité chiffrée dans différents sites opérationnels de confiance, ce qui élimine les points de défaillance centraux. Afin de soutenir un consensus pour le règlement et l'état global des transactions, le système se sert d'un livre de transactions distribué et chiffré, qui est basé sur une technologie de chaîne de blocs avec permissions pour enregistrer les actions dans le système.

Le nouveau système est essentiellement un courtier décentralisé qui :

1. Permet aux utilisateurs d'effectuer une authentification à l'aide d'un fournisseur qualifié auquel ils font déjà appel fréquemment;
2. Favorise les interactions à distance fiables parmi les organisations et les utilisateurs via un marché masqué, ce qui élimine le besoin d'avoir une autorité centralisée;
3. Donne la possibilité de transférer l'identité et les données vérifiées de l'utilisateur, avec son consentement;
4. Protège l'identité des participants et le droit de l'utilisateur à la confidentialité de l'interaction;
5. Met en place les contrôles et les pistes d'audit nécessaires pour permettre des fonctions administratives libre-service tout en maintenant une sécurité rigoureuse, en protégeant la vie privée et en évitant le suivi ou le profilage des activités de l'utilisateur.

Le principe de conception principal est basé sur la mise en œuvre d'un flux d'authentification décentralisé et asynchrone entre les participants de l'écosystème, en déplaçant plusieurs fonctions de courtage traditionnelles vers un agent d'utilisateur fiable que l'utilisateur contrôle.

Le diagramme qui suit montre les composantes générales du système et le flux des transactions dans le système.



L'utilisateur peut désormais donner à l'agent d'utilisateur qu'il contrôle l'instruction d'accepter et d'autoriser les demandes provenant des consommateurs de données.

Le fournisseur de données n'a plus nécessairement besoin d'être en ligne pendant une transaction, car un utilisateur est authentifié auprès de son fournisseur principal sur son propre agent d'utilisateur (représenté par une application mobile sécurisée) dont l'utilisateur a le contrôle. Comme les fournisseurs de données n'interviendront pas nécessairement pendant une transaction, il faut un nœud d'évidence pour certifier qu'un utilisateur contrôle certaines données. En outre, un nœud de vérificateur est également nécessaire pour permettre à toutes les parties de vérifier les transactions qu'elles ont effectuées (avec des permissions spéciales).

L'architecture propose un modèle pour de tels nœuds d'évidence et de vérificateur, où les livres de service assureront l'intégrité des données, notamment en identifiant l'éditeur de données des événements enregistrés et les détails des transactions effectuées dans le service, tout en protégeant la vie privée et la confidentialité des utilisateurs et des participants. En outre, les identifiants et les données des utilisateurs sont entreposés dans une case postale numérique qui est sécurisée. La case postale numérique chiffrée est distribuée par nature et, de ce fait, les données utilisateur chiffrées peuvent être entreposées chez ce fournisseur de données en particulier ou dans un entrepôt distribué (avec un accès contrôlé par l'agent d'utilisateur) en fonction des exigences du scénario spécifique. Le fournisseur d'authentification de l'utilisateur (rôle joué par le fournisseur de cases postales numériques) fournit l'authentification à la case postale numérique.

Le système s'assure aussi que les utilisateurs partagent uniquement les données qu'ils ont transmises d'un fournisseur de données fiable au consommateur de données demandeur et légitime, tout en respectant les exigences en matière de protection de la vie privée et de consentement de l'utilisateur. Pour faciliter la validité d'une transaction, le système met en place un mécanisme pour lier la déclaration d'identité d'un utilisateur à une transaction en ligne, comme un tatouage numérique. Les utilisateurs qui partagent leurs actifs numériques avec les consommateurs d'actifs numériques doivent être authentifiés par le fournisseur de cases postales numériques. Les clés de chiffrement qui protègent l'actif numérique que l'utilisateur contrôle sont uniquement libérées quand l'utilisateur a consenti à partager ses actifs numériques.

Il est important de permettre au système de récupérer les détails des transactions de l'utilisateur au cas où il y aurait une enquête et de fournir ces renseignements tout en protégeant le système contre les abus. Cela est effectué en utilisant plusieurs livres comptables à l'intérieur du système de livres distribué. Un livre public global est partagé par l'ensemble du consortium, tandis que des sous-ensembles de membres du consortium ont accès à plusieurs livres privés. Ces livres privés contiennent des segments de transactions qui associent les transactions à des utilisateurs spécifiques et permettent aux enquêteurs de vérifier les transactions. Toutefois, les renseignements sont divisés entre différents livres privés pour éviter un point de confiance unique. Le livre distribué sert à entreposer des entrées immutables prouvant que les dossiers des transactions existent, ce qui rend toutes les données vérifiables sans permettre la lecture des détails de l'identification. Il faut, pour les consulter, la coopération de plusieurs parties pour s'assurer qu'aucun organisme n'y ait accès isolément. En entreposant les données de cette façon, l'intendant du réseau peut créer des rapports de facturation et de remise sans être autorisé à associer les transactions à des utilisateurs en particulier.

Application commerciale

La technologie de courtier décentralisé permet à des personnes de partager rapidement l'information sur leur identité pour avoir accès à des services commerciaux et gouvernementaux. Ils peuvent utiliser le système pour accéder aux services sans créer de nouveaux mots de passe ou identifiants, et permettre aux organisations de partager, mettre à jour et valider en leur nom leurs attributs avec d'autres organisations.

Ces capacités sont utilisées dans plusieurs situations, entre autres :

- Gouvernement qui s'assure que le compte bancaire d'un citoyen lui appartient;
- Citoyen qui valide son revenu auprès d'une institution financière en se référant aux dossiers du gouvernement;
- Création de comptes vérifiés dans des environnements d'économie du partage comme les marchés P2P et les services de location;
- Authentification rapide pour les vérifications d'antécédents et le contrôle de l'emploi;
- Transmission de renseignements sur les voyageurs pour les services de transport :
- Signature de formulaires d'autorisation et de contrats.

Les utilisateurs jouissent d'un avantage essentiel qui consiste à pouvoir mettre à jour les renseignements sur leur identité à un seul endroit à mesure que leurs circonstances changent, et ce, sans avoir à informer manuellement des dizaines d'institutions.

L'approche de l'écosystème de SecureKey en matière de gestion de l'identité et de l'accès cible initialement les fournisseurs de services comme les banques, les sociétés de télécommunications et les organismes gouvernementaux, qui ont tous dû composer avec des méthodes inefficaces, encombrantes et peu sécuritaires pour valider l'identité. Cette approche va réduire les taux de fraude et accroître les taux d'exécution des transactions en réduisant la friction de l'utilisateur.

À la longue, elle séduira un éventail d'industries allant de l'immobilier aux voyages et aux soins de santé. N'importe quel environnement avec un volume de transactions élevé, en particulier ceux qui utilisent des transactions en ligne, peut bénéficier de cette approche de courtage décentralisée.

L'approche basée sur l'écosystème va s'étendre graduellement à mesure que ces organisations seront plus nombreuses à participer. Les principales banques du Canada ont déjà accepté de soutenir l'écosystème et d'y participer avec les sociétés de télécommunications et divers ordres de gouvernement.

Le processus d'adoption est conçu pour être relativement facile pour toutes les parties. Les personnes qui utilisent le service ont besoin d'un peu plus qu'un téléphone mobile, tandis que les fournisseurs et les consommateurs d'actifs numériques peuvent utiliser des protocoles standard de l'industrie comme OAUTH, Open ID Connect ou REST APIs.

Les fournisseurs d'actifs numériques partagent des revenus de l'utilisation quand les consommateurs d'actifs numériques utilisent les attributs vérifiés des fournisseurs d'actifs numériques provenant du service. Les consommateurs d'actifs numériques reçoivent une liste de prix pour des ensembles d'attributs qu'ils peuvent demander au consortium et l'intendant du réseau les facture pour leur utilisation avant de payer les parts de revenus correspondantes aux fournisseurs d'actifs numériques, en gardant un pourcentage pour son rôle dans le système.

Les consommateurs et les fournisseurs d'actifs numériques bénéficieront tous en réduisant la friction du client, en réduisant les taux de fraude et en éliminant les coûts de soutien. Les consommateurs ne paient rien.

Le processus d'adoption a besoin de « champions » pour susciter l'intérêt pour le modèle. Du côté de l'approvisionnement, les banques et autres fournisseurs de données fiables doivent commencer à offrir des identifiants hautement fiables et éduquer les consommateurs. En ce qui concerne la demande, les organismes gouvernementaux peuvent donner l'exemple en démontrant les avantages du système.

Conclusion : une proposition pour le consommateur

SecureKey a démontré son expérience commerciale en gestion de l'identité et de l'accès grâce à son travail avec le gouvernement fédéral canadien et d'autres instances nationales et mondiales. Même si la technologie de chaîne de blocs est nouvelle, SecureKey se base sur Hyperledger, une initiative transsectorielle, pour bâtir une technologie de chaîne de blocs robuste et ouverte.

Grâce à un ensemble de partenaires de confiance, une approche de livres distribuée pour la gestion de l'identité offre l'avantage de pouvoir surpasser les risques de l'adoption associés à une technologie relativement nouvelle. Les normes d'anonymat robustes du système permettent aux concurrents potentiels de travailler ensemble dans le même écosystème. Sa nature décentralisée élimine les points de défaillance uniques, ce qui améliore considérablement la résilience. Et cela protège complètement la vie privée des utilisateurs, tout en maintenant la commodité et la facilité d'accès. Les participants du réseau auront ainsi une robuste proposition client.

Pour obtenir plus de renseignements sur les occasions de recherche appliquée du DIACC, veuillez écrire à info@diacc.ca. Pour en savoir davantage sur les sujets discutés dans ce document, veuillez communiquer avec Dmitry Barinov, le chef des projets de recherche appliquée : dmitry.barinov@securekey.com.