DIGITAL ID AND AUTHENTICATION COUNCIL OF CANADA

Aperçu du cadre de confiance pancanadien

Une approche collaborative pour développer un cadre de confiance pancanadien

Auteurs : Comité d'experts du cadre de confiance du DIACC

Août 2016

Résumé : Ce document a pour but de décrire la genèse, le contexte et l'approche collaborative entourant le développement d'un cadre de confiance pancanadien (CCP). Le CCP permettra au Canada de participer en toute sécurité à l'économie numérique mondiale tout en soutenant l'innovation économique, la prestation des services et les principes d'un gouvernement ouvert.

Table des matières

Synopsis **3**

Genèse et contexte **3**

Perspective du DIACC sur les écosystèmes de l'identité numérique 3

Exigences de l'écosystème canadien de l'identité numérique *5*

Cadres de confiance – aperçu **8**

Buts des cadres de confiance 9

Le cadre de confiance pancanadien **9**

Auditoire, application et autorité visés 10

Portée du cadre de confiance pancanadien 10

Valeur du cadre de confiance pancanadien 10

Structure du cadre de confiance pancanadien 11

Conclusion **11**

À propos du DIACC **12**

Synopsis

Un cadre de confiance est un terme général qui décrit un ensemble de règles commerciales, techniques et juridiques vérifiables qui s'appliquent à l'identification, à l'authentification et à l'autorisation de l'accès aux ressources des organisations.

Cet aperçu présente l'approche collaborative du cadre de confiance pancanadien (CCP). Le CCP permet au Canada de participer pleinement et en toute sécurité à l'économie numérique mondiale en introduisant des innovations dans le secteur économique et en contribuant à moderniser la prestation des services numériques. Le CCP soutient les principes d'un gouvernement ouvert.

Le CCP se fonde sur les connaissances et l'expérience globales qui ont été acquises avec le temps et la pratique. Il est le fruit d'une collaboration entre le Digital ID and Authentication Council of Canada (DIACC), qui est une tribune neutre sans but lucratif, et le Sous-comité de la gestion de l'identité (SCGI) pancanadien relevant des conseils mixtes du Canada, qui regroupe le Conseil des dirigeants principaux de l'information du secteur public (CDPISP) et le Conseil de la prestation des services du secteur public (CPSSP).

Le travail déjà accompli par le SCGI soutient la création et la communication d'identités numériques de confiance. Les identités sont ancrées dans les sources de la fonction publique qui font autorité et mises à profit par les services à valeur ajoutée du secteur privé. En outre, le CCP s'inspire des notions abordées dans les Principes d'authentification électronique[1].

Le CCP décrit les rôles, les services et les exigences devant être convenus entre les organismes participants qui fournissent des services et du secteur commercial afin de répondre aux besoins actuels et futurs en matière d'innovation canadienne. Le CCP tire parti des principes des écosystèmes de l'identité numérique présentés dans ce document. Les organismes et les particuliers désirant collaborer au développement du CCP sont invités à communiquer avec le DIACC.

Genèse et contexte

Perspective du DIACC sur les écosystèmes de l'identité numérique[2]

Partout dans le monde, les gouvernements et les industries développent des cadres technologiques et politiques, plus connus comme des cadres de confiance. Un cadre de confiance permet de créer une identité numérique et, par extension, facilite les transactions électroniques fiables.

À mesure que les modèles de prestation des services numériques gagnent en maturité, les gouvernements, les entreprises et les particuliers ont besoin de savoir que les renseignements personnels sous forme électronique sont protégés lorsqu'ils franchissent les limites juridictionnelles et organisationnelles.

[1] Principes d'authentification électronique, Industrie Canada
[2] Forger l'avenir de l'identité numérique du Canada, DIACC

Les cadres de confiance définissent et uniformisent les processus et les pratiques, et ils spécifient les politiques en matière de protection des données que les organismes gouvernementaux, les banques, les sociétés de télécommunications, les prestataires de soins de santé et les entreprises conviennent de suivre en ce qui concerne les pratiques de certification de l'information.

Pour que le Canada participe pleinement à la transformation numérique et à l'économie numérique mondiale, il faut développer des solutions fiables, sûres, évolutives, plus confidentielles et pratiques pour l'identité numérique. Celles qui sont conçues pour le Canada reflètent et intègrent les principes, intérêts commerciaux et modèles techniques canadiens, et elles démontrent leur conformité aux règlements canadiens. Les solutions destinées au Canada pavent aussi la voie à des transactions et la prestation de services transfrontalières sécuritaires et sûres.

L'écosystème canadien de l'identité numérique doit être digne de confiance et fiable, et permettre à une personne de gérer en toute sécurité l'accès à ses renseignements et services personnels. Ces aspects constituent les principes fondamentaux qui sous-tendent les solutions conçues pour le Canada. Les Canadiens s'attendent à ce que l'infrastructure de leur identité numérique fonctionne d'une façon transparente qui garantit un traitement équitable pour tous. Ils s'attendent aussi à ce qu'on leur indique d'une façon claire et convaincante pourquoi et comment leurs renseignements personnels peuvent être recueillis et divulgués.

L'utilisation des identités numériques doit, pour être vraiment réussie, ne doit pas se cantonner à une organisation ou un secteur en particulier. Les identités numériques doivent pouvoir être utilisées au Canada, entre les secteurs, par différents ordres de gouvernement et à l'échelle internationale. Les processus, les systèmes et les infrastructures opérationnels doivent permettre aux particuliers de gérer d'une façon transparente leur identité numérique et leurs renseignements personnels dans différents contextes.

Les Canadiens s'attendent à ce qu'on leur indique d'une façon claire et convaincante comment, par qui et à quelle fin leurs renseignements personnels sont utilisés.

Il est impératif de créer et de mettre en place un cadre politique et technologique pour un écosystème de l'identité numérique qui inspire la modernisation des services numériques. L'innovation sur le plan de l'économie numérique va permettre aux Canadiens d'avoir des interactions électroniques sécuritaires, plus confidentielles et pratiques au pays et à l'étranger. Les Canadiens doivent avoir l'assurance que les services offerts dans l'écosystème de l'identité numérique protègent leurs renseignements personnels et en réduisent le partage. Les Canadiens doivent connaître leur droit à la confidentialité, à la protection et à la gestion de leurs renseignements personnels. Les Canadiens doivent avoir accès à des outils qui les aident à gérer en toute sécurité l'accès à leurs renseignements personnels pour des motifs spécifiques.

Les documents canadiens qui servent à identifier les personnes sont en voie de modernisation. Le passeport électronique canadien et la Services Card du gouvernement de la Colombie-Britannique, une carte de services intelligente émise par la province, sont deux exemples de documents modernisés. Ce sont des pièces d'identité physiques dotées de caractéristiques électroniques permettant aux particuliers de s'identifier électroniquement, d'une façon anonyme s'ils le désirent, conformément aux règlements canadiens.

Les documents modernisés offrent plus de commodité et d'efficacité aux particuliers, tout en réduisant les coûts des entreprises et des gouvernements. Ils renforcent l'exactitude, la sécurité et la protection de la confidentialité des transactions, mais nous devons permettre aux Canadiens de s'adapter à une économie entièrement numérique où les documents et les renseignements qu'ils

contiennent peuvent être entreposés en toute sécurité dans le nuage ou les appareils auxquels ils font confiance.

Exigences de l'écosystème canadien de l'identité numérique

Le DIACC propose 10 exigences pour l'écosystème numérique canadien[3]. Il reconnaît que d'autres principes peuvent être identifiés et pris en compte pour les besoins spécifiques du secteur économique et des services, notamment les Principes d'authentification électronique publiés par Innovation, Sciences et Développement économique Canada (auparavant Industrie Canada) en 2004[4].

1. Robuste, sûr, adaptable

L'écosystème de l'identité numérique du Canada doit être assez robuste pour être sûr, disponible et accessible en tout temps. Il faut aussi, pour avoir accès à temps plein aux services, des outils de redondance et de reprise après catastrophe.

L'infrastructure de l'écosystème doit permettre aux secteurs économique et des services numériques d'adopter les dernières innovations technologiques et politiques en matière de sécurité. La protection des renseignements personnels est une priorité non négociable. La conception de l'infrastructure doit protéger les renseignements personnels qui sont en transit et au repos. L'infrastructure doit être étayée par une sensibilisation et une formation permettant d'acquérir de l'expertise, notamment sur le contrôle de l'accès, l'audit et l'imputabilité, l'évaluation des risques, les essais de pénétration et la gestion de la vulnérabilité.

Un cadre de confiance qui régit les solutions et les services rattachés à l'écosystème de l'identité numérique doit pouvoir évoluer de façon à permettre une innovation sécuritaire. Certaines entités sont prêtes à accepter l'identité numérique, d'autres non. Un cadre de confiance de l'écosystème d'identification numérique doit être conçu pour que les secteurs économique et des services puissent être intégrés.

2. Instauration, protection et amélioration de la protection intégrée de la vie privée

Les outils visant à améliorer la confidentialité numérique permettent à une personne de gérer l'accès à ses renseignements personnels dans un but spécifique. Les membres du DIACC mettent l'accent sur l'identification et le développement d'outils et de politiques qui respectent la protection intégrée de la vie privée en tant qu'aspect fondamental des interactions liées à l'identité numérique. Les solutions doivent pouvoir démontrer qu'elles sont conformes aux lois et aux règlements canadiens applicables sur la protection des données.

3. Transparence de la gouvernance et des opérations

Les Canadiens doivent avoir la certitude que les services offerts dans l'écosystème canadien de l'identité numérique vont respecter et remplir leurs besoins. Ils doivent faire confiance aux politiques et aux pratiques qui régissent l'écosystème canadien de l'identité numérique. Il est essentiel que les Canadiens aient la transparence et les occasions voulues pour s'impliquer auprès des experts qui influencent les politiques et la technologie ayant trait à la gouvernance de l'écosystème de l'identité numérique.

[3] Forger l'avenir de l'identité numérique du Canada, DIACC
[4] Principes d'authentification électronique, Industrie Canada

4. Un écosystème inclusif et ouvert qui répond aux besoins des parties prenantes

Les services et les outils de l'écosystème de l'identité numérique doivent être abordables, uniformisés et avantageux pour les Canadiens. Les services doivent être sécurisés et innovateurs, tout en réduisant les coûts d'exploitation. Un cadre de confiance doit être assez flexible pour fonctionner avec des technologies et des services établis et innovateurs. L'écosystème doit être avantageux pour les particuliers ainsi que les fournisseurs de services commerciaux et de technologie en atténuant les risques tout en favorisant les occasions de développer les sources de rentrées.

Les entités des secteurs commercial et public ont en commun le besoin de fournir des services électroniques sécurisés et modernisés tout en réduisant les coûts. Les particuliers doivent avoir un accès égal et commode aux services, peu importe leur emplacement géographique. Tous les Canadiens doivent pouvoir comprendre et utiliser les services offerts dans l'écosystème canadien de l'identité numérique, quelles que soient leurs capacités individuelles[5].

Tous les Canadiens doivent pouvoir comprendre et utiliser facilement les services offerts dans l'écosystème canadien de l'identité numérique, quelles que soient leurs capacités individuelles.

5. Choix, contrôle et commodité pour les Canadiens

Les services qui respectent et améliorent la vie privée se fondent sur le principe voulant que les particuliers soient informés des détails ainsi que des avantages et des conséquences possibles de la gestion des renseignements personnels. Les personnes informées sont susceptibles de prendre de meilleures décisions quant à la façon dont leurs renseignements personnels sont fournis, partagés et utilisés.

Les personnes doivent, pour donner leur consentement en connaissance de cause, bien comprendre les faits, les implications et les conséquences possibles d'une intervention. Il faut pour cela leur fournir les connaissances et les outils voulus pour gérer d'une façon sécuritaire l'accès à leurs renseignements personnels.

Les services et les outils de l'écosystème de l'identité numérique doivent être faciles à utiliser. Le fait de mémoriser des dizaines de mots de passe ou d'avoir sur soi 15 cartes différentes n'est pas une approche adaptable ou sécuritaire. Si une personne oublie son mot de passe (ou un autre identifiant) ou si elle perd sa pièce d'identité (ou l'appareil sur laquelle elle est entreposée), elle doit pouvoir revalider d'une façon sécuritaire et pratique son identité numérique auprès des services de l'écosystème. Les services de l'écosystème de l'identité numérique doivent être suffisamment sécuritaires pour éviter la fraude et pratique pour permettre une authentification et un contrôle de l'accès rapides.

Les utilisateurs doivent pouvoir utiliser leur identité numérique d'une façon sécuritaire et commode.

6. Écosystème construit sur un protocole basé sur des normes ouvertes

L'utilisation de normes ouvertes et de bonnes pratiques applicables pour l'écosystème canadien de l'identité numérique aidera à le protéger contre la désuétude, assurera son interopérabilité, et favorisera un marché proposant des solutions dynamiques et concurrentielles. Le fait de bâtir l'écosystème canadien de l'identité numérique sur des protocoles basés sur des normes ouvertes

[5] Principles for Electronic Authentication, Industry Canada

évitera aux Canadiens d'être limités à une technologie ou un fournisseur unique. Il faut réduire le risque que les gouvernements et les entreprises soient prisonniers d'écosystèmes fermés.

L'adoption d'une approche basée sur des normes ouvertes permet que différents services utilisant des technologies normalisées communiquent d'une façon transparente. C'est essentiel pour permettre aux secteurs économique et des services de tirer parti des solutions interopérables et vérifiables qui répondent le mieux à leurs besoins.

7. Interopérabilité avec les normes internationales

L'interopérabilité et l'uniformisation mondiale des technologies et des politiques sont essentielles pour le monde branché d'aujourd'hui. De même que l'écartement uniformisé entre les rails de chemin de fer permet de voyager et d'acheminer des marchandises d'un pays à l'autre, et l'uniformisation de la taille des conteneurs de fret réduit les coûts d'expédition, l'interopérabilité et l'uniformisation des technologies et des politiques permettent aux services numériques de communiquer tout offrant plus d'occasions d'innover. Pour que le Canada prospère dans l'économie numérique mondiale, nous devons nous assurer que notre écosystème de l'identité numérique est capable d'interagir avec les systèmes d'information qui existent dans le monde, tout en respectant nos propres besoins culturels, constitutionnels, législatifs et réglementaires.

Pour que le Canada prospère dans l'écosystème numérique mondial, nous devons nous assurer que notre écosystème de l'identité numérique est capable d'interagir avec les systèmes qui existent dans le monde …

8. Écosystème économique et ouvert à la concurrence du marché

Il est essentiel que l'écosystème de l'identité numérique respecte les contraintes budgétaires d'aujourd'hui et de demain. Le fait d'avoir un écosystème ouvert à la concurrence, qui représente plusieurs secteurs économiques jouant chacun des rôles différents, va réduire les coûts des particuliers et favoriser l'innovation.

9. Écosystème pouvant être évalué et vérifié d'une façon indépendante, et assujetti à l'application de la loi

Il faut, pour que les Canadiens fassent confiance à un écosystème de l'identité numérique, mettre en place des mécanismes de contrôle essentiels. Des évaluations continues et fonctionnellement indépendantes menées par de tierces parties permettent de s'assurer que les entités et les services de l'écosystème remplissent les exigences du cadre de confiance. Les services qui prouvent leur conformité peuvent en retirer une marque de confiance, tandis que ceux qui ne sont pas conformes ne seront pas considérés comme étant dignes de confiance et ne profiteront pas des avantages de l'écosystème de l'identité numérique inspirant confiance. Dans la mesure du possible, le CCP s'inspirera des uniformisations technologiques et politiques adoptées à l'échelle internationale. Cela étant dit, les entités et les services participant au CCP sont assujettis aux lois et aux codes canadiens pour les opérations à l'intérieur des provinces et des territoires canadiens.

Des évaluations fonctionnellement indépendantes par de tierces parties permettent de s'assurer que les entités et les services de l'écosystème sont conformes au cadre de confiance d'un écosystème de l'identité numérique.

10. Réduction du transfert de données entre les sources autorisées et pas de création de nouvelles bases de données d'identification

On ne devrait demander aux utilisateurs des services de l'écosystème d'identification numérique de ne fournir que le minimum de renseignements personnels nécessaire pour effectuer une interaction. Les transactions anonymes devraient être encouragées dans la mesure du possible, et lorsque c'est approprié. C'est essentiel si le Canada doit adopter un écosystème où les gens s'impliquent dans des activités comme le vote électronique.

Cadres de confiance – aperçu

Un cadre de confiance consiste en une série de définitions, d'exigences, de normes, de spécifications, de processus et de critères convenus. L'ensemble de ces détails permet que les décisions concernant les processus et les autorisations relatifs à la gestion de l'identité qui sont prises par d'autres organisations et instances bénéficient d'un niveau de confiance uniformisé. En clair, un cadre de confiance permet à une organisation de se fier à un processus commercial ou technique d'une autre organisation.

Un cadre de confiance a pour but d'aider à définir et à implanter des solutions innovatrices pouvant être offertes dans tout le pays. Il ne vise pas à imposer ou à freiner les décisions ayant trait à la conception ou la technologie. Un cadre de confiance aide plutôt à définir la façon dont des solutions nouvelles et existantes peuvent fonctionner ensemble d'une manière uniformisée et fiable.

Un cadre de confiance se doit d'être compris par de nombreuses parties prenantes, et suffisamment clair pour être adopté et appliqué d'une façon uniforme par de multiples communautés, prestataires de services et intervenants. Enfin, et surtout, un cadre de confiance se veut un instrument d'habilitation essentiel pour l'ensemble de l'économie numérique. S'il est bien fait, un cadre de confiance est invisible pour ceux qui dépendent de lui au quotidien – les particuliers et les entreprises qui effectuent des transactions électroniques en sachant que la confiance sous-tend tout ce qu'ils font.

Les cadres de confiance permettent d'améliorer les services et les transactions électroniques en assurant une identification uniforme des personnes et des organisations. Les cadres de confiance uniformisent les interactions entre les institutions, les entreprises et les particuliers dès lors qu'il est question d'identification, d'authentification et d'autorisation.

Les cadres de confiance sont utilisés par une communauté animée par le même intérêt d'accroître l'expérience de la prévisibilité et de la transparence, et de gérer les risques quand les services sont utilisés dans cette communauté en particulier. Les éléments du cadre de confiance identifient, définissent et spécifient les processus et les attentes qui sont communs aux entités participant à la communauté numérique.

Buts du cadre de confiance

La notion de cadre de confiance décrit d'une façon générale plusieurs utilisations pour différents buts et intérêts.

But	Intérêt
Fédération d'accès	Émission fiable d'authentifiants, attribution de permissions et politiques de contrôle de l'accès, spécification technique et audit.
Fédération d'identités numériques	Établissement des renseignements sur l'identité, « association » des dossiers d'identité et des authentifiants, protection de la vie privée, interopérabilité technique.
Interopérabilité technique	Définition des spécifications et des profils de normes pour permettre à plusieurs systèmes d'interagir et d'échanger des renseignements d'une façon fiable.
Interopérabilité des politiques	Mise en place de politiques de compatibilité entre les organisations pour soutenir des résultats prévisibles entre et au sein des organisations.
Administration juridique	L'uniformisation des modalités, attentes et processus définis communs d'un cadre de confiance permet d'élaborer des modèles de contrats et d'ententes efficaces. Les contrats et les ententes des entités s'inspirent d'un cadre de confiance, sans en faire partie.

Le cadre de confiance pancanadien

Le CCP est essentiel pour s'assurer que l'écosystème canadien de l'identité numérique est digne de confiance et favorise un environnement équitable, innovateur et concurrentiel. Et comme l'écosystème émergent de l'identité numérique est pancanadien, le CCP soutient, par sa portée, l'inclusion de participants qui offrent un large éventail de services aux secteurs économique et des services électroniques.

Le CCP procure une valeur commerciale à une diversité de participants, qui correspond aux risques et tient compte des différentes perspectives des parties prenantes des secteurs public et privé :

- **Particuliers et organisations (en tant qu'utilisateurs ultimes des services –** Le CCP augmente la confiance dans la protection, la divulgation et l'utilisation de leur identité et de leurs renseignements personnels, ce qui favorise une approche axée sur la « divulgation unique » pour avoir un accès pratique à des services, d'une manière fiable, sûre et plus confidentielle.
- **Gouvernements, institutions et entreprises :** Le CCP donne l'occasion d'offrir des services uniformisés, de grande valeur et hautement intègres entre les provinces et territoires et le secteur privé. Il permet également de compter sur de nombreux prestataires de services fiables, ce qui améliore l'intégrité, l'efficacité et la rationalisation globales des services numériques complexes et à forte valeur.

Auditoire, application et autorité visés

Le CCP vise à être appliqué dans l'ensemble des industries et à être assujetti aux lois et aux règlements canadiens. Il va favoriser un écosystème de services de confiance, qui sera un socle fiable pour les interactions électroniques. Le CCP aide les concepteurs, les constructeurs et les fournisseurs de systèmes d'identification, d'authentification et d'autorisation en ligne basés sur des normes, et ceux qui souhaitent se fier et faire confiance à des identités numériques établies. L'autorité et la gouvernance spécifiques et applicables des services des entités participantes seront développées grâce à une collaboration et publiées dans des documents spécifiés à l'avenir.

Portée du cadre de confiance pancanadien

Le CCP tire parti des résultats et des accomplissements antérieurs du SCGI grâce à une collaboration avec le secteur économique canadien. Il développe des mécanismes permettant aux participants de l'écosystème de l'identité numérique d'interagir avec intégrité en se basant sur une terminologie, des notions et des spécifications techniques communes. Le CCP est conçu pour convenir aux systèmes d'identification numérique, d'authentification électronique, d'authentifiants en ligne et d'autorisation utilisés pour fournir des services aux entités gouvernementales, aux citoyens, aux partenaires d'affaires et aux clients.

Le CCP étend les résultats et les accomplissements antérieurs du SCGI en collaborant avec le secteur économique canadien pour décrire les mécanismes afin que les participants à l'écosystème de l'identité numérique interagissent d'une façon intègre.

Les citoyens et les consommateurs canadiens, c.-à-d. les utilisateurs finaux, sont les bénéficiaires ultimes de la confiance qui est créée grâce à l'uniformisation des services et à l'imputabilité envers le CCP. Les participants et les exécutants visés du CCP sont des entités gouvernementales, commerciales, sans but lucratif et autres qui offrent et utilisent des services d'identité afin de soutenir leurs activités et programmes.

Le CCP a été créé pour faire de l'écosystème canadien de l'identité numérique une réalité et il servira à déterminer les normes applicables en matière de politiques et de technologie, qui répondent aux besoins définis dans le CCP. Le CCP peut servir à identifier de futurs domaines de collaboration, de développement et d'uniformisation.

Valeur du cadre de confiance pancanadien

Le CCP peut procurer de la valeur sur les plans suivants :

- Représente les points de vue des secteurs public et privé au Canada en ce qui concerne la prestation des services et la pleine participation à l'économie numérique mondiale;
- Définit les rôles, les droits et les responsabilités uniformisés de l'écosystème canadien de l'identité numérique;
- Décrit les pratiques opérationnelles attendues des participants afin de gérer les risques des interactions;
- Permet aux propriétaires de ressources de mieux comprendre les opportunités et les responsabilités lorsqu'ils donnent accès à leurs ressources ou en autorisent l'utilisation ;
- Reconnaît les contextes, ainsi que les exigences uniques et communes des organismes publics et privés;

- Est structuré pour tenir compte des exigences futures du gouvernement et de l'industrie;
- Définit des bases communes pour un écosystème de producteurs et de consommateurs d'identité numérique afin de soutenir l'obtention d'un accès autorisé aux services en ligne.

Fruit de la collaboration des secteurs des services numériques et économique au Canada, le CCP représente l'ensemble des exigences, spécifications, normes, politiques, procédures et critères d'évaluation commerciaux qui ont été convenus. Il établit aussi des exigences, règles et outils de participation, qui permettent aux organisations partenaires de s'entendre plus rapidement en tirant parti d'une compréhension commune des définitions, spécifications et accords de fédération multilatérale ou centralisée.

Structure du cadre de confiance pancanadien

Le CCP consistera en une série de documents connexes, à savoir :

- Aperçu
- Glossaire
- Éléments du cadre de confiance et principaux critères de conformité
- Profils des critères d'interopérabilité technologique et politique
- Processus supplémentaires en matière de gouvernance et d'instructions

Conclusion

Le CCP a été développé selon une approche collaborative entre le DIACC et le SCGI relevant des conseils mixtes du Canada, une tribune formée du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) et du Conseil de la prestation des services du secteur public (CPSSP). Le CCP permet de fournir des solutions innovatrices, sûres, confidentielles et pratiques à tous les Canadiens, qui permettent d'offrir des services modernisés, et qui fait en sorte que le Canada participe pleinement et d'une façon avantageuse à l'économie numérique mondiale.

Le DIACC est une tribune neutre sans but lucratif qui a été créée pour identifier et développer des uniformisations et des innovations qui soutiennent des interactions de confiance basées sur l'identité numérique dans l'intérêt économique et sociétal du Canada.

Le travail accompli précédemment par le CCP soutient la création et la communication d'identités numériques fiables, ancrées dans des sources qui font autorité. Le CCP élargit les résultats et les réalisations antérieures du SCGI en décrivant les mécanismes permettant aux autres participants de l'écosystème de l'identité numérique d'interagir avec une terminologie, des notions et des spécifications communes.

À mesure que le développement du CCP progresse, la communauté du DIACC va mettre sur pied un plan en vue de consulter le grand public pour recueillir des points de vue à étudier. Le DIACC est une tribune neutre sans but lucratif qui a été créée pour identifier et développer des uniformisations et des innovations qui soutiennent des interactions de confiance basées sur l'identité numérique dans l'intérêt économique et sociétal du Canada. Les entités et les organisations qui souhaitent prendre part à ces efforts de collaboration sont invitées à communiquer avec le DIACC pour obtenir plus de renseignements.

À propos du DIACC

Fruit du groupe de travail sur les systèmes de paiement mis sur pied par le gouvernement fédéral, le DIACC est une coalition technologique agnostique sans but lucratif de leaders des secteurs public et privé qui a pour vocation de développer un cadre canadien d'identification et d'authentification numériques afin de permettre au Canada de participer pleinement et en toute sécurité à l'économie numérique mondiale.

Le DIACC a pour objectif d'offrir des débouchés économiques aux citoyens, aux consommateurs et aux entreprises du Canada en fournissant le cadre voulu pour développer un écosystème d'identification et d'authentification numériques à la fois robuste, sécuritaire, évolutif et plus confidentiel, qui va réduire les coûts des gouvernements, des consommateurs et des entreprises tout en favorisant la croissance du PIB.

Les membres du DIACC collaborent en mettant en commun leurs ressources en vue de déterminer et d'élaborer des normes de l'industrie, des études et des validations de principe qui répondent aux exigences commerciales, juridiques, techniques et des politiques en ce qui concerne l'interopérabilité et l'adoption de services d'identité numérique fiables. Le DIACC invite les entités et les organismes du Canada et de l'étranger à participer aux efforts, et il enjoint les intéressés à visiter diacc.ca et à communiquer avec l'équipe pour obtenir plus de renseignements.