Recommandation d'ébauche de modèle de cadre de confiance pancanadien V1.0

Cette ébauche de recommandation a été préparée par le Comité d'experts du cadre de confiance (TFEC) du Digital ID & Authentication Council of Canada (DIACC). Le TFEC est régi par les politiques du DIACC en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'entente de contributeur du DIACC.

Le DIACC prévoit modifier et améliorer cette ébauche de recommandation en fonction des commentaires du public. Les commentaires ouverts ont pour but d'assurer la transparence de l'élaboration et la diversité d'un apport véritablement pancanadien. Les commentaires effectués pendant l'examen seront pris en considération en vue d'être incorporés dans la prochaine ébauche. Le DIACC va regrouper les commentaires afin de montrer d'une façon transparente comment chacun a été traité.

Les prochaines versions du cadre de confiance pancanadien vont étoffer, clarifier et peaufiner le contenu de ce document. L'auditoire ciblé inclut des décideurs qui peuvent être ou non des experts dans la technologie des domaines.

En examinant cette ébauche de recommandation, veuillez tenir compte de ce qui suit :

1. Êtes-vous d'accord avec l'emploi de « représentation numérique » pour faire référence à l'information en cause? Dans la négative, suggérez un autre terme.
2. Le document fait-il un bon équilibre entre une perspective à long terme et l'état actuel des choses?
3. Le document fournit-il assez de détails pour donner une bonne vue d'ensemble, en sachant que les composantes et les profils du cadre de confiance pancanadien aborderont de nombreux aspects considérés comme débordant de la portée de ce document?
4. Les processus de confiance et les descriptions qui y sont associées couvrent-ils tous les principaux processus qui devraient intéresser le cadre de confiance?

Table des matières

1. Introduction

À mesure que la prestation des services devient de plus en plus numérique, les particuliers, les gouvernements et les entreprises constatent qu'il leur faut faire confiance aux renseignements sur ceux avec qui ils interagissent; que la personne à l'autre bout d'une connexion est bien celle qu'elle prétend être ou que les renseignements à son sujet sont exacts. Les fournisseurs de services et leurs clients ont aussi besoin de savoir que ces renseignements sont protégés lorsqu'ils circulent dans les réseaux, franchissent les limites organisationnelles et sont entrés dans des documents juridiques en guise de preuve de transaction. C'est notamment le cas des transactions de grande valeur ou hautement sensibles qui sont actuellement difficiles à effectuer d'une manière numérique, entre autres certaines opérations financières, les achats immobiliers, l'envoi de réponses à des demandes de propositions, l'accès aux dossiers médicaux, l'achat de marchandises contrôlées en ligne et la gestion des prestations gouvernementales pour le compte d'un proche âgé.

En réponse à cela, les gouvernements et les industries du monde entier sont en train de développer des cadres pour promouvoir des environnements de confiance en ligne. Ces cadres sont habituellement un ensemble d'exigences commerciales et techniques vérifiables s'appliquant aux processus. Les exigences juridiques peuvent aussi être mentionnées dans le cadre. Habituellement appelés cadres de confiance, ils permettent des interactions sûres et privées entre les parties et à l'échelle de divers réseaux et organismes. Bien des réseaux actuels dans les domaines de la finance, de la gestion de la chaîne d'approvisionnement et de l'identité numérique sont basés sur une certaine forme de cadre de confiance. Les cadres de confiance sont plus évolutifs et plus transparents, et, sans doute, une façon de créer un environnement de confiance plus économique qu'une série d'ententes privées entre une poignée d'organisations. Ils présentent en outre l'avantage de fournir des améliorations et des catalyseurs qui peuvent accélérer la cadence et augmenter le taux d'adoption des systèmes partagés par rapport à d'autres approches.

Le cadre de confiance pancanadien assure des représentations numériques fiables (c.-à-d. identités, attributs, relations) des personnes et autres types d'entités au Canada.

Étant donné que le cadre de confiance pancanadien est destiné à être utilisé par une série de parties prenantes dans différentes communautés, n'importe quelle partie prenante peut adopter

les exigences du cadre. Elle démontre ainsi une volonté de se conformer aux conventions acceptées, ce qui se traduit par des niveaux accrus de confiance et d'assurance notamment parmi les clients et les partenaires d'affaires de la partie prenante.

1.1 À propos de ce document

Ce document vise à fournir un aperçu très général du modèle de cadre de confiance pancanadien. Il inclut une récapitulation des renseignements contextuels ainsi que des buts et objectifs du cadre.

Il fournit aussi un aperçu des domaines fonctionnels principalement visés par le cadre de confiance pancanadien. L'aperçu (voir la section 5) donne une idée générale des représentations numériques intéressant le cadre, ainsi que des divers processus intervenant dans la création, la gestion et l'utilisation de ces objets numériques.

Les composantes et les profils individuels du cadre de confiance pancanadien fournissent des descriptions détaillées des processus mis en évidence dans ce document.

Ce document s'adresse notamment aux :

- membres de la communauté de l'identité numérique dans les secteurs privé et public (notamment les organismes de réglementation et de normalisation) – en tant que parties prenantes et contributeurs clés du cadre de confiance pancanadien;
- fournisseurs de technologie et de services d'identité numérique – pour comprendre où ils se situent dans le cadre de confiance pancanadien, afin de les aider à définir des exigences pour leurs produits et services, et d'évaluer l'intégrité de leurs processus;
- fournisseurs et consommateurs de services – pour déterminer l'intérêt d'employer des solutions et processus de confiance en matière d'identité numérique pour les interactions en ligne.

2. À propos du cadre de confiance pancanadien

2.1 Contexte

La technologie et les services qui permettent aux personnes d'interagir avec les gouvernements, les entreprises et entre elles grâce à la commodité et à l'efficacité numériques offrent un potentiel énorme pour l'innovation et le développement social et économique. Le fait de pouvoir se fier aux renseignements sur les participants lors de ces interactions est une condition préalable essentielle pour saisir ce potentiel. Le cadre de confiance pancanadien soutient cet aspect des services numériques en tant que cadre fiable fournissant des processus uniformes et vérifiables pour la création, la gestion et l'utilisation des représentations numériques des personnes et autres entités.

Mais l'utilisation des représentations numériques doit, pour être concluante, déborder d'un nombre limité de relations et des intégrations ponctuelles limitées. Comme la plupart des parties

prenantes se focalisent principalement sur les clients, les consommateurs et les utilisateurs, des représentations numériques de ces entités doivent être acceptées entre les prestataires de services, les secteurs économiques, les ordres de gouvernement et les territoires de compétence. Dans la pratique, cela signifie que les particuliers et autres participants doivent pouvoir utiliser et gérer les renseignements qui existent sur eux dans de multiples contextes et l'ensemble de l'économie.

Un haut niveau d'interopérabilité exige une confiance mutuelle. Les fournisseurs de services doivent savoir avec qui ils interagissent d'une manière numérique. Les consommateurs de services, les particuliers et autres doivent faire confiance à l'identité des services avec lesquels ils interagissent. Sans interopérabilité et confiance, le Canada risque de perpétuer les barrières organisationnelles, politiques et techniques qui ont :

- contribué à un excès de procédures de vérification, d'inscriptions, de comptes, de mots de passe, de profils d'utilisateurs et de systèmes nécessaires pour tout administrer;
- entravé les efforts de modernisation qui favorisent l'innovation, et améliorent l'expérience, l'efficacité et l'efficience liées aux services.

En outre, les Canadiens s'attendent à ce que leur écosystème de l'identité numérique fonctionne d'une manière transparente, en étant équitable pour tous et en soutenant les droits au respect de la vie privée dès la conception. Ils veulent avoir un avis indiquant clairement et d'une façon explicite pourquoi et comment les renseignements à leur sujet sont recueillis, gérés et divulgués.

2.2 But

Le cadre de confiance pancanadien a pour but de permettre et de soutenir la mise sur pied d'un écosystème canadien de l'identité numérique qui est innovateur et sécuritaire, qui renforce la confidentialité—et qui respecte les droits fondamentaux de la personne à l'ère numérique—à l'échelle de l'économie. À cet égard, le cadre de confiance pancanadien cherche à faciliter la migration des interactions en personne traditionnelles ou complexes vers des interactions numériques qui placent les personnes au centre de l'écosystème de l'identité numérique, tout en reconnaissant que les processus d'affaires analogiques vont continuer d'exister quelque temps.

Afin de soutenir le développement d'un écosystème canadien de l'identité numérique, le cadre de confiance pancanadien adopte une approche pancanadienne de l'identité numérique, qui est fondée sur une acceptation générale des principes et des normes pour la conception de solutions destinées à être utilisées par tous les Canadiens.

Le cadre de confiance pancanadien soutient le développement d'un écosystème canadien de l'identité en :

- assurant la fiabilité de cet écosystème – il donne le contrôle aux consommateurs tout en favorisant un environnement équitable, innovateur et compétitif pour les participants;

- mettant l'accent sur la transparence et la confidentialité en ce qui concerne l'utilisation et la divulgation des renseignements personnels;
- soutenant l'inclusion des participants qui offrent un large éventail de services;
- identifiant les normes existantes en matière de politiques et de technologie qui s'appliquent à l'écosystème;
- maintenant une perspective à long terme et en révélant les futurs domaines de collaboration, de développement et d'uniformisation.

2.3 Objectifs

Le cadre de confiance pancanadien reconnaît qu'une approche uniforme du développement de l'écosystème peut être réalisée en mettant en œuvre d'une manière uniforme des normes acceptées à grande échelle, et ce, en dépit des dépendances et des différences entre les territoires de compétences, les industries et les participants individuels. Par conséquent, les objectifs du cadre de confiance pancanadien visent surtout à assurer la fiabilité de l'écosystème canadien de l'identité numérique en :

1. définissant les rôles et fonctions des participants au sein de l'écosystème. Le présent document décrit ces rôles, fonctions et processus connexes en termes généraux comme modèle pour le cadre de confiance pancanadien. Les composantes et profils du cadre de confiance pancanadien fournissent au besoin des exigences et des lignes directrices plus détaillées;
2. facilitant les interactions à l'intérieur de l'écosystème en définissant des exigences et lignes directrices qui établissent un niveau de confiance pour les processus exécutés par les participants à l'écosystème. Les composantes du cadre de confiance pancanadien fournissent des descriptions détaillées et des spécifications techniques de ces exigences.

2.4 Portée

Le succès de l'écosystème canadien de l'identité numérique dépendra des utilisateurs, lesquels doivent faire confiance au système et toujours le contrôler. Le cadre de confiance pancanadien établit un cadre fiable à l'intérieur duquel des solutions innovatrices peuvent être développées, mesurées et reconnues. Il définit les critères de conformité nécessaires pour que les participants à l'écosystème de l'identité puissent interagir avec assurance.

Comme c'est le cas pour d'autres cadres fiables, le cadre de confiance pancanadien ne définit pas un système ou un produit en soi. Il ne s'occupe pas non plus des aspects commerciaux de l'écosystème, entre autres les modèles commerciaux, la tarification, la responsabilité, les droits de propriété intellectuelle et l'assurance.

2.5 Principes directeurs

Le cadre de confiance pancanadien atteint ses buts et objectifs en partie grâce à des normes et des lignes directrices qui reflètent les principes directeurs suivants :

1. **Soutenir des solutions robustes, sécuritaires et évolutives** – L'écosystème canadien de l'identité numérique doit être suffisamment robuste pour offrir en tout temps une sécurité, une disponibilité et une accessibilité.
2. **Mettre en œuvre, protéger et améliorer le respect de la vie privée dès la conception** – Les outils visant à améliorer le respect de la vie privée permettent à une personne de gérer ses renseignements et l'emploi qui en est fait. Ces outils peuvent servir notamment à soutenir le « droit à l'oubli » d'un utilisateur (lorsque c'est approprié dans le contexte législatif du participant au cadre fiable).
3. **Être inclusif et ouvert, et répondre aux besoins généraux des parties prenantes** – Les services et outils de l'écosystème de l'identité numérique doivent être abordables et uniformisés, et créer de la valeur pour les utilisateurs dans le but d'être adoptés à grande échelle et de procurer des avantages à tous les Canadiens.
4. **Faire preuve de transparence dans la gouvernance et le fonctionnement** – Les Canadiens doivent être convaincus que les services offerts dans l'écosystème canadien de l'identité numérique vont respecter et satisfaire leurs besoins et attentes.
5. **Procurer choix, contrôle et commodité aux Canadiens** – Les services sont basés sur le principe voulant que les personnes puissent choisir l'information à partager et les services à utiliser et en provenance de quels pays, et sont informées des avantages et conséquences possibles des identités numériques.
6. **Tirer parti des protocoles basés sur des normes ouvertes** – Le fait d'utiliser des normes ouvertes et les meilleures pratiques applicables pour l'écosystème canadien de l'identité numérique fournit une protection contre l'obsolescence, assure une interopérabilité, et favorise un marché de solutions dynamique et compétitif.
7. **Maintenir une interopérabilité internationale** – L'interopérabilité et l'uniformisation de la technologie et des politiques à l'échelle globale sont essentielles pour le monde branché d'aujourd'hui. De même que les gabarits uniformisés d'écartement des voies ferrées favorisent la circulation des personnes et l'acheminement des marchandises entre les pays, l'interopérabilité et l'uniformisation de la technologie et des politiques permettent aux services numériques de communiquer et d'abaisser les coûts tout en augmentant les possibilités d'innovation.
8. **Être rentable et ouvert aux forces de la concurrence** – C'est essentiel que l'écosystème de l'identité numérique respecte les contraintes budgétaires d'aujourd'hui et de demain. Le fait de s'assurer que l'écosystème est ouvert à la concurrence représentant de multiples secteurs économiques, où chacun joue différents rôles, va contribuer à abaisser les coûts pour toutes les parties prenantes et à accroître l'innovation.
9. **Soutenir une évaluation, une vérification et une application indépendantes** – Pour que les Canadiens fassent confiance à un écosystème de l'identité numérique, il doit y avoir des mécanismes de contrôle en place. Les évaluations permanentes, fonctionnellement indépendantes et tierces permettent de s'assurer que les parties intéressées à l'écosystème se conforment aux exigences du cadre de confiance.
10. **Réduire le transfert de données entre les sources et éviter de créer de nouveaux répertoires de renseignements sur l'identité** – Les utilisateurs des services de l'écosystème de l'identité numérique ne devraient avoir à fournir qu'un minimum de renseignements personnels lors d'une transaction.

3. Structure du cadre de confiance pancanadien

Le cadre de confiance pancanadien comprend l'aperçu du modèle (décrit dans le présent document) et les éléments suivants :

1. Composantes du cadre de confiance pancanadien
2. Critères de conformité
3. Processus de confiance
4. Profils du cadre de confiance pancanadien

Chacun de ces éléments est décrit dans cette section.

3.1 Composantes du cadre de confiance pancanadien

Les composantes du cadre de confiance pancanadien définissent les processus de confiance et les critères de conformité pour des aspects spécifiques du cadre de confiance pancanadien. Elles précisent, étoffent et fournissent des détails supplémentaires qui ne sont pas présentés dans l'aperçu du modèle.

La composante avis et consentement du cadre de confiance pancanadien, par exemple, définit un ensemble de processus utilisés pour formuler une déclaration et obtenir un consentement sur cette déclaration de la part d'une personne autorisée à le faire. Les exigences contenues dans la composante respect de la vie privée du cadre de confiance pancanadien font en sorte que les systèmes suivent des pratiques qui respectent la vie privée, en s'assurant que les renseignements personnels sont convenablement recueillis, protégés, tenus à jour et, lorsqu'on le demande, détruits s'ils font partie de l'écosystème de l'identité numérique.

Les composantes du cadre de confiance pancanadien visent avant tout à spécifier une base commune de critères de conformité et de processus de confiance. Les participants peuvent élargir et raffiner la base par le biais des profils du cadre de confiance pancanadien.

3.2 Critères de conformité

Des critères de conformité sont appliqués en guise de norme ou utilisent des normes et/ou des lignes directrices existantes pour la prestation de processus de confiance dans les secteurs public et privé. Les critères de conformité sont les exigences, spécifications, recommandations et lignes directrices qui constituent une norme pour des processus spécifiques. Les participants peuvent utiliser ces critères pour informer la conception et le développement de leurs produits et services.

Les critères de conformité du cadre de confiance pancanadien visent à compléter les lois et règlements existants; on s'attend à ce que les participants à l'écosystème de l'identité numérique se conforment aux exigences et aux règlements applicables en vertu de la loi dans leurs territoires de compétence.

S'alignant sur les principes directeurs pour tirer parti des normes ouvertes et maintenir une interopérabilité nationale et internationale, le cadre de confiance pancanadien accepte que :

- Les normes et les spécifications existantes puissent être incorporées dans les critères de conformité du cadre de confiance pancanadien par référence. Cela assure une

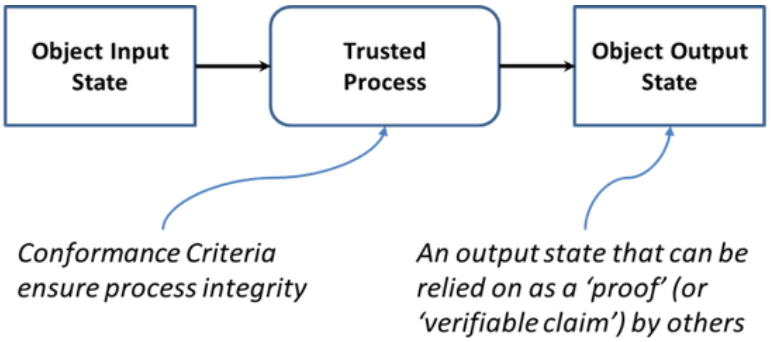
compatibilité à grande échelle, et réduit la duplication et le chevauchement du contenu et des spécifications techniques.

- Lorsque des normes existantes sont incorporées dans le cadre de confiance pancanadien, on le fait avant en pensant à une mise en œuvre au Canada. Cela peut obliger à interpréter et à appliquer des normes internationales dans un contexte canadien (p. ex., pour des questions de législation du respect de la vie privée ou de souveraineté des données au Canada). Les normes existantes peuvent être incorporées dans les composants de base ou les profils du cadre de confiance pancanadien.

Les critères de conformité du cadre de confiance pancanadien sont développés dans le but de s'assurer que la conformité aux divers critères peut être évaluée pour déterminer la fiabilité d'un processus donné.

3.3 Processus de confiance

Un processus est une activité commerciale ou technique (ou un ensemble de telles activités) qui transforme une condition d'entrée en condition de sortie. Un processus commercial ou technique qui est conçu comme un processus de confiance est évalué selon les critères de conformité définis dans les composantes et profils du cadre de confiance pancanadien. La figure 1 illustre le modèle de processus de confiance selon lequel un processus de confiance transforme l'*état d'entrée* d'un objet en *état de sortie*.



État d'entrée d'un objet Processus de confiance État de sortie d'un objet

Les critères de conformité assurent l'intégrité du processus

État de sortie auquel d'autres peuvent se fier comme « preuve » (ou « revendication vérifiable »)

Figure 1. Modèle de processus de confiance

Les processus de confiance sont essentiels pour assurer l'intégrité globale de l'écosystème de l'identité numérique et pour celle du cadre de confiance. L'intégrité d'un processus de confiance est fondamentale, car beaucoup de participants se fient aux extrants d'un processus de confiance – à travers les frontières territoriales et sectorielles, et à court et long terme. Le cadre de confiance pancanadien assure l'intégrité d'un processus de confiance grâce à des critères de conformité convenus et bien définis qui favorisent une méthode d'évaluation transparente et

basée sur des preuves. Cette évaluation explicite contraste avec de nombreux processus analogiques existants auxquels on ne fait confiance que dans la mesure où ils sont adoptés à grande échelle et à long terme.

Un processus commercial ou technique existant peut être conçu comme un processus de confiance assujetti aux critères de conformité, au processus d'évaluation et à la certification définis par le cadre de confiance pancanadien. Par exemple, des programmes ou services existants ont généralement des processus intégrés liés à l'identité, parfois appelés preuve ou inscription de l'identité. Les processus conçus à l'origine pour fonctionner dans un contexte particulier (p. ex., inscription d'une personne à un service, délivrance d'un permis de conduire) peuvent être mis à profit et tenus pour fiables en tant que processus de confiance à l'intérieur du cadre de confiance pancanadien. Cela se fait en associant les processus (ou sous-processus) existants dans les définitions des processus de confiance. Une fois cartographiés, ces processus peuvent être évalués et certifiés en utilisant les critères de conformité définis qui sont associés aux processus de confiance correspondants.

3.4 Profils du cadre de confiance pancanadien

Le cadre de confiance pancanadien, qui a une très grande envergure, vise à fournir une norme de base à l'échelle de l'économie canadienne dans le contexte des secteurs public et privé. Les profils du cadre de confiance pancanadien permettent aux industries, aux secteurs de l'économie et à d'autres communautés ayant des intérêts communs de déterminer comment le cadre de confiance pancanadien va s'appliquer dans des contextes et cas d'utilisation spécifiques ou répondre à des besoins commerciaux particuliers.

Les profils du cadre de confiance pancanadien permettent aux participants d'adapter les critères de conformité de base à des exigences ou applications spécifiques. Cela pourrait consister, sans s'y limiter, à :

- exiger une conformité obligatoire à tous les critères de conformité;
- définir des niveaux d'assurance;
- définir des sources de preuves acceptables;
- spécifier des technologies acceptables;
- étendre certains critères de conformité (p. ex., exiger des processus d'audit et de journalisation supplémentaires).

4. Principes clés

Le cadre de confiance pancanadien est basé sur un petit nombre de principes clés. Il y a tout d'abord l'idée selon laquelle la confiance est établie et peut être évaluée à de multiples points d'une chaîne de processus qui créent et utilisent des représentations numériques des personnes et autres entités.

Les principes clés peuvent être résumés comme suit :

- Les participants à l'écosystème de l'identité numérique créent, utilisent et/ou gèrent des **représentations numériques**;

- Lorsqu'ils traitent des représentations numériques, les participants assument un ou plusieurs **rôles** dans l'écosystème;
- Chaque rôle accomplit un certain nombre de fonctions qui sont constituées d'un ou de plusieurs **processus de confiance;**
- La conformité à des **critères de conformité** spécifiques définissant les processus de confiance.

Les sections suivantes fournissent une description de ces principes dans le contexte du cadre de confiance pancanadien.

4.1 Représentations numériques

Une représentation numérique est un ensemble de données électroniques faisant référence à n'importe quel type d'entité pouvant être assujetti à des lois, politiques ou règlements dans un contexte et pouvant avoir certains droits, devoirs et obligations. Les représentations numériques sont destinées à être associées à des modèles d'acteurs véritables, comme des personnes et des organisations bénéficiant de la mise en œuvre ou de l'utilisation du cadre de confiance pancanadien.

Des représentations numériques peuvent être créées et gérées pour des entités autres que des personnes :

1. **Personne** – Individu, être humain. Il peut s'agir des résidents d'un territoire (pays, province, etc.), des clients d'une entreprise ou de particuliers.
2. **Organisation** – Entité dont l'existence est établie par une convention ou des statuts juridiques. Cela inclut notamment des entreprises (propriétaires uniques, partenariats, sociétés), organismes gouvernementaux, coopératives et œuvres de bienfaisance enregistrées.
3. **Machine** – Logiciels et matériel (agissant potentiellement comme agents intelligents). Règle générale, les machines qui agissent pour le compte d'une personne ou d'une organisation ne sont pas des identités autonomes en soi. À mesure que le cadre de confiance pancanadien évoluera, la technologie future résultant de la création de machines qui ont un certain degré d'autonomie pourrait entraîner des critères de conformité et des processus de confiance spécifiques à ce genre d'entités.

Le développement de critères de conformité et de processus de confiance étroitement associés aux « personnes » est la priorité pour les composantes du cadre de confiance pancanadien. Les critères liés aux « machines » sont moins prioritaires dans le développement du cadre de confiance pancanadien.

4.2 Rôles des participants

Les représentations numériques ont un cycle de vie qui commence avec la création, passe ensuite à l'utilisation active (pendant laquelle les données peuvent changer, être ajoutées ou supprimées, etc.) puis à l'archivage et, dans certains cas, à la destruction. La confiance est créée pendant l'exécution des processus clés tout au long du cycle de vie. Le cadre de confiance pancanadien définit les normes et lignes directrices pour ces processus.

Les processus clés d'un écosystème de l'identité numérique se divisent en trois grandes fonctions qui consistent à :

1. Créer et gérer les représentations numériques;
2. Utiliser les représentations numériques;
3. Activer les systèmes d'identité numérique.

Les participants à l'écosystème exécutent ces fonctions. Il s'agit de particuliers, d'entreprises ou d'organismes à but non lucratif et (de plus en plus) de machines. Dans le modèle de cadre de confiance pancanadien, les participants qui exécutent des processus clés dans le cycle de vie des représentations numériques jouent un ou plusieurs des rôles définis ci-dessous dans le contexte du cadre de confiance pancanadien.

	Fonction	**Rôle**	**Description**
334-b	Créer et gérer les représentations numériques	Fournisseurs d'identités	Participants qui créent et gèrent des identités. Ils sont parfois appelés fournisseurs de services d'identité ou émetteurs d'identités. Dans certains cas, le sujet est celui qui crée et gère sa propre identité.
334-c		Fournisseurs de justificatifs	Participants qui créent et gèrent des justificatifs. Ils sont parfois appelés fournisseurs d'attributs.
334-d		Fournisseurs d'authentificateurs	Participants qui créent et gèrent des authentificateurs. Ils sont parfois appelés fournisseurs de services de justificatifs. À ne pas confondre avec les fournisseurs de justificatifs du cadre de confiance pancanadien. Voir la section 5.1.2 pour les détails.
334-e	Utiliser les représentations numériques	Parties utilisatrices	Participants qui se fient aux représentations numériques créées et gérées par d'autres participants.
334-f		Sujets de la représentation numérique	Entité que la représentation numérique représente. Il s'agit habituellement de l'entité à qui la représentation numérique est émise. Dans bien des cas, le sujet d'une représentation numérique remplira des fonctions et/ou représentations explicites. Il peut aussi y avoir des fonctions implicites exécutées par le sujet dans le contexte de l'écosystème de l'identité numérique. C'est le cas, par exemple, des fonctions associées à une « motivation pour récupérer » une représentation numérique quand des problèmes ou des événements suspects sont décelés.

334-g	Activer les systèmes d'identité numérique	Fournisseurs d'infrastructures	Participants qui fournissent l'infrastructure physique et électronique nécessaire pour permettre des interactions numériques.
334-h		Évaluateurs	Participants qui évaluent la conformité d'autres participants au cadre de confiance pancanadien.

Étant donné la variété de modèles techniques, de services et commerciaux qui définissent l'écosystème, les rôles peuvent être remplis par de multiples participants dans un contexte donné ou un seul participant peut jouer plusieurs rôles (p. ex., être une partie utilisatrice et un fournisseur de justificatifs).

Le cadre de confiance pancanadien permet aussi d'abaisser les barrières donnant accès à l'écosystème de l'identité; autrement dit, certaines organisations peuvent réutiliser la technologie mise en place par les participants au cadre de confiance pancanadien, sans toutefois intégrer complètement le cadre de confiance pancanadien pour des raisons qui leur sont propres (p. ex., coût ou retards de l'évaluation de conformité, ce qui pourrait représenter un fardeau pour les entreprises en démarrage).

Rôle de gouvernance

En tant que cadre fiable destiné à être adopté à grande échelle, le cadre de confiance pancanadien définit des rôles de gouvernance pour certaines parties prenantes de l'écosystème. Les participants qui jouent ces rôles sont chargés de concevoir et de maintenir les diverses composantes du cadre de confiance pancanadien et d'aider à s'assurer qu'elles sont adoptées de manière uniforme. Les rôles de gouvernance peuvent aussi être étendus à la gouvernance de l'utilisation et de l'application de l'écosystème numérique du cadre de confiance pancanadien.

5. Aperçu fonctionnel

Cette section présente les fonctions et les processus liés à l'identité qui interviennent dans le cadre de confiance pancanadien.

5.1 Création et gestion des représentations numériques

Les fonctions dans cette catégorie consistent à prouver ou à vérifier l'identité ou les caractéristiques d'une entité réelle (p. ex., une personne) et à créer une représentation numérique pour cette entité. Une fois créée, une représentation numérique est gérée par le biais de processus qui permettent de mettre à jour, de supprimer et de revérifier au besoin les données – pour faire en sorte que la représentation reste à jour et exacte.

Actuellement, le cadre de confiance pancanadien définit trois types de représentation numérique :

1. **Identité** – Information qui permet d'identifier une entité unique (p. ex., renseignements personnels), seule ou avec des renseignements connexes qui la justifient. Exemples pour des personnes : nom, date de naissance, déclaration de naissance (à l'avenir) ou biométrie. Exemples pour des machines : numéro de série, certificat numérique de confiance ou adresse MAC réseau.
2. **Justificatif** – Information décrivant les attributs ou propriétés d'une entité. Cette information peut exister en soi (p. ex., comme justificatif qui ne renferme pas de renseignements personnels, seulement un identifiant unique faisant partie d'une chaîne) ou être reliée à des renseignements personnels. Exemples : niveaux d'études (p. ex., diplôme universitaire en génie), permission d'utiliser un véhicule (p. ex., permis de conduire), niveau de revenu ou statut d'employé dans une entreprise donnée.
3. **Authentificateur** – Données émises à une entité qui permettent d'utiliser des systèmes à accès restreint ou protégés. Exemples d'authentificateurs ordinaires : combinaisons nom d'utilisateur-mot de passe et jetons d'accès qui génèrent des codes d'utilisation limitée.

À mesure que le cadre de confiance pancanadien évoluera, ces représentations pourraient s'étendre à des types d'entités comme des actifs et des contrats (c.-à-d., actifs numériques et contrats intelligents).

5.1.1 Identités

Les identités représentent des entités distinctes au sein de l'écosystème, des parties souhaitant interagir entre elles. Les identités sont essentiellement des renseignements qui identifient d'une façon unique une entité dans un contexte donné (p. ex., nom juridique et identifiant enregistrés pour une entreprise). Dans le cas des personnes, les identités démontrent qu'elles sont bien celles qu'elles affirment être.

Dans le contexte du cadre de confiance pancanadien, les **fournisseurs d'identité** sont responsables de créer et de gérer les identités numériques qui relèvent d'eux. Ils remplissent des fonctions qui comprennent des processus visant à s'assurer que :

- une entité est connue pour être réelle et identifiable, et n'est pas une création frauduleuse;
- une entité est unique dans une population (p. ex., citoyens, clients, sociétés) de sorte qu'il ne soit pas possible de créer et d'utiliser d'une manière frauduleuse de multiples identités numériques;
- l'identité numérique représente l'entité à qui elle a été attribuée.

Ces fonctions fournissent une base à partir de laquelle des représentations numériques peuvent être créées; elles permettent de créer un « dossier » ou « compte » pour l'entité. D'autres participants peuvent créer des justificatifs et des authentificateurs associés à ce dossier.

Types d'identités

Le cadre de confiance pancanadien définit deux types de renseignements nécessaires pour établir une identité numérique :

388-a

Type	Description	Émis à	Émis par	Exemples

388-b	De base	Établit l'existence et la représentation numérique d'entités réelles légalement reconnues.	Personnes, organisations	Certains organismes du secteur public ayant pour mandat de créer et gérer des identités légalement acceptées (p. ex., registres, agences de citoyenneté et d'immigration).	Ensemble de données attestant de l'identité du sujet, comme l'équivalent numérique d'un certificat de naissance ou des statuts constitutifs.
388-c	Contextuel	Établit l'identité et la représentation numérique d'entités dans des contextes ou cas d'utilisation spécifiques. Ce type inclut les identifiants qui sont autoémis ou attribués.	Personnes, organisations, machines	Fournisseurs d'identité publics, privés et sans but lucratif.	Identité numérique des entreprises, identité numérique d'un corps professionnel. Identité sur les réseaux sociaux, identité autoattribuée. Dans le cas de machines, il pourrait s'agir d'identifiants numériques attribués par des fabricants ou des agents intelligents

465 **Processus habituellement exécutés par des fournisseurs d'identité**

	Processus	**Description**
389-b	Résolution de l'identité	Établissement du caractère unique d'un sujet au sein d'une population de programmes ou services par l'utilisation des renseignements sur l'identité. Un programme ou service définit ses exigences en matière de résolution de l'identité sous la forme d'attributs de l'identité; il spécifie l'ensemble d'attributs de l'identité nécessaires pour résoudre l'identité au sein de sa population.
389-c	Établissement de l'identité	Création d'un dossier d'identité faisant autorité, auquel d'autres peuvent se fier pour des programmes, services et activités ultérieurs.

389-d	Entretien de l'identité	Processus consistant à s'assurer que les renseignements sur l'identité sont exacts, complets et à jour, tel qu'exigé. L'entretien de l'identité inclut aussi la *notification de l'identité*, autrement dit la divulgation des renseignements sur l'identité déclenchée par un changement dans les renseignements sur l'identité (p. ex. événement vital ou important dans la vie) ou une indication comme quoi les renseignements sur l'identité ont été exposés à un facteur de risque. Cela peut être fonction du moment ou de l'événement.

5.1.2 Justificatifs

Les justificatifs sont des représentations numériques qui fournissent des renseignements sur les attributs ou propriétés d'une entité. Ils contiennent généralement plus de renseignements que ce qui est nécessaire pour identifier une entité individuelle unique. Un justificatif inclut un ou plusieurs identifiants qui peuvent être des pseudonymes et des attributs vérifiés par l'émetteur du justificatif.

Un justificatif peut être quelque chose de simple qui confirme l'âge d'une personne ou le statut d'enregistrement d'une entreprise dans une province donnée. Il peut aussi être plus complexe et représenter des relevés de notes universitaires, des historiques d'emploi ou un poste dans une organisation. Dans le cas des personnes, les justificatifs permettent de confirmer, par exemple, si elles sont légalement autorisées à acheter des marchandises en ligne ou si elles répondent aux exigences nécessaires pour recevoir ces prestations gouvernementales.

Les justificatifs sont utilisés par les fournisseurs de services et les parties utilisatrices pour s'assurer que les caractéristiques spécifiques de l'entité en question (p. ex., âge pour acheter un produit financier) sont vraies. Dans certains cas d'utilisation, l'existence des justificatifs et leur utilisation peuvent fournir une empreinte ou preuve numérique de vie pouvant aider à prouver l'identité et à évaluer et atténuer les risques.

Un justificatif n'est pas synonyme d'un nom d'utilisateur et d'un mot de passe ou d'un mécanisme similaire utilisé pour contrôler l'accès à un système géré. Dans le contexte du cadre de confiance pancanadien, le nom d'utilisateur et le mot de passe attribués à une personne pour accéder à un site Web spécifique, par exemple, est appelé un *authentificateur*.

Dans le contexte du cadre de confiance pancanadien, les **fournisseurs de justificatifs** sont chargés de créer et de gérer les justificatifs. Ils conçoivent et fournissent des fonctions qui sont des processus visant à s'assurer que :

- les justificatifs sont émis (ou liés) au bon sujet;
- les justificatifs sont révoqués ou suspendus si et quand nécessaire;
- les renseignements enregistrés dans les justificatifs sont à jour et exacts.

Compte tenu de la façon dont les justificatifs sont enregistrés et gérés, les fournisseurs peuvent aussi être responsables des processus visant à s'assurer que :

- les justificatifs peuvent être divulgués au besoin et selon des critères de conformité spécifiés;
- les parties utilisatrices peuvent vérifier les renseignements contenus dans un justificatif;

- les parties utilisatrices peuvent vérifier le statut des justificatifs (p. ex., si un justificatif a été révoqué ou invalidé ou non).

Types de justificatifs

Le cadre de confiance pancanadien définit deux types de justificatifs qui fournissent chacun des renseignements spécifiques :

	Type de justificatif	Description
421-b	Attribut	Justificatif qui fournit un ou plusieurs renseignements sur une seule entité. Exemples : Justificatif simple émis par une province, qui contient un seul renseignement attestant l'âge de l'entité. Justificatif simple attestant le niveau d'autorisation de sécurité de l'entité. Justificatif attestant qu'un certain numéro de téléphone mobile est attribué au combiné de l'entité. Justificatif plus complexe comme un relevé universitaire comprenant des données qui identifient les cours suivis par un étudiant.
421-c	Relations	Justificatif qui atteste qu'une entité est associée, affiliée ou autrement liée d'une certaine façon à une deuxième entité. Exemple : justificatif émis par le registraire d'une entreprise, qui atteste qu'une personne est un dirigeant de société et justificatifs émis par la société à ses employés pour prouver qu'ils travaillent pour la compagnie. Une délégation de pouvoirs est un type particulier de relation. Ces justificatifs attestent qu'une entité a délégué certains droits, privilèges, pouvoirs, etc. à une deuxième entité. Exemple : justificatif simple attestant qu'un dirigeant de société a délégué des pouvoirs financiers à une entité.

Processus habituellement accomplis par des fournisseurs de justificatifs

	Processus	Description
422-b	Émission d'un justificatif	Processus pendant lequel un justificatif est créé, attribué à un sujet (c.-à-d., une personne, une organisation, une application ou un appareil) et facultativement liée à un ou plusieurs authentificateurs. Les authentificateurs peuvent servir ensuite à prouver qu'un justificatif fait référence au même sujet initialement lié au justificatif.
422-c	Association identité-justificatif	Processus consistant à associer des justificatifs à un acteur attribué.
422-d	Entretien du justificatif	Le processus inclut des activités faisant partie du cycle de vie comme la mise à jour des détails des justificatifs. Ce processus est habituellement amorcé par le sujet, mais il peut l'être également par un administrateur de système ou automatiquement par le système.

422-e	Suspension du justificatif	Ce processus suspend un justificatif émis. Cela peut être déclenché par le sujet (p. ex. mot de passe oublié) ou le système (p. ex., blocage par suite d'une succession d'authentifications ayant échoué, d'une inactivité, d'une activité suspecte, etc.). Cela empêche de passer un justificatif suspendu à une partie utilisatrice, ce qui permet de s'assurer que l'accès est refusé au sujet.
422-f	Récupération du justificatif	Ramène un justificatif suspendu à un état utilisable (c.-à-d. justificatif émis). Le processus peut être déclenché par le sujet, l'administrateur de système ou automatiquement par le système.
422-g	Révocation du justificatif	Fait en sorte qu'un justificatif soit désactivé ou supprimé d'une façon permanente. Une fois révoqué, le justificatif ne peut plus être utilisé. Le processus peut être initié par le sujet, l'administrateur de système ou automatiquement par le système.
422-h	Authentification du justificatif	Vérifie qu'un sujet contrôle le justificatif qu'il a émis.

504 5.1.3 Authentificateurs

505 Les authentificateurs sont des données servant à accéder à des systèmes gérés ou protégés
506 (p. ex., site Web d'une institution financière). Un authentificateur peut être une simple
507 combinaison nom d'utilisateur-mot de passe ou un objet plus complexe comme un jeton d'accès
508 ou des données biométriques.

509 Dans le contexte du modèle de cadre de confiance pancanadien, le terme « authentificateur »
510 n'est pas synonyme de « justificatif ».

511 Les **fournisseurs d'authentificateurs** sont responsables de créer et de gérer les
512 authentificateurs. Ils remplissent des fonctions qui assurent la gestion du cycle de vie de
513 l'authentificateur (notamment les processus d'émission, de suspension, de récupération,
514 d'entretien et de révocation des authentificateurs).

515 **Processus généralement exécutés par les fournisseurs d'authentificateurs**

431-a	**Processus**	**Description**
431-b	Émission de l'authentificateur	Processus pendant lequel un authentificateur est créé et attribué ou lié à un sujet (c.-à-d., une personne, une organisation, une application ou un appareil) et lié à un ou plusieurs authentificateurs.
431-c	Association identité-authentificateur	Processus consistant à associer des authentificateurs à un acteur attribué.

431-d	Entretien de l'authentificateur	Le processus inclut des activités liées au cycle de vie comme la suppression d'authentificateurs, le fait de lier de nouveaux authentificateurs et de les mettre à jour (p. ex., changement de mot de passe, mise à jour des questions et réponses de sécurité). Ce processus est habituellement initié par le sujet, mais il peut l'être aussi par un administrateur de système ou automatiquement par le système.
431-e	Suspension de l'authentificateur	Transforme un authentificateur émis en authentificateur suspendu. Cela peut être déclenché par le sujet (p. ex. mot de passe oublié) ou le système (p. ex., blocage par suite d'une succession d'authentifications ayant échoué, d'une inactivité, d'une activité suspecte, etc.). Cela empêche de passer un justificatif suspendu à une partie utilisatrice, ce qui permet de s'assurer que l'accès est refusé au sujet.
431-a	Récupération de l'authentificateur	Rétablit un justificatif suspendu à un état utilisable (c.-à-d. justificatif émis). Le processus peut être déclenché par le sujet, l'administrateur de système ou automatiquement par le système. Exemples : • Le sujet répond correctement aux questions de sécurité pour réinitialiser un mot de passe oublié • Un administrateur de système libère un authentificateur qui a été suspendu à la suite d'une inactivité • Au bout de 24 heures, le système libère automatiquement un authentificateur suspendu à la suite d'un nombre excessif de tentatives d'authentification ayant échoué

5.2 Utilisation des représentations numériques

Pour la plupart des gens, la preuve d'identité, l'accès à un compte ou le fait de démontrer que certains critères sont remplis (p. ex., résidence, âge, possession d'un permis) est un aspect nécessaire des interactions en ligne. Les fonctions dans cette catégorie concernent l'utilisation des représentations numériques à ces fins.

Les interactions qui dépendent des représentations numériques de confiance se passent souvent entre une partie utilisatrice et un sujet des représentations numériques :

- **Partie utilisatrice** – Dans ce contexte, une partie utilisatrice est le participant à l'interaction qui a besoin d'une représentation numérique pour un motif valide. Les parties utilisatrices ont normalement besoin d'information pour identifier les sujets, vérifier certains attributs ou accorder l'accès à un système protégé. Dans bien des cas, la partie utilisatrice est un programme gouvernemental, un organisme à but non lucratif ou une entreprise privée qui offre des services en ligne au public ou à un nombre limité d'utilisateurs. La partie utilisatrice peut être une unité d'affaires au sein d'une grande organisation. L'unité bancaire de détail qui gère un système d'ouverture de comptes en ligne pour une grande institution financière peut, par exemple, dépendre des

renseignements émis par une entité interne et une unité de sécurité pour interagir avec ses clients.

- **Sujet de la représentation numérique** – L'entité représentée par un objet numérique auquel se rapportent les données qu'il contient (p. ex., la personne dont l'âge peut être vérifié à l'aide d'un justificatif). Dans ce contexte, le sujet de la représentation numérique est généralement une personne qui souhaite effectuer une transaction, accéder à un système ou interagir autrement avec une partie utilisatrice.

Étant donné la diversité des modèles techniques, de services et commerciaux qui définissent les interactions numériques et la façon dont les renseignements sur les participants sont incorporés dans ces interactions, le cadre de confiance pancanadien accepte que :

- d'autres participants à l'écosystème puissent être impliqués dans des fonctions spécifiques reliées à l'utilisation des représentations numériques**;**
- les sujets de la représentation numérique puissent interagir directement entre eux (c.-à-d., dans une interaction de pair à pair sans impliquer des parties supplémentaires);
- des interactions puissent survenir sans que le sujet de la représentation numérique n'intervienne directement.

Du fait de la nature variée de ces modèles d'interaction, le présent document se borne à donner un aperçu des processus fondamentaux impliqués dans l'utilisation des représentations numériques.

5.2.1 Confirmation d'une représentation numérique

Les processus de confirmation font en sorte que :

1. l'identité d'une entité est connue avec un certain degré de certitude;
2. l'information qui fait partie d'une représentation numérique est exacte, valide ou adaptée aux besoins.

Processus	**Description**
Validation de l'identité	La confirmation de l'exactitude des renseignements sur l'identité d'un sujet telle qu'établie par une partie ayant autorité. Il faut noter que la validation de l'identité ne garantit pas que l'entité utilise ses propres renseignements sur l'identité (il s'agit de la vérification de l'identité) – elle assure seulement que les renseignements sur l'identité que le sujet utilise sont exacts lorsqu'ils sont comparés à un dossier qui fait autorité.

466-c	Vérification de l'identité	Confirmation que les renseignements sur l'identité fournis sont reliés au sujet qui fait la déclaration. Il est à noter que la vérification de l'identité est un processus distinct de la validation de l'identité, et qu'elle peut employer différentes méthodes et utiliser des renseignements personnels qui ne sont pas reliés à l'identité. Différentes méthodes peuvent être utilisées (séparément ou combinées), notamment : • Confirmation basée sur les connaissances • Confirmation biologique ou comportementale • Confirmation d'un arbitre de confiance • Confirmation de la possession physique
466-d	Authentification du justificatif ou de l'authentificateur	Ce processus établit un niveau de confiance selon lequel une entité contrôle un justificatif ou un authentificateur émis à cette entité.
466-e	Association de l'identité	Processus consistant à s'assurer que le bon sujet est convenablement associé à différents contextes de prestation de services. Ce processus dépend des contraintes d'autorisation et de respect de la vie privée, et peut permettre d'associer une identité à un identifiant attribué à un service et/ou à relier plusieurs identifiants de services associés à une identité.
466-f	Présentation de l'identité	Confirmation dynamique qu'un sujet a une existence continue dans le temps (c.-à-d., une « présence réelle »). Elle peut servir à s'assurer qu'il n'y a pas d'activité malveillante ou frauduleuse (passée ou présente) et à régler des préoccupations en ce qui concerne l'usurpation d'identité.

556 ### 5.2.2 Consentement à l'utilisation de la représentation numérique

557 Ces processus font en sorte que les sujets de la représentation numérique comprennent quels
558 renseignements sont utilisés dans une représentation numérique et dans quel but – et qu'ils
559 autorisent son utilisation le cas échéant.

	Processus	**Description**
470-a		
470-b	Formuler l'avis	Produit une déclaration qui décrit les renseignements personnels recueillis; les parties avec lesquelles les renseignements personnels sont partagés; à quelles fins les renseignements personnels sont recueillis, utilisés ou divulgués; comment les renseignements personnels seront traités et/ou protégés; le temps pendant lequel la déclaration s'appliquera; et le territoire de compétence ou l'autorité dont relève la déclaration. Cette déclaration est présentée au sujet (c.-à-d., la personne naturelle à qui les renseignements personnels en question appartiennent) sous la forme d'un avis.

470-c	Demander le consentement	Présente l'avis au sujet et fournit à celui-ci la capacité de donner ou de refuser son consentement basé sur le contenu de l'avis, ce qui aboutit à une décision.
470-d	Enregistrer le consentement	Maintient l'avis et la décision du sujet relative au consentement en les enregistrant. En outre, il est possible d'enregistrer les renseignements sur le sujet, la version de l'avis ainsi que la date et l'heure où il a été présenté, et, le cas échéant, la date d'expiration de la décision. Une fois que le consentement a été enregistré, un avis sur la décision relative au consentement peut être adressé aux parties pertinentes à la décision.
470-e	Gérer le consentement	Le processus de gestion du consentement gère le cycle de vie des décisions relatives au consentement et comprend deux sous-processus : 1. Examen – Le processus d'examen du consentement consiste à rendre les détails d'une décision enregistrée visibles pour le sujet ou un examinateur; 2. Mise à jour – La mise à jour d'une décision relative au consentement fait intervenir le sujet qui révise une décision préalablement enregistrée. Le sujet pourrait notamment révoquer le consentement. Ce processus aboutit à la mise à jour d'une décision relative au consentement (ce qui obligera à la maintenir par le biais du processus d'enregistrement du consentement).

5.3 Activation des systèmes d'identité numérique

Le cadre de confiance pancanadien a pour but de mettre en place et de soutenir un écosystème canadien de l'identité numérique. L'interopération et la collaboration combinées à un processus de gouvernance responsable parmi les participants dans un environnement sûr qui accroît le respect de la vie privée est au cœur d'un tel écosystème. Pour atteindre ce but, le cadre de confiance pancanadien définit des exigences et des lignes directrices qui établissent un niveau de confiance dans les processus menés à l'intérieur de l'écosystème. Ces processus sont exécutés au moyen d'une infrastructure partagée publique, privée, fiable et non fiable : il s'agit des appareils, réseaux, logiciels et installations qui permettent aux participants de développer, déployer, gérer et soutenir les services qu'ils fournissent à leurs clients et au public.

L'objectif du cadre de confiance pancanadien relativement à ces infrastructures est de faire en sorte que la confiance créée au niveau des fonctions et processus soit également présente dans l'infrastructure de l'écosystème de l'identité numérique. Cela permet de s'assurer que l'infrastructure soutient la prestation de services de confiance et relève les défis communs à tous les participants.

À cette fin, le cadre de confiance pancanadien établit des lignes directrices et des normes pour les processus que les **fournisseurs d'infrastructures** procurent à d'autres participants. Ces processus, qui relèvent de l'infrastructure technique et opérationnelle, incluent :

- la sécurité physique et des systèmes;
- la confidentialité, l'intégrité et la disponibilité des données;

- le signalement des incidents;
- la tenue des dossiers.

5.3.1 Infrastructure technique

Ces processus assurent la sécurité et l'intégrité de la mise en œuvre des composantes de l'infrastructure.

	Processus	Description
492-b	Sécurité	Pratiques de sécurité TI conçues pour assurer la confidentialité, l'intégrité et la disponibilité de l'infrastructure de soutien.
492-c	Gestion des données	Processus et politiques pour la gestion du cycle de vie des données sur la représentation numérique, notamment la supervision de la collecte, de la validation, de l'entreposage et de l'accessibilité des données sur une base permanente.
492-d	Vérification et journalisation	Processus pour établir et maintenir un ou des registres chronologiques qui fournissent la preuve des événements et activités entourant des événements (système, transaction ou autre) liés aux fonctions soutenues.
493-e	Normes techniques	Référence du cadre de confiance pancanadien aux normes pertinentes de l'industrie pour soutenir des fonctions spécifiques.

5.3.2 Infrastructure des opérations

Ces processus font en sorte qu'il y a des principes et pratiques opérationnels bien définis pour l'écosystème de l'identité numérique.

	Processus	Description
495-b	Gestion des risques	Processus permettant d'identifier les risques directs ou indirects pour les fonctions soutenues et les efforts qui y sont associés pour réduire ou éliminer la probabilité que ces risques ne surviennent.
495-c	Gestion des dossiers	Processus qui soutiennent les activités habituelles de tenue de dossiers pour les fonctions soutenues. Cela inclut la classification, la garde des calendriers, la préservation et l'élimination.
495-d	Gestion des incidents et des conflits	Processus servant à identifier et à évaluer des événements qui se répercutent négativement sur les fonctions soutenues et (en cas de différends) les participants à l'écosystème, et à y réagir – notamment les efforts pour réduire ou éliminer la probabilité que l'incident ne se répète.

6. Glossaire

La terminologie peut varier selon le contexte ou le secteur où un terme est utilisé. La liste qui suit définit les principaux termes employés dans le contexte du présent document intitulé Modèle de cadre de confiance pancanadien.

Authentificateur – Méthodes que les entités dans l'écosystème utilisent pour accéder à des systèmes d'accès restreint ou protégés (p. ex., site Web d'une institution financière).

Justificatif – Information décrivant les attributs ou propriétés d'une entité.

Représentation numérique – Ensemble de données électroniques faisant référence à n'importe quel type d'entité pouvant être assujettie à des lois, politiques ou règlements dans un contexte et pouvant avoir certains droits, devoirs et obligations.

Entité – Chose qui a une existence à part et distincte, et qui peut être assujettie à des lois, politiques ou règlements dans un contexte et avoir certains droits, devoirs et obligations.

Identité – Information sur une entité qui la décrit d'une façon unique dans un contexte donné.

Rôle – Ensemble de fonctions et obligations qui sont attribuées à une position particulière dans le contexte du cadre de confiance, p. ex. un « fournisseur d'identité » ou une « partie utilisatrice ».

Sujet – Entité à laquelle s'applique une représentation numérique dans un système de gestion de l'identité.

Utilisateur – Personne qui a accès à des services ou ressources numériques.