Modèle de CCP

Statut du document : Recommandation finale version 1.0

Conformément aux procédures opérationnelles du CCIAN, une recommandation finale est un livrable qui représente les conclusions d'un comité d'experts du CCIAN qui ont été approuvées par un comité d'experts et ratifiées par un vote des membres bienfaiteurs du CCIAN.

Ce document a été préparé par le Comité d'experts du Cadre de confiance pancanadien du CCIAN avec l'apport du public recueilli et traité par le biais d'un processus d'examen ouvert mené par des pairs. On s'attend à ce que le contenu de ce document soit examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois, règlements et politiques. Les avis concernant les changements apportés à ce document seront partagés au moyen de communications électroniques, notamment le courriel et les réseaux sociaux. Les notifications seront également consignées dans le programme de travail du Cadre de confiance pancanadien (CCP). Les changements apportés à ce document qui pourraient se répercuter sur l'état des certifications et des marques de confiance seront définis dans la composante « Évaluation » du CCP.

Table des matières

1 Introduction

À mesure que la prestation des services devient de plus en plus numérique, les particuliers, les entreprises et d'autres types d'organisations constatent un besoin de faire confiance aux renseignements sur ceux avec qui ils interagissent, autrement dit que la personne (ou l'autre type d'entité) à l'autre extrémité d'une connexion est bien celle qu'elle prétend être ou que les renseignements que cette personne fournit sont exacts. Certains fournisseurs et leurs clients ont aussi besoin de savoir que ces renseignements sont protégés pendant qu'ils circulent dans les réseaux et traversent les frontières organisationnelles, et qu'ils sont saisis d'une manière numérique en guise de preuve dans des transactions hautement sensibles. C'est particulièrement le cas des transactions de grande valeur ou très sensibles qui sont actuellement difficiles à effectuer sous une forme numérique. Ces transactions incluent notamment certaines opérations financières, les achats immobiliers, l'envoi de réponses à des demandes de propositions, l'accès aux dossiers de santé, l'utilisation des passeports en ligne, l'achat de marchandises contrôlées en ligne et la gestion des prestations gouvernementales au nom de parents aînés.

En réponse à cela, des organisations publiques et privées dans le monde entier sont en train de développer des cadres pour promouvoir des environnements de confiance en ligne. De tels cadres consistent habituellement en une série d'exigences commerciales et techniques vérifiables pour des processus. Les exigences juridiques peuvent aussi être mentionnées dans le cadre. Ces cadres de confiance, comme on les appelle habituellement, permettent des interactions sûres et privées entre des parties et divers réseaux et organisations. Bien des réseaux financiers, de gestion de chaînes d'approvisionnement et d'identité numérique qui existent actuellement sont basés sur une forme de cadre de confiance. Plus évolutifs et plus transparents, les cadres de confiance sont de toute évidence une approche plus économique pour créer un environnement de confiance qu'un assortiment varié d'ententes privées entre quelques organisations privilégiées. Comparés à d'autres approches, ils présentent en outre l'avantage d'offrir des améliorations et des catalyseurs qui peuvent accélérer la cadence et augmenter le rythme d'adoption des systèmes partagés.

Le Cadre de confiance pancanadien (CCP) est un ensemble de ressources visant à procurer des avantages économiques, qui sont développées avec la collaboration du Comité d'experts du Cadre de confiance (TFEC) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN), publiées sous la gouvernance neutre du CCIAN, et qui bénéficient du vaste apport du secteur économique et des représentants fédéraux, provinciaux et territoriaux du Canada faisant partie du Sous-comité de gestion de l'identité des conseils mixtes (SGIC). Pour obtenir plus de renseignements sur le CCIAN, visitez www.diacc.ca.

Comme le CCP est destiné à être utilisé par une série de parties prenantes dans différentes communautés, n'importe quelle partie prenante peut adopter les exigences du CCP et réduire ainsi les coûts de développement et de prestation des services. Mais cela démontre surtout une volonté de se conformer aux conventions acceptées, ce qui a pour effet d'augmenter les niveaux de confiance et d'assurance parmi les clients, les partenaires d'affaires et autres interlocuteurs des parties prenantes.

1.1 À propos de ce document

Ce document a pour but de fournir un aperçu général du modèle de cadre de confiance. Il donne une vue d'ensemble du contexte environnant, et présente les buts et objectifs du CCP.

Ce document présente aussi les domaines fonctionnels auxquels le CCP s'intéresse en priorité. L'aperçu (fourni à la section 5) donne une idée générale des représentations numériques dont s'occupe le CCP et des divers processus intervenant dans la création, la gestion et l'utilisation de ces renseignements reliés à l'identité numérique.

Les composantes et profils individuels du CCP fournissent des descriptions détaillées des processus mis en évidence dans ce document.

Ce document s'adresse :

- aux membres des secteurs privé et public de la communauté de l'identité numérique (incluant les organes réglementaires et de normalisation) – en tant que parties prenantes et contributeurs clés du CCP;
- aux fournisseurs de technologies et de services d'identité numérique – pour comprendre où ils se situent dans le CCP, pour aider à définir les exigences pour leurs produits et services, et pour évaluer l'intégrité de leurs processus;
- aux innovateurs et chercheurs en matière d'identité numérique – qui peuvent remédier aux problèmes en proposant différentes approches; et
- aux consommateurs et aux organisations qui les servent en ligne – pour évaluer l'intérêt d'employer des solutions et des processus d'identité numérique de confiance lorsqu'ils interagissent en ligne.

2 À propos du CCP

2.1 Contexte

La technologie et les services qui permettent à des personnes d'interagir avec les gouvernements, les entreprises et entre elles grâce à la commodité et à l'efficacité numériques offre un potentiel considérable pour l'innovation et le développement au niveau social et économique. La capacité de faire confiance aux renseignements sur les participants dans ces interactions est une condition préalable essentielle pour tirer parti de ce potentiel. Le CCP soutient cet aspect des services numériques en tant que cadre de confiance 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 d'intégrations individuelles. Les clients et les utilisateurs revêtant un intérêt fondamental pour la plupart des parties prenantes, les représentations numériques de ces entités doivent être acceptées entre les fournisseurs de services, les secteurs économiques, les ordres de gouvernement et les provinces et territoires. Dans la pratique, cela

signifie que les particuliers et les autres participants doivent être capables d'utiliser et de gérer les renseignements à leur sujet dans de multiples contextes à l'échelle de l'économie.

L'interopérabilité, surtout dans un environnement en ligne qui s'attend à une instantanéité et une flexibilité, exige qu'une confiance mutuelle soit instaurée rapidement. Les consommateurs de services, particuliers ou autres, doivent faire confiance à l'identité des services avec lesquels ils interagissent. Sans interopérabilité et confiance, le Canada risque de perpétuer l'existence des barrières organisationnelles, politiques et techniques qui ont :

- contribué à un excès de procédures de vérification, d'inscriptions, de comptes, de mots de passe, de noms d'utilisateurs et de systèmes nécessaires pour tous les administrer;
- nuit aux efforts de modernisation qui favorisent l'innovation et améliorent l'expérience, l'efficience et l'efficacité des services; et
- créé un risque que si le Canada ne mène pas dans ce domaine, il devra adopter des solutions étrangères et l'impact économique négatif qui y est associé.

De plus, les Canadiens s'attendent à ce que leur écosystème de l'identité numérique fonctionne d'une manière transparente, en assurant une équité pour tous et en étant faisant la promotion des droits à la protection de la vie privée dès la conception. Ils s'attendent à ce qu'on leur dise d'une manière claire et concrète pourquoi et comment les renseignements à leur sujet sont recueillis, gérés et divulgués.

2.2 But

Le but du CCP est de permettre et de soutenir l'établissement d'un écosystème canadien de l'identité numérique qui soit innovateur et sûr et qui renforce le respect de la vie privée—et respecte aussi les droits humains fondamentaux dans l'ère numérique—pour tous les secteurs de l'économie. À cet égard, le CCP cherche à faciliter la migration des interactions en personne traditionnelles ou complexes vers des intégrations numériques qui mettent les gens au cœur de l'écosystème de l'identité numérique tout en reconnaissant que l'existence de processus analogues est également probable.

Le CCP adopte une approche pancanadienne de l'identité numérique afin de soutenir le développement d'un écosystème canadien de l'identité numérique. Cette approche se fonde sur une entente à grande échelle à propos des principes qui y sont énoncés et les normes fournies ou mentionnées dans les composantes du CCP pour :

- développer des solutions qui donnent la priorité aux perspectives sociales, juridiques et économiques canadiennes; et
- servir les besoins de tous les Canadiens.

Le CCP soutient le développement d'un écosystème canadien de l'identité numérique en :

- faisant en sorte que l'écosystème canadien de l'identité numérique soit fiable – en donnant le contrôle aux consommateurs, en préservant la sécurité et la fiabilité techniques, et en encourageant un environnement équitable, innovateur et concurrentiel pour les participants;

- mettant l'accent sur la transparence et le respect de la vie privée en ce qui concerne l'utilisation et la divulgation des renseignements personnels – en considérant le respect de la vie privée comme étant pertinente à toutes les composantes du CCP;
- soutenant l'inclusion des participants qui offrent un large éventail de services – en restant neutre du point de vue technologique;
- adoptant et adaptant les conventions existantes – en identifiant des normes politiques et technologiques existantes pour l'écosystème; et
- maintenant une perspective avant-gardiste – en cherchant de futurs domaines pour la collaboration, le développement et l'uniformisation.

2.3 Objectifs

Le CCP reconnaît que, même s'il y a des dépendances et des différences entre les provinces et territoires, les industries et les participants individuels, une approche uniforme du développement de l'écosystème peut être obtenue en adoptant systématiquement des normes acceptées à grande échelle. C'est pourquoi le CCP vise avant tout à assurer la fiabilité de l'écosystème canadien de l'identité numérique en :

1. Définissant les rôles et les fonctions des participants au sein de l'écosystème. Ce document décrit dans des termes généraux ces rôles, ces fonctions et les processus qui y sont associés pour servir de modèle pour le CCP. Les composantes et les profils du CCP fournissent au besoin des exigences et des lignes directrices plus détaillées;
2. Facilitant les interaction au sein de l'écosystème en définissant les exigences et les lignes directrices qui établissent un niveau de confiance pour les processus suivis par les participants de l'écosystème. Les composantes et les profils du CCP fournissent des descriptions et des spécifications techniques détaillées de ces exigences.

2.4 Portée

La réussite de l'écosystème canadien de l'identité numérique dépendra des utilisateurs; ceux qui accèdent à des services ou des ressources numériques doivent faire confiance au système en tout temps. Le CCP établit un cadre de confiance à l'intérieur duquel des solutions innovatrices peuvent être développées, mesurées et reconnues. Il définit les critères de conformité nécessaires pour les participants et les utilisateurs de l'écosystème de l'identité numérique d'interagir avec assurance.

Comme c'est le cas avec d'autres cadres de confiance, le CCP ne définit pas un système ou produit comme tel. De même, il ne couvre pas les aspects commerciaux de l'écosystème, notamment les modèles commerciaux, l'établissement des prix, la responsabilité, les droits de propriété intellectuelle et l'assurance.

2.5 Principes directeurs

Le CCP 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, sûres et évolutives** – L'écosystème canadien de l'identité numérique doit être suffisamment robuste pour offrir en tout temps sécurité, disponibilité et accessibilité.
2. **Instaurer, protéger et améliorer le respect de la vie privée dès la conception** – Les outils qui améliorent la protection de la vie privée permettent à une personne de gérer ses renseignements et la ou les fins spécifiques pour lesquelles ils sont utilisés. Ces outils peuvent inclure un soutien pour le « droit à l'oubli » d'un utilisateur (lorsque c'est approprié dans le contexte législatif du participant au cadre de confiance).
3. **Être inclusif et ouvert, et répondre aux besoins globaux des parties prenantes** – Les services et outils de l'écosystème de l'identité numérique doivent être abordables et uniformes, et procurer de la valeur aux utilisateurs en vue d'une adoption à grande échelle et dans l'intérêt de tous les Canadiens.
4. **Faire preuve de transparence dans la gouvernance et le fonctionnement** – Les Canadiens doivent avoir l'assurance que les services offerts dans l'écosystème canadien de l'identité numérique respecteront et satisferont leurs besoins et attentes.
5. **Offrir choix, contrôle et commodité aux Canadiens** – Les services partent du principe que les personnes peuvent choisir les renseignements qu'elles veulent partager et les services qu'elles veulent utiliser et en provenance de quels pays, et qu'elles sont au courant des avantages et conséquences possibles des identités numériques.
6. **Tirer parti des protocoles basés sur des normes ouvertes** – L'utilisation de normes ouvertes et de pratiques exemplaires applicables pour l'écosystème de l'identité numérique aide à se protéger contre l'obsolescence, à assurer une interopérabilité, et à avoir un marché de solutions dynamique et compétitif.
7. **Maintenir l'interopérabilité internationale** – L'interopérabilité et l'uniformisation mondiale des technologies et politiques sont à la base du monde connecté d'aujourd'hui. Tout comme les écartements uniformisés des voies ferrées permettent les voyages et le mouvement de marchandises entre les pays, l'interopérabilité et l'uniformisation des technologies 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 et qu'il représente de multiples secteurs économiques jouant chacun des rôles différents, va engendrer des coûts moindres pour tous les participants et davantage d'innovation.
9. **Soutenir des évaluations, des audits et une application indépendantes** – Pour que les Canadiens fassent confiance à un écosystème de l'identité numérique, il faut mettre en place des contrôles de la gouvernance. Les évaluations continues, fonctionnellement indépendantes et de tierces parties sont une façon de s'assurer que les participants à l'écosystème se conforment aux exigences du cadre de confiance.
10. **Réduire le transfert de données entre les sources et éviter de créer des référentiels de renseignements d'identité nouveaux ou agrandis** – Les utilisateurs de services de l'écosystème de l'identité numérique devraient être invités à ne fournir que le minimum de renseignements personnels nécessaires dans une interaction donnée (ce qui contribuerait à réduire la création de soi-disant « pots de miel informatiques »).

3 Structure du CCP

Le CCP comprend un aperçu du modèle (décrit dans ce document) et les éléments suivants :

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

Chacun de ces éléments est décrit dans la présente section.

3.1 Composantes du CCP

Les composantes du CCP définissent les processus de confiance et les critères de conformité pour des aspects spécifiques relevant du champ d'application du CCP. Elles précisent, étoffent et fournissent des détails supplémentaires qui ne sont pas présentés dans cet aperçu du modèle.

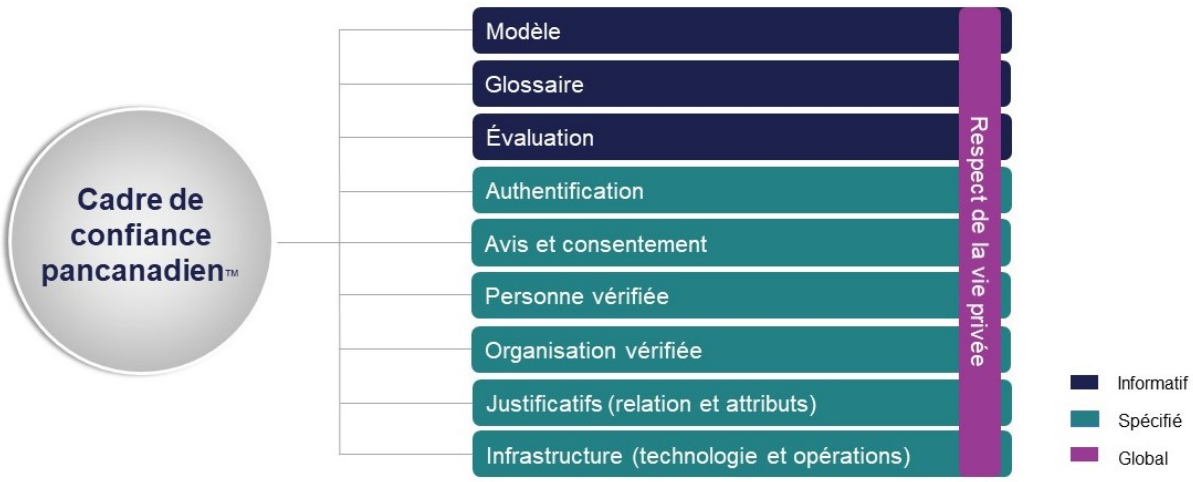

Figure 1. PCTF Composantes

La figure 1 illustre les composantes de l'ébauche de CCP. Les composantes du CCP visent avant tout à spécifier une base commune de critères de conformité et de processus de confiance. Les parties prenantes du CCIAN peuvent élargir et raffiner la base en définissant des profils du CCP.

3.1.1 Modèle

Ce modèle, l'aperçu du modèle de CCP, décrit les buts et objectifs du CCP, donne un aperçu général du modèle de CCP et fournit des renseignements contextuels.

3.1.2 Glossaire

Le glossaire du CCP fournit des définitions et des exemples de termes qui apparaissent dans les différents documents sur le CCP du CCIAN. Il vise à s'assurer que toutes les parties prenantes ont une compréhension commune et uniforme des termes utilisés dans le contexte du CCP. Étant donné que les termes et leur utilisation peuvent varier à l'échelle de l'industrie, le glossaire est une lecture recommandée à quiconque veut avoir une bonne compréhension de base du CCP.

Le glossaire du CCP contient ce qui suit :

1. **Termes** – Mots ou expressions qui apparaissent fréquemment et sont utilisés dans un but spécifique (c.-à-d. pas dans le sens de tous les jours en français) dans les documents du CCP
2. **Définitions** – Énoncé qui fournit la signification acceptée et précise du terme associé dans le contexte du CCP
3. **Exemples** – Des exemples ou non-exemples peuvent être inclus pour aider à clarifier la signification recherchée d'un terme; les exemples fournis ne visent pas à constituer une liste exhaustive.
4. **Synonymes** – Termes ayant la même signification ou une signification similaire, qui sont utilisés dans d'autres communautés d'intérêts

3.1.3 Évaluation

La composante « Évaluation » du CCP décrit le fonctionnement du programme de certification de la conformité du CCP et les rôles et responsabilités des parties prenantes qui en sont des acteurs pendant le processus d'évaluation et de certification. Elle inclut spécifiquement :

1. Les rôles et principales responsabilités des organisations responsables de l'évaluation et de la conformité :
    1. Autorité qui certifie
    2. Émetteur de marques de confiance
    3. Évaluateur accrédité
    4. Candidat à la certification
2. Une ventilation des rôles et responsabilités *pro forma* dans chacune des organisations identifiées
3. Des descriptions générales des méthodes et procédures d'évaluation, et de leur application
4. Des procédures et normes pour les programmes de certification, notamment :
    1. Émission, publication et maintien des certificats
    2. Procédures de renouvellement des certifications
    3. Procédures d'appel des évaluations.

La portée de cette composante du CCP n'inclut pas :

1. Les processus internes du candidat à la certification reliés aux processus de certification. La préparation interne pour les procédures d'évaluation du profil de conformité et la réponse à celles-ci varieront en fonction des processus de gouvernance et de gestion internes établis du candidat à la certification. Toutefois, les points de contact et les exigences fondamentaux sont régis par la composante « Évaluation » du CCP;
2. Évaluation et critères de conformité pour les profils individuels du CCP, lesquels fournissent des critères spécifiques sur la certification quand et là où c'est nécessaire.

3.1.4 Personne vérifiée

La composante « Personne vérifiée » du CCP spécifie les processus et les critères de conformité utilisés pour déterminer qu'une personne naturelle est réelle, unique et identifiable. Il s'agit d'un ingrédient essentiel pour s'assurer qu'une représentation numérique d'une personne est convenablement créée et utilisée exclusivement pour représenter la même personne, et qu'on peut s'y fier pour déterminer si la personne devrait recevoir des services de valeur et pour effectuer des transactions avec confiance et assurance.

La composante « Personne vérifiée » du CCP définit les processus et spécifie les critères de conformité pour :

1. **Vérifier une personne** - Il s'agit des processus qui permettent de s'assurer que l'identité numérique d'une personne est une représentation exacte de cette personne, et auxquels on peut se fier pour la prestation de services numériques et des transactions numériques. Une personne vérifiée est un être humain réel, unique et identifiable au moment de la vérification; et dans le contexte du CCP, une telle personne peut être assujettie à des lois, des politiques ou des règlements faisant partie d'un contexte. Ces processus assurent qu'une personne a été convenablement vérifiée et qu'il s'agit de la personne qui a initié, directement ou par l'entremise d'un représentant autorisé par la loi, la demande de service ou de transaction;
2. **Créer une identité numérique de confiance pour une personne** - Il s'agit des processus utilisés pour établir et tenir à jour le dossier numérique pour une personne vérifiée afin de la distinguer d'une façon unique des autres personnes. Le processus assure que le dossier numérique d'une personne est convenablement créé et utilisé exclusivement par cette même personne, directement ou avec l'aide de son représentant autorisé par la loi, et qu'on peut s'y fier pour effectuer des transactions en ligne. On parle aussi de dossier d'une personne vérifiée.

La portée de la composante « Personne vérifiée » du CCP inclut :

1. La création d'une preuve d'identité contextuelle chez une partie faisant autorité;
2. La dépendance à un preuve d'identité essentielle pour vérifier une personne;
3. La dépendance à une preuve d'identité contextuelle pour vérifier une personne;
4. Les niveaux d'assurance 1 à 3 pour l'identité; les cas d'utilisation de niveau 4 ne sont pas actuellement inclus dans la portée mais seront pris en compte pour des versions futures;
5. La création, la mise à jour et la gestion d'un dossier de personne vérifiée (c.-à-d. une représentation numérique de confiance);

6. Les acteurs incluent les gouvernements fédéral, provinciaux et territoriaux du Canada, et les organisations canadiennes conformes au CCP en tant que parties faisant autorité pour la preuve d'identité.

La portée de la composante « Personne vérifiée » du CCP n'inclut pas :

1. La création d'une preuve d'identité essentielle. L'établissement et le maintien d'une preuve d'identité essentielle relève exclusivement du secteur public, spécifiquement les services de l'état civil des provinces et des territoires, et Immigration, Réfugiés et Citoyenneté Canada;
2. L'utilisation de gouvernements ou d'organismes internationaux comme seules sources faisant autorité en matière de preuve d'identité pour vérifier une personne. On peut faire indirectement référence à des gouvernements internationaux pour établir des sources d'identité essentielles ou contextuelles. Les cas d'utilisation qui se fient uniquement à une preuve d'identité internationale peuvent être pris en compte dans des versions ultérieures du CCP;
3. La vérification des attributs non identitaires. Les processus relatifs à la personne vérifiée n'établissent pas de renseignements particuliers à propos de la personne, si ce n'est uniquement le fait qu'une personne est réelle, unique et identifiable dans un contexte donné. Les autres renseignements ou attributs personnels comme l'adresse de résidence peuvent être nécessaires pour fournir un service. La vérification des attributs non requis pour vérifier l'identité numérique d'une personne déborde de la portée de cette composante; veuillez vous référer à la composante « Justificatifs (relations et attributs) » du CCP.

3.1.5 Organisation vérifiée

La composante « Organisation vérifiée » du CCP vise à spécifier les processus de confiance et les critères de conformité associés qui déterminent qu'une organisation est réelle, unique et identifiable. Une fois qu'un processus est certifié conforme aux critères de conformité associés, il devient un processus de confiance auquel peuvent alors se fier les autres participants à un écosystème d'identité numérique.

La composante « Organisation vérifiée » du CCP définit les processus et spécifie les critères de conformité pour :

1. **Établir et vérifier l'identité d'une organisation** - Cela inclut les processus pour s'assurer qu'une organisation a été convenablement vérifiée comme étant le participant prévu dans une interaction donnée. Une organisation qui n'existe plus comme entité juridique peut encore avoir une identité numérique avec un attribut indiquant son statut;
2. **Créer une représentation numérique de confiance (c.-à-d. une identité numérique) pour une organisation** - Cela inclut les processus pour établir et maintenir une représentation numérique pour une organisation vérifiée.

Cette composante du CCP met l'accent sur les processus de confiance qui établissent l'identité des organisations et la gestion continue des identités numériques associées. Cela inclut :

1. L'établissement de l'identité organisationnelle;
2. L'émission de l'identité organisationnelle;
3. La résolution de l'identité organisationnelle;
4. La validation de l'identité organisationnelle;
5. La vérification de l'identité organisationnelle;
6. La tenue à jour de l'identité organisationnelle;
7. Le maillage de l'identité organisationnelle.

La portée de cette composante du CCP n'inclut pas :

1. Les gouvernements ou organisations étrangers en tant que sources faisant autorité en matière de preuve d'identité pour vérifier une organisation. On peut y faire indirectement référence pour établir les sources d'identité essentielles ou contextuelles;
2. Les processus auxquels les parties prenantes ont recours pour confirmer que les personnes représentant des organisations sont autorisées à le faire;
3. La structure de la propriété d'une organisation, et les conditions et processus pertinents pour accorder l'accès à des services et systèmes (secteur privé ou public).

3.1.6 Justificatifs : relations et attributs

Cette composante du CCP spécifie les critères de conformité que les participants à l'écosystème peuvent utiliser pour évaluer dans quelle mesure l'écosystème protège l'utilisation des justificatifs numériques. La portée de cette composante inclut les caractéristiques du cycle de vie des justificatifs numériques, et s'attache à assurer la transparence et la vérifiabilité comme méthodes principales pour instaurer la confiance parmi les entités impliquées. Les éléments spécifiques considérés comme étant inclus ou en dehors de la portée sont décrits dans les sections qui suivent.

Sont inclus dans la portée de cette composante du CCP les justificatifs qui :

1. Contiennent ou fournissent des renseignements sur un sujet (p. ex., preuve numérique du niveau d'études) et un émetteur;
2. Contiennent ou fournissent des renseignements sur la relation entre deux entités (p. ex., preuve numérique qu'une personne est employée par une entreprise);
3. Sont émis par un émetteur à un sujet qui n'est pas l'émetteur;
4. Contiennent des renseignements qu'une entité fournit sur ou à une autre entité;
5. Décrivent les relations entre un ou plusieurs sujets et leurs relations avec une ou plusieurs autres entités.

Indépendamment du contenu des justificatifs ou de la relation entre un émetteur et un sujet, la portée de cette composante inclut :

1. L'émission de justificatifs à des sujets;
2. Les renseignements qui augmentent la fiabilité des justificatifs;
3. Des conseils pour protéger l'intégrité et l'exactitude des renseignements sur les justificatifs;

4. Des consignes pour gérer les justificatifs compromis.

La vérification et la validation des entités uniques, réelles et identifiables débordent de la portée de cette composante. Ces processus, et la création et l'utilisation des renseignements d'identité dont ils dépendent, sont couverts dans les composantes « Personne vérifiée » et « Organisation vérifiée » du CCP.

Ce qui suit déborde aussi de la portée de cette composante du CCP :

1. Émission d'un justificatif par de multiples émetteurs;
2. Règles et politiques déterminant qui peut obtenir un justificatif ou un type de justificatif spécifique (p. ex., exigences pour obtenir un permis de conduire dans une province ou un territoire en particulier);
3. Processus pour évaluer la qualification ou l'admissibilité pour un justificatif ou un type de justificatif spécifique (p. ex., faire passer un examen aux nouveaux conducteurs), indépendamment des documents exigés pour de tels processus;
4. Acceptation d'un justificatif pour un besoin donné (p. ex., permis de conduire accepté ou non comme preuve d'adresse).

3.1.7 Authentification

La composante « Authentification » du CCP vise à assurer l'intégrité continue des processus de connexion et d'authentification en certifiant, au moyen d'un processus d'évaluation, qu'ils se conforment à des critères de conformité uniformisés. Les critères de conformité pour cette composante peuvent servir à assurer :

1. Que les processus de confiance donnent la représentation d'un sujet unique à un niveau d'assurance qu'il s'agit du même sujet à chaque connexion réussie avec le fournisseur de services d'authentification;
2. La prévisibilité et la continuité des processus de connexion qu'ils offrent ou dont ils dépendent.

La composante « Authentification » du CCP définit :

1. Un ensemble de processus qui permettent d'avoir accès à des systèmes numériques;
2. Un ensemble de critères de conformité pour chaque processus qui, lorsqu'un processus s'avère conforme, permettent de faire confiance au processus

3.1.8 Avis et consentement

La composante « Avis et consentement » du CCP spécifie les critères de conformité qui définissent les exigences pour faire en sorte que les énoncés des avis sont formulés d'une manière exacte, que le consentement est donné lorsque c'est nécessaire, que la personne qui décide de donner son consentement est autorisée à le faire et que c'est possible de gérer les consentements. La composante « Avis et consentement » du CCP spécifie les critères de conformité pour les processus qui :

1. Formulent une déclaration sur la collecte, l'utilisation, la divulgation et la rétention des renseignements personnels;
2. Obtiennent un consentement pertinent et éclairé basé sur cette déclaration de la part d'une personne autorisée à la faire.

La portée de la composante « Avis et consentement » du CCP et des critères de conformité associés inclut :

1. La collecte, l'utilisation, la divulgation et la rétention des renseignements personnels dans le but d'établir et de confirmer une identité numérique et des renseignements personnels connexes et vérifiés qui sont spécifiques à une personne;
2. Le consentement obtenu par une organisation différente de celle qui recueille, utilise ou divulgue des données – des circonstances qui pourraient se produire dans un système d'identité fédérée;
3. Un consentement unique obtenu lorsque de multiples renseignements personnels sont recueillis, utilisés ou divulgués par plusieurs organisations, dans le cadre d'une seule transaction;
4. Des situations où le sujet peut ou non avoir une relation explicite avec le fournisseur de renseignements (p. ex., quand une vérification des antécédents est effectuée auprès d'une source tierce conformément à la loi applicable);
5. La divulgation (ou le partage) de données pouvant faire suite à un mode « requête » ou « demande de renseignements ».

La portée de la composante « Avis et consentement » n'inclut pas :

1. L'utilisation subséquente des renseignements personnels par les organisations pour fournir leurs services. Le traitement des renseignements personnels spécifiques à un sujet par une organisation requérante est assujetti à la législation, aux politiques et/ou aux règlements pertinents, et il n'est généralement pas censé être couvert par la portée des exigences de l'écosystème de l'identité numérique une fois que les données ont été partagées en dehors de l'écosystème de l'identité numérique. Il y a toutefois une exception à cela quand une organisation divulgatrice a des exigences spécifiques pour le traitement des renseignements personnels par le destinataire (l'organisation requérante). Ces exigences feront donc partie de la gouvernance de l'écosystème de l'identité numérique et constitueront les exigences « en aval » auxquelles doit se conformer toute organisation requérante qui reçoit des données de cette organisation divulgatrice.
2. Les cas d'utilisation où une autre personne agit au nom du sujet (p. ex., fondé de pouvoir, parent agissant pour le compte d'un enfant). Cette version de la composante « Avis et consentement » tient uniquement compte des sujets qui donnent leur consentement pour l'obtention, l'utilisation et la divulgation des renseignements personnels les concernant. Ces cas d'utilisation seront ajouté dans une version ultérieure.

3.1.9 Infrastructure : technologie et opérations

La composante « Infrastructure : technologie et opérations » du CCP spécifie les critères de conformité qui fournissent les exigences et les lignes directrices générales concernant la fiabilité de l'infrastructure TI permettant la mise en œuvre et la prestation des processus de confiance définis dans d'autres composantes du CCP. Les principaux sujets de la composante sont la sécurité et l'intégrité des composantes techniques. Dans ces domaines d'intérêt, la portée de la composante inclut :

1. La sécurité TI (d'un point de vue général)
2. La préservation de la confidentialité et de l'intégrité de l'infrastructure TI qui sert de soutien;
3. La supervision de la collecte, la validation, l'entreposage et l'accessibilité des données;
4. L'audit et la journalisation;
5. La prévention et le traitement des incidents TI qui compromettent la fiabilité de l'écosystème de l'identité numérique;
6. Les politiques et les plans qui soutiennent la gestion fiable de la technologie et des opérations technologiques.

La portée de cette composante du CCP n'inclut pas :

1. L'à-propos des produits spécifiques pour soutenir un processus de confiance donné;
2. L'à-propos des normes, processus, technologies ou protocoles pouvant être exigés par un écosystème de l'identité numérique en particulier;
3. L'obligation d'utiliser un ensemble spécifique de pratiques ou cadres standard pour gouverner les opérations technologiques (p. ex. ITIL, COBIT)

3.1.10 Respect de la vie privée

La composante « Respect de la vie privée » du CCP spécifie les critères de conformité qui définissent les exigences générales afin d'assurer l'intégrité permanente des processus, politiques et contrôles relatifs au respect de la vie privée qui sont en place dans les organisations faisant partie d'un écosystème de l'identité numérique. La composante « Respect de la vie privée » du CCP porte sur le traitement des données personnelles pour les besoins de l'identité numérique.

Les critères de conformité de la composante « Respect de la vie privée » du CCP spécifient comment les principes de la LPRPDE relatifs à l'équité dans le traitement de l'information, définis par le Commissariat à la protection de la vie privée du Canada, s'appliquent au traitement des renseignements d'identité numérique. Étant donné cela, la portée de cette composante du CCP s'aligne sur les 10 principes de la LPRPDE relatifs à l'équité dans le traitement de l'information, à savoir :

1. Responsabilité
2. Détermination des fins de la collecte des renseignements
3. Consentement
4. Limitation de la collecte

5. Limitation de l'utilisation, de la communication et de la conservation
6. Exactitude
7. Mesures de sécurité
8. Transparence
9. Accès aux renseignements personnels
10. Possibilité de porter plainte à l'égard du non-respect des principes

Le respect de la vie privée dès la conception est un des principes directeurs du CCIAN pour un écosystème canadien de l'identité numérique, spécifiquement « pour instaurer, protéger et améliorer le respect de la vie privée dès la conception ». Les considérations liées au respect de la vie privée font partie intégrante de – et devraient être pris en compte à - tous les stades du développement d'une solution d'identité numérique. C'est pourquoi les critères de conformité spécifiés dans la composante « Respect de la vie privée » du CCP peuvent s'appliquer aux processus de confiance et aux critères de conformité spécifiés dans d'autres composantes du CCP – et sont par conséquent considérés comme englobant toutes les autres composantes dans le contexte du CCP.

3.2 Critères de conformité

Les critères de conformité sont appliqués en tant que norme ou ils 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 servant à évaluer la fiabilité de processus spécifiques. Les participants peuvent utiliser ces critères pour concevoir et développer leurs produits et services.

Les critères de conformité du CCP visent à compléter les lois et règlements existants; on s'attend à ce que les participants à l'écosystème de l'identité numérique remplissent les exigences juridiques et réglementaires applicables dans leurs provinces et territoires.

Conformément aux principes directeurs énoncés en 2.5, qui prônent l'établissement de normes ouvertes et le maintien d'une interopérabilité nationale et internationale, le CCP accepte que :

- Des normes et spécifications existantes puissent être intégrées dans les critères de conformité du CCP en y faisant référence. Cela assure une compatibilité étendue, et réduit la duplication et le chevauchement du contenu et des spécifications techniques;
- Lorsque des normes existantes sont incorporées dans le CCP, la priorité étant accordée à une mise en œuvre canadienne. Cela peut nécessiter que les normes internationales soient interprétées et appliquées dans un contexte canadien (p. ex., en ce qui concerne les considérations légales sur la protection de la vie privée ou la souveraineté des données au Canada). Des normes existantes peuvent être intégrées dans les composantes ou les profils de base du CCP.

Les critères de conformité du CCP sont développés dans le but de s'assurer que la conformité aux exigences qu'ils représentent peuvent être évalués. Cela permet aux participants de 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 désigné comme étant un processus de confiance est évalué selon des critères de conformité définis dans les composantes et profils du CCP. 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*.

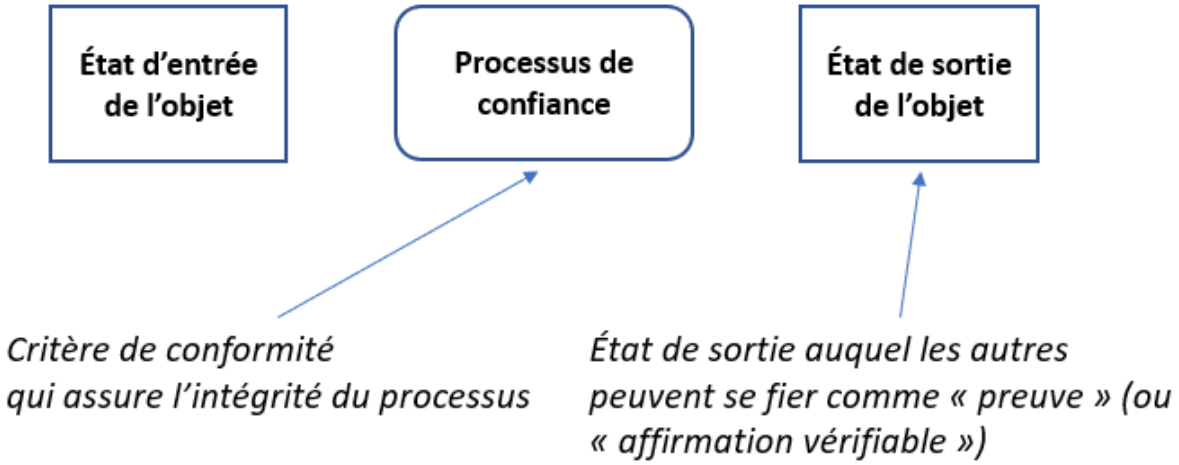

Figure 2. Modèle de processus de confiance

Les processus de confiance sont fondamentaux pour assurer l'intégrité globale de l'écosystème de l'identité numérique et pour l'intégrité globale du cadre de confiance. L'intégrité d'un processus de confiance est fondamentale, car de nombreux participants se fient à la sortie d'un processus de confiance – par-delà les frontières provinciales, territoriales et sectorielles, et à court et long terme. Le CCP assure l'intégrité d'un processus de confiance grâce à des critères de conformité convenus et bien définis qui permettent d'avoir une méthode d'évaluation transparente et basée sur des preuves. Cette évaluation explicite contraste avec de nombreux processus analogues existants auxquels on fait confiance non pas parce qu'ils comportent des protections naturelles inhérentes mais parce qu'ils sont largement adoptés à long terme.

Un processus commercial ou technique existant peut être désigné comme un processus de confiance qui est assujetti aux critères de conformité, au processus d'évaluation et à la certification définis par le CCP. Par exemple, des programmes ou services existants ont habituellement des processus reliés à l'identité qui sont intégrés, parfois appelés preuve d'identité ou enregistrement de l'identité. Des processus développés 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 utilisés et considérés fiables dans le contexte du CCP. Cela est fait en cartographiant les processus (ou sous-processus existants dans les définitions des processus de confiance. Une fois cartographiés, ces processus peuvent être évalués et certifiés à l'aide des critères de conformité définis associés aux processus de confiance correspondants.

3.4 Profils du CCP

La portée du CCP, qui est très étendue, vise à fournir une norme de base à l'échelle de l'économie canadienne dans le contexte des secteurs public et privé, et à d'autres communautés qui ont des intérêts communs pour définir la façon dont le CCP va s'appliquer dans des contextes et cas d'utilisation ou pour répondre à des besoins commerciaux particuliers.

Les profils du CCP permettent aux parties prenantes du CCIAN d'adapter les critères de conformité de base à des exigences ou des applications spécifiques. Cela pourrait consister, sans s'y limiter, à :

- Exiger de se conformer obligatoirement aux critères de conformité définis comme étant facultatifs à la base;
- Définir des niveaux d'assurance et des sources de preuves acceptables;
- Spécifier des technologies acceptables; ou
- Élargir certains critères de conformité (p. ex., exiger des processus d'audit et d'enregistrement supplémentaires).

4 Notions essentielles

Le CCP est basé sur un petit nombre de notions essentielles. Il y a d'abord et avant tout l'idée que la confiance est établie et peut être évaluée à de multiples points dans une chaîne de processus qui créent et utilisent des représentations numériques de personnes et autres entités.

Les notions essentielles peuvent être résumées comme suit :

- Les participants à l'écosystème de l'identité numérique créent, utilisent et/ou gèrent des **représentations numériques** des **sujets**;
- Lorsqu'ils traitent des représentations numériques, les participants jouent un ou plusieurs **rôles** dans l'écosystème;
- Chaque rôle consiste en un certain nombre de fonctions qui comprennent un ou plusieurs **processus de confiance**; et
- La conformité aux critères de conformité spécifiés qui définissent les processus de confiance.

Les sections qui suivent fournissent une description de ces notions dans le contexte du CCP.

4.1 Représentations numériques

Une représentation numérique est un ensemble de données électroniques faisant référence à une entité qui peut être identifiée d'une manière unique dans un contexte, qui est assujetti à des lois, politiques ou règlements dans le cadre de ce contexte, et qui peut avoir certains droits, devoirs et obligations. Dans le contexte du CCP, les entités qui détiennent ou sont sur le point d'obtenir une représentation numérique au sein de l'écosystème sont appelés des sujets. Les représentations numériques sont destinées à être cartographiées pour modéliser des acteurs

dans la vraie vie, comme des personnes et des organisations qui bénéficient de la mise en œuvre ou de l'utilisation du CCP.

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

1. **personnes** – être humain biologique individuel qui est vivant ou décédé. Exemples : résidents d'un territoire de compétence (pays, province, etc.), clients d'une entreprise et particuliers.
2. **organisations** – entité qui consiste en une personne ou un corps organisé de personnes ayant une vocation particulière et dont l'existence est établie par un statut juridique. Exemples : entreprises (incluant entreprises à propriétaire unique, partenariats et sociétés), organismes gouvernementaux, coopératives et œuvres de bienfaisance enregistrées.
3. **machines** – logiciels et matériel qui peuvent agir comme des agents intelligents pour effectuer des transactions d'une manière indépendante (c.-à-d., exige une vérification de l'identité de la machine). Les machines qui agissent pour le compte d'une personne ou d'une organisation sont habituellement des identités non autonomes de leur plein droit. À mesure que le CCP évoluera, la technologie future qui entraînera la création de machines présentant un certain niveau d'autonomie pourrait donner des critères de conformité et des processus de confiance spécifiques à ces types d'entités.

L'élaboration de critères de conformité et de processus de confiance le plus étroitement reliés à des *personnes* est la priorité pour les composantes du CCP, suivi de ceux pour les *organisations*. Ceux qui sont reliés à des *machines* sont moins prioritaires dans le développement du CCP.

4.2 Rôles des participants

Les représentations numériques ont un cycle de vie qui commence avec la création, se poursuit avec l'utilisation active (pendant laquelle les données peuvent changer, être ajoutées ou supprimées, etc.) et aboutit à l'archivage et, dans certains cas, à la suppression. La confiance s'établit pendant l'exécution des processus clés tout au long de ce cycle de vie. Le CCP définit des normes et des lignes directrices pour ces processus.

Les processus clés d'un écosystème d'identité numérique sont répartis entre trois grandes fonctions :

1. Création et gestion des représentations numériques
2. Utilisation des représentations numériques
3. Activation des systèmes d'identité numérique

Les participants à l'écosystème accomplissent ces fonctions. Il s'agit de particuliers ou d'organisations (publiques, commerciales ou à but non lucratif) qui acceptent de fonctionner selon les paramètres du CCP. Dans le modèle de CCP, les participants qui exécutent des processus clés dans le cycle de vie des représentations numériques assument un ou plusieurs rôles qui sont définis comme suit :

Fonction	Rôle	Description
Créer et gérer des représentations numériques	Fournisseurs d'identité	Rôle qu'un participant exécute pour créer, maintenir et fournir des représentations numériques. On parle parfois de fournisseurs de services d'identité ou d'émetteurs d'identité. Dans certains cas, le sujet est le créateur et le gestionnaire de sa propre identité (p. ex., dans certains cas d'utilisation auto-souveraine).
	Fournisseurs de justificatifs	Rôle qu'un participant exécute pour créer et gérer des authentifiants. On parle parfois de fournisseurs d'attributs.
	Fournisseur de services d'authentification	Rôle qu'un participant exécute pour créer et gérer des authentifiants. On parle parfois de fournisseurs de services de justificatifs. Ce n'est pas la même chose que des fournisseurs de justificatifs du CCP. Voir 5.1.3 pour les détails.
Utiliser des représentations numériques	Parties dépendantes	Rôle qu'une organisation ou une personne exécute pour consommer des représentations numériques créées et gérées par des participants pour effectuer des transactions numériques avec des sujets.
	Sujets	Personne, organisation ou machine qui détient ou est en voie d'obtenir une représentation numérique dans le système de l'écosystème d'identité numérique réglementé par le CCP, et qui peut être assujettie à des lois, des politiques et des règlements dans un contexte. Le sujet d'une représentation numérique peut assumer des fonctions et/ou représentations explicites (p. ex. une obligation de protéger la représentation numérique et d'empêcher les abus). Il peut aussi y avoir des fonctions implicites exécutées par le sujet dans le contexte de l'écosystème d'identité

		numérique (p. ex. fonctions associées à la « motivation de récupérer » une représentation numérique qui a été compromise ou corrompue).
Activer des systèmes d'identité numérique	Fournisseurs d'infrastructures	Rôle qu'un participant exécute pour fournir les infrastructures physiques et électroniques nécessaires pour permettre des interactions numériques.
	Évaluateurs accrédités	Rôle qu'un participant exécute pour évaluer la conformité d'autres participants au CCP, y compris les profils de conformité au CCP.

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

Les parties prenantes incapables de participer pleinement à l'écosystème de l'identité (p. ex., à cause du coût ou de retards dans l'évaluation de la conformité, ce qui pourrait être un fardeau pour des entreprises en démarrage) peuvent réutiliser la technologie et les processus mis en place par les participants du CCP dans le cadre des efforts pour participer plus pleinement dans un rôle ou à un titre quelconque. Cela donne au CCP la possibilité d'éliminer les obstacles qui bloquent l'accès à l'écosystème de l'identité.

4.3 Rôles de gouvernance

En tant que cadre de confiance destiné à une adoption à grande échelle, le CCP définit les rôles de gouvernance pour certaines parties prenantes de l'écosystème. Les participants qui jouent ces rôles sont responsables de préparer des ébauches des diverses composantes du CCP, de les tenir à jour et de veiller à leur adoption uniforme. Ces rôles peuvent aussi inclure la gouvernance de l'utilisation et de l'application du CCP dans l'écosystème numérique.

5 Aperçu fonctionnel

Cette section présente les fonctions et processus reliés à l'identité qui sont inclus dans la portée du CCP.

5.1 Créer et gérer des représentations numériques

Les fonctions dans cette catégorie consistent à prouver ou à vérifier l'identité ou les caractéristiques d'une entité réelle (c.-à-d. une personne, une organisation ou une machine) et à créer une représentation numérique pour cette entité. Une fois qu'une représentation numérique est créée, elle est gérée au moyen de processus qui permettent aux données d'être

mises à jour, supprimées et revérifiées au besoin – dans le but de s'assurer que la représentation reste actuelle et exacte.
Actuellement, le CCP définit trois types de représentation numérique :

1. **Identité** – Renseignements permettant d'identifier une entité unique (p. ex., renseignements personnels), par eux-mêmes ou avec des renseignements connexes à l'appui. Exemples pour les personnes : noms, dates de naissance, adresses, anciens noms, numéros de téléphone et données biométriques. Exemples pour les machines : numéro de série, certificat numérique de confiance ou adresse MAC réseau.
2. **Justificatif** – Renseignements décrivant les attributs ou les propriétés d'une entité. Ces renseignements peuvent exister par eux-mêmes (p. ex., en tant que justificatif qui ne renferme pas de renseignements personnels, uniquement une chaîne d'identification unique) ou être reliés à des renseignements personnels. Exemples : niveaux d'éducation (p. ex., diplôme universitaire en génie), permission d'utiliser un véhicule (p. ex., permis de conduire), niveau de revenu ou statut d'un employé dans une entreprise.
3. **Authentifiant** – Renseignements ou caractéristiques biométriques contrôlés par une personne qui sont des cas spécifiques d'une chose que le sujet a, connaît ou fait. Exemples d'authentifiants habituels : clés de signature privées, mots de passe utilisateurs ou visage d'une personne.

5.1.1 Identités

Les identités numériques sont des représentations électroniques qui font référence à des entités distinctes à l'intérieur de l'écosystème; des parties désirant interagir entre elles. Les identités consistent en des renseignements qui identifient d'une manière unique une entité dans un contexte donné (p. ex., raison sociale enregistrée et identifiant d'une entreprise). Pour des personnes, les identités démontrent que l'individu est ce qu'il est ou prétend être.

À l'intérieur du CCP, les **fournisseurs d'identité** sont responsables de créer et de gérer les identités numériques sur lesquelles ils ont une latitude. Ils remplissent des fonctions consistant en des processus visant à s'assurer que :

- une entité est connue pour être réelle et identifiable, et non une création frauduleuse; et
- une entité est unique au sein d'une population (p. ex., citoyens, clients, sociétés), de sorte que des identités numériques multiples ne peuvent pas être créées et utilisées d'une manière frauduleuse;
- l'identité numérique représente l'entité à qui elle a été délivrée.

Ces fonctions fournissent une base sur 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 authentifiants reliés à ce dossier.

5.1.1.1 Types d'identités

Le CCP définit deux types de renseignements pour établir une identité numérique :

Type	Description	Destinataires	Émetteurs	Exemples
Identité de base	Établit l'existence et la représentation numérique de sujets réels légalement reconnus	Personnes, organisations	Certains organismes du secteur public ayant pour mandat de créer et de gérer des identités légalement acceptées (p. ex., registraires, organismes de citoyenneté et d'immigration).	Ensemble de données qui atteste l'identité du sujet, comme l'équivalent numérique d'un certificat de naissance ou des statuts d'incorporation.
Identité contextuelle	Établit des représentations identitaires et numériques des sujets dans des contextes ou cas d'utilisation spécifiques. Ce type inclut des identités qui sont auto-émises ou attribuées.	Personnes, organisations, machines	Fournisseurs d'identité publics et privés ou sans but lucratif.	Identité d'entreprise numérique, identité numérique provenant d'un corps professionnel. Identité sur les réseaux sociaux, identité auto-émise. Dans le cas des machines, il pourrait s'agir d'identifiants numériques attribués par des fabricants ou des agents intelligents.

5.1.1.2 Processus habituellement effectués par des fournisseurs d'identité

Processus	Description
Résolution de l'identité	Établissement du caractère unique d'un sujet au sein de la population d'un programme ou service en utilisant les renseignements d'identité. Un programme ou service définit ses exigences en matière de résolution de l'identité en termes d'attributs de l'identité; autrement dit, il spécifie l'ensemble d'attributs de l'identité qui est nécessaire pour résoudre l'identité au sein de sa population.
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.
Maintenance de l'identité	Processus qui consiste à s'assurer que les renseignements d'identité sont exacts, complets et à jour, tel que requis. La maintenance de l'identité inclut aussi la *notification de l'identité*, qui est la divulgation des renseignements d'identité déclenchée par un changement apporté à ces renseignements (p. ex., événement démographique ou événement de la vie important) ou une indication que les renseignements d'identité ont été exposés à un facteur de risque. Cela peut être basé sur le temps ou des événements.

5.1.2 Justificatifs

Les justificatifs sont des représentations numériques qui fournissent des renseignements sur les attributs ou propriétés d'une entité. Les justificatifs contiennent habituellement des renseignements débordant de ce qui est nécessaire pour identifier une entité individuelle unique. Pour les personnes, les justificatifs aident à répondre à des questions comme « cette personne est-elle autorisée par la loi à acheter ces marchandises en ligne? » ou « cette personne remplit-elle les exigences nécessaires pour recevoir ces prestations gouvernementales? ». Exemples de justificatifs :

- concept simple qui atteste l'âge d'une personne ou le statut d'enregistrement d'une entreprise dans une province donnée;
- concept complexe qui représente les relevés de notes universitaires, les antécédents professionnels ou un poste au sein d'une organisation.

Les justificatifs sont utilisés par les fournisseurs de services et les parties dépendantes pour avoir l'assurance que les caractéristiques spécifiques de cette entité (p. ex., âge pour acheter un produit financier) sont vraies. Dans certains cas, l'existence du justificatif et son utilisation

peuvent fournir une empreinte numérique ou preuve d'existence qui peut aider à prouver l'identité et à évaluer et atténuer les risques.

Un justificatif inclut un ou plusieurs identifiants et une ou plusieurs valeurs d'attributs générés par l'émetteur de justificatifs. Compte tenu des détails de la mise en œuvre :

- les identifiants peuvent être des pseudonymes; et
- il peut être possible de vérifier d'une manière cryptographique les valeurs des attributs.

Dans le contexte de ce document, un justificatif n'est pas synonyme de nom d'utilisateur et de mot de passe ou d'un mécanisme similaire utilisé pour contrôler l'accès à un système géré. Dans l'aperçu du modèle de CCP, on parle d'authentifiants pour désigner le nom d'utilisateur et le mot de passe attribués à une personne pour accéder à un site web spécifique, par exemple.

Dans le contexte du CCP, les **fournisseurs de justificatifs** sont responsables de créer et de gérer les justificatifs. Ils créent et fournissent des fonctions qui consistent en des processus visant à s'assurer que :

- les justificatifs sont émis (ou envoyés) au bon sujet;
- les justificatifs sont révoqués ou suspendus si et quand nécessaire;
- les renseignements enregistrés dans les justificatifs sont à jour et exacts; et
- les justificatifs sont détruits d'une façon appropriée à la fin de leur cycle de vie utile.

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

- les renseignements sur les justificatifs peuvent être divulgués au besoin et selon les critères de conformité spécifiés;
- les parties dépendantes peuvent vérifier les renseignements divulgués dans un justificatif selon les circonstances et les détails de mise en œuvre (p. ex. entièrement, certaines données ou comme preuve à divulgation nulle; et
- les parties dépendantes peuvent vérifier le statut des justificatifs (p. ex., si les justificatifs ont été ou non révoqués ou rendus invalides).

5.1.2.1 Types de justificatifs

Le CCP définit deux types de justificatifs qui fournissent chacun un type spécifique de renseignements :

Justificatif	Type de description
Attribut	Justificatif qui fournit un ou plusieurs renseignements à propos d'une entité. Justificatif simple émis par une province, qui contient un seul renseignement attestant l'âge de l'entité. Justification simple attestant le niveau d'autorisation de sécurité de l'entité. Justificatif attestant le fait qu'un certain numéro de téléphone mobile est attribué à l'appareil de

	l'entité. Justificatif plus complexe qui est un relevé de notes universitaire comportant des données identifiant les cours qu'un étudiant a suivis.
Relation	Justificatif qui atteste qu'une entité est rattachée, affiliée ou reliée d'une certaine façon à une deuxième entité. Exemple : justificatif émis par un registraire d'entreprise attestant qu'une personne est un dirigeant de société ou justificatifs émis par la société à ses employés prouvant qu'ils travaillent pour l'entreprise. Une délégation de pouvoirs est un type de relation particulier. Ces justificatifs attestent qu'une entité a délégué certains droits, privilèges, autorisations, etc. à une deuxième entité. Exemple : un simple justificatif attestant le fait qu'un dirigeant d'entreprise a délégué une autorisation financière à une entité.

5.1.2.2 Processus habituellement exécutés par des fournisseurs de justificatifs

Processus	**Description**
Émission d'un justificatif	Processus au cours duquel un justificatif est créé, attribué à un sujet (c.-à-d. une personne, une organisation, une application ou un appareil) et optionnellement relié à un ou plusieurs authentifiants. Les authentifiants peuvent être ensuite utilisés pour prouver qu'un justificatif fait référence au même sujet initialement relié au justificatif.
Maillage identité-justificatif	Processus consistant à associer des justificatifs à un acteur attribué.
Maintenance d'un justificatif	Le processus inclut des activités propres au cycle de vie, comme la mise à jour des détails des justificatifs. Il est habituellement entrepris par le sujet, mais peut aussi l'être par un administrateur de système ou automatiquement par le système.
Suspension d'un justificatif	Un justificatif émis est suspendu. Cela peut être déclenché par le sujet (p. ex., mot de passe oublié) ou le système (p. ex., blocage après une succession d'authentifications ratées, une inactivité, une activité suspecte, etc.). Un justificatif suspendu ne peut être transmis à une partie dépendante, ce qui assure que le sujet se voit refuser l'accès.
Récupération d'un justificatif	Un justificatif suspendu revient à un état stable (c.-à-d. un justificatif émis). Le processus peut être déclenché par le sujet, l'administrateur de système ou automatiquement par le système.
Révocation d'un justificatif	Cela permet de s'assurer qu'un justificatif est 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.
Authentification d'un justificatif	Ce processus consiste à s'assurer qu'un sujet contrôle le justificatif qui lui a été émis.

5.1.3 Authentifiants

Renseignements ou caractéristiques biométriques contrôlés par une personne qui est un cas spécifique de quelque chose que le sujet a, connaît, est ou fait. Les authentifiants sont utilisés à l'intérieur de l'écosystème pour utiliser des systèmes à accès restreint ou protégés (p. ex., protocole de connexion au site web d'une institution financière). Un authentifiant peut être une simple combinaison nom d'utilisateur-mot de passe ou un objet plus complexe comme un jeton d'accès ou des données biométriques.

Dans le contexte du modèle de CCP, le terme « authentifiant » n'est pas synonyme de « justificatif ».

Les **fournisseurs de services d'authentification** sont responsables de créer et de gérer des authentifiants. Ils exécutent des fonctions qui assurent la gestion du cycle de vie de l'authentifiant (y compris les processus d'émission, de suspension, de récupération, de maintenance, de révocation et de destruction des authentifiants).

5.1.3.1 Processus habituellement exécutés par des fournisseurs de services d'authentification

Processus	**Description**
Émission d'un authentifiant	Processus au cours duquel un authentifiant 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 authentifiants.
Maillage identité-authentifiant	Processus consistant à associer des authentifiants à un acteur attribué.
Maintenance d'un authentifiant	Le processus inclut des activités propres au cycle de vie, comme la suppressions des authentifiants, le maillage de nouveaux authentifiants et la mise à jour des authentifiants (p. ex., changement de mot de passe, mise à jour des questions et réponses de sécurité). Il est habituellement entrepris par le sujet, mais peut aussi l'être par un administrateur de système ou automatiquement par le système.
Suspension d'un authentifiant	Un authentifiant émis est suspendu. Cela peut être déclenché par le sujet (p. ex., mot de passe oublié) ou le système (p. ex., blocage après une succession d'authentifications ratées, une inactivité, une activité suspecte,

	etc.). Un authentifiant suspendu ne peut être transmis à une partie dépendante, ce qui assure que le sujet se voit refuser l'accès.
Récupération d'un authentifiant	Un authentifiant suspendu revient à un état stable. 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 authentifiant qui avait été suspendu en raison d'une inactivité; • Après un délai prédéfini, le système libère automatiquement un authentifiant qui a été suspendu à la suite d'un excès de tentatives d'authentification infructueuses.

5.2 Utilisation des représentations numériques

Pour la plupart des gens, l'identification, l'accès à un compte ou la démonstration 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 de représentations numériques à ces fins.

Les interactions qui dépendent de représentations numériques de confiance sont souvent des interactions entre une parie dépendante et le sujet d'une représentation numérique :

- **Partie dépendante** – Dans ce contexte, une partie dépendante est le participant à l'interaction qui requiert une représentation numérique pour une raison valable. Les parties dépendantes ont normalement besoin de renseignements pour identifier des sujets, vérifier certains attributs ou accorder l'accès à un système protégé. Dans bien des cas, la partie dépendante est un programme gouvernemental, un organisme sans but lucratif, ou une entreprise privée qui offre des services en ligne au public ou à un nombre limité d'utilisateurs. La partie dépendante peut être une unité d'affaires au sein d'une organisation plus grande. L'unité bancaire de détail qui gère un système d'ouverture de compte en ligne pour une grande institution financière peut, par exemple, se fier aux renseignements fournis par une unité d'identité et de sécurité interne pour interagir avec ses clients.
- **Sujet** – L'entité représentée par le sujet et à laquelle appartiennent les données contenues dans une représentation numérique (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 habituellement une personne qui souhaite effectuer une transaction, accéder à un système ou interagir d'une façon quelconque avec une partie dépendante.

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

- D'autres participants à l'écosystème puissent intervenir dans des fonctions spécifiques reliées à l'utilisation de représentations numériques;

- Des interactions peuvent se produire directement entre des sujets (c.-à-d., dans une interaction de pair à pair sans que d'autres parties interviennent); et
- Des interactions peuvent se produire sans intervention directe du sujet.

Étant donné la nature variée de ces modèles d'interaction, ce document se limite à donner un aperçu des processus fondamentaux intervenant dans l'utilisation de représentations numériques.

5.2.1 Confirmation d'une représentation numérique

Les processus de confirmation assurent que :

1. L'identité d'une entité est connue avec un certain degré de certitude; et
2. Les renseignements qui font partie d'une représentation numérique sont exacts, valides ou appropriés pour l'usage.

Processus	**Description**
Validation d'une identité	Confirmation de l'exactitude des renseignements d'identité à propos d'un sujet telle qu'établir par une partie faisant autorité. Il est à noter que la validation de l'identité n'assure pas que l'entité utilise ses propres renseignements d'identité (il s'agit de la vérification de l'identité) – seulement que les renseignements d'identité que le sujet utilise sont exacts par rapport à un dossier qui fait autorité.
Vérification d'une identité	Confirmation que les renseignements d'identité présentés sont associés au sujet qui fait l'affirmation. 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 des méthodes différentes et utiliser des renseignements personnels qui ne sont pas reliés à l'identité. Différentes méthodes peuvent être utilisées (séparément ou combinés), par exemple : • Confirmation basée sur les connaissances (p. ex., questions pour vérifier les réponses) • Confirmation biologique ou comportementale (p. ex., utilisation des empreintes digitales) • Confirmation d'une référence de confiance (p. ex., confirmation de l'identité basée sur des renseignements détenus par un organisme gouvernemental • Confirmation de possession physique (p. ex., possession d'un jeton ou d'un dispositif spécifique

Authentification d'un justificatif ou d'un authentifiant	Ce processus donne un niveau d'assurance quant au fait qu'une entité contrôle un justificatif ou un authentifiant émis à cette entité.
Maillage d'une identité	Processus qui consiste à s'assurer que le bon sujet est convenablement associé dans différents contextes de prestation de services. Ce processus dépend des contraintes d'autorisation et respect de la vie privée, et il peut entraîner l'association d'une identité à un identifiant de service et/ou la cartographie de plusieurs identifiants de services associés à une entité.
Présentation d'une identité	Confirmation dynamique qu'un sujet a une existence continue à la longue (c.-à-d., une « réelle présence »). Cela peut servir à s'assurer qu'il n'y a pas d'activité (passée ou présente) malveillante ou frauduleuse et à répondre aux craintes d'usurpation d'identité.

5.2.2 Consentement pour l'utilisation de la représentation numérique

Ces processus assurent que les sujets des représentations numériques comprennent quels renseignements dans une représentation numérique sont utilisés et à quelle fin – et permettent qu'ils soient utilisés là où c'est applicable.

Processus	**Description**
Formuler l'avis	Produit une déclaration qui décrit quels renseignements personnels sont recueillis; avec quelles parties 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; la période de validité de la déclaration; et la province, le territoire ou l'autorité où la déclaration est applicable. La déclaration est présentée au sujet (c.-à-d. la personne naturelle à qui appartiennent les renseignements personnels en question) sous la forme d'une notification.
Demander le consentement	Présente la notification au sujet et fournit au sujet un moyen de donner ou non son consentement en fonction du contenu de la notification, ce qui résulte en un consentement.
Enregistrer le consentement	Entrepose la notification et le consentement du sujet. En outre, les renseignements sur le sujet, la version de la notification présentée, la date et l'heure où la notification a été présentée et, le cas échéant, la date d'expiration du consentement peuvent être entreposés. Une fois les renseignements sur le consentement

	entreposés, une notification du consentement peut être transmise aux parties pertinentes au consentement.
Gérer le consentement	Le processus de gestion du consentement gère le cycle de vie des consentements et comporte deux sous-processus : 1. Examen : Le processus d'examen du consentement consiste à rendre les détails d'un consentement enregistré visibles pour le sujet ou une autre personne autorisée; 2. Mise à jour : La mise à jour d'un consentement consiste pour le sujet à donner un consentement révisé à partir d'un consentement préalablement enregistré. Le sujet pourrait notamment révoquer le consentement. Ce processus aboutit à un consentement mis à jour (qui devra être maintenu par le biais du processus d'enregistrement du consentement).

5.3 Habiliter les systèmes d'identité numérique

Le but du CCP est de permettre la mise en place d'un écosystème canadien de l'identité numérique et de le soutenir. L'interfonctionnement et la collaboration, combinés à un processus de gouvernance responsable parmi les participants dans un environnement sûr et qui protège davantage la vie privée sont au cœur d'un tel écosystème. Afin de réussir à atteindre ce but, le CCP définit des exigences et des lignes directrices qui établissent un niveau de fiabilité pour les processus menés à l'intérieur de l'écosystème. Ces processus sont exécutés dans une infrastructure partagée publique, privée, fiable et non fiable : les 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 CCP en ce qui concerne cette infrastructure est de s'assurer que la confiance créée au niveau des fonctions et des processus est également présente dans l'infrastructure qui est propice à l'écosystème de l'identité numérique. Cela permet de s'assurer que l'infrastructure soutient la prestation de services de confiance et s'attaque aux défis communs à tous les participants.

À cette fin, le CCP définit des normes et des lignes directrices pour les processus que les **fournisseurs d'infrastructures** procurent à d'autres participants. Ces processus, qui relèvent d'une infrastructure technique et opérationnelle, incluent :

- La sécurité physique et des systèmes;
- La confidentialité, l'intégrité et la disponibilité des données
- Le signalement des incidents; et
- La tenue des dossiers.

5.3.1 Infrastructure technique

Ces processus assurent la sécurité et l'intégrité des composantes de l'infrastructure habilitante.

Processus	Description
Sécurité	Pratiques de sécurité TI conçues pour assurer la confidentialité, l'intégrité et la disponibilité de l'infrastructure de soutien.
Gestion des données	Processus et politiques pour la gestion du cycle de vie des données de représentation numérique, incluant la supervision permanente de la collecte, de la validation, de l'entreposage et de l'accessibilité des données.
Audit et journalisation	Processus et politiques pour la gestion du cycle de vie des données de représentation numérique, incluant la supervision permanente de la collecte, de la validation, de l'entreposage, de l'accessibilité et de la destruction des données.
Normes techniques	Référence du CCP aux normes de l'industrie pertinentes afin de soutenir des fonctions spécifiques, incluant l'interaction entre les participants au CCP.

5.3.2 Infrastructure des opérations

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

Processus	Description
Gestion des risques	Processus pour identifier les risques directs et indirects pour les fonctions soutenues et les efforts connexes afin de réduire ou d'éliminer la probabilité que ces risques ne surviennent. Les catégories de risques habituelles incluent les processus opérationnels, la gestion de l'information, et l'intendance des renseignements personnels.
Gestion des dossiers	Processus qui soutiennent les activités habituelles de tenue de dossiers pour les fonctions soutenues. Cela inclut la classification, les calendriers de rétention, la préservation et l'élimination.
Gestion des incidents et différends	Processus pour identifier les évenements qui affectent négativement les fonctions soutenues et (dans le cas de différends) les participants à l'écosystème, les évaluer et y réagir – y compris les efforts pour réduire ou éliminer la probabilité que les incidents ne se répètent.

6 Contrôle des versions du document

Numéro de version	Date de publication	Auteurs	Description
0.01	2019-01-16	Gregory Natran	Ébauche initiale de recommandations pour discussion
0.02	2019-02-04	Gregory Natran	Ébauche mise à jour incorporant les commentaires du TFEC à ce jour
0.03	2019-05-08	Gregory Natran	Ébauche mise à jour incorporant la rétroaction provenant d'un examen ouvert
1.0	2019-05-15	Gregory Natran	Ébauche de recommandations V1.0
1.1	2019-09-19	Gregory Natran	Ébauche mise à jour incorporant la plus récente rétroaction publique
1.1.1	2019-10-18	Équipe de rédaction du CCP	Mise à jour des descriptions des composantes du CCP
1.1.2	2019-11-30	Équipe de rédaction du CCP	Mise à jour des définitions des termes pour assurer une uniformité avec le glossaire du CCP
1.1.3	2019-12-12	Équipe de rédaction du CCP	Mises à jour faisant suite aux commentaires reçus lors de l'examen du TFEC qui a pris fin le 6 décembre
1.1.4	2020-05-28	Équipe de rédaction du CCP	Mises à jour basées sur les énoncés de portée révisés « Connexion vérifiée » a été changé pour « Authentification » « Gouvernance » a été changé pour « Évaluation »
1.0	2020-07-02	Équipe de rédaction du CCP	Recommandation finale V1.0