SOUS-COMITÉ
LA GESTION DE L'IDENTITÉ (SCGI)

LE PROFIL DU SECTEUR PUBLIC DU CADRE DE CONFIANCE PANCANADIEN (CCP) DU SCGI
VERSION 1.0

Document Version :	0.6
État du document :	Ébauche aux fins de recommandation
Date :	2019-07-04
Classification de sécurité :	NON CLASSIFIÉ

CONTRÔLE DES VERSIONS DU DOCUMENT

Numéro Nombre	Date de publication	Auteur(s)	Courte description
0.1	2019-02-20	GT CCP SCGI	Première ébauche
0.2	2019-02-28	GT CCP SCGI	Version révisée de l'ébauche
0.3	2019-03-21	GT CCP SCGI	Version révisée de l'ébauche
0.4	2019-03-28	GT CCP SCGI	Ébauche aux fins de consultation
0.5	2019-05-30	GT CCP SCGI	Ébauche aux fins de consultation
0.6	2019-07-04	GT CCP SCGI	Ébauche aux fins de recommandation

TABLE DES MATIÈRES

LISTE DES FIGURES

RÉSUMÉ

Le présent document décrit la **version 1.0** du profil du secteur public du ***Cadre de confiance pancanadien (CCP)***. Le présent document est structuré de la façon suivante :

- **Les parties 1 à 4 présentent l'objet et le contexte liés à l'origine et à l'application du CCP.**
- **La partie 5** présente les principaux concepts et éléments du CCP.
- **La partie 6, l'annexe, donne un aperçu du matériel de gestion de l'identité, bénéfique pour le lecteur qui a besoin d'informations complémentaires.**

Le CCP est conçu pour permettre la transition vers un écosystème de l'identité numérique qui est bénéfique pour tous les Canadiens et toutes les entreprises. Le CCP est conçu pour être simple et intégré; pour être technologiquement agnostique; pour compléter les cadres existants; et pour être clairement mis en correspondance avec des politiques, des règlements et des lois. Il est également conçu pour appliquer les normes pertinentes aux processus et aux capacités clés.

Le CCP définit deux types de ***représentations numériques de confiance*** requises pour l'écosystème des identités numériques : 1) ***les identités numériques de confiance*** de personnes et d'organisations et 2) ***les relations numériques de confiance*** entre les personnes, entre les personnes et les organisations et entre les organisations.

Le CCP est conçu pour répondre aux besoins des différentes collectivités qui ont besoin d'identités numériques dignes de confiance, dans le secteur public et le secteur privé. Le CCP a été défini d'une façon qui encourage l'innovation et l'évolution de l'écosystème des identités numériques. Le CCP permet l'interopérabilité des différentes plates-formes, des services, des architectures et des technologies, travaillant de concert en formant un ensemble cohérent.

Le CCP appuie l'acceptation des identités et des relations numériques de confiance en définissant un ensemble de processus atomiques qui peuvent être mis en correspondance avec des processus opérationnels existants, évalués de façon indépendante à l'aide de critères de conformité et certifiés comme étant dignes de confiance et interopérables dans les nombreux contextes qui composent l'écosystème des identités numériques.

Enfin, le CCP sert à habiliter les Canadiens en veillant à ce que le droit d'une personne à une identité ne puisse pas être compromis, que la protection de la vie privée et la sécurité demeurent essentielles à la pleine participation, et que la commodité et le choix fassent partie des facteurs d'adoption. Grâce au CCP, les Canadiens seront en mesure de choisir tout partenaire approuvé, d'utiliser tout appareil sur une plate-forme et d'avoir accès à tous les services dont ils ont besoin.

Remarque : Le jaune indique le texte centré sur les personnes qui sera modifié afin d'inclure les organisations dans la prochaine itération du document.

1 OBJET DU PRÉSENT DOCUMENT

Le présent document vise à décrire le profil du secteur public du Cadre de confiance pancanadien (CCP)[1].

Le public cible de ce document comprend :

- les membres de la collectivité de l'identité numérique issus des secteurs public et privé (y compris les organismes de réglementation et de normes) – à titre d'intervenants et de contributeurs clés du CCP;
- les fournisseurs de services et de technologies d'identité numérique – afin de leur montrer où ils cadrent dans le CCP et de les aider à définir les exigences relatives à leurs produits et services et à évaluer l'intégrité de leurs processus;
- les fournisseurs de services et les consommateurs de services – pour évaluer l'utilité d'employer des solutions et des processus d'identité numérique de confiance au moment d'interagir en ligne.

2 PORTÉE ET APPLICATION DU CCP

La portée du CCP englobe ce qui suit :

- l'univers des personnes se trouvant au Canada, qui est défini comme toutes les personnes vivantes qui résident au Canada ou qui visitent le pays, ainsi que toutes les personnes décédées dont une identité a été établie au Canada;
- l'univers des organisations au Canada, qui est défini comme toutes les organisations enregistrées et en activité au Canada, de même que les organisations inactives, dont une identité a été établie au Canada;
- l'univers des relations au Canada de personnes à personnes, d'organisations à organisations et de personnes à organisations.

Le CCP permet de réaliser un processus d'évaluation complet dans le cadre de programmes d'identité numérique au Canada.

[1] Le cadre de confiance pancanadien est le résultat d'une collaboration entre le Conseil de l'identification et de l'authentification numériques du Canada (CIANC) et le Sous-comité sur la gestion de l'identité (SCGI), issu des conseils mixtes du Canada. Les conseils mixtes du Canada sont un forum composé du Conseil de la prestation des services du secteur public (CPSSP) et du Conseil des dirigeants principaux de l'information du secteur public (CDPISP). Le présent document a été élaboré par le groupe de travail du SCGI sur le CCP (GT SCGI CCP) aux fins de discussion et de consultation, et son contenu n'a pas encore été approuvé, ni par le SCGI ni par le Conseil de l'identification et de l'authentification numériques du Canada (DIACC. Ce document est publié en vertu de la Licence du gouvernement ouvert – Canada, qui se trouve à l'adresse suivante : https://ouvert.canada.ca/fr/licence-du-gouvernement-ouvert-canada.

3 TERMES ET DÉFINITIONS

La définition des divers termes utilisés dans le présent document se trouve à l'annexe B : Termes et définitions.

4 RENSEIGNEMENTS GÉNÉRAUX ET CONTEXTE

4.1 L'approche pancanadienne pour la gestion de l'identité

L'approche pancanadienne pour la gestion de l'identité[2] est une entente de principes et de normes en vue d'élaborer des solutions qui peuvent être utilisées par tous les Canadiens[3]. Cette approche reconnaît que, même s'il y a des dépendances et des différences entre les organisations, il est possible d'appliquer une approche homogène et axée sur les citoyens dans le cadre de la prestation de services numériques, en définissant une approche convenue qui est mise en œuvre et évaluée de façon uniforme.

4.2 Évolution des modèles d'identité et des cadres de confiance

Le modèle d'identité centralisé est le modèle d'identité le plus ancien et le plus couramment utilisé. Chaque organisation ou programme avec lequel une personne interagit, émet un justificatif à cette dernière (habituellement un nom d'utilisateur et un mot de passe) qui ne peut être utilisé que pour avoir accès à son service. Ainsi, cette personne finit par posséder de nombreux noms d'utilisateur et mots de passe qui sont difficiles, voire impossibles à gérer.

Le modèle de l'identité fédérale est un modèle d'identité plus récent qui s'attaque au problème de l'émission de multiples justificatifs à des personnes. Au lieu de gérer de multiples justificatifs, une personne reçoit un justificatif par fédération. Cette fédération permet à la personne d'avoir accès, à partir de ce justificatif unique, à toutes les organisations et tous les programmes qui ont accepté de faire partie de la fédération.

Une fédération est un accord de coopération entre des entités autonomes qui ont convenu de travailler ensemble. Elle repose sur des relations et des normes de confiance à l'appui de son interopérabilité. Une fédération peut regrouper des organisations du secteur public et du secteur privé, différentes administrations ou divers pays.

À mesure qu'elles évoluent, les fédérations établissent des processus formalisés d'évaluation, des accords contractuels, des ententes de service, des obligations juridiques et des mécanismes de règlement des différends. Collectivement, ces composantes sont appelées cadres de confiance fédérés.

L'identité auto-souveraine est le modèle émergeant le plus récent. Le modèle de l'identité auto-souveraine redonne le contrôle aux personnes et aux organisations. Ce modèle élimine le besoin de recourir aux tiers de confiance pour effectuer certains types d'interactions comme l'authentification et la vérification des preuves.

---

[2] Pour une introduction générale aux concepts de gestion de l'identité, voir l'*annexe A : Aperçu de la gestion de l'identité*.

[3] Disponible à (inscription au secteur public requise) : https://gccollab.ca/file/view/36223/imsc-paper-trusting-identities-consultation-draft-enpdf.

Il existe un nouvel écosystème mondial émergent, comprenant des technologies plus récentes, notamment : les grands livres décentralisés et les protocoles de consensus. Cette nouvelle infrastructure n'exclut pas nécessairement mutuellement les régimes existants : elle est capable d'intégrer des bases de données centralisées et des systèmes fédérés d'identité établis. Ces technologies devraient coexister dans un avenir prévisible. Il est également possible que les plateformes autonomes décentralisées émergent et fonctionnent indépendamment de l'un(e) ou l'autre organisation ou État nation.

On s'attend à ce que, avec le temps, les différents modèles (centralisés, fédérés, et de l'identité auto-souveraine) évoluent, coexistent, et soient en concurrence les uns avec les autres. Les cadres de confiance, notamment le cadre de confiance pancanadien, font partie d'un contexte numérique plus grand. Le CCP ne vise pas à privilégier un modèle particulier d'identité ou de plateforme technologique. Il a plutôt pour objectif d'évoluer parallèlement et favorablement aux divers écosystèmes numériques qui se développeront.

4.3 Contexte

Les technologies et les services qui permettent aux gens d'interagir avec les gouvernements, les entreprises et d'autres personnes de façon pratique et efficace sur le plan numérique offrent des possibilités considérables sur le plan de l'innovation et du développement économique et social. Pour exploiter ce potentiel, il faut absolument pouvoir faire confiance aux renseignements concernant les différents participants à ces interactions. Le CCP appuie cet aspect des services numériques en tant que cadre de confiance fournissant des processus cohérents et vérifiables pour la création, la gestion et l'utilisation de représentations numériques de personnes et d'organisations.

Toutefois, pour être efficace, l'utilisation de représentations numériques doit adopter une échelle allant au-delà d'un nombre limité de relations. Il faut s'en servir au-delà des intégrations ponctuelles. Les clients, les consommateurs et les utilisateurs étant un centre d'intérêt pour la plupart des intervenants, les représentations numériques de ces entités doivent être acceptées entre les différents fournisseurs de service, secteurs économiques, ordres de gouvernement et administrations. En pratique, cela signifie qu'une personne, ou tout autre participant, doit pouvoir utiliser et gérer les renseignements qui les concernent dans des contextes multiples de l'économie.

Pour atteindre un haut degré d'interopérabilité, il faut établir une confiance mutuelle. Les fournisseurs de services doivent savoir avec qui ils interagissent par voie numérique. Les consommateurs de services, les particuliers et d'autres encore doivent avoir confiance dans l'identité des services avec lesquels ils interagissent. Sans confiance et interopérabilité, le Canada risque de perpétuer l'existence d'obstacles organisationnels, politiques et techniques qui :

- ont contribué à la surabondance des procédures de vérification, des inscriptions, des comptes, des mots de passe, des noms d'utilisateurs, des profils d'utilisateur et des systèmes nécessaires à leur administration;

- nuisent aux efforts de modernisation qui visent à favoriser l'innovation et améliorer l'expérience, l'efficacité et l'efficience des services.

Qui plus est, les Canadiens s'attendent à ce que leur écosystème de l'identité numérique fonctionne de manière transparente, veillant à l'équité pour tous et promouvant la protection du droit à la vie privée dès la conception. Ils s'attendent à être avertis de manière claire et utile lorsque des renseignements à leur sujet sont recueillis, gérés et divulgués.

4.4 But

L'objectif du CCP est de permettre et d'appuyer l'établissement d'un écosystème numérique canadien novateur, sécuritaire et respectant la vie privée – tout en respectant les droits humains fondamentaux à l'ère numérique – dans l'ensemble de l'économie. À cet égard, le CCP cherche à faciliter la migration des interactions en personne traditionnelles ou complexes vers des interactions numériques qui placent les gens au cœur de l'écosystème de l'identité numérique, tout en reconnaissant que les processus opérationnels analogues continueront d'exister pendant un certain temps.

Le CPCFI facilite l'élaboration d'un écosystème canadien d'identité numérique en :

- garantissant que l'écosystème de l'identité numérique canadien est digne de confiance;
- encourageant un environnement équitable, novateur et compétitif pour les participants;
- encourageant les institutions du secteur public à investir dans les biens publics;
- se concentrant sur la transparence et la vie privée en ce qui concerne l'utilisation et la divulgation des renseignements personnels;
- appuyant l'intégration de participants offrant une vaste gamme de services;
- cernant les politiques et les normes technologiques existantes s'appliquant à l'écosystème de l'identité numérique;
- maintenant une perspective prospective et déterminant les éventuels secteurs de collaboration, de développement et de normalisation.

4.5 Objectifs

Le CCP reconnaît que malgré les dépendances et les différences entre les administrations, les industries et les participants individuels, on peut réaliser une approche uniforme en matière de développement de l'écosystème de l'identité numérique en mettant en œuvre, de manière uniforme, des normes, des lignes directrices, des critères et des pratiques généralement acceptés. Conséquemment, les objectifs du CPCFI visent à garantir la fiabilité de l'écosystème canadien d'identité numérique en :

1. définissant les rôles et les fonctions des participants dans l'écosystème de l'identité numérique;
2. facilitant les interactions au sein de l'écosystème de l'identité numérique en définissant les exigences et les lignes directrices qui établissent le niveau de fiabilité pour les processus exécutés par les participants de l'écosystème.

4.6 Principes directeurs

Pour atteindre ses buts et ses objectifs, le CCP est orienté par l'ensemble de principes publics et privés qui régissent le développement de l'écosystème numérique canadien.

En 2018, trois principes directeurs[4] ont été établis par le SCGI :

1. le droit d'une personne à avoir une identité ne peut être remis en question;
2. la protection des renseignements personnels et la sécurité sont des éléments essentiels pour permettre aux Canadiens de participer avec confiance à la société numérique;
3. la commodité et le choix sont des facteurs clés pour les citoyens.

En 2019, dix principes directeurs ont été établis par le DIACC :

1. **Appuyer des solutions robustes, sûres et évolutives** – L'écosystème de l'identité numérique canadien doit être suffisamment robuste pour garantir la sécurité, la disponibilité et l'accessibilité en tout temps.
2. **Mettre en œuvre, protéger et améliorer la protection des renseignements personnels par la conception** – Les outils d'amélioration de la protection des renseignements personnels permettent à une personne de gérer ses renseignements personnels ainsi que les fins auxquelles ils sont utilisés. Ces outils peuvent notamment appuyer le droit d'un utilisateur d' « être oublié » (lorsque cela est justifié dans le contexte législatif du participant au cadre de confiance).
3. **Être inclusif, ouvert et répondre aux besoins généraux des intervenants** – Les services et outils de l'écosystème de l'identité numérique doivent être abordables, normalisés, et créer de la valeur pour les utilisateurs afin de favoriser une adoption généralisée et profiter à tous les Canadiens.
4. **Faire preuve de transparence en matière de gouvernance et de fonctionnement** – Les Canadiens doivent être confiants quant au fait que les

[4] Le texte intégral du document stratégique se trouve à l'adresse suivante : https://drive.google.com/a/gcdigital.canada.ca/file/d/13Q5hTrvSVlBSIjbzQ0jaV0kjNVaC_edw/view?usp=sharing.

services offerts dans l'écosystème de l'identité numérique respecteront et répondront à leurs besoins et à leurs attentes.

5. **Permettre aux Canadiens d'avoir le choix, le contrôle et de bénéficier de la commodité** – Les services reposent sur le principe que les personnes peuvent choisir quels renseignements peuvent être partagés, quels services utiliser, et de quels pays, et ils sont informés des avantages et des conséquences des identités numériques.
6. **Miser sur des protocoles fondés sur des normes ouvertes** – L'utilisation de normes ouvertes et des meilleures pratiques applicables dans le cadre de l'écosystème canadien d'identités numériques permet de se protéger contre l'obsolescence, d'assurer l'interopérabilité, et de favoriser un marché proposant des solutions dynamiques et concurrentielles.
7. **Maintenir l'interopérabilité internationale** – L'interopérabilité, la technologie mondiale et la normalisation des politiques sont fondamentales pour le monde connecté d'aujourd'hui. Tout comme les rails de chemin de fer à écartement standard permettent le déplacement et le transport des marchandises d'un pays à l'autre, la technologie ainsi que l'interopérabilité et la normalisation des politiques favorisent la communication dans le cadre des services numériques et permettent de réduire les coûts tout en augmentant les possibilités d'innovation.
8. **Être rentable et ouvert aux forces concurrentielles** – Il est essentiel que l'écosystème de l'identité numérique respecte les contraintes budgétaires du présent et de l'avenir. Le fait de veiller à ce que l'écosystème de l'identité numérique soit ouvert à la concurrence, représentant plusieurs secteurs économiques, chacun jouant des rôles différents, entraînera une diminution des coûts pour tous les intervenants ainsi qu'un renforcement de l'innovation.
9. **Appuyer l'évaluation indépendante, la vérification et l'application des règles** – Pour que les Canadiens fassent confiance à un écosystème de l'identité numérique, des règles en matière de mesures de contrôle doivent être mises en place. Les évaluations permanentes, indépendantes du point de vue fonctionnel et réalisées par des tiers représentent un moyen de faire en sorte que les intervenants de l'écosystème de l'identité numérique respectent les exigences du cadre de confiance.
10. **Réduire le transfert de données entre les sources et éviter la création de nouveaux centres de stockage de renseignements liés à l'identité** – Les utilisateurs de services de l'écosystème numérique ne devraient avoir à fournir que les renseignements personnels nécessaires à une interaction précise.

5 CADRE DE CONFIANCE PANCANADIEN

5.1 Aperçu du CCP

Le Cadre de confiance pancanadien possède les caractéristiques suivantes :

1. **Il s'agit d'un cadre simple d'intégration qui est certes facile à comprendre, mais qui peut être appliqué dans des environnements complexes.**
2. **Technologie agnostique : Offre une flexibilité et une précision logique dans le cadre de l'évaluation de la fiabilité des solutions et des fournisseurs d'identité numérique.**
3. **Il complète les cadres existants (en matière de sécurité, de protection de la vie privée, de prestation de services, etc.).**
4. **Il fournit des liens clairs aux politiques, règlements et lois applicables, en établissant des critères de conformité qui peuvent être facilement adaptés.**
5. **Il normalise les processus et les capacités clés** afin de permettre la collaboration intersectorielle et le développement de l'écosystème de l'identité numérique.

Il convient de faire remarquer que le CCP, en soi, n'est pas un cadre de gouvernance. Il s'agit plutôt d'un outil permettant de mettre en œuvre les lois, les politiques et la réglementation pertinentes ainsi que les ententes entre les parties.

Le CCP est composé d'un ensemble de processus normalisés distincts pouvant être évalués de façon indépendante et certifiés comme interopérant l'un avec l'autre dans un écosystème de l'identité numérique. Un processus atomique est un ensemble d'activités logiquement mis en correspondance qui entraînent un état de transition. Le CCP peut aussi comprendre des processus composés. Un processus composé est un ensemble de processus atomiques et/ou d'autres processus composés qui entraînent un ensemble de transitions d'état. Tous les processus atomiques ont été conçus de façon à pouvoir être mis en œuvre en tant que services modulaires et à être évalués de façon indépendante aux fins de certification. Des processus atomiques supplémentaires peuvent être ajoutés au besoin et tous les processus atomiques peuvent être adaptés à divers critères de conformité.

Une fois qu'un processus atomique est attesté, on peut s'appuyer sur lui ou lui « faire confiance » et l'intégrer à d'autres plateformes de confiance de l'écosystème de l'identité numérique. Cet écosystème de l'identité numérique vise une interopérabilité absolue entre les différents secteurs, organisations et territoires, ainsi qu'avec d'autres cadres de confiance.

5.2 Principaux concepts

5.2.1 Cas d'utilisation initiaux pour le modèle du CCP

L'accent initial du CCP est les cas d'utilisation liés aux identités et aux relations numériques. Dans l'avenir, le CCP sera étendu à d'autres cas d'utilisation (p. ex., des biens, des contrats). En ce qui concerne les identités et les relations numériques, le CCP peut être considéré comme un ensemble de représentations numériques de confiance jumelées à une infrastructure de soutien. Cela est illustré dans la figure 1.

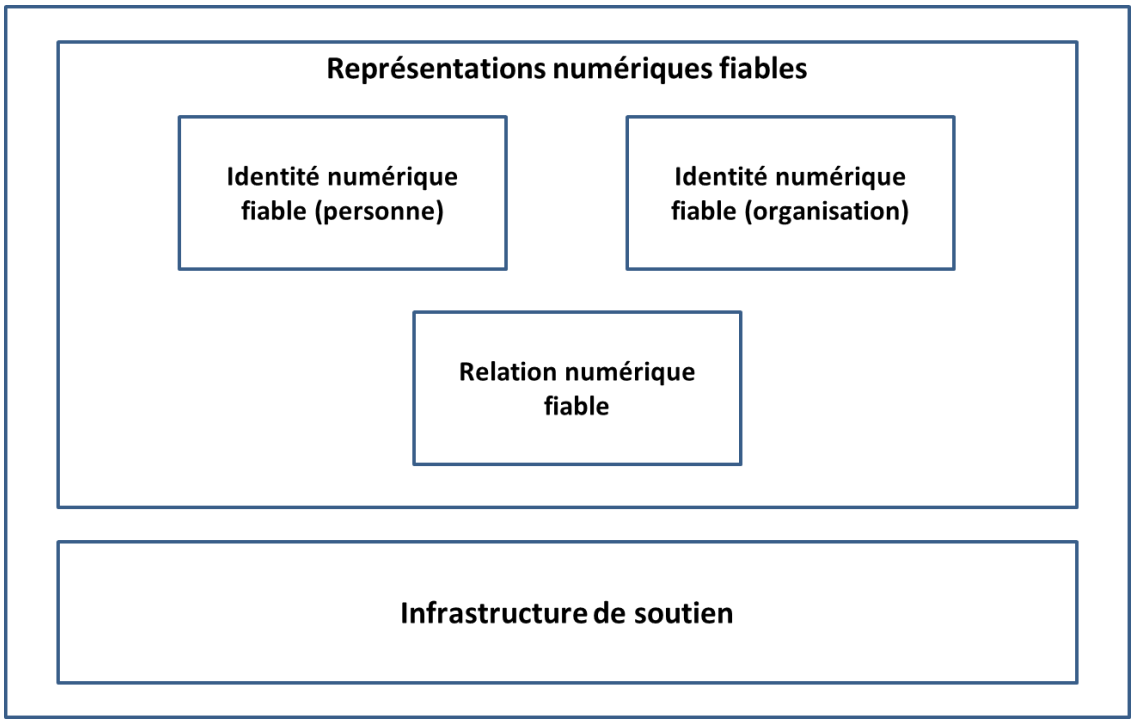

Figure 1 : Cas d'utilisation initiaux du modèle du CCP

5.2.2 Représentations numériques fiables

Une représentation numérique fiable est une entité pouvant être assujettie aux lois, aux politiques ou aux règlements dans un contexte, et pouvant avoir certains droits, devoirs et obligations. Les représentations numériques fiables sont destinées à être adaptées et à refléter les acteurs du monde réel, notamment les personnes et les organisations qui bénéficient de la mise en œuvre ou de l'utilisation du CCP. Ces acteurs du monde réel peuvent également être régis par une loi, une politique ou un règlement adapté au CCP, ce qui permet de clarifier les droits, les devoirs et les obligations qui peuvent s'étendre sur différents contextes (p. ex., compétences).

Actuellement, le CCP reconnaît deux types de représentations numériques fiables – les identités et les relations – qui sont définies comme suit :

1. **Identité numérique fiable :** Une identité numérique de confiance est une représentation électronique d'une personne ou d'une organisation employée exclusivement par la personne ou l'organisation en question, dans le but d'accéder à des services appréciables ou d'effectuer des transactions en toute confiance et avec assurance.
2. **Relation numérique fiable :** Une relation numérique fiable est une représentation électronique de la relation entre une personne et une autre personne, une organisation et une autre organisation, ou une personne et une organisation.

Au fur et à mesure que le CCP évolue, ces représentations peuvent s'étendre à des entités telles que les actifs et les contrats (c.-à-d., des actifs numériques et des contrats intelligents).

5.2.3 Infrastructure de soutien

L'infrastructure de soutien est l'ensemble des facilitateurs techniques, opérationnels, et stratégiques qui tiennent lieu d'infrastructure sous-jacente du CCP. Même si ces facilitateurs sont essentiels au CCP, ils font partie de l'infrastructure de soutien parce que des outils et des processus y sont déjà associés (p. ex., évaluation des répercussions sur la vie privée, évaluation et autorisation de sécurité). Le CCP vise à tirer parti de ces outils et processus autant que possible, tout en maintenant une série de processus atomiques précis au CCP et des critères de conformité.

La figure 3 illustre l'itération actuelle de l'infrastructure de soutien. Dans cette version, bon nombre de cases sont des espaces réservés pour indiquer un examen plus approfondi ou un développement futur.

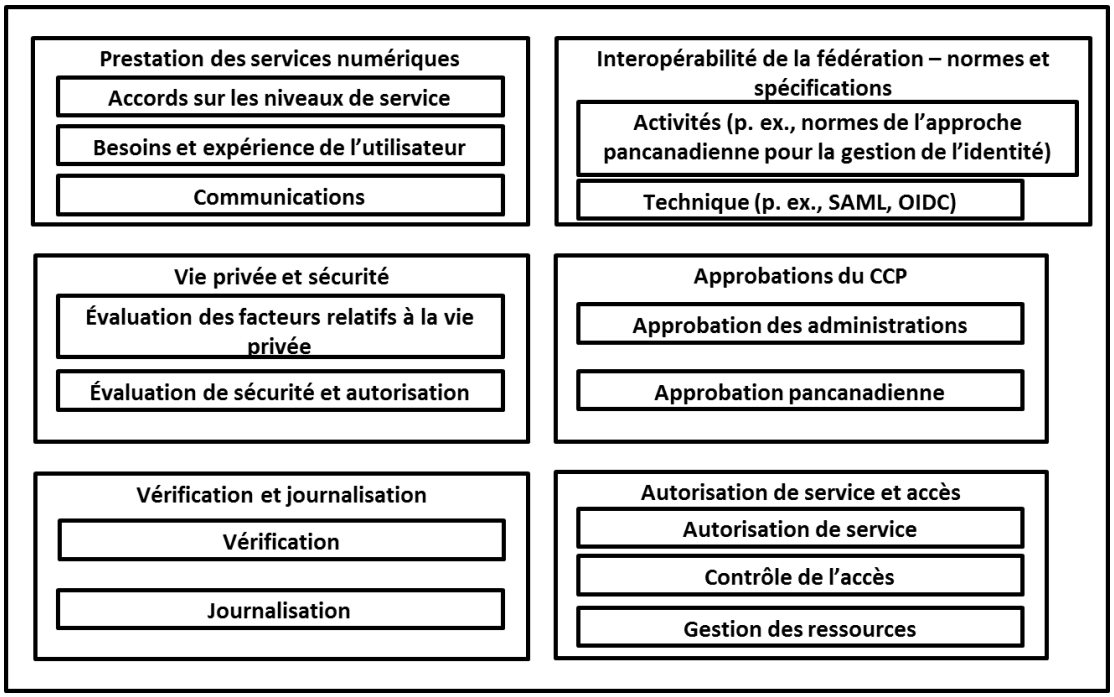

Figure 2 : Infrastructure de soutien

5.2.4 Domaines liés à l'identité

Le CCP établit une distinction claire entre l'identité principale et l'identité contextuelle. Une identité fondamentale est une identité qui a été établie ou changée à la suite d'un événement fondamental (p. ex., naissance, changement légal de nom, décès, immigration, résidence légale, citoyenneté, insérer des exemples d'organisations). Une identité contextuelle est une identité qui est utilisée à des fins précises dans un contexte d'identité précis[5]. Une identité contextuelle peut être liée ou non à une identité fondamentale. L'établissement et le maintien des identités fondamentales relèvent exclusivement du secteur public (plus précisément, les bureaux de l'état civil (BEC) et les registres des entreprises des provinces et des territoires (PT), Immigration, Réfugiés et Citoyenneté Canada (IRCC) et le registre des organisations de régime fédéral. L'identité contextuelle relève à la fois des secteurs public et privé. La figure 2 montre les domaines d'identité.

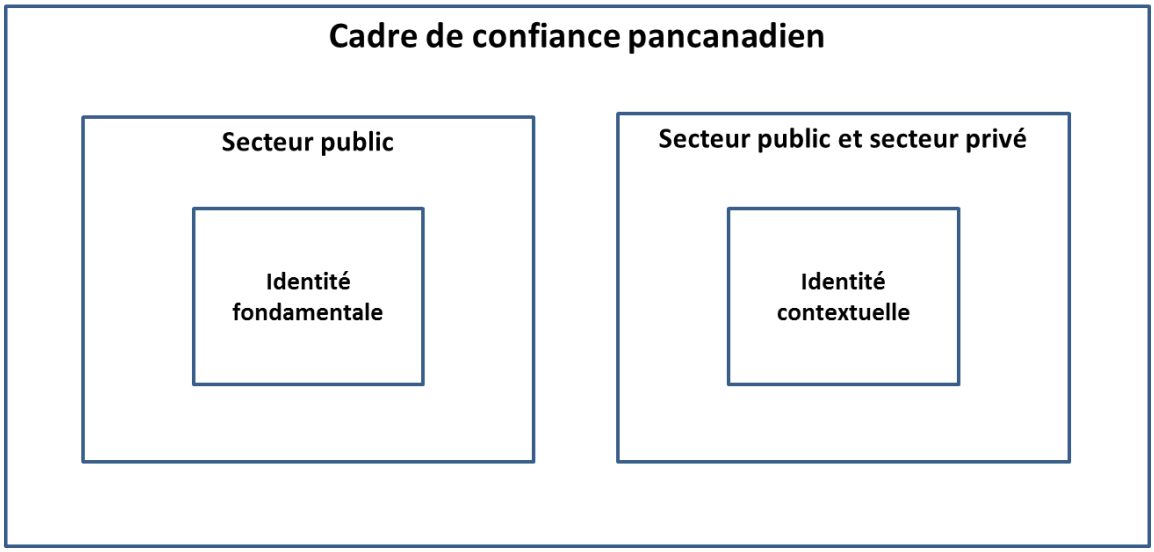

Figure 3 : Domaines d'identité

[5] En fournissant leurs programmes et leurs services, les organisations fonctionnent au sein d'un environnement ou d'un ensemble de circonstances particulières. C'est ce qu'on appelle le contexte de l'identité dans le domaine de la gestion de l'identité. Le contexte de l'identité est déterminé par des facteurs comme le mandat, la population cible (c.-à-d. les clients, la clientèle), et les autres responsabilités établies en vertu d'une loi, d'un accord ou d'une entente. Digital Identity and Authentication Council of Canada (DIACC)

5.3 Aperçu des processus du CCP

5.3.1 Processus fiables

Un *processus fiable* est un ensemble d'activités qui entraînent la transition de l'état d'un objet. D'autres processus peuvent se fier à l'état de sortie de l'objet à titre de *preuve*. La figure 4 illustre le *modèle de processus fiables*.

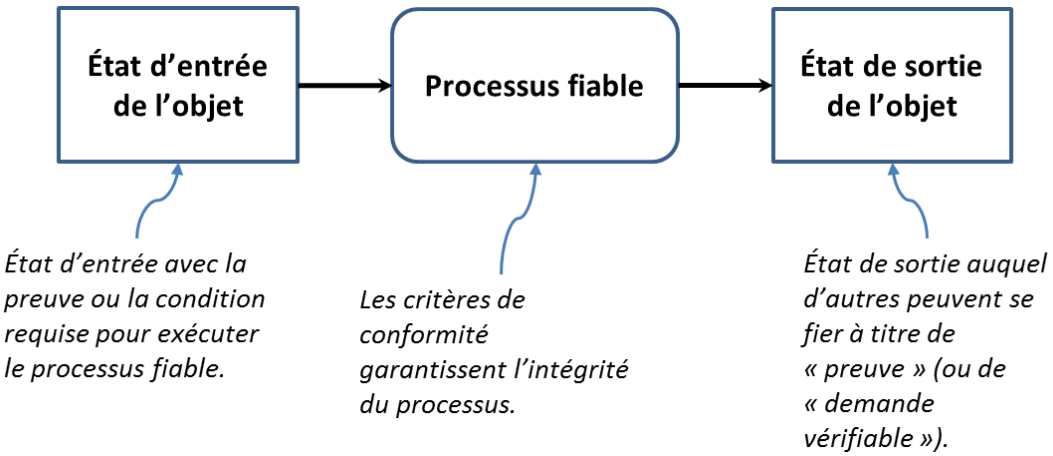

Figure 4 : Modèle de processus fiables

Les processus fiables sont des constituants essentiels permettant de veiller à l'intégrité générale de la chaîne d'approvisionnement numérique et, par extension, à l'intégrité des services numériques. L'intégrité du processus fiable relève de la plus haute importance, puisque le produit de ce processus est utilisé par de nombreux participants issus des secteurs public et privé et des administrations, et ce, à court et à long termes. Le CCP veille à l'intégrité des processus fiables, en établissant des critères de conformité convenus et bien définis qui facilitent la réalisation d'évaluations et d'attestations impartiales, transparentes et fondées sur les données probantes.

Les critères de conformité associés aux processus fiables précisent les étapes à suivre pour faire passer un objet de son état d'entrée à son état de sortie. Les critères de conformité ont pour but de veiller à ce que les processus fiables soient effectués avec intégrité. Par exemple, un processus fiable pourrait impliquer l'affectation d'un code d'identification à une personne. Les critères de conformité pourraient indiquer qu'une organisation responsable de gérer des processus fiables doit veiller à ce que le code d'identification en question soit unique au sein d'une population donnée.

5.3.2 Preuves de processus fiable et transmission

Le CCP a été élaboré de manière à être appliqué par différentes plateformes et architectures, qui peuvent toutes coexister l'une avec l'autre dans l'écosystème de l'identité numérique. À titre d'exemple, les plateformes et solutions d'identité fédérée utilisant les protocoles Secure Assertion Markup Language (SAML) et Open ID Connect (OIDC) peuvent coexister avec les nouvelles approches décentralisées axées sur les demandes, au moyen des porte-monnaie électroniques. Le CCP ne limite pas la possibilité de recourir à plusieurs fournisseurs concurrents et on s'attend à ce que de nombreux fournisseurs coexistent pour répondre aux besoins des différentes collectivités dans l'ensemble du secteur public et du secteur privé.

Afin de faciliter la coexistence de ces différents fournisseurs et différentes approches de solutions, le CCP établit une distinction entre les intrants et les extrants (c.-à-d., preuves) qui sont consommés et fabriqués grâce à des processus fiables, et le moyen de transmission (c.-à-d., la façon dont une preuve est transmise à travers un réseau et mise à la disposition de l'autre partie).

Les preuves de processus fiables sont indépendantes du modèle de transmission. Les preuves peuvent être transmises entre les parties, au moyen d'un modèle traditionnel/centralisé (p. ex., un tiers de confiance) ou d'un modèle décentralisé (p. ex., un registre distribué) ou des deux à la fois. Les preuves peuvent également être transmises directement entre les parties. Comme on peut le constater dans la figure 5, il existe une méthode de transmission entre les parties émettrices et destinataires des preuves.

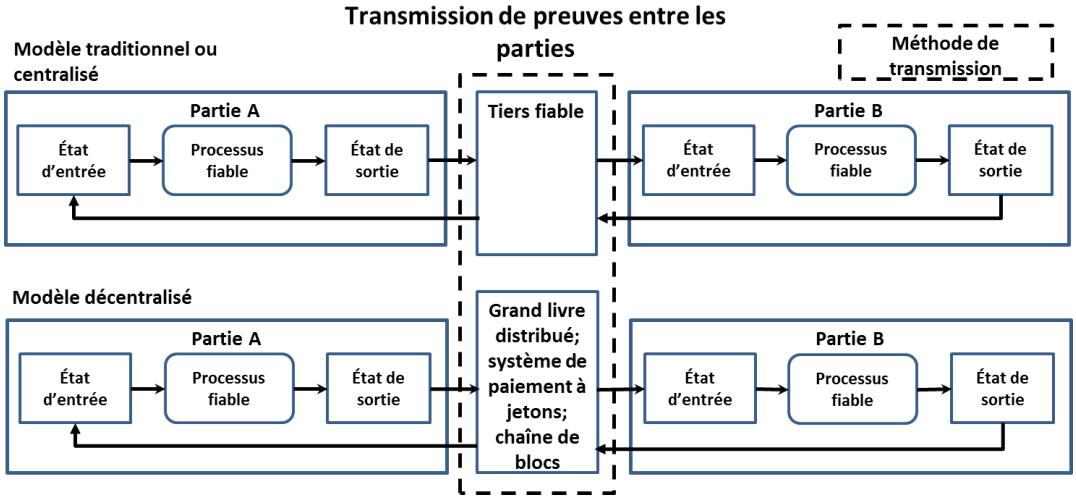

Figure 5 : Transmission de preuves entre les parties

Les exigences propres aux méthodes de transmission sont considérées comme faisant partie de l'infrastructure de soutien, et seront élaborées dans le cadre des exigences, normes et spécifications d'interopérabilité technique.

5.3.3 Aperçu des processus atomiques

Un processus atomique est un ensemble d'activités logiquement mis en correspondance qui entraînent un état de transition. À l'heure actuelle, le CCP reconnaît 24 processus atomiques :

- Résolution de l'identité
- Établissement de l'identité
- Validation de l'identité
- Vérification de l'identité
- Validation de la preuve
- Présentation de l'identité
- Maintien de l'identité
- Liaison identité-justificatif
- Établissement de liens pour déterminer l'identité
- Émission d'un justificatif
- Liaison justificatif-authentifiant
- Suspension d'un justificatif
- Recouvrement d'un justificatif
- Révocation d'un justificatif
- Authentification du justificatif
- Création de la signature
- Vérification de la signature
- Formulation d'avis
- Demande de consentement
- Enregistrement du consentement
- Examen du consentement
- Renouvellement du consentement
- Expiration du consentement
- Révocation du consentement

Pour une description détaillée des processus atomiques, consulter la section 5.4.

La figure 6 illustre quelques modèles de diagrammes des trois processus atomiques.

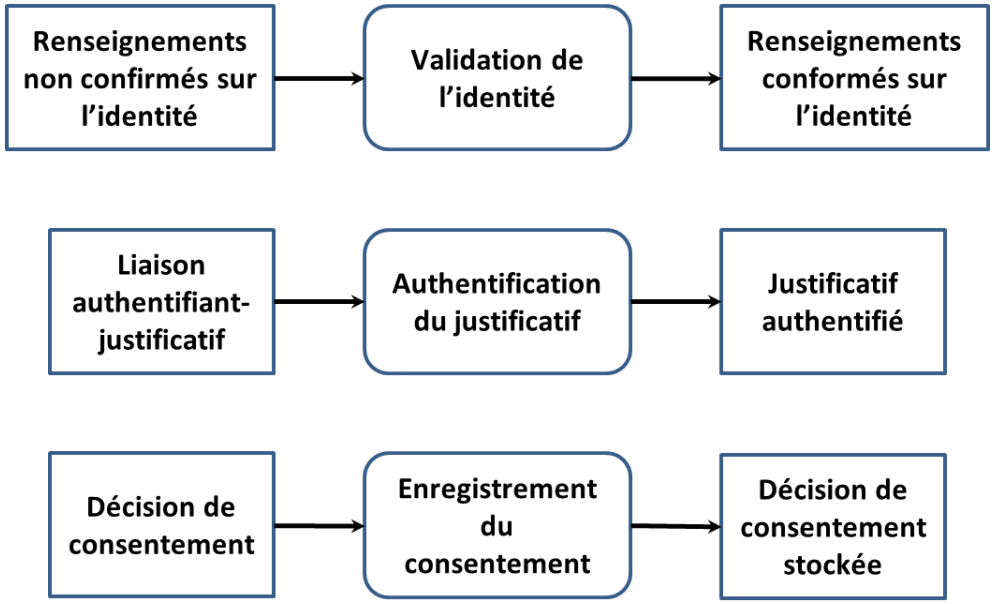

Figure 6 : Exemples de processus atomiques (modélisés)

5.3.4 Aperçu des processus composés

Dans la plupart des cas, le CCP servira à évaluer de processus opérationnels existants. Lorsqu'ils sont analysés, ces processus opérationnels sont souvent composés de plusieurs processus atomiques. Le CCP permet de regrouper un ensemble de processus atomiques pour former un *processus composé* qui entraîne un ensemble de transitions d'état. Optionnellement, un processus composé peut aussi comprendre d'autres processus composés. Trois processus composés – ***l'assurance de l'identité, l'assurance du justificatif*** *et le* ***consentement éclairé*** – représentaient la conception initiale d'une identité numérique fiable et ont servi à élaborer les exigences de la politique; ces trois processus composés sont exposés en détail dans la section 5.5.

D'autres processus composés qui ont été cernés comprennent les suivants :

- la création de l'identité;
- la confirmation de l'identité;
- la création du justificatif;
- la confirmation du justificatif;
- l'enregistrement de l'identité;
- l'enregistrement du service;
- la création de l'identité numérique fiable;
- l'inscription au service.

Par exemple, la *confirmation de l'identité* est un processus composé comprenant 5 processus atomiques, selon ce qui est montré dans la figure 7 (remarque : il ne faut pas déduire un ordre particulier des processus atomiques à partir du diagramme).

À l'aide de ce modèle, la sortie d'un processus composé est un ensemble de preuves.

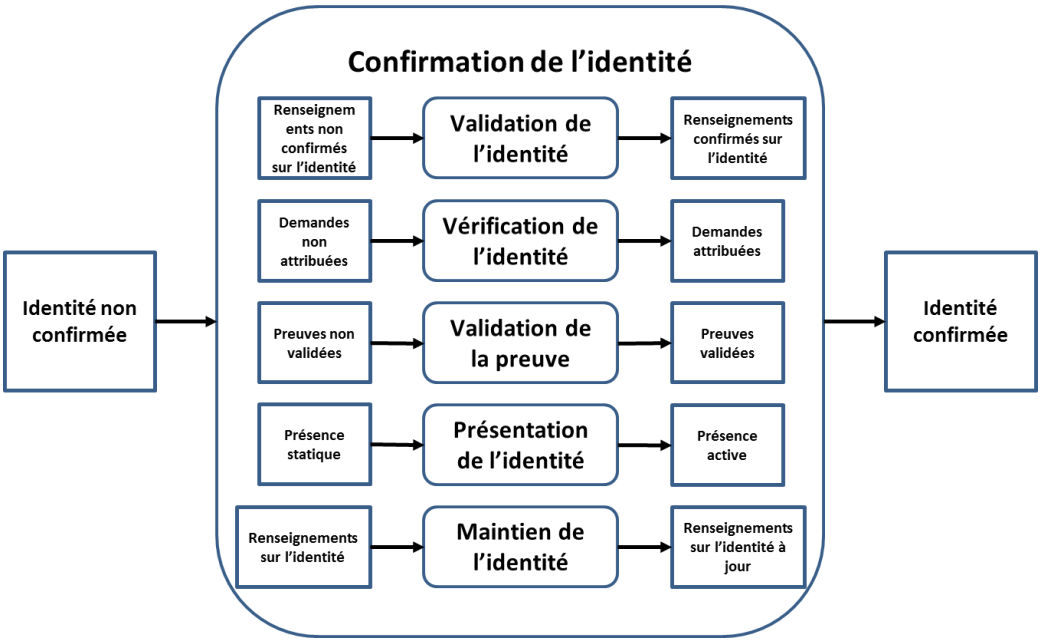

Figure 7 : Processus composé de confirmation de l'identité

5.3.5 Dépendances

Même si chaque processus atomique est fonctionnellement discret, pour produire une sortie acceptable, un processus atomique peut nécessiter qu'un autre processus atomique soit exécuté avec succès au préalable. On appelle cela une dépendance. Par exemple, même si l'*établissement de l'identité* d'une personne peut être exécuté de manière indépendante en tout temps, il est logiquement exact de ne le faire qu'après la *résolution de l'identité* de cette personne.

5.3.6 Relier des processus atomiques à des processus opérationnels existants

Un processus opérationnel ou technique existant pourrait être désigné à titre de processus atomique assujetti aux critères de conformité, au processus d'évaluation et à l'attestation prévus par le CCP. De plus, les programmes et les services existants intègrent souvent des processus composés liés à l'identité (p. ex., « preuve de l'identité », « inscription de l'identité ») qui sont composés de plusieurs processus atomiques.

Les processus qui ont été initialement mis au point pour travailler dans un contexte particulier peuvent être obtenus et considérés comme fiables dans le cadre de confiance pancanadien. Cela est accompli en reliant les processus existants aux définitions des processus atomiques. Une fois mis en correspondance, les processus existants peuvent faire l'objet d'une évaluation et d'une attestation fondées sur les critères de conformité associés avec les processus atomiques correspondants.

Le tableau qui suit énumère quelques exemples de mise en correspondance de processus atomiques avec des processus opérationnels existants :

Processus atomique	Exemples de processus opérationnels existants
Résolution de l'identité	Un processus d'enregistrement de statistiques essentielles, qui recueille des données biographiques ou « de base » à identifiant unique (nom, date de naissance) liées à une personne.
Établissement de l'identité	Un processus d'enregistrement de naissance qui consiste à créer un certificat de naissance faisant autorité. Un processus d'inscription à un programme qui consiste à créer un compte utilisateur.
Validation de l'identité	Un processus de demande de permis de conduire qui confirme l'exactitude les renseignements présentés sur les documents physiques ou au moyen d'un service de validation électronique.
Vérification de l'identité	Un processus de demande de passeport qui consiste à comparer les traits biométriques inscrits sur un document (p. ex., photographie du visage, couleur des yeux, taille) afin de veiller à ce qu'il s'agisse du demandeur en question. Poser à un demandeur des questions auxquelles lui seul pourrait répondre (p. ex., questions sur son dossier de crédit, secrets partagés, codes d'accès envoyé par courriel).
Maintien de l'identité	Services de mise à jour de notifications (push) par messagerie. Services réguliers de validation (pull). Mises à jour obligatoires en fonction des dates d'expiration ou des périodes de validité appliquées.
Émission d'un justificatif	Délivrer un document faisant autorité, notamment un certificat de naissance ou un permis de conduire. Émettre un justificatif numérique vérifiable.

La mise en correspondance devra probablement s'étendre à plusieurs organisations. Il est possible qu'une seule organisation ne puisse pas exécuter tous les processus atomiques liés à un processus composé – certains processus atomiques pourraient être effectués par d'autres organisations. Il est également possible que les processus atomiques soient répétés dans un autre contexte. À titre d'exemple, une partie de confiance, en utilisant une identité numérique fiable émise par un fournisseur, peut exécuter le processus atomique de résolution de l'identité dans son propre contexte afin de veiller à ce qu'elle ait affaire à la bonne personne. De plus, le CPP peut être utilisé par une partie de confiance pour mettre en correspondance ses propres processus existants lors de l'utilisation d'une identité numérique fiable émise par un fournisseur.

5.4 Processus atomiques

5.4.1 Résolution de l'identité

Description du processus	La résolution de l'identité est le processus établissant l'unicité d'une personne à l'intérieur de la population d'un programme ou d'un service au moyen de renseignements sur l'identité. Le programme ou le service en question définit les exigences relatives à la résolution de l'identité, au sens des attributs d'identité; en d'autres mots, il détermine l'ensemble d'attributs d'identité requis pour assurer la résolution de l'identité au sein de la population en question.
État d'entrée	**Renseignements non uniques sur l'identité : Les renseignements sur l'identité ne se rapportent pas uniquement à une seule personne.**
État de sortie	**Renseignements uniques sur l'identité : Les renseignements sur l'identité se rapportent uniquement à une seule personne.**

5.4.2 Établissement de l'identité

Description du processus	L'établissement de l'identité est le processus de création d'un dossier d'identité faisant autorité, sur lequel peuvent s'appuyer d'autres programmes, services ou activités.
État d'entrée	**Aucun dossier faisant autorité : Aucun dossier faisant autorité n'existe.**
État de sortie	**Dossier faisant autorité : Un dossier faisant autorité existe.**

5.4.3 Validation de l'identité

Description du processus	La validation de l'identité est le processus de confirmation de l'exactitude des renseignements sur l'identité d'une personne établie en vertu d'une partie faisant autorité. Il est important de remarquer que ce processus ne garantit pas qu'une personne utilise ses propres renseignements sur l'identité. La validation de l'identité permet seulement de déterminer que les renseignements sur l'identité fournis par une personne sont exacts lorsqu'on les compare aux dossiers d'identité faisant autorité.
État d'entrée	**Renseignements non confirmés sur l'identité : Les renseignements sur l'identité n'ont pas été confirmés à l'aide d'un document faisant autorité.**
État de sortie	**Renseignements confirmés sur l'identité : Les renseignements sur l'identité ont été confirmés à l'aide d'un document faisant autorité.**

5.4.4 Vérification de l'identité

Description du processus	La vérification de l'identité est le processus de confirmation que les renseignements sur l'identité présentés concernent la personne qui présente la demande. Il convient de noter que ce processus peut s'appuyer sur des renseignements personnels qui ne relèvent pas de l'identité.
État d'entrée	**Demandes non attribuées : Il n'est pas confirmé que la demande de renseignements sur l'identité provient du propriétaire légitime/de l'utilisateur de ces renseignements.**
État de sortie	**Demandes attribuées : Il est confirmé que la demande de renseignements sur l'identité provient du propriétaire légitime/de l'utilisateur de ces renseignements.**

5.4.5 Validation de la preuve

Description du processus	La validation de la preuve est le processus par lequel on confirme qu'un objet (physique ou électronique) peut être accepté ou admis en tant que preuve (p. ex., la détermination hors de tout doute raisonnable, la prépondérance des probabilités, la possibilité marquée).
État d'entrée	**Preuves non validées : Il n'a pas été confirmé que l'objet est une preuve recevable.**
État de sortie	**Preuves validées : Il a été confirmé que l'objet est une preuve recevable.**

5.4.6 Présentation de l'identité

Description du processus	La présentation de l'identité est le processus de confirmation dynamique de l'existence continue d'une personne au fil du temps (c.-à-d. « une présence authentique »). Ce processus peut être utilisé afin de veiller à ce qu'aucune activité frauduleuse ou malveillante n'ait été effectuée (dans le présent ou par le passé).
État d'entrée	**Présence statique : L'identité existe seulement de façon sporadique et souvent uniquement en association avec un événement vital (p. ex., naissance, décès).**
État de sortie	**Présence active : L'identité existe de façon permanente en association avec de nombreuses transactions.**

5.4.7 Maintien de l'identité

Description du processus	Le maintien de l'identité est le processus par lequel on veille à ce que les renseignements sur l'identité soient exacts, complets et à jour, comme exigé.
État d'entrée	**Renseignements sur l'identité : Les renseignements sur l'identité ne sont pas à jour.**
État de sortie	**Renseignements sur l'identité à jour : Les renseignements sur l'identité sont à jour.**

5.4.8 Liaison identité-justificatif

Description du processus	La liaison identité-justificatif est le processus qui consiste à associer une identité à un justificatif émis.
État d'entrée	**Justificatif émis : Un justificatif unique a été assigné à l'objet**
État de sortie	**Liaison identité-justificatif : Un justificatif émis a été associé à un acteur attribué**

5.4.9 Établissement de liens pour déterminer l'identité

Description du processus	L'établissement de liens pour déterminer l'identité est le processus de mise en correspondance entre deux identifiants ou plus et la même identité.
État d'entrée	**Identifiant lié : L'identifiant n'est pas associé à un autre identifiant.**
État de sortie	**Identifiant lié : L'identifiant est associé à un ou plusieurs autres identifiants.**

5.4.10 Émission d'un justificatif

Description du processus	L'émission d'un justificatif est le processus consistant à créer et à attribuer un justificatif unique à un objet (p. ex., une personne, une organisation ou un dispositif). Un justificatif peut comprendre un ou plusieurs codes d'identification. Ceux-ci peuvent être des pseudonymes, ou peuvent renfermer différents attributs vérifiés par l'émetteur.
État d'entrée	**Pas de justificatif : Aucun justificatif n'est attribué au sujet.**
État de sortie	**Justificatif émis : Un justificatif unique a été assigné à l'objet.**

5.4.11 Liaison justificatif-authentifiant

Description du processus	La liaison justificatif-authentifiant est le processus qui consiste à associer un justificatif émis à un ou plusieurs authentifiants. Ce processus comprend également des activités liées au cycle de vie telles que la suppression d'authentifiants, la liaison d'autres authentifiants et la mise à jour d'authentifiants (p. ex., changement de mot de passe, mise à jour des questions et réponses de sécurité, nouvelle photo).
État d'entrée	**Justificatif émis : Un justificatif unique a été assigné à l'objet.**
État de sortie	**Liaison authentifiant-justificatif : Un justificatif émis a été associé à un ou plusieurs authentifiants.**

5.4.12 Suspension d'un justificatif

Description du processus	La suspension d'un justificatif est un processus qui consiste à transformer un justificatif émis en un justificatif suspendu en marquant le justificatif émis comme temporairement inutilisable.
État d'entrée	**Justificatif émis : Un justificatif unique a été assigné à l'objet.**
État de sortie	**Justificatif suspendu : Le sujet n'est pas en mesure d'utiliser le justificatif.**

5.4.13 Recouvrement d'un justificatif

Description du processus	Le recouvrement d'un justificatif est un processus qui consiste à transformer à nouveau un justificatif suspendu en justificatif utilisable (c.-à-d. un justificatif utilisable).
État d'entrée	**Justificatif suspendu : Le sujet n'est pas en mesure d'utiliser le justificatif.**
État de sortie	**Justificatif émis : Un justificatif unique a été assigné à l'objet.**

5.4.14 Révocation d'un justificatif

Description du processus	La révocation d'un justificatif est le processus permettant de garantir qu'un justificatif émis est en permanence marqué comme inutilisable.
État d'entrée	**Justificatif émis : Un justificatif unique a été assigné à l'objet.**
État de sortie	**Pas de justificatif : Aucun justificatif n'est attribué au sujet.**

5.4.15 Authentification du justificatif

Description du processus	L'authentification d'un justificatif est le processus de vérification, à l'aide d'un authentificateur, qu'un sujet a le contrôle sur le justificatif qui lui a été assigné et que ce justificatif est valide (c'est-à-dire, ni suspendu ni révoqué).
État d'entrée	**Liaison authentifiant-justificatif : Un justificatif émis a été associé à un ou plusieurs authentifiants.**
État de sortie	**Justificatif authentifié : Il a été confirmé que le sujet a le contrôle sur le justificatif émis et que ce justificatif est valide.**

5.4.16 Création de la signature

Description du processus	La création de la signature est un processus qui consiste à créer une représentation électronique dans laquelle, à tout le moins : la personne qui signe les données peut être associée aux représentations électroniques; il est clair que la personne avait l'intention de signer; la raison ou le but de la signature est communiquée; et l'intégrité des données de la transaction signée est maintenue, y compris l'original.
État d'entrée	**Aucune signature : Aucune signature n'existe.**
État de sortie	**Signature : Il existe une signature.**

5.4.17 Vérification de la signature

Description du processus	La vérification de la signature est le processus permettant de confirmer que la signature des données est valide.
État d'entrée	**Signature : Il existe une signature.**
État de sortie	**Signature vérifiée** : La signature est valide.

5.4.18 Formulation d'avis

Description du processus	La formulation d'avis est le processus consistant à produire un énoncé d'avis décrivant les renseignements personnels qui sont recueillis ou qui peuvent l'être; les parties auxquelles les renseignements personnels sont transmis, et le type de renseignements personnels transmis; les fins auxquelles les renseignements personnels sont recueillis, utilisés ou divulgués; le risque de préjudice et d'autres conséquences de la collecte, de l'utilisation ou de la divulgation; la façon dont les renseignements personnels seront traités et protégés; la période d'application de l'avis; et la personne ou l'entité ayant compétence ou autorité pour l'énoncé d'avis émis.
État d'entrée	**Aucun énoncé d'avis : Aucun énoncé d'avis n'existe.**
État de sortie	**Énoncé d'avis : Un énoncé d'avis existe.**

5.4.19 Demande de consentement

Description du processus	La demande de consentement est le processus consistant à présenter un énoncé d'avis au sujet (c'est-à-dire, la personne physique à qui les renseignements personnels en question se rapportent) [6] et à demandant au sujet de demander son consentement (« Oui ») ou de refuser de donner son consentement (« Non ») en fonction du contenu de l'énoncé d'avis, ce qui entraîne une décision de consentement par « oui » ou par « non ».
État d'entrée	**Énoncé d'avis : Un énoncé d'avis existe.**
État de sortie	**Décision de consentement** : Une décision de consentement existe.

[6] Le processus fiable de la demande de consentement part du principe que la personne donnant son consentement a été l'objet des processus composés de l'assurance de l'identité et de l'assurance du justificatif, et que, par la suite, la personne à qui l'on demande de donner son consentement a le pouvoir de le faire.

5.4.20 Enregistrement du consentement

Description du processus	L'enregistrement du consentement est le processus consistant à stocker de manière persistance un énoncé d'avis et la décision de consentement connexe du sujet. Plus d'information peut également être stockée. Par exemple : des renseignements sur le sujet, la version de l'avis qui lui a été présentée, la date et l'heure à laquelle l'avis a été présenté et, le cas échéant, la date d'expiration relative à la décision de consentement. Une fois les renseignements relatifs au consentement stockés, une notification sur la décision de consentement prise par le sujet est envoyée aux parties concernées.
État d'entrée	**Décision de consentement :** Une décision de consentement existe.
État de sortie	**Décision de consentement stockée :** Une décision de consentement stockée existe.

5.4.21 Examen du consentement

Description du processus	L'examen du consentement est un processus qui consiste à rendre les détails d'une décision de consentement stockée visibles pour le sujet ou pour un examinateur autorisé.
État d'entrée	**Décision de consentement stockée :** Une décision de consentement stockée existe.
État de sortie	**Décision de consentement stockée :** Une décision de consentement stockée existe.

5.4.22 Renouvellement du consentement

Description du processus	Le renouvellement du consentement est le processus consistant à prolonger la validité d'une décision de consentement par « oui » en reportant la date d'expiration.
État d'entrée	**Décision de consentement stockée :** Une décision de consentement stockée existe.
État de sortie	**Décision de consentement stockée :** Une décision de consentement stockée existe.

5.4.23 Expiration du consentement

Description du processus	L'expiration du consentement est le processus consistant à suspendre la validité d'une décision de consentement par un « oui » en raison d'une date d'expiration dépassée.

État d'entrée	**Décision de consentement stockée :** Une décision de consentement stockée existe.
État de sortie	**Décision de consentement stockée :** Une décision de consentement stockée existe.

5.4.24 Révocation du consentement

Description du processus	La révocation du consentement est le processus consistant à suspendre la validité d'une décision de consentement par un « oui » à la suite du retrait explicite du consentement par le sujet (c'est-à-dire qu'une décision de consentement par un « oui » est convertie en une décision de consentement par un « non »).
État d'entrée	**Décision de consentement stockée :** Une décision de consentement stockée existe.
État de sortie	**Décision de consentement stockée :** Une décision de consentement stockée existe.

5.5 Processus composés

5.5.1 Assurance de l'identité

Le processus composé de l'assurance de l'identité établit une mesure de certitude (ou un niveau d'assurance) qu'une personne, une organisation ou un appareil est ce qu'il prétend être. Ce processus sert à répondre à la question suivante : « À quel point êtes-vous certain qu'il s'agit de la bonne personne, de la bonne organisation ou du bon appareil? ». Le processus composé de l'assurance de l'identité est constitué de neuf processus atomiques. À chaque processus atomique (décrit en détail à la section 5.4) correspond un **état d'entrée**, un **état de sortie** et des **critères conformité** servant à normaliser ce processus atomique et à en évaluer intégrité. Les critères de conformité peuvent aussi être classés selon des qualificatifs indiquant une exigence qui peut être retracée à un niveau d'assurance, une exigence concernant un domaine lié à l'identité, une autre exigence liée à un cadre de confiance, ou une exigence opérationnelle, juridique, politique ou réglementaire applicable. La figure 8 illustre le processus atomique de l'assurance de l'identité.

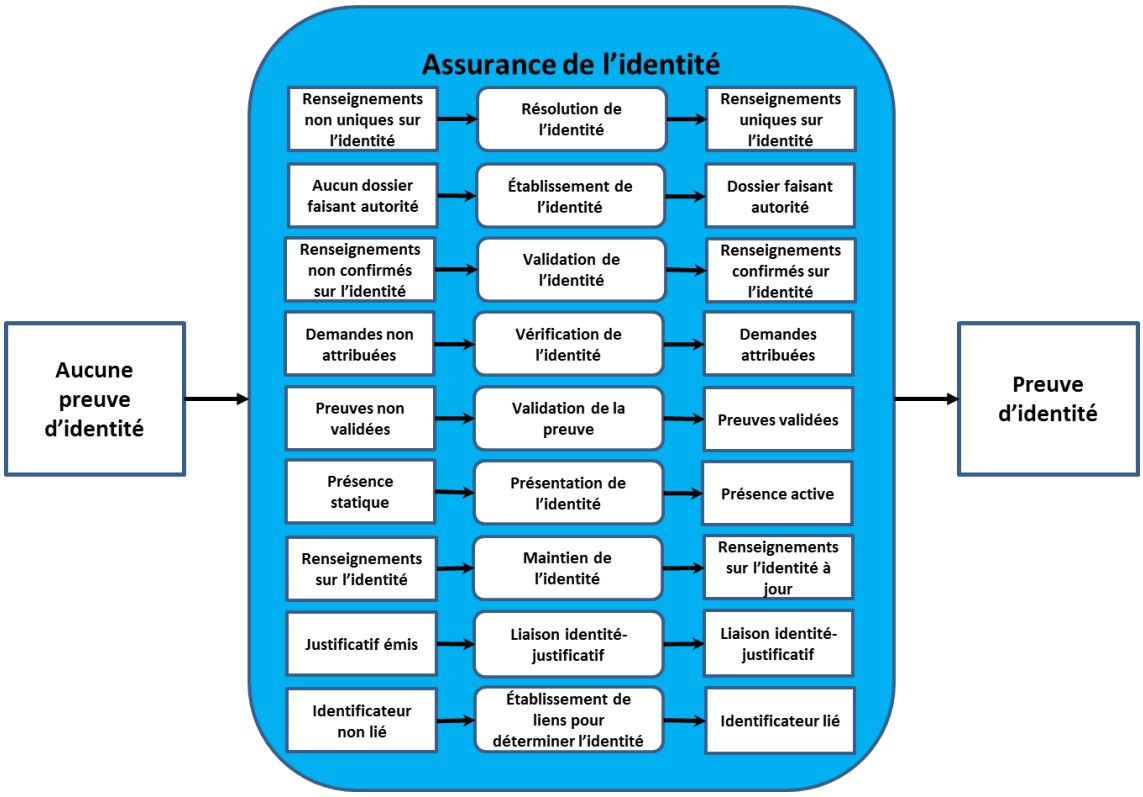

Figure 8 : Processus atomique de l'assurance de l'identité

Les processus atomiques liés à l'assurance de l'identité ne peuvent être exécutés que par plusieurs organisations. Différentes organisations pourraient être chargées de l'exécution de différents processus atomiques. Par exemple, la validation de l'identité pourrait relever de la responsabilité d'un registraire de l'état civil, alors que la vérification de l'identité pourrait incomber au responsable du service. La participation de multiples organisations peut entraîner une certaine complexité dans les processus d'évaluation et d'assertion. Le CCP permet et appuie différentes approches à la mise en œuvre.

Les processus atomiques de l'assurance de l'identité peuvent comprendre des renseignements personnels autres que ceux liés à l'identité. Dans certains cas, il est nécessaire de valider et vérifier des renseignements personnels en plus des renseignements sur l'identité. Cela pourrait comprendre des renseignements personnels comme le statut de citoyen, l'adresse de la résidence, etc. Le processus composé de l'assurance de l'identité est axé sur l'identité, mais pourrait s'étendre à d'autres renseignements personnels, au besoin.

5.5.2 Assurance du justificatif

Le processus composé de l'assurance du justificatif établit une mesure de certitude (ou un niveau d'assurance) qu'une personne, une organisation ou un appareil a maintenu le contrôle d'un justificatif qu'on lui avait confié (ou émis) et que le justificatif n'a pas été compromis (p. ex., falsifiés, corrompus, modifiés, volés ou utilisés sans l'autorisation appropriée). Le processus composé de l'assurance du justificatif est constitué de huit processus atomiques. À chaque processus atomique (décrit en détail à la section 5.4) correspond un **état d'entrée**, un **état de sortie** et des **critères conformité** servant à normaliser ce processus atomique et à en évaluer intégrité. Les critères de conformité peuvent aussi être classés selon des qualificatifs indiquant une exigence qui peut être retracée à un niveau d'assurance, une exigence concernant un domaine lié à l'identité, une autre exigence liée à un cadre de confiance, ou une exigence opérationnelle, juridique, politique ou réglementaire applicable. La figure 9 illustre le processus composé de l'assurance du justificatif.

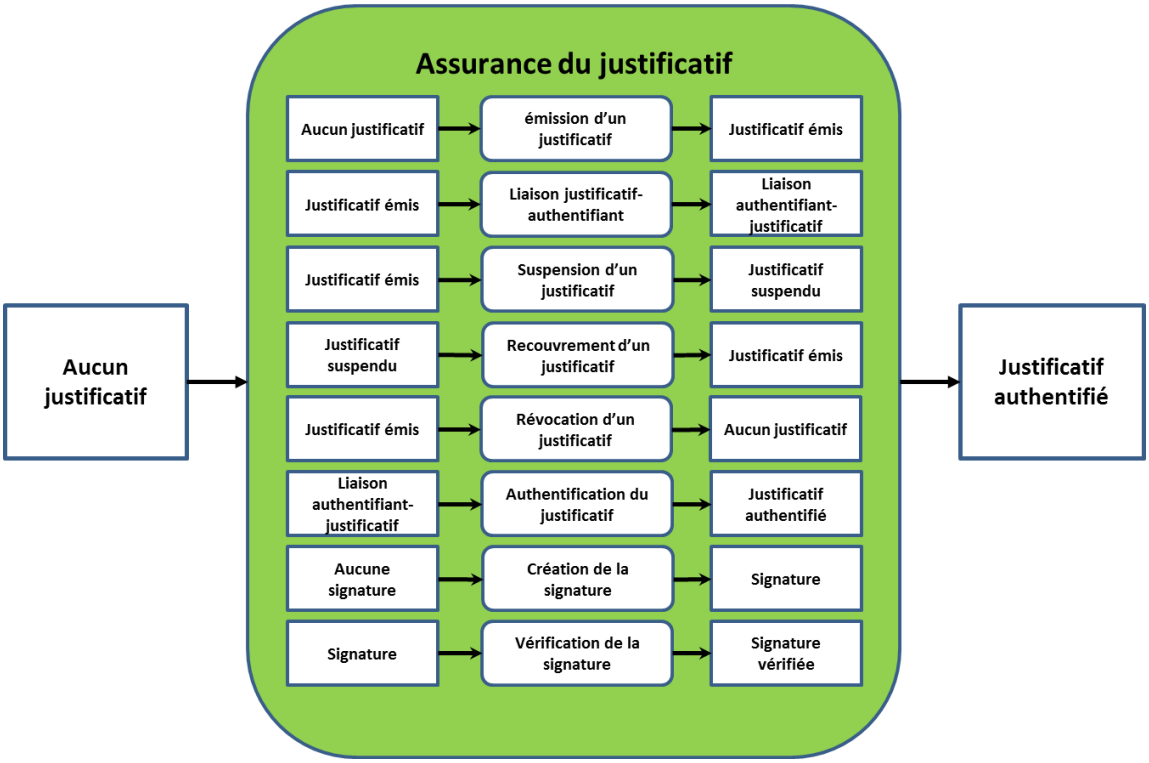

Figure 8 : Processus composé de l'assurance du justificatif

Les processus atomiques liés à l'assurance du justificatif ne peuvent être exécutés que par plusieurs organisations. Différentes organisations pourraient être chargées de l'exécution de différents processus atomiques. Par exemple, l'émission du justificatif pourrait relever de la responsabilité d'une organisation donnée, alors que l'authentification du justificatif pourrait relever de la responsabilité d'une autre organisation. La participation de multiples organisations peut entraîner une certaine complexité dans les processus d'évaluation et d'attestation. Le CCP n'impose pas de restriction sur les différentes approches à la mise en œuvre.

5.5.3 Consentement éclairé

Le processus composé du consentement éclairé consiste à obtenir d'une personne[7] son consentement significatif à recueillir, à utiliser et à divulguer ses renseignements personnels. Le processus composé du consentement éclairé est constitué de sept processus atomiques. À chaque processus atomique (décrit en détail à la section 5.4) correspond un **état d'entrée**, un **état de sortie** et des **critères conformité** servant à normaliser ce processus atomique et à en évaluer intégrité. Les critères de conformité peuvent aussi être classés selon des qualificatifs indiquant une exigence qui peut être retracée à un niveau d'assurance, une exigence concernant un domaine lié à l'identité, une autre exigence liée à un cadre de confiance, ou une exigence opérationnelle, juridique, politique ou réglementaire applicable. La figure 10 illustre le processus composé du consentement éclairé.

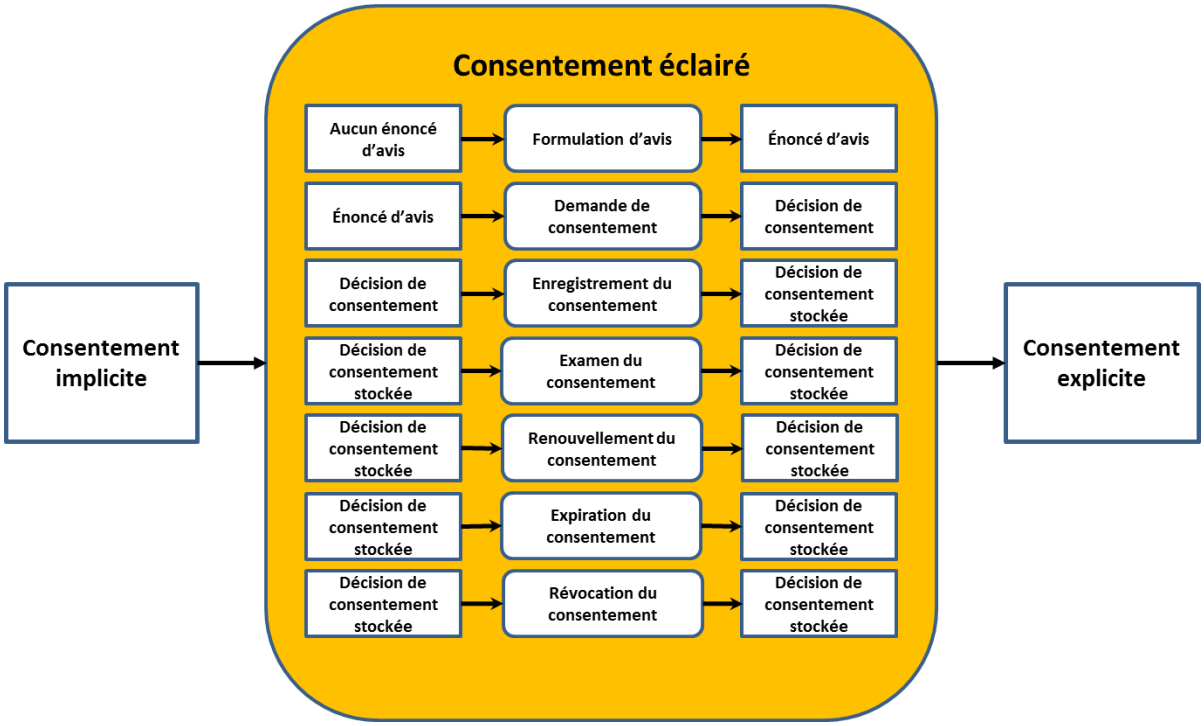

Figure 9 : Processus composé du consentement éclairé

[7] Le processus fiable du consentement éclairé part du principe que la personne donnant son consentement a été l'objet des processus composés de l'assurance de l'identité et de l'assurance du justificatif, et que, par la suite, la personne à qui l'on demande de donner son consentement a le pouvoir de le faire.

Les processus atomiques de consentement éclairé ne peuvent être exécutés que par plusieurs organisations. Différentes organisations pourraient être chargées de l'exécution de différents processus atomiques. Par exemple, la demande de consentement pourrait relever de la responsabilité d'une organisation donnée, alors que l'enregistrement du consentement pourrait relever de la responsabilité d'une autre organisation. La participation de multiples organisations peut entraîner une certaine complexité dans les processus d'évaluation et d'attestation. Le CCP n'impose pas de restriction sur les différentes approches à la mise en œuvre.

5.5.4 Création d'une identité numérique fiable (personne)

Le processus composé de création de l'identité numérique fiable est constitué de trois processus composés : assurance de l'identité, assurance du justificatif et consentement éclairé – décrits ci-dessus. Ces trois processus composés, activés par l'infrastructure de soutien, se combinent pour créer une identité numérique fiable. La figure 11 illustre le processus composé de la création de l'identité numérique fiable.

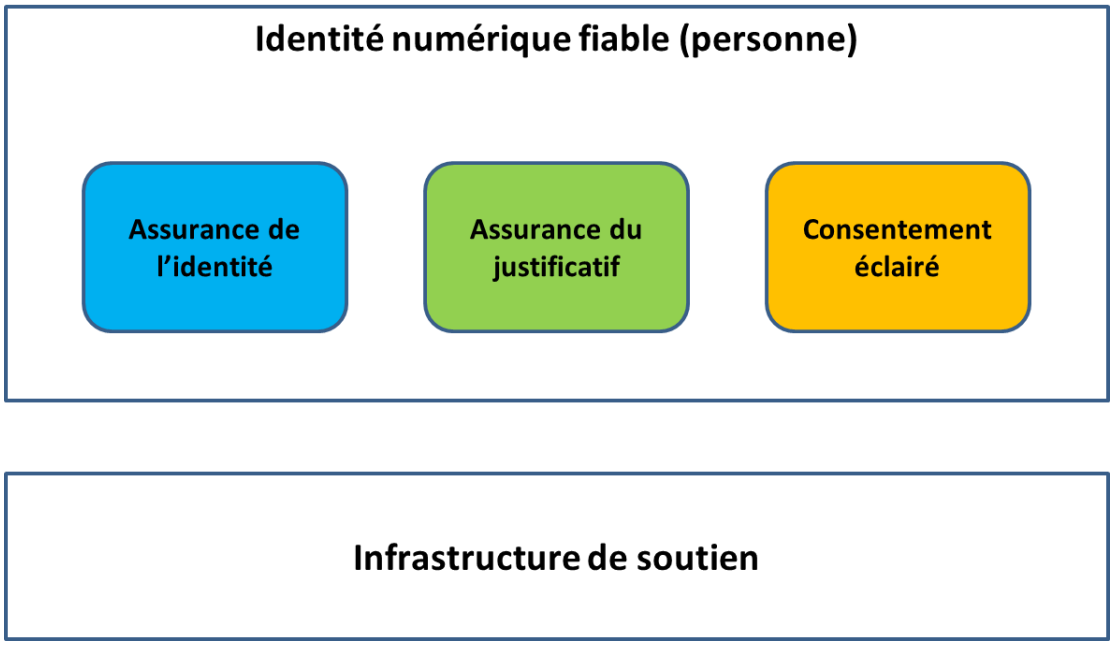

Figure 11 : Création de l'identité numérique fiable (personne)

Une identité numérique fiable peut également être conceptualisée comme un ensemble d'extrants (preuves) de processus fiables. Comme il a été mentionné précédemment, ces preuves sont indépendantes du moyen de transmission. En fonction de l'écosystème de l'identité numérique, plusieurs parties peuvent exécuter certains de ces processus fiables à divers moments. La figure 12 illustre l'identité numérique fiable en tant qu'ensemble de preuves.

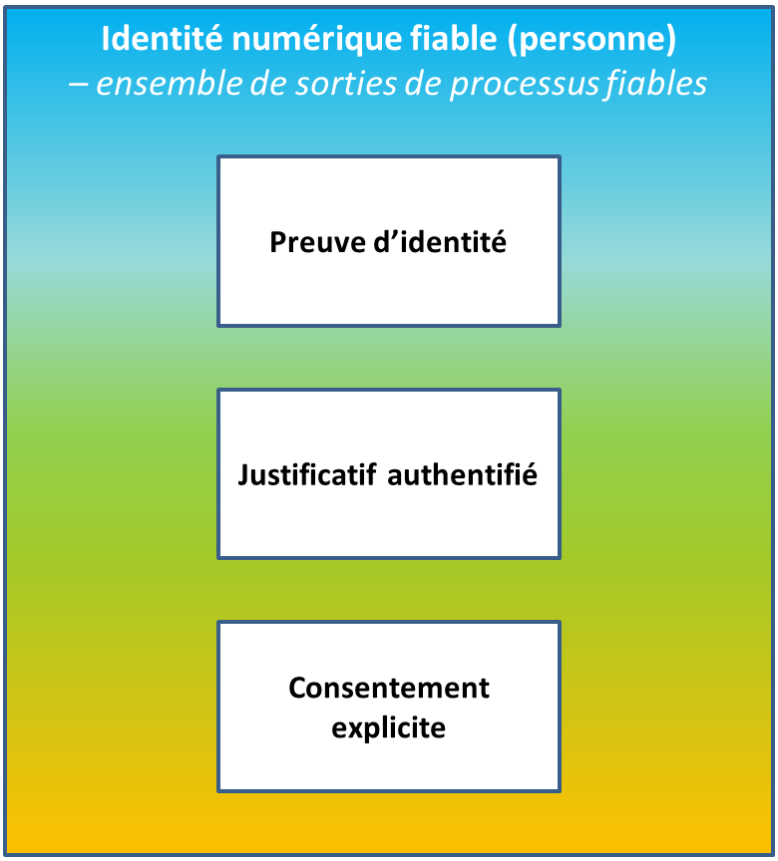

Figure 10 : Identité numérique fiable en tant qu'ensemble de preuves

5.6 Intervenants et rôles

5.6.1 Intervenants de l'écosystème de l'identité numérique canadien

L'écosystème d'identité numériques canadien permet d'exploiter et de développer l'économie numérique au Canada. Cet écosystème se veut ouvert et axé sur le client, un environnement où tous les participants se conforment au Cadre de confiance pancanadien. Il en découle un ensemble de réseaux et de services interopérables où des identités numériques fiables peuvent être fournies et utilisées dans toutes les industries et tous les ordres de gouvernement au Canada, permettant ainsi aux fournisseurs de programmes et de services de mettre l'accent sur la prestation de services de base.

Le CCP ne définit pas de façon normative les intervenants ou les rôles au sein de l'écosystème de l'identité numérique. Cependant, le CCP peut servir à clarifier les rôles et les intérêts spécifiques des intervenants en ce qui concerne la mise en place de processus fiables, l'utilisation d'extrants de processus fiables et la transmission d'extrants de processus fiables entre les réseaux et les systèmes interopérables.

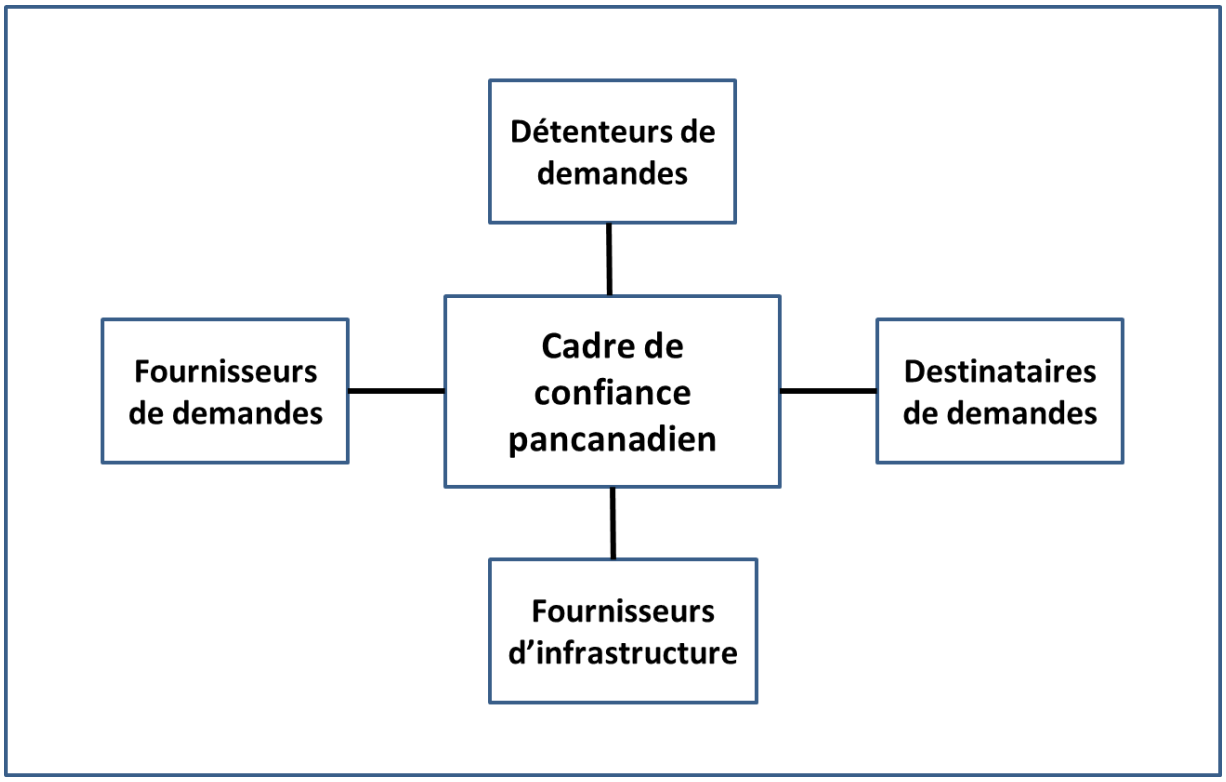

Figure 11 : Intervenants de l'écosystème d'identité numérique canadien

La figure 13 illustre une vue d'ensemble des rôles de l'écosystème d'identité numérique canadien par rapport au CCP. Le diagramme indique quatre types d'intervenants :

- **Fournisseurs de demandes** – Entités (habituellement des organisations) qui émettent des demandes aux *détenteurs de demandes*. Les fournisseurs de demandes sont aussi appelés ***parties faisant autorité*** ou ***émetteurs de demande***.
- **Détenteurs des demandes** – Entités qui détiennent des demandes qui sont soumises et acceptées comme preuves par les *destinataires des demandes*. Les détenteurs de demandes sont habituellement, mais pas toujours, le ***sujet*** d'une demande.
- **Destinataires des demandes** – Entités (habituellement des organisations) qui utilisent les demandes au cours de leurs activités. Les destinataires des demandes acceptent les demandes des *détenteurs de demandes* aux fins de la prestation de services ou de l'administration de programmes. Les destinataires de demandes sont également appelés ***parties de confiance*** et ***vérificateurs de demandes***.
- **Fournisseurs d'infrastructures** – Entités (habituellement des organisations) qui fournissent des services de soutien, à valeur ajoutée, ou agissent à titre d'intermédiaires entre les parties.

Il convient de noter qu'une entité peut être plus d'un type d'intervenant.

Le diagramme ci-dessus peut permettre d'élaborer un ensemble commun de définitions de rôles où plusieurs modèles d'identité peuvent coexister au sein de l'écosystème d'identité numérique.

Il convient de noter que même si le principal objectif du CCP est de contribuer au développement de l'écosystème d'identité numérique canadien, sa portée peut être élargie (p. ex., définition de nouveaux processus atomiques) afin d'intégrer d'autres demandes contextuelles qui ne sont pas liées à l'identité, notamment les demandes d'ordre pédagogique ou professionnel (p. ex., les diplômes universitaires, les permis d'exercice).

5.6.2 Rôles des participants au CCP

Comme il a déjà été indiqué, le CCP ne définit pas les rôles des participants de façon normative, mais peut servir à identifier les rôles pouvant être normalisés dans le cadre de l'approvisionnement, des offres à commandes ou d'accords d'approvisionnement. Ci-après, quelques-uns des rôles des participants au CCP qui ont été identifiés :

- **Fournisseurs d'assurance de l'identité** – Les participants au cadre de confiance qui établissent et gèrent l'identité, et fournissent des services de vérification de l'identité. Les fournisseurs d'assurance de l'identité sont en quelque sorte des fournisseurs de demandes.

- **Fournisseurs d'assurance du justificatif** – Participants au cadre de confiance qui émettent des justificatifs électroniques aux fins d'authentification, ou des justificatifs vérifiables afin de prouver une identité et/ou à titre de qualification. Les fournisseurs d'assurance de justificatif sont en quelque sorte des fournisseurs de demandes.
- **Fournisseurs d'identité numérique fiable (INF)** – Participants au cadre de confiance qui fournissent le produit final d'une identité numérique fiable. Habituellement, il s'agit d'un programme provincial, territorial ou fédéral d'identité numérique, qui fournit des identités numériques fiables à une autre instance. Des fournisseurs d'INF peuvent également se desservir les uns les autres dans un secteur de l'industrie. Les fournisseurs d'identité numérique fiable sont en quelque sorte des fournisseurs de demandes.
- **Parties de confiance (en tant que destinataires d'INF)** – Participants au cadre de confiance mettant essentiellement l'accent sur la prestation des services, ou même si l'identité est cruciale, elle est considérée comme un outil habilitant (ou centre de coûts) plutôt qu'un processus opérationnel stratégique. Toutes les parties de confiance sont des destinataires de demandes.
- **Détenteurs d'identité numérique** – Participants au cadre de confiance à qui une identité numérique est attribuée. Les détenteurs d'identité numérique sont en quelque sorte des détenteurs de demandes.

La figure 14 illustre quatre de ces rôles de participants par rapport aux processus atomiques qu'ils exécutent. Comme il a déjà été indiqué, les définitions de ces rôles ne sont pas destinées à être normatives. Dans plusieurs cas, il y a chevauchement (et confusion) entre les définitions de rôles, et celles-ci peuvent être clarifiées en mettant l'accent sur la personne qui exécute tel ou tel processus atomique et qui en est responsable.

Nº	Processus atomique	Fournisseur d'assurance de l'identité	Fournisseur d'assurance du justificatif	Fournisseur d'identité numérique fiable (INF)	Partie de confiance (en tant que consommateur d'INF)
1	Résolution de l'identité	X		X	X
2	Établissement de l'identité	X		X	X
3	Validation de l'identité	X		X	
4	Vérification de l'identité	X		X	
5	Validation de la preuve	X		X	
6	Présentation de l'identité	X		X	
7	Maintien de l'identité	X		X	
8	Liaison identité-justificatif			X	
9	Établissement de liens pour déterminer l'identité				X
10	Émission d'un justificatif		X	X	
11	Liaison justificatif-authentifiant		X	X	
12	Suspension d'un justificatif		X	X	
13	Recouvrement d'un justificatif		X	X	
14	Révocation d'un justificatif		X	X	
15	Authentification du justificatif		X	X	
16	Création de la signature			X	X
17	Vérification de la signature			X	X
18	Formulation d'avis			X	X
19	Demande de consentement			X	X
20	Enregistrement du consentement			X	X
21	Examen du consentement			X	X
22	Renouvellement du consentement			X	X
23	Expiration du consentement			X	X
24	Révocation du consentement			X	X

Figure 12 : Processus atomiques par rôle des participants

En termes de prestation de services, les rôles des participants au CCP ne se limitent pas aux trois rôles de fournisseurs énumérés ci-dessus. De plus en plus, il y aura des fournisseurs de services qui se spécialiseront dans un seul ou quelques-uns des processus atomiques du CCP. Ces fournisseurs de services spécialisés dans les domaines de la *présentation de l'identité* ou de l'*authentification du justificatif*, par exemple, une fois le CCP évalué et certifié, peuvent à leur tour être sollicités par d'autres fournisseurs de services au niveau global et supérieur ou directement par des parties de confiance.

5.7 Approche d'évaluation

Le CCP permet de réaliser un processus d'évaluation complet dans le cadre de programmes d'identité numérique au Canada. Le CCP a été conçu pour divers contextes, impliquant de nombreuses parties ayant chacune des rôles différents selon le contexte.

Par exemple, dans le contexte fédéral-provincial-territorial, le gouvernement du Canada est une partie de confiance lorsqu'il accepte les identités numériques fiables d'une province ou d'un territoire en vue de leur usage dans le cadre de programmes et de services fédéraux. La province ou le territoire est un fournisseur d'identité numérique fiable et est chargée de vérifier que la personne en question existe réellement, contrôle sa représentation numérique, et agit de son propre gré.

Le gouvernement du Canada, en tant que partie de confiance, se base sur les critères de conformité du processus de confiance afin de veiller à ce que l'identité numérique fiable fournie par la province ou le territoire corresponde à l'individu concerné dans chaque programme.

5.7.1 But général

Le but du processus d'évaluation du CCP est d'évaluer formellement un programme d'identité numérique afin de fournir un degré de confiance global qu'une partie de confiance, de son propre chef, ou pour le compte d'autrui, peut accepter une identité numérique fiable. L'acceptation d'une identité numérique fiable est une décision prise par une partie de confiance, qui peut à son tour, avoir besoin de retracer cette décision par rapport à des exigences législatives, stratégiques ou réglementaires spécifiques qui ne relèvent pas de la portée du CCP. La partie de confiance peut également avoir besoin de tenir compte des exigences spécifiques au programme ou de gérer les risques qui ne relèvent pas de la responsabilité du fournisseur d'identité numérique fiable. Enfin, le CCP est un outil permettant à toutes les parties de comprendre qui est responsable de quoi et de clarifier les responsabilités particulières.

Pour le moment, le processus d'évaluation du CCP en est encore à ses débuts. Des directives détaillées seront mises au point au fur et à mesure que le processus d'évaluation évolue. Le contenu des sections qui suivent provient des principales leçons tirées à ce jour et sera modifié suite à une demande ultérieure.

5.7.2 Gestion de projets, engagement et gouvernance (approbations).

Le processus d'évaluation du CCP devrait être intégré à titre de volet distinct dans un processus de gestion plus vaste. Il existe généralement d'autres volets de travail, notamment :

- Surveillance par la direction, gouvernance dans le cadre du projet et architecture intégrée.
- Intégration et mise à l'essai (technique/UX).

- Évaluation et autorisation de sécurité, évaluations des répercussions sur la vie privée et ententes de service.
- Communication et participation des intervenants.

Les membres de l'équipe chargés d'exécuter le processus d'évaluation du CCP doivent être intégrés dans l'équipe de projet plus vaste, chargée de fournir la solution. Cette mesure est avantageuse à deux égards :

1. Les évaluateurs du CCP bénéficient des connaissances opérationnelles et techniques détaillées des autres membres de l'équipe.
2. Les autres membres de l'équipe pourront bénéficier du point de vue de l'évaluateur du CCP – il faut répondre à la question « quoi » pour accepter une identité numérique fiable sur la base des critères de conformité.

5.7.3 Aperçu du processus d'évaluation

Le processus d'évaluation du CCP est destiné à être adaptable. Au besoin, l'évaluateur peut souhaiter adapter les critères de conformité au contexte particulier. Il convient de souligner que certains critères de conformité (au moyen de qualificateurs) peuvent faire l'objet d'une gouvernance spécifique.

Une feuille de travail détaillée a été mise au point pour faciliter le processus d'évaluation du CCP. Cette feuille de travail consolide les processus atomiques et leurs critères de conformité connexes sur une seule feuille de calcul pour faciliter la mise en correspondance des processus opérationnels existants, et aider l'évaluateur à recouper et synthétiser les données aux fins d'analyse. Les critères de conformité sont compilés sous forme de tableau, avec les qualificateurs, pour faciliter la sélection des critères de conformité s'appliquant au processus d'évaluation.

La première étape du processus d'évaluation du CCP consiste à mettre en correspondance les processus opérationnels avec les définitions de processus atomiques. La figure 15 illustre une mise en correspondance des processus opérationnels d'un fournisseur d'identité numérique fiable avec des définitions de processus atomiques. Ce processus de mise en correspondance peut également être utilisé par une partie de confiance ayant probablement besoin d'augmenter ou de gérer les risques liés à certains processus atomiques dans leur propre contexte.

Une fois que les processus opérationnels existants ont été mis en correspondance, ils peuvent être évalués et une décision peut être prise par rapport à chacun des critères de conformité des processus atomiques connexes. Les décisions officielles actuellement appliquées sont les suivantes :

- **Accepter** – Les critères de conformité sont respectés.

- **Accepter en faisant une observation** – Les critères de conformité sont respectés, mais une dépendance ou un risque sur lequel la partie faisant l'objet d'une évaluation n'a peut-être pas de contrôle direct a été relevé.
- **Accepter en émettant une recommandation** – Les critères de conformité sont respectés, mais une amélioration ou un perfectionnement doit être constaté à l'avenir.
- **Accepter en posant une condition** – Les critères de conformité ne sont pas respectés, mais le processus atomique est accepté en raison de la démonstration des mesures de sauvegarde, des facteurs compensatoires ou d'autres garanties mises en place.
- **Ne pas accepter** – Les critères de conformité ne sont pas respectés.
- **Sans objet** – Les critères de conformité ne s'appliquent pas.

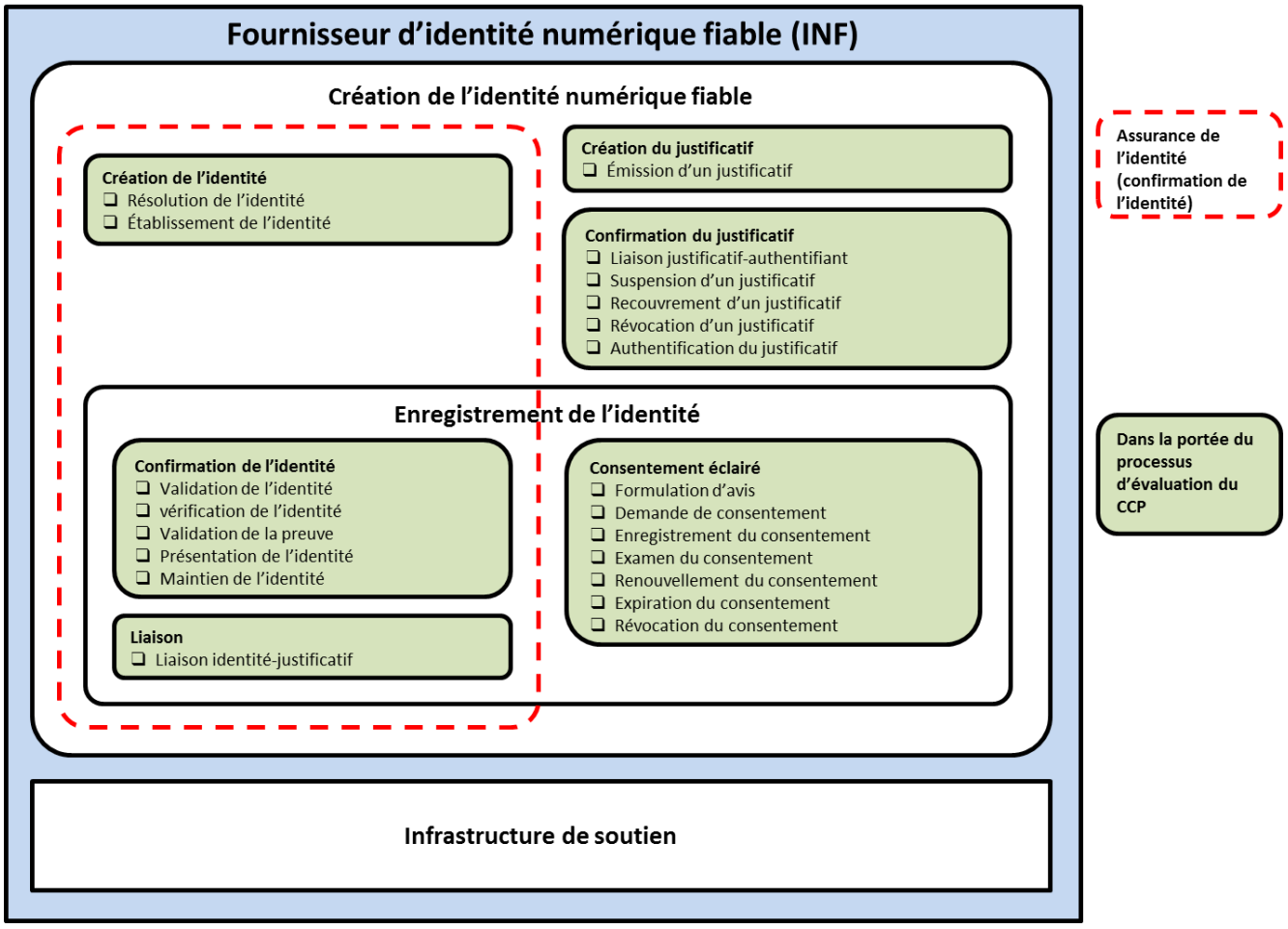

Figure 13 : Processus opérationnel pour la mise ne correspondance des processus atomiques

Les preuves fournies à l'appui de l'analyse et de la justification de la décision doivent être recueillies et compilées de manière à être facilement recoupées par rapport aux critères de conformité applicables.

À la fin du processus d'évaluation, la partie de confiance peut émettre une lettre d'acceptation d'une identité numérique fiable. Cette lettre est semblable, de par sa nature, à l'évaluation des facteurs relatifs à la vie privée (ÉFVP) ou à une autorisation d'exploitation (ATO) et doit respecter les critères suivants :

- Être adressée à la personne/l'organisation/l'instance agissant à titre de fournisseur d'identité numérique fiable.
- Être signée par le personnel, l'organisation ou l'administration acceptant l'identité numérique fiable, à un niveau de qualificateur donné.
- Indiquer la portée ou à quelle fin spécifique l'identité numérique fiable sera utilisée, y compris la durée d'utilisation.
- Comporter une annexe énumérant les qualificateurs spécifiques (p. ex., niveaux d'assurance), et indiquant toute observation, condition ou recommandation découlant du processus d'évaluation.

5.7.4 Certification et accréditation

L'Organisation internationale de normalisation (ISO)[8] définit la certification et l'accréditation comme suit :

- **Certification – Assurance écrite (sous la forme d'un certificat) donnée par une tierce partie qu'un produit, service ou système est conforme à des exigences spécifiques.**
- **Accréditation – Reconnaissance formelle par un organisme indépendant (en général un organisme d'accréditation) qu'un organisme de certification se conforme aux normes internationales.**

En principe, une fois que les programmes de certification et d'accréditation seront élaborés, des tiers indépendants seront autorisés à procéder aux évaluations du CCP. Pour le moment, de nombreux organismes de normalisation nationaux et internationaux ont reconnu les normes et programmes d'évaluation de la conformité. À titre d'exemple, le Conseil canadien des normes, une société d'État fédérale, a pour mandat de

[8] Site Web de l'ISO : https://www.iso.org/certification.html.

promouvoir la normalisation volontaire au Canada, où la normalisation n'est pas expressément prévue par la loi.

Il convient également de relever que, de par sa conception, le CCP ne présume pas qu'une organisation est la seule responsable de l'exécution de tous les processus de confiance. Par conséquent, plusieurs organismes pourraient être impliqués dans le processus d'évaluation du CCP, en mettant l'accent sur les différents processus de confiance ou les différents aspects (p. ex., la sécurité, la protection de la vie privée, la prestation de services). Il faut tenir compte de la façon de coordonner plusieurs organisations qui pourraient avoir besoin de travailler ensemble pour produire une évaluation globale du CCP.

Au fur et à mesure que le processus d'évaluation du CCP évolue, il faudra déterminer quelles organisations ou quelles normes sont mieux indiquées pour répondre aux exigences des intervenants et mieux appliquées en ce qui concerne le CCP.

Enfin, les lois et règlements peuvent changer en réponse à l'évolution de l'écosystème d'identité numérique. Les leçons tirées de la mise en œuvre de solutions fondées sur le CCP peuvent être considérées comme un apport précieux pour toute éventuelle modification législative ou réglementaire.

5.8 Critères de conformité

Les critères de conformité sont un ensemble d'énoncés d'exigences définissant ce qu'il faut pour assurer l'intégrité d'un processus atomique. Les critères de conformité servent à appuyer une évaluation et un processus de certification réalisés de façon impartiale et transparente, et fondée sur des preuves.

À titre d'exemple, le processus atomique de résolution de l'identité peut consister à attribuer un identificateur à un individu. Le critère de conformité précise que le processus atomique doit garantir que l'identificateur attribué à l'individu soit unique pour une population ou un contexte spécifique (p. ex., une province).

5.8.1 Qualificateurs

Des qualificateurs peuvent être appliqués aux critères de conformité. Les qualificateurs permettent de mieux décrire un niveau de confiance, la rigueur requise ou une exigence spécifique, en ce qui concerne un autre cadre de confiance, une exigence quant à un domaine lié à l'identité, ou une exigence stratégique ou réglementaire spécifique. Les qualificateurs peuvent être utilisés pour sélectionner les critères de conformité applicables à un processus d'évaluation. Les qualificateurs peuvent aussi être utilisés pour faciliter la mise en correspondance des équivalences de critères de conformité dans divers cadres de confiance.

Il est possible que les critères de conformité ne comprennent aucun qualificateur (applicable dans tous les cas) ou qu'ils comprennent un seul qualificatif (applicable dans certains cas), ou plusieurs qualificatifs (applicables dans plusieurs cas).

5.8.2 Qualificateurs de domaines liés à l'identité

Leurs qualificateurs peuvent être utilisés pour qualifier les critères de conformité spécifiques à un domaine lié à l'identité. Actuellement, il existe deux qualificateurs de domaines liés à l'identité : fondamental et contextuel.

- **Fondamental** – Critères de conformité qui sont rattachés à un événement fondamental (p. ex., naissance, changement légal de nom, décès, immigration, résidence légale, citoyenneté, insérer des exemples d'organisations) qui relèvent exclusivement du secteur public (plus précisément, les bureaux de l'état civil (BEC) et les registres des entreprises des provinces et des territoires (PT), Immigration, Réfugiés et Citoyenneté Canada (IRCC) et le registre des organisations de régime fédéral).
- **Contextuel – Critères de conformité qui sont propres à un contexte d'identité (identité contextuelle).** À titre d'exemple, pour que des éléments de preuve d'identité contextuelle soient admis, il se peut que les critères de conformité exigent que les éléments de preuve d'identité contextuelle soient émis directement au destinataire avec accusé de réception.

5.8.3 Qualificateurs de niveaux d'assurance (NA) à l'échelle pancanadienne

La version actuelle des critères de conformité au CCP utilise les quatre niveaux d'assurance (NA) à l'échelle pancanadienne :

- **Niveau 1 : Peu ou pas de confiance requise**
- **Niveau 2 : Un certain niveau de confiance requis**
- **Niveau 3 : Un niveau élevé de confiance requis**
- **Niveau 4 : Un niveau très élevé de confiance requis**

5.8.4 Qualificateurs eIDAS

Les qualificateurs peuvent être fondés sur les trois niveaux d'assurance définis par le Règlement européen nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (connu sous le nom d'« eIDAS ») :

- **Faible : Faible degré de confiance**
- **Important : Degré de confiance important**
- **Élevé : Degré de confiance élevé**

5.8.5 Qualificateurs de vecteurs de confiance

Les qualificateurs peuvent se fonder sur des vecteurs de confiance, une norme proposée par l'IETF (RFC 8485, octobre 2018). Actuellement, le vecteur de confiance propose quatre composantes qui peuvent être utilisées à titre de qualificateurs :

- **Vérification d'identité (P) : Décrit la probabilité qu'une transaction relative à l'identité numérique corresponde à un sujet d'identité particulier dans le monde réel.**
- **Utilisation du justificatif principal (C) : Indique à quel point le justificatif principal peut être vérifié par le TDIP.**
- **Gestion du justificatif principal (M) : Transmet les renseignements liés au cycle de vie prévu du justificatif principal utilisé, y compris sa liaison, rotation, et révocation.**
- **Présentation de l'argument (A) : Décrit l'efficacité avec laquelle le TDI peut être communiqué dans tout le réseau sans fuite d'information aux parties non visées et sans usurpation.**

5.8.6 Publication spéciale 800 63-3 du National Institute of Standards and Technology (NIST) – Qualificateurs

Les qualificateurs peuvent être fondés sur les niveaux définis dans les directives sur l'identité numérique énoncées dans la publication spéciale 800-63 de la NIST :

- **Niveau d'assurance de l'identité : Désigne le niveau de vérification de l'identité.**
- **Niveau d'assurance de l'authentification : Fait référence au processus d'authentification.**
- **Niveau d'assurance de la fédération : Désigne la force d'une affirmation dans un environnement fédérée, utilisée pour communiquer les renseignements liés à l'authentification et aux attributs (le cas échéant) à une partie de confiance.**

5.8.7 Qualificateurs de signatures électroniques sécurisées

La partie 2 de la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) définit une signature électronique comme « une signature constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres symboles sous forme numérique incorporée, jointe ou associée à un document électronique ». La partie 2 de la LPRPDE aborde certains cas spécifiques à la technologie et exige l'utilisation d'une catégorie particulière de signatures électroniques appelée signature électronique sécurisée (qui est définie en détail dans le *Règlement sur les signatures électroniques sécurisées* (RSES) ci-joint).

Les qualificateurs de signature électronique sécurisée peuvent se fonder sur les facteurs suivants :

- **Signature : Les données électroniques ont été signées par la personne identifiée dans le certificat de signature numérique ou au moyen de celui-ci.**
- **Algorithmes :** Des algorithmes asymétriques précis doivent être utilisés.
- **Reconnaissance :** L'autorité de certification (AC) émettrice est reconnue par le Secrétariat du Conseil du Trésor.
- **Capacité : Preuve que l'autorité de certification a la capacité de délivrer les certificats de signature numérique de façon sécurisée et fiable.**

6 ANNEXE A : APERÇU DE LA GESTION DE L'IDENTITÉ

La présente annexe fait le survol général d'aspects particuliers de la gestion d'identité. Des renseignements supplémentaires sont disponibles dans la Ligne directrice sur l'assurance de l'identité [SCT, 2015].

6.1 Identité

6.1.1 Identité réelle

> « Les multiples facettes de l'identité sont riches. Inévitablement, nous apportons nos propres cordes sensibles et un lot d'intentions à toute discussion portant sur « la nature de l'identité ». Certains s'y engagent d'un point de vue philosophique et d'autres d'un point de vue psychologique. Certains plongent dans les enjeux politiques et culturels, alors que d'autres décortiquent l'identité d'un point de vue métaphysique ou spirituel. Ces différentes perspectives sont toutes des points de vue valides sur l'incidence de l'identité sur nos vies... Elles nous permettent de répondre à la question « Pourquoi »; pourquoi la question identitaire est-elle importante et pourquoi doit-on s'en soucier? Malheureusement, il arrive que ces perspectives attisent nos passions et nous poussent à parler sans nous écouter les uns les autres, afin de présenter des points à première vue impertinents pour l'autrui, laissant derrière des gens frustrés et mis de côté.
>
> C'est grâce à l'identité que nous reconnaissons des choses et des personnes précises, que nous nous souvenons d'elles et, en dernier recours, que nous réagissons face à elles. Lorsque nous rencontrons une personne, nous lui demandons son nom. Nous l'observons, nous écoutons les rumeurs qui la concernent, et il arrive même que nous consommions des médias qui s'y rapportent. Nous nous souvenons de ce que nous apprenons. Nous nous appuyons ensuite sur ces connaissances pour éclairer nos interactions futures. Il en est de même pour les autres, en ce qui nous concerne. Même notre propre perception identitaire se fonde sur ce que nous reconnaissons et ce dont nous nous souvenons de nos propres actions et réactions.
>
> [...] Nous tirons autant d'avantages du concept de l'identité parce qu'elle nous permet de suivre des choses et des personnes. Il nous aide à reconnaître nos amis et nos familles, et à distinguer les menaces; il nous permet de nous souvenir des anniversaires, des préférences et des histoires; il nous donne la capacité de répondre à chaque individu en tant que personne unique.
>
> [...] Nos identités sont plus larges que nos incarnations numériques. Nos identités existaient avant elles, et elles continuent d'exister en toute indépendance. L'identité numérique est simplement un outil qui permet aux personnes et aux organisations de mieux gérer leur identité réelle.

— *A Primer on Functional Identity*, par Joe Andrieu[9]

6.1.2 L'identité dans la gestion de l'identité

L'identité, dans le domaine de la gestion de l'identité, renvoie à une notion beaucoup plus étroite que celle que l'on trouve dans le monde réel. Dans le domaine de la gestion de l'identité, l'identité est définie comme une référence ou une désignation unique utilisée pour distinguer une personne, organisation, ou un dispositif particulier.

Une identité doit être unique[10]. L'unicité est une exigence qui permet d'établir :

- que les personnes peuvent être distinguées les unes des autres et, au besoin, être identifiées de façon unique;
- qu'un service peut être fourni à une personne particulière (p. ex., une personne s'étant déjà enregistrée ou inscrite);
- qu'un service a été fourni à la bonne personne; l'unicité permet de réduire le risque que le service ou l'avantage soit fourni à la mauvaise personne (c'est-à-dire, que le service ou l'avantage était destiné à une autre personne).

6.2 Définir la population

Au Canada, l'univers peut être défini comme étant toutes les personnes vivantes résidant ou en visite au Canada, ainsi que toutes les personnes décédées pour qui une identité a été établie au Canada. Les personnes visées par un programme ou un service constituent la population du programme ou du service[11].

Voici quelques exemples de populations visées par des programmes et des services du secteur public canadien :

- les personnes nées en Alberta;
- les personnes qui doivent remplir une déclaration de revenus destinée au gouvernement fédéral;
- les personnes qui sont autorisées à conduire un véhicule au Québec;
- les personnes qui sont des anciens combattants;
- les personnes qui ne sont pas nées au Canada;

[9] Le texte intégral de cet article est disponible à : http://bit.ly/FunctionalIdentityPrimer.

[10] Il s'agit d'une des exigences à respecter pour établir le niveau d'assurance de l'identité. Aperçu de la composante vérification des identifiants de connexion (janvier 2018)

[11] Les caractéristiques d'une population de programme/service constituent le facteur clé pour déterminer le contexte de l'identité. Modèle d'assurance pancanadien

- les personnes qui sont assurées par le régime d'assurance-santé de l'Ontario;
- les personnes qui ont le statut d'Indiens inscrits au Canada;
- les personnes qui touchent des prestations d'aide sociale en Colombie-Britannique.

6.3 Définir le contexte de l'identité

En fournissant leurs programmes et leurs services, les organisations fonctionnent au sein d'un environnement ou d'un ensemble de circonstances particuliers. C'est ce qu'on appelle le contexte de l'identité dans le domaine de la gestion de l'identité. Le contexte de l'identité est déterminé par des facteurs comme le mandat, la population cible (c.-à-d. les clients, la clientèle), et les autres responsabilités établies en vertu d'une loi, d'un accord ou d'une entente.

Comprendre et définir le contexte de l'identité aide les organisations à déterminer quels renseignements sur l'identité sont requis ou non. Le contexte de l'identité aide également à déterminer les points communs entre les différentes organisations. Il permet de déterminer si les renseignements sur l'identité ou les processus d'assurance peuvent être utilisés dans d'autres contextes.

Les facteurs suivants devraient être pris en considération au moment de définir le contexte de l'identité d'un programme ou d'un service donné :

- le destinataire prévu d'un service : le destinataire peut ne pas faire partie de l'organisation (p. ex., un citoyen, une personne non canadienne, une entreprise, un organisme à but non lucratif) ou en faire partie (p. ex., un employé, un ministère);
- la taille, les caractéristiques et la composition de la clientèle;
- les points communs avec d'autres services (c.-à-d. entre organisations);
- les organisations avec des mandats semblables;
- l'utilisation de services partagés.

6.4 Déterminer les exigences en matière de renseignements sur l'identité

Une propriété ou une caractéristique associée à une personne identifiable est appelée attribut d'identité ou élément de donnée sur l'identité. Les attributs d'identité comprennent, par exemple, le nom, la date de naissance et le sexe. Dans le cadre d'un programme ou d'un service, quel qu'il soit, les renseignements sur l'identité constituent l'ensemble des attributs d'identité qui est à la fois :

- suffisant pour faire la distinction entre les différentes personnes appartenant à la population d'un programme ou d'un service (c.-à-d. qui permet de satisfaire à l'exigence d'unicité de l'identité);
- suffisant pour décrire une personne en fonction des exigences du programme ou du service.

Lorsqu'elle détermine la suffisance des renseignements sur l'identité dans le cadre d'un programme ou d'un service, l'organisation doit faire la distinction entre un renseignement sur l'identité et un renseignement personnel propre à un programme, car il arrive que ceux-ci se chevauchent. Par exemple, la date de naissance peut être utilisée pour déterminer l'unicité de l'identité (et dans ce cas, elle est utilisée à titre de renseignement sur l'identité), mais elle peut également être utilisée comme critère d'admissibilité en fonction de l'âge (et dans ce cas, elle est utilisée comme renseignement personnel propre à un programme). Lorsqu'il y a un chevauchement entre les renseignements sur l'identité et les renseignements personnels propres au programme, une bonne pratique consiste à décrire les deux utilités. On veille ainsi à ce que l'utilisation des renseignements sur l'identité soit cohérente avec le but initial, en vertu duquel lesdits renseignements ont été collectés. On veille également à ce que les renseignements obtenus puissent être gérés séparément, ou faire l'objet d'une protection accrue au moyen des mesures de sécurité et de protection de la vie privée appropriées. Il est recommandé aux organisations de réduire, autant que possible, le chevauchement entre les renseignements sur l'identité et les renseignements propres à un programme.

6.4.1 Identificateur

Un identificateur désigne l'ensemble d'attributs d'identité qui sont utilisés uniquement pour distinguer une personne donnée dans une population de programme ou de service. Cet ensemble d'attributs est habituellement un sous-ensemble des renseignements sur l'identité requis par un programme ou un service.

Différents ensembles d'attributs d'identité peuvent être désignés à titre d'identificateur selon les exigences du programme ou du service, voire parfois de la loi. Par exemple, un programme peut définir le nom et la date de naissance comme ensemble d'attributs d'identité constituant l'identificateur. Un autre programme pourrait définir le nom, la date de naissance et le sexe comme ensemble d'attributs d'identité constituant l'identificateur. Un troisième programme pourrait utiliser un identificateur attribué (comme le numéro d'assurance-maladie) à titre d'attribut d'identité constituant l'identificateur.

Au moment de déterminer l'ensemble d'attributs d'identité qui sera utilisé à titre d'identificateur, les facteurs suivants doivent être pris en considération :

- **Universalité – Chaque personne faisant partie de la population du programme ou du service doit posséder l'ensemble d'attributs d'identité constituant l'identificateur.** Par exemple, inclure le numéro de téléphone cellulaire dans les

attributs peut donner lieu à un grand nombre de valeurs nulles parce que la possession d'un téléphone cellulaire pourrait ne pas être suffisamment universelle dans la population visée. Même quand un attribut d'identité est universel, un grand nombre de valeurs manquantes ou incomplètes peut le rendre inutile comme élément de l'identificateur. Par exemple, pour de nombreuses personnes nées hors du Canada, la date de naissance comprend seulement l'année et le mois de naissance.

- **Unicité – Les valeurs associées aux attributs d'identité doivent être suffisamment différentes pour que chaque personne faisant partie de la population du programme ou du service puisse être distinguée des autres.** Par exemple, la date de naissance à elle seule n'est pas suffisante pour distinguer une personne d'une autre puisque de nombreuses personnes ont la même date de naissance.
- **Constance – Les valeurs données aux attributs d'identité doivent varier aussi peu que possible (voire pas du tout) au fil du temps.** Par exemple, l'adresse comme attribut pose problème, puisque les gens ont tendance à déménager plusieurs fois au cours de leur vie.
- **Facilité d'obtention – Il devrait être relativement facile d'obtenir l'attribut d'identité.** Par exemple, les séquences d'ADN des êtres humains sont universelles, uniques et très stables dans le temps, mais elles sont difficiles à obtenir.

6.4.2 Identificateur attribué

Il est généralement convenu que le nom et la date de naissance constituent l'ensemble d'attributs d'identité minimal nécessaire pour constituer un identificateur. Des analyses[12] ont démontré qu'une combinaison de nom (nom de famille + premier prénom) et de date de naissance complète fera une différence de plus de 96 % des personnes dans toute population. L'ajout d'autres attributs d'identité (p. ex., le sexe, le lieu de naissance) permet d'améliorer marginalement l'unicité au sein d'une population, mais aucune combinaison d'attributs d'identité ne peut garantir à 100 % l'unicité au sein d'une population donnée. Par conséquent, afin d'éviter que des identités se chevauchent au sein du pourcentage résiduel de la population dont l'unicité n'est pas garantie, les organisations ont recours aux identificateurs attribués. Un identificateur attribué est un attribut d'identité artificiel dont la seule utilité est de garantir l'unicité des identités. L'identificateur attribué se composera d'une chaîne numérique ou alphanumérique automatiquement générée et attribuée à une personne au moment où elle s'inscrit ou s'enregistre. Toutefois, avant d'associer une personne à un identificateur attribué, il faut établir l'unicité de l'identité de la personne au sein de la population visée (en d'autres mots, il faut effectuer une résolution de l'identité (voir la prochaine section) par

[12] Projet de vérification de l'identité de la NASPO, Rapport sur le projet de résolution de l'identité (vérification de l'identité), 17 février 2014

l'intermédiaire d'autres attributs d'identité (p. ex., le nom, la date de naissance, etc.). Par conséquent, l'utilisation d'un identificateur attribué n'élimine pas la nécessité des méthodes traditionnelles de résolution de l'identité, mais elle réduit cette nécessité à une occurrence ponctuelle isolée pour chaque personne au sein d'une population.

Une fois associé à une personne, un identificateur attribué permet d'établir l'unicité de cette personne parmi toutes les autres personnes au sein de la population sans qu'il soit nécessaire de recourir à d'autres attributs d'identité. Le numéro d'enregistrement de naissance, le numéro du permis de conduire, le numéro d'assurance sociale et le numéro de compte client sont tous des exemples d'identificateurs attribués. Les éléments suivants doivent être pris en considération au moment d'utiliser des identificateurs attribués :

- L'accès aux identificateurs attribués peut être réservé à l'utilisation interne du programme qui les gère.
- Les identificateurs attribués entretenus dans le cadre d'un programme peuvent être fournis à d'autres programmes, afin que ceux-ci puissent également y recourir pour faire la distinction entre les différentes personnes au sein de leurs propres populations ou services. Il se peut toutefois que des restrictions soient mises en place sur cette pratique en raison de lois ou de considérations relatives à la protection de la vie privée.
- Certains identificateurs attribués peuvent faire l'objet de restrictions imposées par des lois ou des politiques. Par exemple, le gouvernement du Canada impose des restrictions sur la collecte, l'utilisation, la conservation, la divulgation et l'élimination du numéro d'assurance sociale.

6.5 Résolution de l'identité

La résolution de l'identité est la détermination de l'unicité d'une personne à l'intérieur de la population d'un programme ou d'un service au moyen de renseignements sur l'identité. Le programme ou le service en question définit les exigences relatives à la résolution de l'identité, au sens des attributs d'identité; en d'autres mots, il détermine l'ensemble d'attributs d'identité requis pour assurer la résolution de l'identité au sein de la population en question. Comme l'identificateur est l'ensemble d'attributs d'identité qui sert à distinguer une personne en particulier à l'intérieur de la population d'un programme ou d'un service, l'identificateur est le moyen qui permet d'assurer la résolution de l'identité.

Comme les exigences relatives à la résolution de l'identité peuvent varier d'un programme ou d'un service à un autre, les responsabilités des parties faisant autorité et des parties utilisatrices en lien avec la résolution de l'identité sont les suivantes :

- Les parties ayant autorité et les parties utilisatrices doivent établir les exigences de résolution de l'identité des populations de leur programme ou de leur service.
- Une partie ayant autorité doit publier les exigences de résolution de l'identité de la population de son programme ou de son service.

6.6 Assurer l'exactitude des renseignements sur l'identité

Les renseignements sur l'identité doivent être exacts, complets et à jour[13]. La qualité des renseignements sur l'identité se mesure par leur exactitude. Elle garantit la véracité des renseignements fournis au sujet d'une personne, en plus de garantir que ces renseignements sont complets et tenus à jour, comme requis.

Pour que les renseignements sur l'identité soient considérés comme étant exacts, trois exigences doivent être respectées :

- **Les renseignements sur l'identité sont exacts et à jour.** Les renseignements sur l'identité peuvent changer au fil du temps, à la suite de certains événements de la vie (p. ex., le mariage). C'est pourquoi il faut toujours mettre à jour les renseignements sur l'identité lorsque le besoin survient, sans quoi ils deviennent inexacts.
- **Les renseignements sur l'identité se rapportent à une personne réelle.** Les renseignements sur l'identité doivent être associés à une personne qui existe vraiment. Dans la plupart des cas, la personne est toujours vivante, mais il arrive aussi que la personne visée soit décédée.

[13] Il s'agit d'une des exigences à respecter pour établir le niveau d'assurance de l'identité. Aperçu de la composante vérification des identifiants de connexion (janvier 2018).

- **Les renseignements sur l'identité renvoient à la bonne personne.** Dans les grandes populations, certaines personnes peuvent présenter les mêmes renseignements sur l'identité que d'autres, ou des renseignements semblables. L'exigence d'unicité permet de régler la situation, mais elle n'élimine pas la possibilité que des renseignements sur l'identité soient associés à la mauvaise personne.

Les organisations sont elles-mêmes responsables de veiller à l'exactitude des renseignements sur l'identité fournis dans le cadre de leurs programmes et de leurs services. Il est possible de veiller à l'exactitude des renseignements sur l'identité au moyen d'une source faisant autorité. Il y a trois façons d'y arriver :

- Au besoin, demander confirmation de l'exactitude des renseignements sur l'identité à une source qui fait autorité. C'est ce qu'on appelle la validation des renseignements sur l'identité. À titre d'exemple, le sexe d'une personne peut être validé par voie électronique au moyen d'un registre provincial des statistiques de l'état civil[14].
- Au besoin, demander les renseignements sur l'identité à une source qui fait autorité. C'est ce qu'on appelle l'extraction des renseignements sur l'identité. Par exemple, le lieu de naissance d'une personne peut être extrait électroniquement du registre fédéral des personnes nées à l'étranger.
- Souscrire à un service de notification offert par une source qui fait autorité. C'est ce qu'on appelle les notifications relatives aux renseignements sur l'identité. Par exemple, des avis de décès pourraient être transmis par un registraire de l'état civil provincial.

Ces méthodes peuvent être utilisées indépendamment les unes des autres ou en combinaison, et une stratégie efficace nécessite généralement le recours aux trois méthodes.

S'il est impossible de vérifier l'exactitude des renseignements sur l'identité au moyen d'une source qui fait autorité, on peut recourir à d'autres méthodes, comme la corroboration des renseignements sur l'identité à l'aide d'une ou de plusieurs preuves d'identité.

Déterminer l'exactitude des renseignements sur l'identité passe notamment par la confirmation que la personne existe réellement ou a déjà existé (c.-à-d. qu'elle est

[14] Les facteurs tels que l'orthographe et les variations phonétiques, les changements de nom, et les différents jeux de caractères peuvent rendre la validation de certains éléments de données d'identité problématique. Fédérer la gestion de l'identité au gouvernement du Canada(2011) Ligne directrice sur la définition des exigences en matière d'authentification (2012) Norme sur l'assurance de l'identité et des justificatifs (2013) Ligne directrice sur l'assurance de l'identité (2015) Particuliers Joe Andrieu A Primer on Functional Identity (2018)

décédée). Cela prouve que les renseignements sur l'identité se rapportent à une personne réelle (vivante ou décédée) et non à une personne inexistante ou à la mauvaise personne. Le décès d'une personne n'a aucune incidence sur l'exactitude des renseignements sur l'identité. Le décès n'invalide pas les renseignements sur l'identité.

7 ANNEXE B : TERMES ET DÉFINITIONS

Les définitions qui suivent sont des définitions qui font autorité, tirées de la Norme sur l'assurance de l'identité et des justificatifs, des définitions provenant de lignes directrices et de documents de référence de l'industrie ainsi que des définitions créées par le Groupe de travail pour les besoins de ce document.

Terme	Définition
assurance	Une mesure de certitude indiquant si une déclaration ou un fait est vrai.
assurance de l'identité	Concerne l'affirmation que la personne est bien qui elle prétend être.
assurance de l'identité	Mesure d'assurance que la personne, l'organisation ou l'appareil est bien ce qu'il affirme être.
assurance du justificatif	Concerne la liaison d'un justificatif à une personne (sans tenir compte de son identité).
assurance du justificatif	L'assurance qu'une personne, une organisation, ou un mécanisme a gardé le contrôle sur un justificatif qui lui ont été attribués (p. ex., clé, jeton, document, identificateur) et que ce justificatif n'a pas été compromis (p. ex., falsifié, corrompu, modifié).
attribut	Propriété ou caractéristique associée à une entité. Voir également « attribut d'identité ».
attribut d'identité	Une propriété ou une caractéristique associée à une personne, une organisation, ou un appareil identifiable (également appelé « élément de donnée sur l'identité »).
authentifiant	Un élément que le demandeur possède et contrôle (généralement un module cryptographique ou un mot de passe) et qui est utilisé pour authentifier l'identité du demandeur (également appelé « jeton »).
authentification	Processus d'établissement de la véracité ou de l'authenticité visant à produire une assurance de justificatif ou d'identité.

Terme	Définition
authentification d'un document	Processus par lequel on confirme l'authenticité d'un document : authentique, contrefait, falsifié, etc. L'authentification d'un document se fait en vérifiant les éléments de sécurité du document en question, comme le laminat sécurisé, les images holographiques, etc.
authentification du justificatif	Processus qui consiste à vérifier qu'un sujet a le contrôle sur le justificatif qui lui a été assigné et que ce justificatif est valide (c'est-à-dire, ni suspendu ni révoqué).
biométrique	Terme général utilisé pour décrire une caractéristique ou un processus. Il s'agit d'une caractéristique biologique (anatomique et physiologique) ou comportementale mesurable, qui peut être utile à la reconnaissance automatisée. Biométrique peut aussi désigner des méthodes automatisées de reconnaissance des personnes fondées sur des caractéristiques biologiques (anatomiques et physiologiques) ou comportementales mesurables.
cadre de confiance	Ensemble de principes, de définitions, de normes, de spécifications, de critères de conformité et d'approche d'évaluation dont on a convenu.
client	Le destinataire prévu de l'extrant d'un service. Les clients externes sont généralement des personnes (citoyens canadiens, résidents permanents, etc.) ou des entreprises (organisations des secteurs public et privé). Les clients internes sont généralement des agents contractuels et des employés de la fonction publique.
confiance	Une croyance ferme quant à la fiabilité ou la véracité d'une personne, d'une organisation ou d'un appareil.
confirmation de caractéristique biologique ou comportementale	Un processus qui consiste à comparer les caractéristiques biologiques (anatomiques et physiologiques) afin d'établir un lien avec une personne (p. ex., comparaison avec une photo du visage).
confirmation de l'identité	Voir « assurance de l'identité ».

Terme	Définition
confirmation de possession physique	Processus qui nécessite la possession physique ou la présentation de preuves pour établir l'identité d'une personne.
confirmation par un arbitre de confiance	Processus dans le cadre duquel on s'appuie sur un arbitre de confiance pour établir un lien avec une personne. L'arbitre de confiance est déterminé selon les critères propres au programme. Les arbitres de confiance peuvent être des répondants, des notaires ou des agents agréés.
confirmation reposant sur les connaissances	Processus qui permet de comparer de l'information personnelle ou privée (p. ex., des secrets partagés) pour établir l'identité d'une personne. Les mots de passe, les numéros d'identification personnelle, les questions secrètes, les renseignements spécifiques aux programmes, et les renseignements liés au crédit ou d'ordre financier sont des exemples de renseignements pouvant être utilisés dans le cadre d'une confirmation reposant sur les connaissances.
demande de consentement	Processus consistant à présenter un énoncé d'avis au sujet (c'est-à-dire, la personne physique à qui les renseignements personnels en question se rapportent) et à demandant au sujet de demander son consentement (« Oui ») ou de refuser de donner son consentement (« Non ») en fonction du contenu de l'énoncé d'avis, ce qui entraîne une décision de consentement par « oui » ou par « non ».
enregistrement du consentement	Processus consistant à stocker de manière persistance un énoncé d'avis et la décision de consentement connexe du sujet. Par exemple : des renseignements sur le sujet, la version de l'avis qui lui a été présentée, la date et l'heure à laquelle l'avis a été présenté et, le cas échéant, la date d'expiration relative à la décision de consentement. Une fois les renseignements relatifs au consentement stockés, une notification sur la décision de consentement prise par le sujet est envoyée aux parties concernées.

Terme	Définition
examen du consentement	Processus qui consiste à rendre les détails d'une décision de consentement stockée visibles pour le sujet ou pour un examinateur autorisé.
contexte	Ensemble de circonstances, situation ou scénario dans lesquels un particulier interagit avec d'autres particuliers ou avec une organisation.
contexte de l'identité	L'environnement ou la série de circonstances où une organisation fonctionne et exécute ses programmes et ses services. Le contexte de l'identité est déterminé par des facteurs comme le mandat, la population cible (c'est-à-dire les clients, la clientèle), et les autres responsabilités établies en vertu d'une loi, d'un accord ou d'une entente.
création de la signature	Processus qui consiste à créer une représentation électronique dans laquelle, à tout le moins : la personne qui signe les données peut être associée aux représentations électroniques; il est clair que la personne avait l'intention de signer; la raison ou le but de la signature sont communiqués; et l'intégrité des données de la transaction signée est maintenue, y compris l'original.
critères de conformité	Ensemble d'énoncés d'exigences définissant ce qu'il faut pour assurer l'intégrité d'un processus fiable.
déclaration d'identité	Assertion de la véracité d'un fait se rapportant à l'identité d'une personne ou d'une organisation.
destinataire de demandes	Entité (habituellement une organisation) qui utilise des demandes au cours de ses activités. Les destinataires des demandes acceptent les demandes des détenteurs de demandes aux fins de la prestation de services ou de l'administration de programmes. Les destinataires de demandes sont également appelés parties de confiance et vérificateurs de demandes.
détenteur de demandes	Entité qui détient des demandes qui sont soumises et acceptées comme preuves par les destinataires des demandes. Les détenteurs de demandes sont habituellement, mais pas toujours, le sujet d'une demande.

Terme	Définition
détenteur d'identité numérique	Participant au cadre de confiance à qui une identité numérique est émise. Les détenteurs d'identité numérique sont en quelque sorte des détenteurs de demandes.
élément de donnée sur l'identité	Voir « attribut d'identité ».
émission d'un justificatif	Processus consistant à créer et à attribuer un justificatif unique à un objet (p. ex., une personne, une organisation ou un dispositif). Un justificatif peut comprendre un ou plusieurs codes d'identification. Ceux-ci peuvent être des pseudonymes, ou peuvent renfermer différents attributs vérifiés par l'émetteur du justificatif.
établissement de l'identité	Processus de création d'un dossier d'identité faisant autorité et sur lequel peuvent se fonder des tiers dans le cadre de programmes, de services et d'activités subséquents.
établissement de liens pour déterminer l'identité	Processus de mise en correspondance entre deux identifiants ou plus et la même identité.
événement organisationnel	Un événement organisationnel désigne un événement important se produisant durant la vie d'une organisation. En vertu de la loi, un événement organisationnel doit être enregistré auprès d'une entité gouvernementale et est assujetti à la loi et aux règlements. Parmi les événements organisationnels, on peut citer l'enregistrement de la charte, la fusion, le regroupement, l'abandon de charte, et la dissolution.
événement vital	Épisode discret important qui survient durant la vie d'une personne. En vertu de la loi, un événement organisationnel doit être enregistré auprès d'une entité gouvernementale et est assujetti à la loi et aux règlements. Parmi les événements organisationnels, on peut citer la naissance vivante, la mort fœtale (c.-à-d. la mortinatalité), l'adoption, la légitimation, la reconnaissance de paternité, le mariage, l'annulation de mariage, la séparation légale, le divorce et le décès.

Terme	Définition
expiration du consentement	Processus consistant à suspendre la validité d'une décision de consentement par un « oui » en raison d'une date d'expiration dépassée.
extraction des renseignements personnels	Divulgation par une partie faisant autorité, de renseignements personnels d'une personne, à une partie destinataire, suite à la demande de cette dernière.
extraction des renseignements sur l'identité	Divulgation par une partie faisant autorité, de renseignements sur l'identité d'une personne, à une partie utilisatrice, suite à la demande de cette dernière.
fédération	Entente de collaboration entre des entités autonomes qui se sont engagées à renoncer à une partie de leur autonomie dans le but de travailler efficacement au déploiement d'un effort collaboratif. La fédération repose sur des relations et des normes de confiance à l'appui de son interopérabilité.
fédération de l'identité	Fédération mise sur pied dans le but de gérer les identités.
fédération des justificatifs	Fédération mise sur pied dans le but de gérer des justificatifs.
fédérer des identités	Mise sur pied d'une Fédération dont les membres partagent les assurances d'identité avec d'autres membres de confiance de la fédération.
fédérer des justificatifs	Mise sur pied d'une Fédération dont les membres partagent les assurances de justificatifs avec d'autres membres de confiance de la fédération.
formulation d'avis	Processus consistant à produire un avis décrivant les renseignements personnels qui sont recueillis ou qui peuvent l'être; les parties auxquelles les renseignements personnels sont transmis, et le type de renseignements personnels transmis; les fins auxquelles les renseignements personnels sont recueillis, utilisés ou divulgués; le risque de préjudice et d'autres conséquences de la collecte, de l'utilisation ou de la divulgation; la façon dont les renseignements

Terme	Définition
	personnels seront traités et protégés; la période d'application de l'avis; et la personne ou l'entité ayant compétence ou autorité pour l'avis émis.
fournisseur d'assurance de l'identité	Participant au cadre de confiance qui établit et gère les identités et qui offre des services de confirmation de l'identité. Les fournisseurs d'assurance de l'identité sont en quelque sorte des fournisseurs de demandes.
fournisseur d'assurance du justificatif	Participant au cadre de confiance qui émet des justificatifs électroniques aux fins d'authentification, ou des justificatifs vérifiables afin de prouver une identité et/ou à titre de qualification. Les fournisseurs d'assurance de justificatif sont en quelque sorte des fournisseurs de demandes.
fournisseur de demandes	Entité (habituellement une organisation) qui émet des demandes à des *détenteurs de demandes.* Les fournisseurs de demandes sont aussi appelés parties faisant autorité ou émetteurs de demande.
fournisseur d'identité numérique fiable (INF)	Participant au cadre de confiance qui fournit le produit final d'une identité numérique fiable. Habituellement, il s'agit d'un programme provincial, territorial ou fédéral d'identité numérique, qui fournit une identité numérique fiable à une autre instance. Des fournisseurs d'INF peuvent également se desservir les uns les autres dans un secteur de l'industrie. Les fournisseurs d'identité numérique fiable sont en quelque sorte des fournisseurs de demandes.
fournisseur d'infrastructure	Entité (habituellement une organisation) qui offre des services de soutien à valeur ajoutée ou qui sert d'intermédiaire entre des parties.
fraude d'identité	Utilisation frauduleuse de renseignements personnels, notamment : utilisation abusive des cartes de débit/crédit ou souscription aux prêts à partir de renseignements personnels volés.
genre	Rôles, comportements, activités, et attributs qu'une société donnée attribue à un homme ou une femme.

Terme	Définition
gestion de l'identité	Ensemble de principes, de pratiques, de processus et de procédures utilisés pour respecter le mandat d'une organisation et ses objectifs en lien avec l'identité.
identificateur	L'ensemble d'attributs d'identificateurs uniques permettant de distinguer une personne, une organisation ou un dispositif particulier dans une population. (Autre définition provenant de la *Norme sur l'assurance de l'identité et des justificatifs*.)
identificateur attribué	chaîne numérique ou alphanumérique automatiquement générée et permettant de faire la distinction entre des personnes ou des organisations sans recourir à un autre attribut d'identité.
identité	Une référence ou une désignation unique utilisée pour distinguer une personne, une organisation ou un dispositif particulier. (Autre définition provenant de la *Norme sur l'assurance de l'identité et des justificatifs*.) On trouve deux types d'identité : fondamentale et contextuelle. Voir « identité fondamentale » et « identité contextuelle ».
identité contextuelle	Identité qui est utilisée à une fin précise dans un contexte d'identité précis.
identité fédérée	Partage des assurances d'identités avec les membres dignes de confiance d'une fédération.
identité fondamentale	Identité qui a été établie ou changée à la suite d'un événement fondamental (p. ex., naissance, changement légal de nom, décès, immigration, résidence légale, citoyenneté, insérer des exemples d'organisations).
identité numérique	Représentation électronique d'une personne ou d'une organisation.
identité numérique fiable (INF)	Représentation électronique d'une personne ou d'une organisation employée exclusivement par la personne ou l'organisation en question, dans le but d'accéder à des services appréciables ou d'effectuer des transactions en toute confiance et avec assurance.

Terme	Définition
interopérabilité	Capacité des organisations à fonctionner en synergie au moyen de pratiques uniformes de sécurité et de gestion de l'identité.
jeton	Voir « authentifiant ».
justificatif	Objet (ou identificateur) physique ou électronique unique émis ou associé à une personne, une organisation ou un appareil (p. ex., une clé, un jeton, un document, un identificateur de programme).
justificatif anonyme	Justificatif qui, tout en faisant une affirmation au sujet d'un bien, d'un statut ou d'un droit d'une personne, ne révèle pas son identité. Un justificatif peut comprendre des attributs d'identité, mais être toujours considéré comme anonyme si les attributs d'identité ne sont pas reconnus ou utilisés aux fins de validation de l'identité. Les justificatifs anonymes permettent aux personnes de prouver des affirmations à leur sujet et au sujet de leurs relations avec les organisations publiques et privées, de façon anonyme.
justificatifs fédérés	Partage des assurances de justificatifs avec les membres dignes de confiance d'une fédération.
liaison identité-justificatif	Processus qui consiste à associer une identité à un justificatif émis.
liaison justificatif-authentifiant	Processus qui consiste à associer un justificatif émis à un ou plusieurs authentifiants. Ce processus comprend également des activités liées au cycle de vie telles que la suppression d'authentifiants, la liaison d'autres authentifiants et la mise à jour d'authentifiants (p. ex., changement de mot de passe, mise à jour des questions et réponses de sécurité, nouvelle photo).
maintien de l'identité	Processus par lequel on veiller à ce que les renseignements sur l'identité soient exacts, complets et à jour, comme il est exigé.
modèle d'identité	Représentation simplifiée (ou sommaire) d'une méthode de gestion de l'identité. Il s'agit par exemple de modèles d'identité centralisés, fédérés et décentralisés.

Terme	Définition
niveau d'assurance	Un niveau d'assurance auquel se fient des tiers.
niveau d'assurance de l'identité	Niveau de confiance qu'une personne, une organisation ou un appareil est bel et bien la personne, l'organisation ou l'appareil qu'il ou elle prétend être.
niveau d'assurance du justificatif	Niveau d'assurance qu'une personne, une organisation ou un mécanisme a gardé le contrôle sur un justificatif qui lui ont été attribués (p. ex., clé, jeton, document, identificateur) et que ce justificatif n'a pas été compromis (p. ex., falsifié, corrompu, modifié).
nom fondamental	Nom d'une personne ou d'une organisation tel qu'il figure dans un enregistrement officiel identifiant la personne ou l'organisation (p. ex., le nom qui figure dans le registre de l'état civil provincial ou territorial, le dossier d'immigration fédéral, le registre des sociétés provincial ou territorial).
nom légal	Voir « nom officiel ».
nom officiel	Nom qu'une personne utilise à des fins formelles et juridiques (aussi appelé « nom légal »).
nom privilégié	Nom informel par lequel une personne préfère être appelée.
notification relative aux renseignements personnels	Communication des renseignements personnels d'une personne par une partie ayant autorité à une partie utilisatrice faisant suite à l'établissement de l'identité d'une personne ou à la modification de ses renseignements personnels, ou à une indication selon laquelle ses renseignements personnels ont été exposés à un facteur de risque (p. ex., décès de la personne, utilisation de documents ayant expiré, violation de la vie privée, utilisation frauduleuse des renseignements sur l'identité).
notification relative aux renseignements personnels	Communication des renseignements personnels d'une personne par une partie ayant autorité à une partie utilisatrice faisant suite à l'établissement de l'identité d'une personne ou à la modification de ses renseignements personnels.

Terme	Définition
partie faisant autorité	Membre de la fédération qui offre des assurances de justificatifs ou d'identité à d'autres membres de la fédération (c.-à-d. aux « parties utilisatrices »).
partie utilisatrice	Membre de la fédération qui utilise des assurances de justificatifs ou d'identité fournies par d'autres membres de la fédération (c.-à-d. « parties ayant autorité »).
personne	Être humain, y compris les « mineurs » et d'autres personnes qui ne sont pas nécessairement réputés être des personnes au sens de la loi.
présence légale	Droit légitime de se trouver ou de résider au Canada.
présentation de l'identité	Processus de confirmation dynamique de l'existence continue d'une personne au fil du temps (c'est-à-dire « une présence authentique »). Ce processus peut être utilisé afin de veiller à ce qu'aucune activité frauduleuse ou malveillante n'ait été effectuée (dans le présent ou par le passé).
preuve à l'appui de l'identité	Preuve de l'identité qui corrobore la preuve essentielle et permet d'établir un lien entre un renseignement d'identité et la personne concernée. Elle peut aussi des renseignements supplémentaires tels qu'une photo, signature, ou adresse. Exemples : dossiers d'assurance sociale; dossiers d'autorisation de voyage, de conduite, ou d'assurance maladie; et des certificats de mariage, de changement de noms, ou de décès délivrés par une instance juridictionnelle.
preuve de l'identité	Document provenant d'une source qui fait autorité et qui indique l'identité d'une personne. Il existe deux catégories de preuves de l'identité : les preuves fondamentales et les preuves à l'appui. Voir « preuve de l'identité essentielle » et « preuve à l'appui de l'identité ».
preuve documentaire	Toute information sur support matériel pouvant servir de preuve. Il est souvent présumé que ce terme désigne les renseignements inscrits sur support papier, mais la définition plus élargie est préférable.

Terme	Définition
preuve électronique ou numérique	Toute donnée enregistrée ou préservée sur n'importe quel support, par un système informatique ou tout autre appareil semblable. Exemples : enregistrements dans une base de données, journaux d'audit ou documents produits au moyen d'un logiciel de traitement de texte.
preuve fondamentale d'identité	Preuve établissant les principaux renseignements liés à l'identité, notamment : le(s) prénom(s), le nom de famille, la date et le lieu de naissance. Exemples : actes de naissance, dossier d'immigration ou dossier de citoyenneté provenant d'une autorité possédant la compétence nécessaire.
processus atomique	Ensemble d'activités logiquement reliées qui entraînent un état de transition.
processus composé	Ensemble de processus atomiques et/ou d'autres processus composés qui entraînent un ensemble de transitions d'état.
processus fiable	Ensemble d'activités qui entraînent la transition de l'état d'un objet. D'autres processus peuvent se fier à l'état de sortie de l'objet à titre de preuve.
recouvrement d'un justificatif	Processus qui consiste à transformer à nouveau un justificatif suspendu en justificatif utilisable (c'est-à-dire un justificatif utilisable).
registre fondamental	Registre qui conserve des dossiers permanents des personnes nées au Canada, des Canadiens nés à l'étranger, ainsi que des étrangers ayant présenté une demande pour entrer au Canada.
relation numérique fiable	Représentation électronique de la relation entre une personne et une autre personne, une organisation et une autre organisation, ou une personne et une organisation.
renouvellement du consentement	Processus consistant à prolonger la validité d'une décision de consentement par « oui » en reportant la date d'expiration.
renseignement d'identité	Ensemble d'attributs d'identité qui sont utilisés uniquement pour distinguer une personne donnée

Terme	Définition
	dans une population de programme ou de service et pour décrire cette personne conformément au programme ou au service. Les renseignements sur l'identité constituent un sous-ensemble de renseignements personnels.
renseignement personnel	Information sur une personne identifiable.
représentation numérique fiable	Entité pouvant être assujettie aux lois, aux politiques ou aux règlements dans un contexte, et pouvant avoir certains droits, devoirs et obligations.
résolution de l'identité	Processus d'établissement de l'unicité d'une personne au sein d'une population de programme/service, grâce à l'utilisation des renseignements sur l'identité.
révocation du consentement	Processus consistant à suspendre la validité d'une décision de consentement par un « oui » à la suite du retrait explicite du consentement par le sujet (c'est-à-dire qu'une décision de consentement par un « oui » est convertie en une décision de consentement par un « non »).
révocation d'un justificatif	Processus permettant de garantir qu'un justificatif émis est en permanence marqué comme inutilisable.
risque	Incertitude entourant les événements et les résultats à venir. C'est l'expression de la probabilité et de l'impact d'un événement susceptible d'affecter la réalisation des objectifs de l'organisation.
risque lié à l'identité	Risque qu'une personne, une organisation ou un appareil ne soit pas la personne, l'organisation ou l'appareil qu'il ou elle prétend être.
risqué lié au justificatif	Risque qu'une personne, une organisation ou un appareil ait perdu le contrôle des justificatifs qui lui ont été attribués.
sexe	Caractéristiques biologiques qui définissent les êtres humains masculins et féminins. Ces ensembles de caractéristiques biologiques ne sont pas mutuellement exclusifs, puisque certaines personnes possèdent à la fois des caractéristiques féminines et masculines.

Terme	Définition
sexe documenté	Un attribut provenant de l'indicateur « sexe » ou « genre » sur un justificatif.
signature	Représentation électronique dans laquelle, à tout le moins : la personne qui signe les données peut être associée aux représentations électroniques; il est clair que la personne avait l'intention de signer; la raison ou le but de la signature sont communiqués; et l'intégrité des données de la transaction signée est maintenue, y compris l'original.
source faisant autorité	Un ensemble ou un registre de dossiers conservés par une autorité qui respecte les critères établis.
suspension d'un justificatif	Processus qui consiste à transformer un justificatif émis en un justificatif suspendu en marquant le justificatif émis comme temporairement inutilisable.
usurpation d'identité	Étape préliminaire d'obtention et de rassemblement des renseignements personnels d'une autre personne à des fins criminelles.
validation de la preuve	Processus par lequel on confirme qu'un objet (physique ou électronique) peut être accepté ou admis en tant que preuve (p. ex., la détermination hors de tout doute raisonnable, la prépondérance des probabilités, la possibilité marquée).
validation des renseignements personnels	Confirmation de l'exactitude des renseignements personnels d'un individu, tels qu'établis par une partie faisant autorité.
validation des renseignements sur l'identité	Processus de confirmation de l'exactitude des renseignements sur l'identité d'une personne, tels qu'établis par une partie faisant autorité (également appelé « validation de l'identité »). Il convient de noter que ce processus ne garantit pas que la personne utilise ses propres renseignements d'identité – seulement que les renseignements d'identité qu'elle utilise sont exacts comparativement à un dossier officiel.
validation de l'identité	Processus de confirmation de l'exactitude des renseignements sur l'identité d'une personne établie

Terme	Définition
	en vertu d'une partie faisant autorité. Il est important de remarquer que ce processus ne garantit pas qu'une personne utilise ses propres renseignements sur l'identité. La validation de l'identité permet seulement de déterminer que les renseignements sur l'identité fournis par une personne sont exacts lorsqu'on les compare aux dossiers d'identité faisant autorité.
vérification de l'identité	Processus consistant à confirmer que les renseignements sur l'identité présentés concernent la personne qui présente la demande.
vérification de la signature	Processus permettant de confirmer que la signature des données est valide.

8 ANNEXE C : BIBLIOGRAPHIE

Organisations

1. Conseils mixtes du Canada (CMC)
    - Priorité des conseils mixtes du Canada en matière d'identité numérique : recommandations en matière de politique publique (2018)
2. Centre de la sécurité des télécommunications Canada (CST)
    - Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (2018)
3. Digital Identity and Authentication Council of Canada (DIACC)
    - Aperçu du cadre de confiance pancanadien (août 2016)
    - Aperçu de la composante vérification de la personne (mai 2017)
    - Aperçu de la composante vérification des identifiants de connexion (janvier 2018)
    - Aperçu de la composante notification et consentement (avril 2019)
    - Aperçu du modèle de cadre de confiance pancanadien (février 2019)
4. Sous-comité sur la gestion de l'identité (SCGI)
    - Modèle d'assurance pancanadien
    - Rapport pancanadien sur la fiabilité des identités
5. Commissariat à la protection de la vie privée du Canada (CPVP)
    - Lignes directrices pour l'obtention d'un consentement valable (mai 2018)
6. Secrétariat du Conseil du Trésor du Canada (SCT)
    - Fédérer la gestion de l'identité au gouvernement du Canada (2011)
    - Ligne directrice sur la définition des exigences en matière d'authentification (2012)
    - Norme sur l'assurance de l'identité et des justificatifs (2013)
    - Ligne directrice sur l'assurance de l'identité (2015)
    - Directive sur la gestion de l'identité (2019)

Personnes

1. Joe Andrieu
    - *A Primer on Functional Identity* (2018)

9 ANNEXE D : ENJEUX THÉMATIQUES

Le Groupe de travail du SCGI sur le CCP a déterminé plusieurs enjeux thématiques de haut niveau qu'il abordera à court ou à moyen termes.

Enjeu thématique 1 : Définition du CCP

Il devient manifeste que le CCP est un ensemble de concepts et de critères acceptés plutôt qu'une sorte de « norme ». Il s'agit effectivement d'un cadre qui contribuer à situer les normes (opérationnelles et techniques) de même que les politiques, les documents d'orientation et les pratiques existants. Tel est certainement le cas au niveau fédéral, où les processus atomiques et leurs critères de conformité associés ont été reliés aux instruments de politique, aux lignes directrices de soutien et aux normes d'interfaces techniques du gouvernement fédéral. Nous devons veiller à ce que cette définition du CCP en tant que cadre stratégique détaillé soit communiquée clairement et uniformément dans le document.

Enjeu thématique 2 : Inclusion des organisations et des relations numériques

Nous commençons à intégrer les travaux qu'ISDE a réalisés à l'égard des organisations. Même si la version actuelle du document est encore principalement centrée sur les personnes, nous sommes prêts à inclure entièrement le type d'entité de l'organisation dans la prochaine version du CCP. De plus, nous devons nous efforcer d'élargir notre traitement et notre couverture des relations numériques dans ce document – à l'heure actuelle, cette couverture ne va guère plus loin qu'une définition et un ensemble d'emplacements réservés.

Enjeu thématique 3 : L'état en évolution des justificatifs et des demandes

Nous nous trouvons au milieu de faits récents très intéressants dans les domaines des justificatifs numériques et des demandes vérifiables. Un changement radical se produit dans l'industrie : on passe de l'« échange de renseignements » à la « présentation de demandes numériques ». De plus, un travail solide lié aux normes est en cours au Consortium World Wide Web (W3C) en ce qui concerne les justificatifs vérifiables et les identificateurs décentralisés.

En raison de cette évolution des faits, nous entrevoyons maintenant la possibilité que les services intermédiés traditionnels (comme les fournisseurs de services d'ouverture de session centralisés ou fédérés) puissent disparaître en raison des nouvelles avancées technologiques. Cela peut ne pas arriver dans un avenir rapproché, mais nous ajustons actuellement le modèle du CCP pour y intégrer l'idée générale d'un « justificatif vérifiable » (plus qu'une ouverture de session) et la généraliser de manière à permettre aux justificatifs physiques (p. ex., le certificat de naissance, le permis de conduire) d'évoluer numériquement dans le modèle.

Nous ne sommes pas (encore) certains que le modèle que nous envisageons soit tout à fait juste. Quoi qu'il en soit, le Canada semble se diriger vers le peloton de tête pour ce qui est de comprendre les conséquences de l'application de ces technologies à l'échelle

écosystémique (autant publique que privée). Ainsi, nous recevons des demandes de renseignements sur la façon dont le CCP pourrait faciliter la migration vers les écosystèmes numériques et vers de nouveaux justificatifs fondés sur des normes, des systèmes de vérification de source ouverte et l'interopérabilité internationale.

Enjeu thématique 4 : Intervenants, rôles et acteurs

La version actuelle du CCP représente toujours les différentes perspectives quant à savoir qui est ou quels sont les intervenants, les rôles et les acteurs dans le CCP. Cela s'explique par le virage prévu du modèle de CCP vers les demandes vérifiables, les justificatifs vérifiables et les identificateurs décentralisés (voir l'enjeu thématique 3). Alors que nous résolvons l'enjeu thématique 3, la définition et la délimitation des intervenants, des rôles et des acteurs du CCP devraient se préciser.

Enjeu thématique 5 : Consentement éclairé

Le consentement éclairé est un domaine en évolution, et nous ne croyons pas que le CCP englobe actuellement tous les enjeux et toutes les nuances gravitant autour de ce sujet. Nous avons intégré du contenu du DIACC et l'avons adapté aux considérations relatives au secteur public. Toutefois, à la suite de la publication récente de la Charte canadienne du numérique, il y a un débat dans le domaine du consentement, surtout en ce qui concerne de possibles modifications législatives nécessaires. Des documents de discussion seront publiés prochainement sur des façons dont le Canada pourrait mettre la législation à jour en ce qui concerne la vie privée, le consentement et l'identité numérique. Nous nous attendons pleinement à ce que l'idée du consentement change; toutefois, entre-temps, nous estimons que le CCP est suffisamment clair pour que l'on procède à des évaluations – mais nous sommes prêts à apporter des changements au besoin.

Enjeu thématique 6 : Portée du CCP

Certaines personnes ont suggéré que la portée du CCP soit élargie de manière à inclure la qualification scolaire, les titres professionnels, etc. Nous menons actuellement des projets pilotes expérimentaux dans ces domaines avec d'autres pays. Nous avons anticipé l'extensibilité par la généralisation du modèle du CCP et l'ajout possible de nouveaux processus atomiques et composés. Il faut toutefois garder à l'esprit que l'identité numérique représente un cas d'utilisation très précis, mais d'une importance énorme que nous devons d'abord établir correctement. Nous ne sommes pas encore prêts à envisager d'étendre la portée du CCP à d'autres domaines, mais nous le serons bientôt.

Enjeu thématique 7 : Autres détails

Un grand nombre de questions ont été posées à propos de la version actuelle du présent document en ce qui concerne l'application précise du CCP. Même si nous en avons une bonne idée, nous n'avons pas encore toutes les réponses. Ces détails seront tirés en grande partie de l'application réelle du CCP (comme on l'a fait précédemment avec

l'Alberta). Le CCP est un cadre, et à mesure qu'il sera appliqué, il sera probablement complété par une orientation détaillée qui sera distincte du CCP lui-même. Nous ne savons pas exactement en quoi consistera ce contenu supplémentaire jusqu'à ce que nous en apprenions davantage par l'application du CCP actuel.