« Personne vérifiée » du CCP

Statut du document : Recommandation finale version 1.2 Errata

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

Ce document a été élaboré par le comité d'experts du cadre de confiance du CCIAN avec les commentaires du public recueillis et traités dans le cadre d'un processus ouvert d'examen par les pairs. On s'attend à ce que le contenu de ce document soit examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois, règlements et politiques. Les avis concernant les changements apportés à ce document seront partagés sous la forme de communications électroniques, notamment le courriel et les réseaux sociaux. Les notifications seront également consignées dans le programme de travail du Cadre de confiance pancanadien (CCP).

Ce document est fourni « TEL QUEL » et aucun participant du CCIAN ne garantit de quelque façon que ce soit, d'une manière expresse ou implicite, y compris d'une manière sous-entendue, sa qualité marchande, le fait qu'il ne viole pas les droits de propriété intellectuelle de tierces parties et qu'il convient à une fin particulière. Les personnes désirant obtenir de plus amples renseignements au sujet de la gouvernance du CCIAN sont invitées à consulter les politiques qui régissent le CCIAN.

Table des matières

1. Introduction à la composante « Personne vérifiée »

Le contenu ici présent concerne un sujet spécifique au domaine de ce composant du Cadre de confiance pancanadien (CPP). La section d'aperçu fournit des informations nécessaires pour une interprétation cohérente des critères de conformité inclus. Pour une introduction générale au CPP, veuillez consulter la vue d'ensemble du CPP, qui décrit le contexte, le but, la portée, les principes et les objectifs du cadre.

1.1 Aperçu

Il est nécessaire de pouvoir vérifier l'identité des personnes qui participent à une transaction en ligne pour assurer la confidentialité, la sécurité et la confiance en ligne. À défaut d'avoir cette capacité, les utilisateurs restent effectivement anonymes, et les craintes suscitées par le vol de données, les responsabilités juridiques et sociales, et les pertes financières persistent. L'éventail de transactions disponibles dans de telles conditions est limité en termes de sensibilité, de valeur et d'utilisation des renseignements personnels. C'est pourquoi le CCIAN investit dans des règles uniformes et vérifiables qui soutiennent la création et l'utilisation d'identités numériques pour les personnes – et sont documentées dans la composante « Personne vérifiée » du CCP. Par extension, ces règles et conventions facilitent la prestation de services numériques de confiance.

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

1.2 Raison d'être et avantages anticipés

La composante « Personne vérifiée » du Cadre de confiance pancanadien vise à assurer l'intégrité continue des processus utilisés pour vérifier l'identité numérique d'une personne. En appliquant les critères de conformité à l'évaluation et la certification du processus, cette composante peut servir à s'assurer de ce qui suit :

- Les processus de confiance donnent une représentation numérique d'un sujet unique avec un niveau d'assurance quant à leur identité correspondant au type de service ou de transaction employé par le sujet;
- La fiabilité des processus de confiance nécessaire pour maintenir l'intégrité et la sécurité de cette identité numérique;
- Une réduction de la possibilité de vol et d'usurpation de l'identité.

Tous les participants bénéficieront :

- Du caractère répétitif, uniforme et continu des processus d'identification.

Les parties dépendantes bénéficieront :

- De la capacité de tirer parti de l'assurance des processus de confiance de la composante « Personne vérifiée » pour identifier d'une manière unique un sujet dans le cadre de ses applications ou programmes.

Remarque : Les critères de conformité du Cadre de confiance pancanadien ne remplacent ou ne supplantent pas des règles existantes; on s'attend à ce que les organisations et les personnes se conforment aux lois, politiques et règlements pertinents dans leur province ou territoire.

1.3 Portée

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

1. **Vérifier une personne** : Il s'agit des processus qui assurent que l'identité numérique d'une personne est une représentation exacte de cette personne et qu'on peut s'y fier pour la prestation de services numériques et des transactions électroniques. Une personne vérifiée est un être humain réel, unique et identifiable, qui est présent au moment de la vérification; et dans le contexte du Cadre de confiance pancanadien, une telle personne peut être assujettie aux lois, politiques ou règlements dans un contexte. Ces processus assurent qu'une personne a été convenablement vérifiée et qu'elle est bien celle qui a demandé, directement ou par l'intermédiaire d'un représentant légalement autorisé, un service ou transaction.

   Remarques :

   - Une personne décédée ne peut plus être vérifiée comme personne, mais elle peut encore avoir une identité numérique avec un attribut indiquant un statut décédé.
   - Une personne qui désire obtenir un service ou une transaction mais qui est incapable de suivre elle-même physiquement le processus de vérification peut demander à un représentant légalement autorisé de l'aider à le faire.

2. **Créer une identité numérique de confiance pour une personne** : Il s'agit des processus pour établir et maintenir un dossier numérique pour une personne vérifiée (on parle aussi de dossier de personne vérifiée) afin de la distinguer d'une façon unique d'autres personnes.

Il existe de nombreuses techniques pouvant être utilisées pour vérifier si une personne est « un être humain réel, unique et vérifiable ». Par exemple, un système pourrait :

- Demander à l'utilisateur de présenter des documents officiels (p. ex., permis de conduire) et confirmer qu'il s'agit de la même personne;
- Exiger qu'on fournisse assez de données biométriques qui permettent à la personne de se distinguer d'une manière unique du reste de la population;

- Saisir une identité numérique à partir de l'appareil de la personne et utiliser les données comportementales (p. ex., vitesse de frappe, pression sur l'écran tactile, foulée mesurée par les accéléromètres d'un appareil mobile) pour déterminer que l'appareil est en la possession de la personne.

Le caractère approprié de ces méthodes sera déterminé par les exigences des parties dépendantes et variera selon les secteurs et les cas d'utilisation. Étant donné la sensibilité potentielle des données biométriques, il est recommandé de consulter les lois, les règlements et/ou autorités en matière de respect de la vie privée pertinents (p. ex. Commissariat à la protection de la vie privée) avant de recueillir des données biométriques afin de s'assurer qu'elles sont obtenues et utilisées d'une manière appropriée.

1.3.1 Inclus dans la portée

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

- La création d'une preuve de l'identité contextuelle chez une partie qui fait autorité;
- La dépendance à une preuve de l'identité essentielle pour vérifier une personne;
- La dépendance à une preuve de l'identité contextuelle pour vérifier une personne;
- Les niveaux d'assurance 1 à 3 pour l'identité; les cas d'utilisation de niveau 4 ne sont pas actuellement inclus dans la portée mais seront pris en compte pour des versions futures;
- La création, la mise à jour et la gestion du dossier d'une personne vérifiée (c.-à-d. une représentation numérique de confiance);
- Les acteurs incluent les gouvernements fédéral, provinciaux et territoriaux du Canada, et les organisations canadiennes conformes au CCP en tant que parties qui font autorité pour la preuve de l'identité.

1.3.2 Exclus de la portée

La portée de la composante « Personne vérifiée » du Cadre de confiance pancanadien n'inclut pas :

- La création d'une preuve essentielle de l'identité. L'établissement et le maintien d'une preuve essentielle de l'identité relève exclusivement du domaine des organisations mandatées comme l'État civil des provinces et territoires, et Immigration, Réfugiés et Citoyenneté Canada.
- L'utilisation de gouvernements ou d'organisations internationaux comme seules sources qui font autorité en matière de preuve de l'identité pour vérifier une personne. On peut faire référence indirectement à des gouvernements internationaux pour établir les sources d'identité de base on contextuelles. Les cas d'utilisation qui dépendent uniquement de preuves d'identité internationales pourraient être pris en considération dans des versions ultérieures du CCP.
- La vérification des attributs non identitaires. Les processus relatifs à la personne vérifiée n'établissent pas de renseignements particuliers à propos de la personne, mis à part le fait qu'il s'agit de quelqu'un de réel, d'unique et d'identifiable dans un contexte donné. Les autres renseignements ou attributs personnels comme l'adresse de résidence

peuvent être nécessaires pour fournir un service. La vérification des attributs non requis pour vérifier l'identité numérique d'une personne est en dehors de la portée de cette composante; veuillez vous référer à la composante « Justificatifs (relations et attributs) » du CCP.

La portée de la composante « Personne vérifiée » n'inclut pas actuellement les éléments suivants :

- Niveau d'assurance 4 pour l'identité, tel que défini par la Directive sur la gestion de l'identité – Annexe A : Norme sur l'assurance de l'identité et des justificatifs du gouvernement du Canada et les cas d'utilisation associés;
- Délégation de pouvoirs (c.-à-d. le fait d'agir au nom d'un sujet, p. ex. un fondé de pouvoir ou un organisme ou encore un signataire autorisé agissant pour le compte d'une organisation).

Ces éléments sont à l'étude pour une version future du CCP.

1.4 Sources des preuves d'identité

Le diagramme de la figure 1 illustre les sources potentielles de preuves de l'identité qui peuvent être utilisées pour vérifier une personne dans le contexte du Cadre de confiance pancanadien. Le nombre et le type de sources utilisées dépendent du cas, du niveau d'assurance que doit avoir l'identité du sujet et des règles, lois ou politiques applicables. Par exemple, le secteur public peut exiger au moins deux sources de preuves d'identité canadiennes conformes au CCP, dont une essentielle. Les sources d'identité internationales sont généralement utilisées uniquement avec des preuves canadiennes de l'identité. Voir le profil de conformité pour les exigences spécifiques du CCP à chaque niveau d'assurance.

Les sources des preuves d'identité pourraient inclure :

- La personne physique, y compris les renseignements biométriques;
- Des preuves documentaires comme un certificat de naissance, un document établissant la résidence permanence, un dossier de citoyenneté et d'autres documents acceptés;
- Des sources en ligne, notamment des bases de données des secteurs public et privé. Elles pourraient inclure des renseignements sur le sujet établis après avoir fourni un service du secteur public ou privé ainsi que des renseignements regroupés à partir de ces sources (indépendamment des exigences en matière de protection et de confidentialité des données, de confidentialité et législatives).

Remarques :

- Les documents délivrés par des gouvernements internationaux ne sont pas tous acceptables – cela dépend du pays et des attributs de l'identité en question.
- Certaines organisations acceptent les sources provenant des réseaux sociaux quand de faibles niveaux d'assurance seulement sont requis. Toutefois, il est recommandé à ceux qui envisagent d'utiliser des sources provenant des réseaux sociaux de faire preuve de prudence, car ces sources ne garantissent pas toutes l'exactitude de leurs

renseignements, ni que les renseignements ont été recueillis avec un consentement donné en connaissance de cause, le cas échéant.

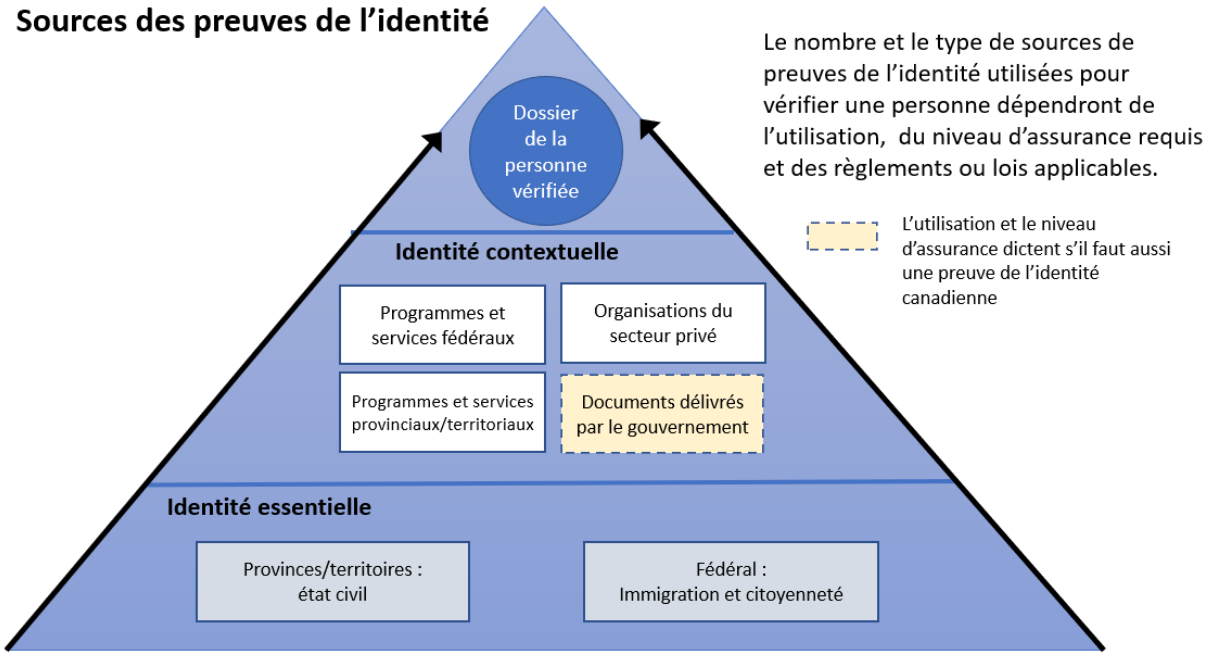

Figure 1. Source des preuves d'identité

1.5 Renseignements sur l'identité suffisants

Les considérations qui suivent s'appliquent lorsqu'il s'agit de déterminer si les renseignements sur l'identité sont suffisants :

- Les renseignements sur l'identité destinés à décrire une personne réelle (existante) ou à distinguer une personne d'une autre sont assujettis à l'exactitude des exigences relatives aux renseignements sur l'identité.
- Pour des raisons de confidentialité et de sécurité, comme la protection de l'identité des personnes, certains attributs de l'identité peuvent être des identifiants, des pseudonymes, des identifiants d'utilisateurs ou des noms d'utilisateurs attribués au hasard.
- Le nom, la date de naissance et le sexe sont des exemples de renseignements sur l'identité dans le cas des personnes.
- Un identifiant peut être un attribut d'identité unique qui est attribué et géré par le programme ou le service. Les identifiants attribués peuvent rester internes au programme ou service.
- Exemples d'identifiants internes : clés de bases de données et identifiants uniques au niveau universel.
- Des identifiants attribués peuvent être fournis à d'autres programmes; toutefois, il peut y avoir des restrictions dues à des questions de confidentialité ou aux lois.

- Des identifiants existants ou précédemment attribués qui répondent à l'obligation d'être uniques peuvent être utilisés comme renseignements sur l'identité. Les organisations doivent savoir que l'utilisation de ces identifiants peut être assujettie à des restrictions ou avoir des conséquences sur la protection de la vie privée.
- Certains identifiants peuvent être assujettis à des restrictions juridiques et en matière de politiques. Exemple : la directive sur le numéro d'assurance sociale énonce des restrictions spécifiques s'appliquant à la collecte, l'utilisation, la rétention, la divulgation et la suppression du numéro d'assurance sociale du gouvernement du Canada.

1.6 Relation avec le Cadre de confiance pancanadien

Le Cadre de confiance pancanadien comprend un ensemble de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées indépendamment les unes des autres pour être considérées comme des composantes de confiance. Le CCP, qui se fonde sur une approche pancanadienne, permet aux secteurs public et privé de collaborer pour protéger les identités numériques en uniformisant les processus et pratiques dans tout l'écosystème numérique canadien.

La figure 2 illustre les composantes de l'ébauche de CCP. Il est à noter que les exigences en matière de protection de la vie privée pour le traitement des renseignements personnels par les processus relatifs à la composante « Personne vérifiée » (et toutes les autres composantes du CCP) dans l'écosystème de l'identité numérique sont définies dans la composante « Respect de la vie privée » du CCP.

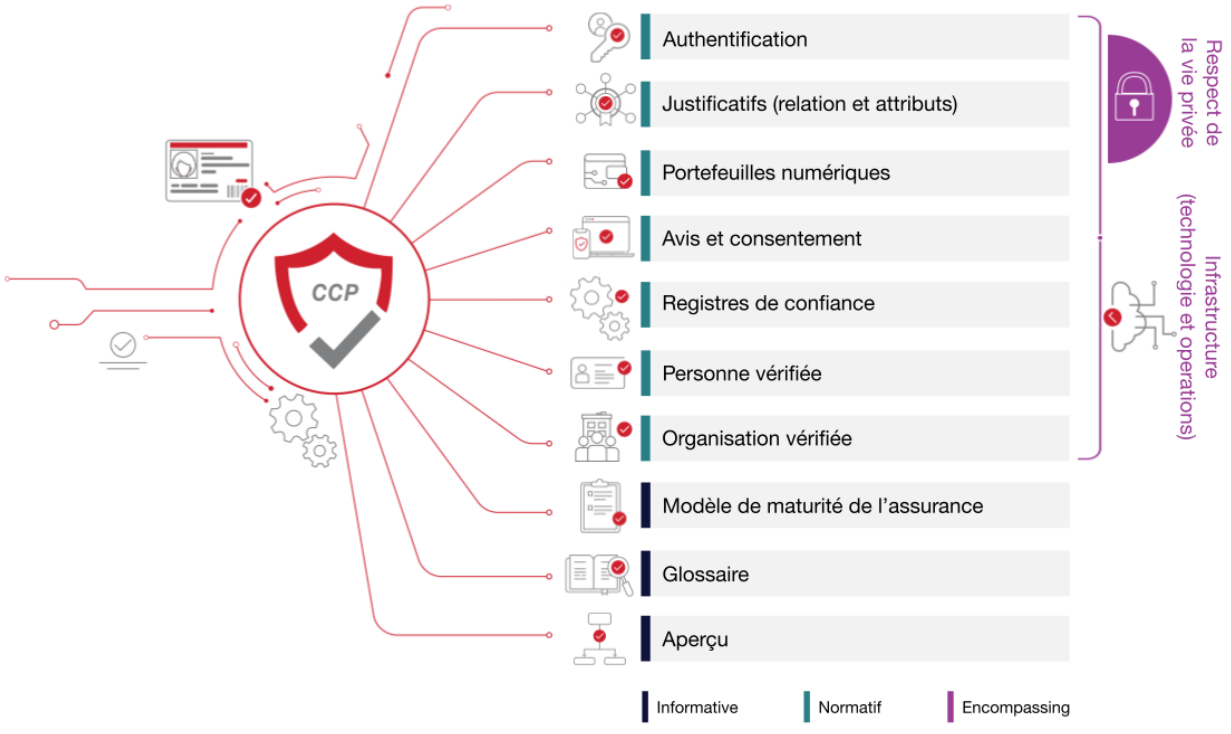

Figure 2. Composantes de l'ébauche du Cadre de confiance pancanadien

2. Conventions de la composante « Personne vérifiée »

Cette section décrit et définit les principaux termes et notions utilisés dans la composante « Personne vérifiée » du Cadre de confiance pancanadien. Ces renseignements sont fournis pour assurer une utilisation et une interprétation uniformes des termes employés dans cet aperçu et le profil de conformité de la composante « Personne vérifiée » du CCP.

2.1 Termes et définitions

La composante « Personne vérifiée » fait référence aux termes et définitions figurant dans le glossaire du CCP ainsi qu'aux termes et définitions qui suivent :

Source qui fait autorité

Collection ou registre de dossiers d'identité tenus par une partie qui fait autorité, qui remplit les critères de conformité du CCP pour établir la preuve d'identité.

- Exemples : registre de l'état civil; dossier de la personne vérifiée; registre d'entreprise; dossier de compte bancaire
- Non-exemples : fil de nouvelles Facebook; compte de réseau social
- Synonyme : Source de l'assurance

Preuve d'identité contextuelle

Preuve d'identité qui établit l'existence et les représentations numériques des entités dans un contexte spécifique et pour des raisons spécifiques. On parle aussi de « preuve d'identité à l'appui ».

- Exemples : compte bancaire; dossier de santé; permis de conduire délivré par une province; passeport canadien; compte d'affaires avec une société de télécommunications; dossier du Conseil canadien des bureaux d'éthique commerciale; carte d'identité délivrée par le gouvernement
- Non-exemples : carte de fidélité d'un magasin; carte de donneur de sang; faux passeport; certificat de naissance valide imprimé; site web d'une entreprise qui a cessé ses activités

Preuve d'identité essentielle

Preuve d'identité qui établit l'existence et la représentation numérique d'entités réelles, légalement reconnues sur la base d'événements factuels essentiels (p. ex., naissance, immigration, incorporation). L'établissement et le maintien de la preuve d'identité essentielle est du domaine exclusif du secteur public. Dans le cas spécifique des personnes, il s'agit des services de l'état civil des provinces et territoires, et d'Immigration, Réfugiés et Citoyenneté Canada; en ce qui concerne les organisations, il s'agit des bureaux d'enregistrement provinciaux et de Corporations Canada.

- Exemples : dossier de naissance provincial; dossier d'immigration fédéral; certificat d'incorporation; dossier de changement de raison sociale
- Non-exemples : permis de conduire; compte bancaire d'affaires

Sujet

Personne qui détient ou est en voie d'obtenir une représentation numérique dans le système de l'écosystème de l'identité numérique réglementé par le CCP, et qui peut être assujettie à des lois, politiques et règlements dans un contexte.

- Exemples : personne qui a la citoyenneté canadienne; organisme de bienfaisance; réfrigérateur intelligent qui peut faire des commandes d'épicerie dans les réserves sont basses; voiture autonome
- Non-exemples : personne sans documents d'identité; personne détenant uniquement un certificat de naissance physique (c.-à-d. pas encore de pièce d'identité électronique); chien de compagnie; faune; service en ligne; passeport

Personne non vérifiée

Personne qui n'est pas une personne vérifiée. Il est à noter qu'une personne non vérifiée *peut* être une personne réelle, unique et identifiable, qui a honnêtement affirmé être cette personne et dont l'identité n'a pas été vérifiée.

Personne vérifiée

Le fait de savoir (ou d'avoir un certain degré de certitude) qu'un être humain est réel, unique et identifiable (c.-à-d. une personne), et qu'il a honnêtement affirmé être cette personne.

Dossier d'une personne vérifiée

Dossier numérique qui montre qu'une personne a été vérifiée dans un contexte spécifique (p. ex., identifiant décentralise (DID), attributs de l'identité, numéro de compte). On parle aussi de représentation numérique de confiance dans le contexte du CCP.

2.2 Abréviations

Les abréviations suivantes sont utilisées tout au long de cet aperçu et dans le profil de conformité de la composante « Personne vérifiée » du CCP :

- CCP – Cadre de confiance pancanadien
- P/T – Provinces et territoires

2.3 Rôles

Les rôles et définitions qui suivent s'appliquent dans la portée et le contexte de la composante « Personne vérifiée » du CCP.

Partie qui fait autorité

Rôle qu'un participant (c.-à-d., organisation conforme au CCP) remplit pour prouver aux parties dépendantes les renseignements sur l'identité ou la preuve d'identité à un certain niveau d'assurance.

Partie dépendante

Rôle qu'une organisation ou personne remplit pour consommer des renseignements sur l'identité numérique créés et gérés par des participants pour effectuer des transactions numériques avec des sujets.

Autorité responsable

Rôle qu'un participant remplit pour fournir un ou plusieurs processus de confiance de la composante « Personne vérifiée » afin d'établir qu'un sujet est réel, unique et identifiable, et qui fait en sorte que les renseignements connexes ne soient pas compromis.

2.4 Niveaux d'assurance

Des niveaux d'assurance sont utilisés dans certains contextes, notamment la composante « Personne vérifiée » du Cadre de confiance pancanadien, pour indiquer la robustesse de la technologie et des processus employés pour vérifier l'identité d'une personne. Les critères de conformité pour la composante « Personne vérifiée » sont profilés en termes de niveaux d'assurance pour ce qui est de l'identité. Un niveau d'assurance associé à chaque critère reflète le niveau de confiance relatif que les parties dépendantes peuvent lui attribuer. Le tableau ci-dessous indique les trois niveaux d'assurance appliqués aux critères de conformité de la composante « Personne vérifiée » du CCP.

Remarque : Les descriptions du tableau 1 s'alignent sur les normes pour les niveaux d'assurance de l'identité spécifiés en A.2.2 de la « Directive sur la gestion de l'Identité - Annexe A : Norme sur l'assurance de l'identité et des justificatifs » (juillet 2019)

Niveau d'assurance de l'identité	**Description de la qualification**
Niveau 1	• Besoin d'un faible niveau d'assurance que le sujet est celui qu'il affirme être. • La personne ayant fait l'affirmation est autoévaluée et/ou des vérifications minimales peuvent être faites. Les vérifications, si elles sont effectuées, n'exigent d'utiliser que des sources de preuve présentant un faible niveau d'assurance. • Répond aux critères de conformité du niveau 1.

Niveau d'assurance de l'identité	Description de la qualification
Niveau 2	• Besoin d'un certain niveau d'assurance qu'un sujet est celui qu'il affirme être. • La validation et la vérification utiliseront des preuves fournissant une assurance moyenne qui sont potentiellement soutenues par des preuves supplémentaires fournissant une faible assurance. • Des moyens à distance peuvent être utilisés pour vérifier la personne. • Répond aux critères de conformité du niveau 2.
Niveau 3	• Besoin d'un niveau élevé d'assurance qu'un sujet est celui qu'il affirme être. • La validation et la vérification utiliseront des preuves offrant un haut niveau d'assurance et potentiellement soutenues par des preuves supplémentaires fournissant un niveau d'assurance moyen et faible. • Des moyens en personne (ou l'équivalent) sont utilisés pour vérifier la personne. • Répond aux critères de conformité du niveau 3.
Niveau 4	• Besoin d'un niveau très élevé d'assurance qu'un sujet est celui qu'il affirme être. • Répond aux critères de conformité du niveau 4, lorsqu'ils sont définis.

Tableau 1. Description de la qualification des niveaux d'assurance

3. Processus de confiance

Le CCP incite à la confiance grâce à une série d'exigences commerciales et techniques vérifiables pour divers processus. Un *processus* est une activité commerciale ou technique (ou un ensemble de telles activités) qui transforme une condition d'entrée en condition de sortie – un extrant auquel d'autres se fient généralement.

Dans le contexte du Cadre de confiance pancanadien, un processus désigné comme étant un *processus de confiance* est évalué selon des *critères de conformité* bien définis et convenus. L'intégrité d'un processus de confiance est de la plus haute importance, car de nombreux participants—couvrant tous les territoires, provinces, organisations et secteurs—se fient au résultat de ce processus.

La séquence selon laquelle les processus de confiance sont exécutés peut varier. Par exemple, la résolution de l'identité peut être le résultat des processus de validation des renseignements sur l'identité ou être un intrant aux processus de validation des renseignements sur l'identité, selon le système d'identité numérique en question.

3.1 Aperçu conceptuel

La composante « Personne vérifiée » définit un ensemble de processus utilisés pour déterminer qu'une personne naturelle est réelle, unique et identifiable. Il s'agit d'un ingrédient essentiel pour établir une identité numérique de confiance, une représentation électronique d'une personne, utilisée exclusivement par cette même personne, pour recevoir des services auxquels elle tient et pour effectuer des transactions avec confiance et assurance.

La composante « Personne vérifiée » a pour objectif d'établir un ensemble de critères de conformité à partir desquels le processus consistant à déterminer qu'une personne est réelle, unique et identifiable peut être évaluée et certifiée. Une fois qu'un processus est certifié, il devient un processus de confiance auquel peuvent se fier d'autres participants du Cadre de confiance pancanadien.

La composante « Personne vérifiée » définit les processus de confiance suivants :

1. Établissement des sources
2. Résolution de l'identité
3. Détermination de l'identité
4. Validation des renseignements sur l'identité
5. Vérification de l'identité
6. Validation des preuves
7. Présentation de l'identité
8. Maintenance de l'identité

La figure 3 fournit un aperçu conceptuel et une organisation logique de la composante « Personne vérifiée ».

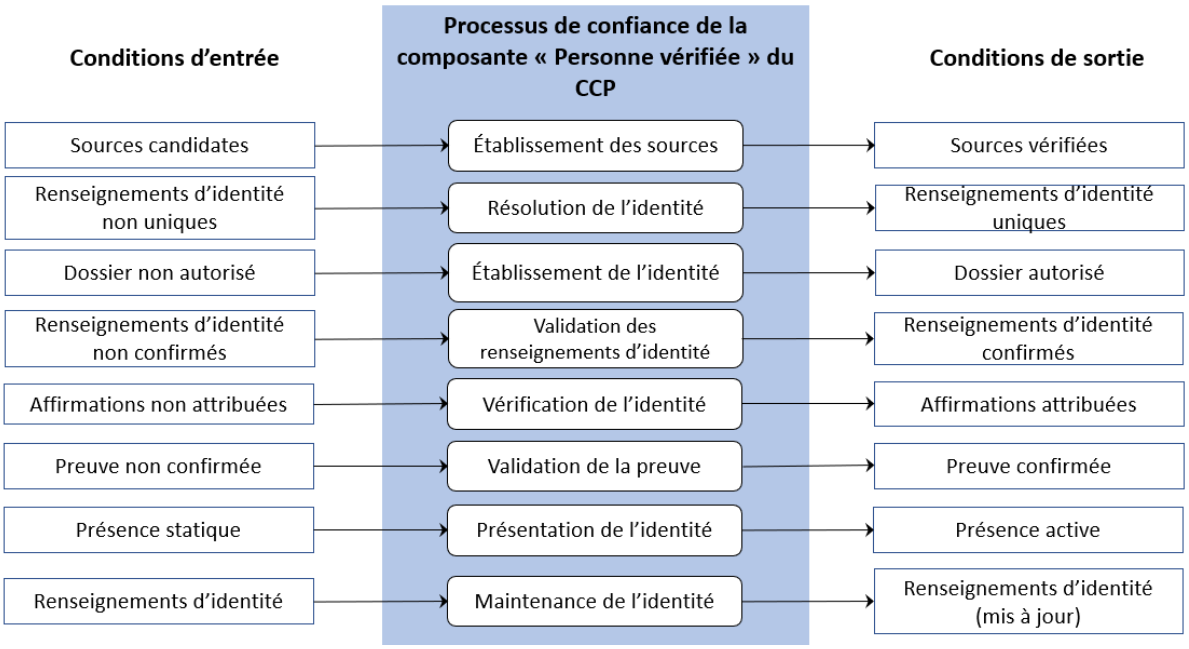

Figure 3. Composante « Personne vérifiée »

Les sections qui suivent fournissent des définitions des processus de confiance de la composante « Personne vérifiée » du Cadre de confiance pancanadien. Le profil de conformité de la composante « Personne vérifiée » du Cadre de confiance pancanadien définit les critères de conformité connexes permettant d'évaluer la fiabilité de ces processus.

Remarque : On ne s'attend pas à ce que tous les processus de confiance et critères de conformité connexes s'appliquent dans toutes les circonstances ou à tous les cas d'utilisation dans l'ordre indiqué plus haut.

Les processus de confiance de la composante « Personne vérifiée » sont définis à l'aide des renseignements suivants :

- Description – Aperçu descriptif du processus
- Intrants – Ce qui est entré, ajouté ou utilisé par le processus
- Extrants – Ce qui est produit par le processus ou en résulte
- Dépendances – Processus de confiance connexes du Cadre de confiance pancanadien, principalement ceux qui produisent des extrants dont le processus dépend
- Renseignements supplémentaires – Autres détails pertinents

3.2 Établissement des sources

Le processus d'établissement des sources est l'activité préparatoire menée pour déterminer quelles sources de preuves d'identité peuvent servir à valider et/ou vérifier des identités, et l'assurance de ces sources. En règle générale, un système d'identité numérique utilisera une série de sources afin de soutenir les exigences pour identifier des sujets dans un contexte donné et pour atteindre des niveaux d'assurance ciblés.

Intrants	Sources candidates	Sources proposées pour être utilisées dans les processus de validation des renseignements sur l'identité et de vérification de l'identité.
Extrants	Sources vérifiées	Sources approuvées pour être utilisées dans les processus de validation des renseignements sur l'identité et de vérification de l'identité.
Dépendances	Aucune	

3.3 Résolution de l'identité

La résolution de l'identité est le processus qui consiste à déterminer le caractère unique d'un sujet à l'intérieur d'une population cible en utilisant des renseignements sur l'identité. Une autorité responsable définit ses propres exigences en matière de résolution de l'identité pour ce qui est des attributs de l'identité; autrement dit, elle spécifie l'ensemble d'attributs de l'identité qui sont nécessaires pour identifier d'une manière unique un sujet au sein d'une population spécifique.

Intrants	Renseignements sur l'identité non uniques, exigences en matière de résolution de l'identité	Ensemble d'attributs de l'identité disponibles pour identifier d'une manière unique le sujet au sein de la population en question.
Extrants	Renseignements sur l'identité uniques	Ensemble d'attributs de l'identité nécessaires qui a été établi pour identifier d'une manière unique un sujet à partir d'autres sujets dans la population en question.
Dépendances	Détermination des sources	

3.4 Établissement de l'identité

L'établissement de l'identité est le processus qui consiste à créer des preuves d'identité (c.-à-d. un dossier d'une personne vérifiée) au sein d'une population de programmes ou services, auxquelles d'autres peuvent se fier pour des programmes, services et activités subséquents.

Intrants	Pas de dossier d'identité	Preuve d'identité inexistante pour un sujet au sein d'une population de programmes ou services.
Extrants	Dossier d'identité	Preuve d'identité (dossier de personne vérifiée) existante pour un sujet au sein d'une population de programmes ou services.

Dépendances	Résolution de l'identité	

3.5 Validation des renseignements sur l'identité

La validation de l'information sur l'identité est le processus qui consiste à confirmer l'exactitude des renseignements sur l'identité d'un sujet par rapport aux renseignements d'identité établis par une partie qui fait autorité. La validation des renseignements sur l'identité se fie aux preuves obtenues des sources obtenues à partir du processus d'établissement des sources pour déterminer si les renseignements sur l'identité fournis existent et sont valides. Il est à noter que ce processus n'assure pas que le sujet utilise ses propres renseignements sur son identité – il sert uniquement à déterminer que les renseignements sur l'identité que le sujet utilise sont exacts lorsqu'on les compare à la preuve de l'identité fournie par une source qui fait autorité.

Intrants	Renseignements d'identité non confirmés	Renseignements d'identité d'un sujet qui n'ont pas été validés d'après une source qui fait autorité.
Extrants	Renseignements d'identité confirmés	Renseignements d'identité d'un sujet qui ont été validés d'après une source qui fait autorité.
Dépendances	Sources établies	

3.6 Vérification de l'identité

La vérification de l'identité est le processus qui consiste à confirmer que les renseignements d'identité fournis sont contrôlés par l'utilisateur. Il est à noter que ce processus peut utiliser des renseignements personnels qui ne sont pas reliés à l'identité. Ce processus peut utiliser les preuves de l'identité obtenues des sources des preuves confirmées dans le processus d'établissement des sources, ainsi que les interactions avec l'utilisateur pour déterminer que l'identité affirmée appartient au sujet qui fait l'affirmation.

Intrants	Contrôle non vérifié	Les renseignements d'identité n'ont pas été vérifiés comme relevant du contrôle de l'utilisateur.
Extrants	Contrôle vérifié	Les renseignements d'identité ont été vérifiés comme relevant du contrôle de l'utilisateur.
Dépendances	Validation des renseignements d'identité	

3.7 Validation de la preuve d'identité

La validation de la preuve d'identité est le processus consistant à confirmer que les preuves (physiques ou électroniques) présentées peuvent être acceptées ou être admissibles comme

preuve (c.-à-d. au-delà du doute raisonnable, prépondérance des probabilités et grande probabilité).

Intrants	Preuve d'identité non confirmée	La preuve d'identité n'a pas été confirmée comme étant admissible.
Extrants	Preuve d'identité confirmée	La preuve d'identité a été confirmée comme étant admissible.
Dépendances	Établissement des sources	

3.8 Présentation de l'identité

La présentation de l'identité est le processus qui consiste à confirmer d'une façon dynamique qu'une personne a une existence continue dans le temps (c.-à-d. « présence authentique »).

Intrants	Présence statique	L'identité (c.-à-d. le dossier de la personne vérifiée) existe d'une manière sporadique et est souvent associée uniquement à un événement lié à l'état civil ou de nature commerciale (p. ex., naissance, décès, faillite)
Extrants	Présence active	L'identité (c.-à-d. le dossier de la personne vérifiée) existe d'une manière continue dans le temps et est associée à de nombreuses transactions
Dépendances	Validation de l'identité, Vérification de l'identité	

3.9 Maintenance de l'identité

La maintenance de l'identité est le processus qui consiste à s'assurer que les renseignements d'identité enregistrés de la personne sont exacts, complets et à jour selon ce qui est nécessaire. Ce processus est lié à des événements qui peuvent se répercuter sur la validité de la validation des renseignements et la vérification de l'identité effectuées préalablement (p. ex., preuve utilisée pour déterminer que la personne vérifiée a changé, expiré ou été révoquée, ce qui invalide le dossier de la personne vérifiée).

Intrants	Dossier de la personne vérifiée	Les renseignements d'identité enregistrés de la personne (c.-à-d. le dossier de la personne vérifiée) ne sont plus valides en raison des changements apportés au statut des renseignements ou parce que les données sont devenues désuètes avec le temps et sont considérées comme expirées.
Extrants	Dossier de la personne vérifiée mis à jour	Les renseignements d'identité de la personne ont été mis à jour, revalidés et revérifiés (c.-à-d. dossier de la personne vérifiée).
Dépendances	Vérification de l'identité	

4. Introduction au profil de conformité « Personne vérifiée » du CCP

Ce document spécifie les critères de conformité pour la composante « Personne vérifiée » du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale au CCP, notamment de l'information contextuelle et les buts et objectifs du CCP, reportez-vous à l'aperçu du modèle de CCP.

Chaque composante du CCP comporte deux documents :

1. **Aperçu** – Il introduit le sujet de la composante. L'aperçu fournit des renseignements essentiels pour comprendre les critères de conformité de la composante, à savoir des définitions des termes clés, des concepts et les processus de confiance qui font partie de la composante.
2. **Profil de conformité** – Il spécifie les critères de conformité utilisés pour uniformiser et évaluer l'intégrité des processus de confiance qui font partie de la composante.

Les critères de conformité de la composante « Personne vérifiée » spécifient les exigences à remplir pour faire en sorte que les processus de confiance donnent la représentation d'une personne réelle, identifiable et unique au niveau d'assurance voulu. À moins d'indication contraire, il s'agit d'un document normatif.

Remarque : Les critères de conformité du CCP ne remplacent et n'annulent pas les règlements existants; on s'attend à ce que les organisations et les personnes se conforment aux lois, politiques et règlements pertinents dans leur province ou territoire.

5. Mots clés des critères de conformité

Les mots clés suivants indiquent la priorité et la rigidité générale d'un critère de conformité, et doivent être interprétés de la façon suivante :

- **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de conformité.
- **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de conformité.
- **DEVRAIT** signifie qu'on s'attend à ce que l'exigence soit remplie, sauf dans les cas limités où le candidat présente des raisons ou des circonstances valables d'ignorer l'exigence. Toutes les implications d'une telle exception doivent être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité comme décrit.
- **NE DEVRAIT PAS** signifie qu'il peut exister une raison valable dans des circonstances particulières pour que l'exigence soit acceptable ou même utile, mais que toutes les implications devraient être comprises et le cas devrait être bien pris en considération avant de choisir de ne pas se conformer aux exigences telles que décrites.
- **PEUT** signifie que l'exigence est discrétionnaire mais recommandée.

Les mots clés apparaissent en **caractères gras** et en MAJUSCULES dans les critères de conformité.

6. Critères de conformité de la composante « Personne vérifiée »

Les critères de conformité sont organisés selon les processus de confiance définis dans **l'**aperçu de la composante « Personne vérifiée » et profilés à l'aide de colonnes pour les niveaux d'assurance de l'identité. Pour faciliter la référence, un critère de conformité spécifique peut être mentionné selon sa catégorie et son numéro de référence. Par exemple, « **SOUR 1** » fait référence à la « référence 1 des critères de conformité pour les sources établies ».

Remarques :

- Dans les critères de la composante « Personne vérifiée », le sujet fait toujours référence à un sujet qui est une personne. Les critères pour les organisations et les machines à vérifier comme sujets doivent être traités dans d'autres composantes du CCP, par exemple la composante « Organisation vérifiée ».
- Les critères de conformité de base, qui s'appliquent indépendamment du processus de confiance qu'une autorité responsable met en place, sont inclus dans le présent profil de conformité
- Le niveau d'assurance 4 pour l'identité déborde de la portée de cette version. La colonne est incluse pour des développements futurs.

Référence	Critères de conformité	Niveau d'assurance de l'identité				
BASE	**Base**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v.1.4**

1	L'autorité responsable **DOIT** fournir une description globale actuelle du programme ou service, notamment :
	• Énoncé de la raison d'être
	  ○ Fonction(s) des services (c.-à-d. authentification, preuve, vérification, etc.).
	  ○ Auditoire visé (c.-à-d. grand public, sous-ensemble, etc.).
	  ○ Industries connexes (toutes, soins de santé, finances, etc.).
	• Description des services
	  ○ Endroit spécifique à partir duquel la solution est gérée.
	  ○ Aperçu ou description de marketing sous forme générale du service.
	  ○ Types de validation, d'authentification ou de technologie que le service comprend :
	  ▪ Biométrie, intégrité des appareils mobiles, validation des pièces d'identité, vivacité, vérifications des risques, mots de passe à usage unique, etc.
	  ▪ Diagramme de conception et/ou d'architecture de haut niveau des services.
	  ▪ Diagramme des utilisateurs/flux de données des services.
		O	O	O		

2	L'autorité responsable **DOIT** documenter son rôle, sa vocation et son autorité sur le plan commercial relativement à l'identification des sujets.	O	O	O		
3	L'autorité responsable **DEVRAIT** être une entité privée enregistrée et en activité au Canada (p. ex., entreprise individuelle, société) ou une entité publique (p. ex., ministère, agence ou registraire) relevant d'un gouvernement fédéral, provincial ou territorial canadien.	O				IDES.01

4	L'autorité responsable **DOIT** être une entité privée enregistrée et en activité au Canada (p. ex., entreprise individuelle, société) ou une entité publique (p. ex., ministère, agence ou registraire) relevant d'un gouvernement fédéral, provincial ou territorial canadien.		O	O		IDES.02
5	L'autorité responsable **DOIT** fournir une référence à l'autorité, la politique ou l'exigence juridique qui soutient le besoin de recueillir des renseignements personnels spécifiques. En Ontario, par exemple, les exigences en matière de protection de la vie privée sont couvertes par la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS).	O	O	O		
6	Si l'autorité responsable dépend d'une autre organisation ou la soutient pour mener à bien le processus d'établissement de l'identité, il **DOIT** y avoir un accord écrit ou encore une loi ou des règlements à l'appui.	O	O	O		
7	L'autorité responsable **DEVRAIT** fournir aux utilisateurs un avis écrit comme quoi toute déclaration fausse ou trompeuse peut entraîner une violation des conditions.	O				
8	L'autorité responsable **DOIT** fournir aux utilisateurs un avis écrit comme quoi toute déclaration fausse ou trompeuse peut entraîner une violation des conditions.		O	O		
9	Si une autorité responsable se fie à une autre organisation pour mener un processus de confiance « Personne vérifiée », assujetti aux critères de conformité de la composante « Personne vérifiée », cette autorité responsable **DOIT fournir** : • de la documentation sur l'accord écrit pour l'arrangement en vigueur; ET • de la documentation sur l'évaluation approuvée des critères de conformité.	O	O	O		

10	Si des cas impliquent des enfants, des mineurs et d'autres sujets vulnérables, l'autorité responsable **DEVRAIT** : • Avoir en place des mesures de protection, des facteurs compensatoires ou un processus d'exception documenté pour réduire les risques et amorcer des interventions, le cas échéant. • Confirmer que le demandeur (par exemple, un parent ou tuteur) est légalement autorisé à faire une demande ou à obtenir un service au nom de l'enfant, du mineur ou d'un autre sujet vulnérable.	O	O			IDDG.11
11	Si les cas impliquent des enfants, des mineurs et d'autres sujets vulnérables, l'autorité responsable **DOIT** • Avoir en place des mesures de protection, des facteurs compensatoires ou un processus d'exception documenté pour réduire les risques et amorcer des interventions, le cas échéant. • Confirmer que le demandeur (par exemple, un parent ou tuteur) est légalement autorisé à faire une demande ou à obtenir un service au nom de l'enfant, du mineur ou d'un autre sujet vulnérable.			O		IDDG.11
12	Les organisations et les personnes **DOIVENT** se conformer aux lois, aux règlements et à la politique applicables dans leur province ou territoire, qui peuvent changer.	O	O	O		
13	L'autorité responsable **DEVRAIT** fournir aux utilisateurs un avis écrit leur demandant d'aviser l'autorité responsable chaque fois que des changements sont apportés aux renseignements d'un sujet.	O				
14	L'autorité responsable **DOIT** fournir aux utilisateurs un avis écrit leur demandant d'aviser l'autorité responsable chaque fois que des changements sont apportés aux renseignements d'un sujet.		O	O		
SOUR	**Établissement des sources**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v1.4**

L'établissement des sources est le processus préparatoire entrepris pour déterminer quelles sources des preuves d'identité peuvent être utilisées pour valider et/ou vérifier une personne (c.-à-d. sujets) et l'assurance de ces sources. Règle générale, un système d'identité numérique utilisera un éventail de sources pour soutenir les exigences afin d'identifier les sujets dans un contexte donné et d'atteindre les niveaux d'assurance ciblés. Remarque : Ces critères ne sont pas inclus dans le profil du secteur public (Sous-comité de gestion de l'identité des conseils mixtes), car ils font partie des exigences des politiques et/ou prescrites par la loi de la partie dépendante.						
1	Si approprié, l'autorité responsable **DOIT** se conformer à son mandat prescrit par la loi pour détenir les renseignements pour lesquels elle est identifiée en tant que source. L'autorité responsable **DOIT** offrir une sécurité, une exactitude, une exhaustivité et une confidentialité appropriées pour ses sources d'identité, et déterminer : • L'origine des preuves. • La robustesse des processus employés pour recueillir et entreposer les preuves. • La performance historique de la source. • La capacité de la source à satisfaire les autorités réglementaires. • La reconnaissance de la source dans la loi.	O	O	O		IDED.03
2	Si l'autorité responsable utilise une source externe pour les preuves d'identité, la source externe des preuves d'identité **DOIT** : • Détenir une marque de confiance de la vérification « Personne vérifiée » du CCIAN, OU • Se soumettre à une évaluation explicite de la part de l'autorité responsable.	O	O	O		IDED.04
3	Une source de preuves d'identité **DOIT** être évaluée comme offrant une assurance faible si : • Ce n'est pas possible de déterminer la provenance des preuves ou des processus employés pour recueillir et entreposer les preuves utilisées par la source.	O	O	O		

4	Une source de renseignements d'identité du secteur privé **DOIT** être évaluée comme offrant une assurance moyenne seulement si : • La provenance des données et des processus employés par la source peut être vérifiée et jugée satisfaisante par les organes de gouvernance ou les organismes de réglementation appropriés, OU • Dans le cas d'une source statistique, quand l'exactitude continue de la source peut être démontrée à partir des données historiques sur la performance.	O	O	O		
5	Une source de renseignements d'identité du secteur public **DOIT** être évaluée comme offrant une assurance moyenne seulement si : • L'origine des données et des processus employés par la source peut être vérifiée et jugée satisfaisante par les organes de gouvernance ou les organismes de réglementation appropriés, OU • Il s'agit d'une source d'identité essentielle (voir la définition dans l'aperçu).	O	O	O		
RESO	**Résolution de l'identité**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v1.4**
La résolution de l'identité est le processus qui consiste à déterminer le caractère unique d'un sujet dans une population de programmes ou services à partir de l'utilisation des renseignements d'identité. Un programme ou service définit ses exigences en matière de résolution de l'identité en termes d'attributs de l'identité; autrement dit, le programme ou service spécifie l'ensemble d'attributs de l'identité qui est nécessaire pour identifier d'une façon unique un sujet dans sa population.						
1	L'autorité responsable **DOIT** spécifier la population ou clientèle pour laquelle ses services sont fournis.	O	O	O		
2	L'autorité responsable **DOIT** s'assurer que le dossier ayant autorité résout d'une façon unique un seul sujet dans sa population d'intérêt spécifiée.		O	O		IDRE.01

3	L'ensemble d'attributs de l'identité **DOIT** être suffisant pour faire la distinction entre différents sujets dans un contexte identitaire; et suffisant pour décrire le sujet tel qu'exigé par le service ou le programme (voir la section 4.1.4 de la Directive du gouvernement du Canada sur la gestion de l'identité (juillet 2019)).	O	O	O		
ESTAB	**Établissement de l'identité (contextuelle)**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v1.4**
L'établissement de l'identité est le processus qui consiste à créer des preuves de l'identité contextuelle auxquelles d'autres peuvent se fier pour fournir des programmes, des services et des activités. Remarque : L'établissement et la maintenance de preuves d'identité essentielles est en dehors de la portée, car elle est du domaine exclusif du secteur public; ces critères se trouvent dans le profil du secteur public du Cadre de confiance pancanadien.						
1	Toute transaction reliée à la création d'un dossier d'une personne vérifiée **DOIT** être vérifiable et faire référence à un événement ou une activité pertinents de nature commerciale.	O	O	O		IDES.05
2	L'autorité responsable **DOIT** justifier et documenter le besoin de recueillir les renseignements d'identité spécifiques qui sont nécessaires pour satisfaire les fins commerciales indiquées.	O	O	O		IDES.05
3	L'autorité responsable **DOIT** avoir en place des politiques et des procédures pour préserver les attributs de l'identité fournis par l'utilisateur.	O	O	O		IDDG.05
4	L'autorité responsable **DOIT** avoir en place des politiques et des procédures pour déceler l'utilisation des attributs de l'identité d'un utilisateur sans son. consentement et y réagir		O	O		IDDG.06
VALID	**Validation des renseignements d'identité**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v1.4**
La validation des renseignements d'identité est le processus qui consiste à confirmer l'exactitude des renseignements d'identité d'un sujet d'après ceux qui ont été établis par une source qui fait autorité. La validation des renseignements d'identité dépend des preuves obtenues à partir du processus d'établissement des sources pour déterminer si les renseignements d'identité affirmés existent et sont valides.						
1	Les renseignements auto-affirmés par un sujet **DEVRAIENT** être acceptés.	O				IDIV.01

2	Les renseignements d'identité **DOIVENT** concorder d'une façon acceptable avec l'affirmation fournie par l'utilisateur et toutes les preuves d'identité (essentielle et/ou contextuelle) présentées par l'utilisateur.		O	O		IDIV.04
3	Les preuves exigées, le cas échéant, **PEUVENT** inclure des sources offrant une assurance faible.	O				
4	Les preuves exigées **DOIVENT**, à tout le moins, inclure des sources offrant une assurance moyenne et **PEUVENT** être soutenues par des sources fournissant une faible assurance.		O			
5	Les preuves exigées **DOIVENT**, à tout le moins, inclure des sources offrant une grande assurance et **PEUVENT** être soutenues par des sources fournissant une assurance moyenne et faible.			O		
6	L'autorité responsable **DEVRAIT** vérifier les preuves pour confirmer qu'elles correspondent aux renseignements d'identité déclarés, et que les preuves existent et sont valides.	O				
7	L'autorité responsable **DOIT** vérifier les preuves pour confirmer qu'elles correspondent aux renseignements d'identité déclarés, et que les preuves existent et sont valides.		O	O		
8	L'autorité responsable **DOIT** documenter la façon dont les différences entre les preuves et les renseignements d'identité déclarés cadre avec sa tolérance au risque. Par exemple, une autorité responsable spécifique pourrait conclure qu'une différence de numéro de téléphone présente un faible risque pour elle dans les cas où toutes les autres preuves sont identiques aux renseignements d'identité déclarés.	O	O	O		
9	Le niveau de risque résultant des différences entre les preuves et les renseignements d'identité déclarés qui est acceptable **PEUT** être déterminé par l'autorité responsable.	O				
10	Le niveau de risque résultant des différences entre les preuves et les renseignements d'identité déclarés qui est acceptable **DOIT** être conforme aux besoins des services réglementés de l'industrie, le cas échéant.		O			

11	Le niveau de risque résultant des différences entre les preuves et les renseignements d'identité déclarés qui est acceptable **DOIT** être minime et bien documenté.			O		
12	Les preuves d'identité contextuelles **DOIVENT** être confirmées comme provenant de l'autorité émettrice. Si la confirmation de l'autorité émettrice n'est pas faisable, la preuve d'identité contextuelle **DOIT** alors être confirmée à l'aide d'un examinateur formé.		O	O		IDIV.05
13	La preuve d'identité essentielle **DOIT** être confirmée comme provenant de l'autorité émettrice, qui a validé les renseignements d'identité à l'aide d'un dossier qui fait autorité ou permet à la partie dépendante de valider les renseignements d'identité auprès de la source qui fait autorité. Si la confirmation de l'autorité d'origine ou la validation à la source n'est pas faisable, la preuve d'identité essentielle **DOIT** être confirmée à l'aide d'un examinateur formé.		O	O		IDVA.8
14	L'autorité responsable **DOIT** s'assurer que les sources et la technologie utilisées pour le processus de validation sont documentées et appropriées dans le contexte du processus de validation.	O	O	O		
15	Lorsque des preuves sont présentées sous la forme de documents physiques qui ne sont pas vérifiables du point de vue cryptographique, la vérification des preuves **DEVRAIT** faire appel à des pratiques exemplaires pour déceler les documents frauduleux.	O				
16	Lorsque des preuves sont présentées sous la forme de documents physiques qui ne sont pas vérifiables du point de vue cryptographique, la vérification des preuves **DOIT** employer et documenter un régime de détection des fraudes spécifique au(x) document(s) en cours d'évaluation.		O	O		
17	Lorsque les preuves sont numériques (y compris basées sur une API et un certificat numérique), des processus appropriés **DEVRAIENT** être employés pour assurer l'intégrité des preuves (p. ex., altération évidente, signature cryptographique, vérification à la machine d'un justificatif).	O				

18	Lorsque les preuves sont numériques (y compris basées sur une API et un certificat numérique), des processus appropriés **DOIVENT** être employés pour assurer l'intégrité des preuves (p. ex., altération évidente, signature cryptographique, vérification à la machine d'un justificatif). Les renseignements fournis dans les profils des justificatifs et de l'infrastructure peuvent fournir d'autres pistes pour ces critères.		O	O		
EVID	**Validation des preuves**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v1.4**
La validation des preuves est le processus consistant à confirmer que les preuves (physiques ou électroniques) fournies peuvent être acceptées ou admissibles comme preuves (c.-à-d. hors de tout doute raisonnable, part de probabilités et forte possibilité).						
1	Il n'y a aucune restriction quant au genre de preuves qu'une organisation accepte.	O				IDEA.02
2	Une preuve d'identité (contextuelle ou essentielle) **DOIT** être évaluée comme ayant au moins un niveau d'assurance moyen conformément aux critères SOUR.		O			IDEA.03
3	Deux preuves d'identité (dont au moins une preuve d'identité essentielle) **DOIVENT** être évaluées comme ayant au moins un niveau d'assurance moyen conformément aux critères SOUR.			O		IDEA.04

4	Les preuves essentielles **DOIVENT** provenir d'une source qui fait autorité relevant du contrôle d'un gouvernement fédéral, provincial ou territorial, ou de l'équivalent local à l'étranger; et elles servent à maintenir l'enregistrement d'événements de l'état civil ou à déterminer le statut juridique. Sources qui font autorité, dossiers et documents acceptables comme preuves essentielles : • Dossiers d'état civil utilisés pour délivrer des certificats de naissance; • Dossiers sur le statut légal utilisés pour délivrer des certificats de citoyenneté et de naturalisation ainsi que des cartes de résidence permanente; et • Autres dossiers faisant autorité permis par la législation ministérielle.		O	O		IDEA.05
5	Les preuves essentielles des renseignements d'identité qui sont incomplètes ou non conformes aux renseignements fournis par l'utilisateur (p. ex. nom, date de naissance ou différence de sexe) **DEVRAIENT** nécessiter une confirmation supplémentaire de la part de la source qui fait autorité ou des preuves contextuelles additionnelles.		O			IDEA.05
6	Les preuves essentielles des renseignements d'identité qui sont incomplètes ou qui ne correspondent pas aux renseignements fournis par l'utilisateur (p. ex., nom, date de naissance ou différence de sexe) **DOIVENT** faire l'objet d'une confirmation supplémentaire par la source qui fait autorité.			O		IDEA.05

7	Les preuves contextuelles **DOIVENT** provenir d'une source qui fait autorité relevant du contrôle d'une organisation qui est approuvée par le CCP ou qui a un équivalent territorial ou d'un domaine ou encore qui a fait l'objet d'une évaluation explicite par l'autorité responsable. Sources qui font autorité, dossiers et documents acceptables comme preuves contextuelles : • Dossiers ou documents de permis et d'enregistrement utilisés pour délivrer un permis de conduire; • Passeport ou certificat de statut indien; et • Organisations professionnelles accréditées utilisées pour attribuer des justificatifs professionnels.		O	O		
8	Si les preuves contextuelles sont acceptées avec des preuves d'identité essentielles (niveau 3) : • Les preuves d'identité contextuelles **DEVRAIENT** être conformes aux renseignements fournis par les preuves d'identité essentielles. • Des preuves contextuelles supplémentaires **PEUVENT** être requises si les renseignements d'identité sont incomplets ou incohérents (p. ex., changement de nom). • Un endos ou une certification **PEUT** être nécessaire pour vérifier que les preuves contextuelles sont une copie conforme d'un original.		O	O		
PRES	**Présentation de l'identité**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v1.4**
La présentation de l'identité est le processus consistant à confirmer d'une manière dynamique qu'un sujet a une existence continue dans le temps (c.-à-d. une « présence authentique »). Ce processus peut être utilisé pour déceler des activités frauduleuses (passées ou présentes) et pour répondre aux préoccupations concernant l'usurpation d'identité.						
	Les critères de conformité pour la présentation de l'identité seront inclus dans une version future du CCP.					

VERIF	Vérification de l'identité	L1	L2	L3	L4	Référence au profil du secteur public v1.4
La vérification de l'identité est le processus consistant à confirmer que les renseignements d'identité fournis sont reliés au sujet qui fait la déclaration. Il est à noter que ce processus peut utiliser des renseignements personnels qui ne sont pas reliés à l'identité.						
1	L'autorité responsable **PEUT** entreprendre les étapes de vérification qu'elle juge nécessaire, le cas échéant.	O				IDVE.01
2	L'autorité responsable **DOIT** s'assurer que les interactions dans un contexte donné peuvent être reliées au sujet qui fait la déclaration.		O	O		IDVE.02
3	L'autorité responsable **DOIT**, à tout le moins, vérifier le sujet à distance (p. ex. vérification basée sur les connaissances ou données contextuelles). La vérification **DOIT** donner l'assurance suffisante que seul le sujet identifiable en question serait capable d'accomplir le processus de vérification.		O			IDVE.03
4	L'autorité responsable **DOIT** utiliser au moins une des méthodes suivantes pour s'assurer que les renseignements d'identité sont reliés à l'utilisateur et au sujet : • Confirmation biologique (p. ex., pièce d'identité avec photo), biométrique (p. ex. empreinte digitale) ou des caractéristiques comportementales. • Vérification face à face en personne (ou l'équivalent). • Confirmation de la possession physique. Si les méthodes ci-dessus ne sont pas faisables, des méthodes de rechange **DOIVENT** alors être définies et documentées dans un processus d'exception, qui **PEUT** inclure : • La confirmation par un référant de confiance (p. ex., garant, notaire, agent certifié) déterminé par des critères spécifiques au programme. • Des protections supplémentaires. • Des facteurs compensatoires.			O		IDVE.03

5	Outre les conditions spécifiées dans la section BASE concernant les sujets vulnérables, les organisations privées et gouvernementales PEUVENT inclure des exigences en matière de preuves d'identité pour un parent ou un tuteur dans le cadre des exigences en matière d'identité pour un enfant, un mineur ou tout autre sujet vulnérable. Par exemple, le passeport d'un parent pourrait servir de preuve d'identité contextuelle pour l'enfant.	O	O	O		IDEA.07
MAINT	**Maintenance de l'identité**	**L1**	**L2**	**L3**	**L4**	**Référence au profil du secteur public v1.4**
La maintenance de l'identité est le processus consistant à s'assurer que les renseignements d'identité sont exacts, complets et à jour tel que requis. Ce processus est relié à des événements qui peuvent avoir une incidence sur la validation des renseignements d'identité et la vérification de l'identité effectuées préalablement (p. ex., la preuve utilisée pour déterminer que la personne vérifiée a changé, expiré ou été révoquée, ce qui invalide le dossier de la personne vérifiée).						
1	L'autorité responsable **PEUT** juger que le sujet n'a plus besoin d'être vérifié si une des situations suivantes est vraie : • Des changements ont été apportés aux preuves contextuelles. • Le statut des preuves essentielles change. Cela pourrait inclure l'immigration, le mariage, le décès ou les changements de statut qui ont une incidence sur les processus préalables de validation et de vérification de l'identité. • La période qui s'est écoulée depuis que les processus de validation ou de vérification de l'identité ont été effectués dépasse un seuil spécifié par la partie dépendante.	O				

2	L'autorité responsable **NE DOIT PAS** présenter un sujet comme ayant été vérifié à une partie dépendante si l'autorité responsable s'aperçoit de l'une ou l'autre des situations suivantes en ce qui concerne un sujet : • Des changements ont été apportés aux preuves contextuelles • Le statut des preuves essentielles change. Cela pourrait inclure l'immigration, le mariage, le décès ou les changements de statut qui ont une incidence sur les processus préalables de validation et de vérification de l'identité. • La période qui s'est écoulée depuis que les processus de validation ou de vérification de l'identité ont été effectués dépasse un seuil spécifié par la partie dépendante.		O	O		
3	L'autorité responsable **PEUT** effectuer des vérifications supplémentaires pour revalider ou revérifier le sujet. Dans certains cas, ces vérifications peuvent être un sous-ensemble des processus de validation des renseignements d'identité et de vérification de l'identité. Dans tous les cas, des vérifications suffisantes **DOIVENT** être effectuées pour s'assurer que toutes les exigences en matière de résolution de l'identité, de validation des renseignements d'identité et de vérification de l'identité sont remplies pour le niveau d'assurance en question.	O				

4	L'autorité responsable **DEVRAIT** être capable de faire des vérifications supplémentaires pour revalider ou revérifier le sujet. Dans certains cas, ces vérifications peuvent être un sous-ensemble des processus de validation des renseignements d'identité et de vérification de l'identité. Dans tous les cas, des vérifications suffisantes **DOIVENT** être effectuées pour s'assurer que toutes les exigences en matière de résolution de l'identité, de validation des renseignements d'identité et de vérification de l'identité sont remplies pour le niveau d'assurance en question.		O			
5	L'autorité responsable **DOIT** être capable de faire des vérifications supplémentaires pour revalider ou revérifier le sujet. Dans certains cas, ces vérifications peuvent être un sous-ensemble des processus de validation des renseignements d'identité et de vérification de l'identité. Dans tous les cas, des vérifications suffisantes **DOIVENT** être effectuées pour s'assurer que toutes les exigences en matière de résolution de l'identité, de validation des renseignements d'identité et de vérification de l'identité sont remplies pour le niveau d'assurance en question.			O		
6	Lorsque l'autorité responsable apprend que des changements ont été apportés à des renseignements d'identité à la suite d'une naissance ou d'un décès, elle **DEVRAIT** corriger ou mettre à jour le ou les dossiers du sujet conformément aux lois ou règlements applicables.	O				
7	Lorsque l'autorité responsable apprend que des changements ont été apportés à des renseignements d'identité à la suite d'une naissance ou d'un décès, elle **DOIT** corriger ou mettre à jour le ou les dossiers du sujet (conformément aux lois ou règlements applicables).		O	O		

8	Les changements aux renseignements d'identité essentiels **DOIVENT** être confirmés par une autorité essentielle pour les types d'événements connexes en cas de : • Changement de nom. • Changement de nom.		O	O		IDMA.04
9	Les naissances et décès **DEVRAIENT** entraîner une notification aux parties dépendantes.		O	O		
10	Quand l'autorité responsable prend connaissance de changements validés à des renseignements d'identité, elle **DEVRAIT** mettre à jour le ou les dossiers du sujet.	O	O			
11	Quand l'autorité responsable prend connaissance de changements validés à des renseignements d'identité, elle **DOIT** mettre à jour le ou les dossiers du sujet.			O		

7. Références

Cette section énumère les normes, lignes directrices et autres documents externes dont il est fait mention dans la composante « Personne vérifiée » du CCP.

Remarque : Le cas échéant, seul le numéro de version ou de diffusion spécifié dans le présent document s'applique à cette composante du CCP.

La composante « Personne vérifiée » du CCP s'est inspirée des normes et documents d'orientation suivants et est basée en partie sur eux :

1. Gouvernement due Canada. Secrétariat du Conseil du Trésor du Canada. *Directive sur la gestion de l'identité*. 2019. <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16577>
2. Gouvernement due Canada. Secrétariat du Conseil du Trésor du Canada. *Directive sur la gestion de l'identité* - Directive sur la gestion de l'identité – Annexe A : Norme sur l'assurance de l'identité et des justificatifs. 2019 https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32612
3. Conseils mixtes. Sous-comité sur la gestion de l'identité. *Ébauche de recommandations pour le profil du secteur public du Cadre de confiance pancanadien version 1.0*. 2019. <https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_0>

8. Contrôle des versions du document

Version	Date de diffusion	Auteur(s)	Brève description
0.01	2018-06-08	Équipe de rédaction du CCP	Première tentative d'ébauche communautaire de critères de conformité de la composante « Personne vérifiée ».
0.02	2019-09-17	Équipe de rédaction du CCP	Mise à jour de l'ébauche conformément à l'équipe de conception de la composante « Personne vérifiée » basée sur l'aperçu de la composante uniformisée du CCP.
0.03	2019-10-16	Équipe de rédaction du CCP	Mise à jour des critères de conformité pour inclure le profil du CCP du secteur public afin d'examiner la comparaison et de déterminer si cela peut s'appliquer au document de base du CCP.
0.04	2019-10-14	Équipe de rédaction du CCP	Mise à jour conformément aux mesures découlant de la réunion de conception du 23 octobre.

0.05	2019-11-12	Équipe de rédaction du CCP	Mise à jour conformément aux mesures découlant des réunions de l'équipe de conception de la composante « Personne vérifiée ».
0.06	2019-11-26	Équipe de rédaction du CCP	Remplacement de l'identité essentielle par l'identité contextuelle conformément au modèle de CCP.
0.07	2020-01-03	Équipe de rédaction du CCP	Mise à jour pour régler les commentaires wiki en suspens, en prévision de la période d'examen.
0.08	2020-01-16	Équipe de rédaction du CCP	Mise à jour à la suite de la réunion de l'équipe de conception de la composante « Personne vérifiée » du 14 janvier et édition finale avant l'examen.
0.09	2020-02-14	Équipe de rédaction du CCP	Mise à jour à la suite de la réunion de l'équipe de conception de la composante « Personne vérifiée » du 12 février pour examiner les commentaires du TFEC.
1.0	2020-02-24	Équipe de rédaction du CCP	Approbation comme ébauche de recommandation V1.0.
1.1	2021-10-29	Rédacteur du CCP et équipe de conception de la composante « Personne vérifiée »	Mise à jour en réponse aux commentaires du public et examen pour vérifiabilité.
1.1	2021-11-10	Rédacteur du CCP et équipe de conception de la composante « Personne vérifiée »	Approbation du TFEC comme candidat à une recommandation finale V1.1.
1.2	2022-02-11	Rédacteur du CCP et équipe de conception de la composante « Personne vérifiée »	Mise à jour en réponse aux commentaires découlant de l'examen public.
1.2	2022-03-02	Rédacteur du CCP et équipe de conception de la composante « Personne vérifiée »	Approbation du TFEC comme candidat à une recommandation finale V1.2.

1.2 Errata	2022-03-09	Rédaction du CCP	Mise à jour des mappages des profils du CCP du secteur public de la v1.3 à la v1.4 : • Ajout : Mappage de SOUR-1 à IDED.03 • Ajout : Mappage de SOUR-2 à IDED.04 • Modification : Mappage de EVID-6 à IDEA.05 à partir de IDEA.06 • Modification : Mappage de VERIF-5 à IDEA.07 à partir de IDVE.03 Ajout : Mappage de ESTAB-2 à IDES.05
1.2 Errata	2022-03-21	Rédacteur du CCP et équipe de conception de la composante « Personne vérifiée »	Approuvé en tant que recommandation finale V1.2 errata par vote du membre de soutien du CCIAN