« Justificatifs (relations et attributs) » du CCP

Statut du document : Recommandation finale version 1.0

Conformément aux procédures opérationnelles du CCIAN, une recommandation finale est un livrable qui représente les conclusions d'un comité d'experts du CCIAN 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).

Table des matières

1. Introduction à la composante « Justificatifs (relations et attributs) » du CCP

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 l'Aperçu du CPP, qui décrit le contexte, le but, la portée, les principes et les objectifs du cadre.

1.1 Contexte

Une tâche fondamentale qui incombe aux participants à l'écosystème de l'identité numérique consiste à transmettre de l'information sur les sujets à d'autres participants. Il est essentiel de pouvoir s'assurer que l'entité à l'autre bout d'une connexion est bien celle qu'elle prétend être pour interagir avec confiance et assurance en ligne. Les processus et les critères de conformité nécessaires pour instaurer cette confiance sont le sujet des composantes « Personne vérifiée » et « Organisation vérifiée » du CCP. Ces critères ne seront pas répétés dans cette composante.

Les participants à l'écosystème de l'identité numérique doivent être certains non seulement de l'identité des autres entités avec lesquelles ils interagissent, mais des autres renseignements qui décrivent davantage ces entités (p. ex. droits, qualifications, coordonnées). Ces renseignements sont fournis par le biais d'attributs ou d'allégations qui sont contenus dans des justificatifs. Ces justificatifs et attributs font l'objet de la présente composante du CCP.

Les justificatifs sont courants dans le monde physique. Prenez des exemples associés au fait de posséder et d'utiliser un véhicule. Le permis de conduire indique aux autres que le sujet est apte et légalement autorisé à conduire un véhicule sur la voie publique. Les feuillets d'assurance auto indiquent aux autres que le sujet a acheté la protection nécessaire en cas d'accident. Les procurations attestent la relation juridique du sujet avec une personne handicapée s'il devient nécessaire de vendre un véhicule que cette personne n'est plus autorisée par la loi à conduire (un fait qui peut être reflété sur un permis de conduire). Les diplômes d'études collégiales et les certificats de formation du fabricant assurent les propriétaires d'automobiles et les propriétaires de garages que le technicien qui répare un véhicule est qualifié pour le faire. Un permis d'affaires et un permis de garage public indiquent aux propriétaires d'automobiles et aux organismes de réglementation que le garage où la voiture est réparée est légalement autorisé à fonctionner. L'adhésion à des associations locales visant à améliorer les affaires renseigne les propriétaires d'automobiles sur la légitimité du garage comme entreprise dans la communauté locale.

Cet ensemble de justificatifs, émis et gérés par des organisations des secteurs public et privé, inspire et soutient la confiance dans une large partie de l'écosystème de transport.

1.2 Raison d'être et avantages anticipés

Cette composante vise à fournir un cadre que les participants à l'écosystème de l'identité numérique peuvent utiliser pour déterminer dans quelle mesure leur écosystème protège les justificatifs numériques et les relations de confiance essentielles. Cela est accompli en identifiant ces relations de confiance générales et en spécifiant les critères de conformité qui favorisent ou augmentent la confiance dans :

- Les entités qui émettent, approuvent ou révoquent les justificatifs;
- Les rapports entre les sujets pour lesquels les justificatifs sont émis et les justificatifs comme tels;
- L'intégrité et la fiabilité des justificatifs et de leur contenu.

Cette composante a pour but d'instaurer et de maintenir la confiance au-delà de l'intégrité des données des Justificatifs comme telles et la capacité de les prouver, de sorte que l'acceptation des justificatifs numériques devient aussi routinière que leurs équivalents physiques. Cette composante accomplit cela en mettant l'accent sur des facteurs qui ne sont pas entièrement techniques et dont voici certains des avantages anticipés :

- Davantage de confiance entre les entités;
- Moins de risques lorsqu'on fait confiance aux renseignements ou qu'on utilise des justificatifs en l'absence d'une relation ou d'un lien directement entre la partie dépendante et la source des renseignements;
- Transparence en ce qui concerne les principaux acteurs;
- Meilleure perspective de la validité des justificatifs grâce aux preuves et à la capacité de les vérifier;
- Méthodes pour associer un justificatif à une personne ou une organisation réelle et unique;
- Compréhension des risques associés à un justificatif grâce à des détails descriptifs;
- Diminution du partage excessif d'information sur les justificatifs afin de réduire la possibilité d'agrégation des renseignements personnels ou de collusion.

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

1.3 Portée

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

1.3.1 Inclus dans la portée

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

- Contiennent ou fournissent des renseignements sur un sujet (p. ex., preuve numérique du niveau d'études ou permis d'exploiter une entreprise) et un émetteur;
- Contiennent ou fournissent des renseignements sur la relation entre un sujet et au moins une autre entité (p. ex., preuve numérique qu'une personne est employée par une entreprise);
- Contiennent des renseignements qu'une entité fournit sur ou à une autre entité;
- Décrivent les relations entre un ou plusieurs sujets et une ou plusieurs entités.

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

- L'émission des justificatifs aux sujets;
- Les renseignements qui augmentent la fiabilité des justificatifs;
- Des conseils pour protéger l'intégrité et l'exactitude des renseignements sur les justificatifs;
- Des consignes pour gérer les justificatifs compromis.

1.3.2 Exclus de la portée

La vérification et la validation de l'identité d'une personne ou d'une organisation sont en dehors de la portée de cette composante. Ces processus, et la création et l'utilisation des renseignements sur l'Identité dont ils dépendent, sont couverts dans les composantes « Personne vérifiée » et « Organisation vérifiée » du CCP.

Ce qui suit est également en dehors de la portée de la présente composante du CCP :

- Critères de conformité spécifiques pour l'émission d'un justificatif par de multiples émetteurs;
- Règles et politiques déterminant qui peut obtenir un justificatif ou un type de justificatif spécifique (p. ex., exigences pour obtenir un permis de conduire dans une administration donnée);
- Processus pour évaluer la qualification ou l'admissibilité pour un justificatif ou un type de justificatif spécifique (p. ex., tester de nouveaux conducteurs), indépendamment des exigences pour fournir les documents de tels processus;
- Acceptation d'un justificatif pour un besoin donné (p. ex., permis de conduire accepté ou non comme preuve d'adresse);
- La délégation de pouvoirs est exclus de la portée pour cette version et sera prise en considération pour une version future.

1.4 Relation avec le Cadre de confiance pancanadien

Le Cadre de confiance pancanadien est un ensemble de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées indépendamment pour être prises en

considération comme 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 les pratiques à l'échelle de l'écosystème numérique canadien.

La figure 1 illustre les composantes du Cadre de confiance pancanadien.

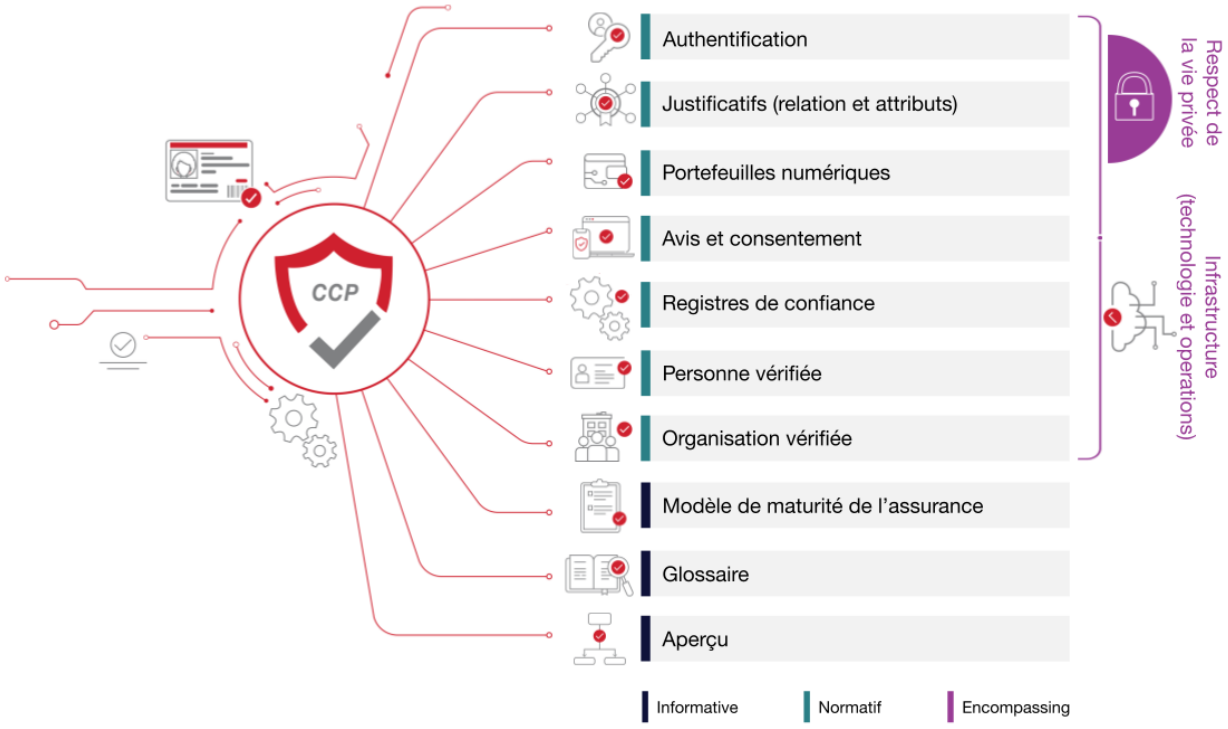

Figure 1. Composantes du Cadre de confiance pancanadien

2. Conventions

Cette section décrit et définit les termes et concepts clés utilisées dans la composante « Justificatifs (relations et attributs) » du CCP. Ces renseignements sont fournis afin d'assurer une utilisation et une interprétation uniformes des termes employés dans cet aperçu et dans le profil de conformité « Justificatifs (relations et attributs) » du CCP.

Remarques :

- Les conventions peuvent varier selon les composantes du CCP. Les lecteurs sont invités à examiner les conventions de chacune des composantes du CCP qu'ils lisent.
- Les principaux termes et concepts décrits et définis dans cette section, dans la section sur les processus de confiance et le glossaire du CCP sont écrits avec une majuscule initiale tout au long du présent document.
- Des liens hypertextes peuvent être intégrés dans les versions électroniques de ce document. Tous les liens étaient accessibles au moment de la rédaction.

2.1 Termes et définitions

Pour les besoins de cette composante du CCP, les termes et définitions du glossaire du CCP et ceux qui figurent dans la présente section s'appliquent.

Allégation

Une allégation est une affirmation à propos d'un sujet (p. ex., le sujet a un permis de conduire; le sujet a plus de 21 ans).

Attribut

Un attribut est de l'information reliée à une caractéristique ou une partie inhérente d'une entité (p. ex., nom donné ou adresse résidentielle d'un sujet). Les attributs sont parfois appelés des « propriétés » ou des « allégations ». Les attributs sont enregistrés dans les justificatifs.

Définition de la relation

Une définition d'une relation est un justificatif qui décrit un *type* spécifique de relation qui existe entre deux sujets ou davantage, ou une classe de relation (p. ex., description de la structure d'un type de mariage d'un justificatif de relation ou type de permis de conduire d'un justificatif de relation). La définition d'une relation ne décrit pas une relation spécifique entre deux entités (p. ex., Fatima a obtenu un doctorat de l'Université de la Colombie-Britannique; Éric est un employé de FictitiousCorp; Diya et Charles sont légalement mariés). La définition de la relation décrit plutôt les *caractéristiques* de ces relations. Les définitions des relations sont créées au moyen du processus Définir la relation.

Définition d'un attribut

Une définition d'un attribut est un justificatif qui décrit un type spécifique, ou une classe, d'attribut. Une définition d'un attribut ne décrit pas un cas spécifique d'attribut (p. ex., date de naissance spécifique de Martina; diplôme spécifique de Hiren). La définition de l'attribut décrit plutôt les *caractéristiques* de tels attributs. Les définitions des attributs sont créées au moyen du processus de confiance « Définir l'attribut » tel que décrit plus loin dans ce document.

Justificatif

Un justificatif est un ensemble d'une ou de plusieurs allégations concernant un sujet (p. ex., le sujet a un permis de conduite, le Sujet réside à une adresse spécifiée ou un sujet a une certification spécifique). Dans ce document, le terme « Justificatifs » n'inclut pas les justificatifs d'authentification, sauf si la désignation « Justificatifs d'authentification » est utilisée explicitement (voir Justificatif vérifiable).

Justificatif vérifiable

Justificatif inviolable qui est codé de telle sorte qu'il permet de confirmer son intégrité et son auteur (c.-à-d.. la source) au moyen d'une vérification cryptographique. Les justificatifs

vérifiables doivent être sûrs du point de vue cryptographique, respecter la vie privée et pouvoir être vérifiés par des machines.

Justificatif vérifié

Justificatif vérifiable qui est jugé authentique par un vérificateur.

Portefeuille numérique ou portefeuille de justificatifs vérifiables

Un portefeuille numérique est un référentiel de justificatifs qui stocke à distance des renseignements pour un titulaire. Selon la nature du portefeuille, celui-ci peut contenir des renseignements comme des justificatifs, des justificatifs vérifiables, des renseignements de paiement et/ou des mots de passe. Un portefeuille de justificatifs vérifiables est un portefeuille numérique qui sert uniquement à stocker des justificatifs vérifiables (voir aussi Référentiel).

Prédicat dérivé

Un prédicat dérivé est une assertion booléenne vérifiable concernant un sujet qui est basée sur la valeur d'un autre attribut décrivant ce sujet. C'est le cas, par exemple, d'un sujet qui souhaite prouver qu'il est admissible à des services uniquement offerts à des personnes âgées d'au moins 21 ans et qui possèdent un justificatif contenant un attribut qui renferme leur date de naissance. Au lieu de fournir sa date de naissance comme preuve d'admissibilité, le sujet pourrait présenter un prédicat dérivé comme « Plus de 21 » qui contient une valeur « Vrai » ou « Faux » indiquant que le sujet est âgé de plus de 21 ans. Le fait d'utiliser de la sorte les prédicats dérivés protège mieux la vie privée d'un sujet en ne divulguant pas de renseignements détaillés permettant d'identifier la personne, tout permettant à un vérificateur de valider l'admissibilité d'un sujet à un service.

Présentation

Données, représentant habituellement une ou plusieurs allégations à propos d'un sujet, qui sont dérivées d'un ou de plusieurs justificatifs, justificatifs vérifiables, relations approuvées ou relations vérifiables et sont partagées avec un vérificateur.

Présentation vérifiable

Présentation inviolable qui est codée d'une façon permettant de confirmer son intégrité et son auteur (c.-à-d. la source) au moyen d'une vérification cryptographique. Les présentations vérifiables doivent être sûres du point de vue cryptographique, conformes aux dispositions qui régissent le respect de la vie privée, respecter la vie privée et pouvoir être vérifiées par des machines.

Référentiel ou référentiel de justificatifs

Système logiciel (application) comme une base de données, un centre de stockage ou un portefeuille de justificatifs vérifiables qui stocke les justificatifs vérifiables d'un titulaire et en contrôle l'accès.

Relation

Une relation est un type spécifique de justificatif qui décrit la façon dont deux entités ou davantage sont reliées (p. ex., Fatima a obtenu un doctorat de l'Université de la Colombie-Britannique; Éric est un employé de FictitiousCorp; Diya et Charles sont légalement mariés).

Relation déclarée

Une relation déclarée est un justificatif qui documente une assertion faite par une entité selon laquelle une relation existe entre deux sujets ou davantage. Une relation déclarée décrit une relation *spécifique* entre les sujets (p. ex., Diya et Charles sont mariés légalement dans une province spécifique, Fatima a obtenu un doctorat de l'Université de la Colombie-Britannique; Louise une administratrice enregistrée au niveau fédéral de FictitiousCorp). La structure d'une relation déclarée est dérivée d'une définition de la relation. Les relations déclarées sont créées par le biais du processus « Déclarer une relation ».

Relation endossée

Une relation endossée est un type spécifique de justificatif qui allègue qu'un sujet ou une tierce partie confirme avoir la conviction qu'une relation déclarée est valide. Une relation peut être endossée par plus d'une entité.

Relation réfutée

Justificatif qui documente une assertion faite par un émetteur d'une relation approuvée selon laquelle il estime que la relation approuvée n'est plus valide (p. ex, une adhésion est expirée; a on a découvert qu'une relation et une ou plusieurs de ses revendications sont frauduleuses). Une fois qu'une relation a été réfutée, ses revendications ne sont plus valides.

Relation vérifiable

Relation déclarée inviolable, relation approuvée ou relation réfutée qui est codée de façon à permettre de confirmer son intégrité et son auteur (c.-à-d. la source) au moyen d'une vérification cryptographique. Les relations vérifiables doivent être sûres du point de vue cryptographique, conformes aux dispositions qui régissent le respect de la vie privée, respecter la vie privée et pouvoir être vérifiées par des machines.

Vérification du justificatif

La vérification du justificatif est une évaluation qui consiste à déterminer si un justificatif vérifiable ou une présentation vérifiable représente d'une manière authentique et exacte l'émetteur ou le présentateur. Cela consiste notamment à vérifier que la preuve est satisfaisante (normalement au moyen d'une validation cryptographique), et à confirmer que le justificatif ou la présentation est valide (p. ex., non suspendu(e), révoqué(e) ou expiré(e)) et est conforme aux spécifications et/ou aux normes pertinentes.

2.2 Abréviations

L'acronyme suivant est utilisé dans le présent aperçu et le profil de conformité « Justificatifs (relations et attributs) du CCP :

- CCP – Cadre de confiance pancanadien

2.3 Rôles

Les rôles et les définitions qui suivent s'appliquent à la portée et dans le contexte de la composante « Justificatifs (relations et attributs) » du CCP.

Remarques :

- Une entité peut assumer un ou plusieurs rôles, compte tenu de l'utilisation. Par exemple, une entité qui est une partie dépendante dans une transaction peut aussi être le vérificateur de cette transaction.
- Les définitions des rôles n'impliquent ou n'exigent pas une solution, une architecture, une mise en œuvre ou un modèle d'affaires spécifique.

Autorité qui révoque

Entité dont la responsabilité exclusive ou principale consiste à révoquer les justificatifs et à tenir à jour les renseignements sur les justificatifs révoqués. L'autorité qui révoque peut être l'émetteur du justificatif révoqué, mais ce n'est pas nécessaire.

Demandeur

Entité qui a demandé, mais pas encore reçu, un justificatif (p. ex., personne qui a demandé, mais pas encore reçu, un permis de conduire d'une province ou d'un territoire). Cette entité peu ou non être un sujet du justificatif.

Émetteur

Entité qui rend disponibles des renseignements à propos d'un Sujet en créant et en émettant un Justificatif ou un Justificatif vérifiable (p. ex., province ou territoire qui délivre un permis de conduire).

Partie dépendante

Entité qui utilise des renseignements d'identité, attributs, relations ou autres justificatifs numériques pour faire des transactions électroniques (p. ex., le propriétaire d'un magasin ou d'une entreprise vendant de l'alcool qui doit s'assurer qu'un client est assez vieux pour acheter de l'alcool).

Partie qui approuve

Entité qui affirme qui affirme avoir la conviction qu'une relation déclarée est valide au moyen du processus Approuver la relation (voir les processus de confiance ci-dessous). Une relation peut être approuvée par plus d'une partie.

Partie qui déclare

Toute entité qui déclare une relation entre deux sujets ou davantage au moyen du processus Déclarer la relation (voir les processus de confiance ci-dessous). La partie qui déclare peut être, ou ne pas être, un sujet de la relation déclarée.

Partie qui définit

Toute entité qui crée une définition de relation au moyen du processus Définir la relation (voir les processus de confiance ci-dessous).

Partie qui réfute

Entité dont la responsabilité exclusive ou principale consiste à réfuter les relations (au moyen du processus Réfuter une relation de confiance décrit ci-dessous) et à tenir à jour les renseignements sur les relations réfutées. La partie qui réfute peut être la partie qui approuve une relation réfutée, ou un sujet de la relation réfutée, mais ce n'est pas nécessaire.

Titulaire

Entité qui possède un ou plusieurs Justificatifs. Le Titulaire est généralement le Sujet du Justificatif, mais ce n'est pas nécessaire (p. ex., un parent peut posséder un justificatif appartenant à son enfant; un avocat peut posséder un justificatif appartenant à son client). Les Titulaires peuvent stocker les justificatifs qu'ils possèdent dans un Référentiel.

Vérificateur

Entité qui reçoit un ou plusieurs justificatifs vérifiables, et qui évalue si les justificatifs représentent d'une manière authentique et exacte l'émetteur ou le sujet (voir Vérification des justificatifs.)

3. Relations de confiance

L'authenticité, la validité, la sécurité et la confidentialité des entités qui interviennent dans la création, l'émission, le stockage, la présentation et la vérification des justificatifs numériques sont essentielles pour évaluer la fiabilité de ces justificatifs. Cette composante du CCP identifie les relations de confiance essentielles qui entrent en ligne de compte pour évaluer la fiabilité des justificatifs numériques. Étant donné cela, les critères de conformité associés aux relations et aux processus de confiance identifiés dans cette composante mettent l'accent sur la transparence, la vérifiabilité et la confidentialité, en plus des méthodes techniques pour instaurer la confiance parmi les parties impliquées. La figure 2 illustre la façon dont les divers rôles sont reliés entre eux et créent le besoin d'avoir ces relations de confiance.

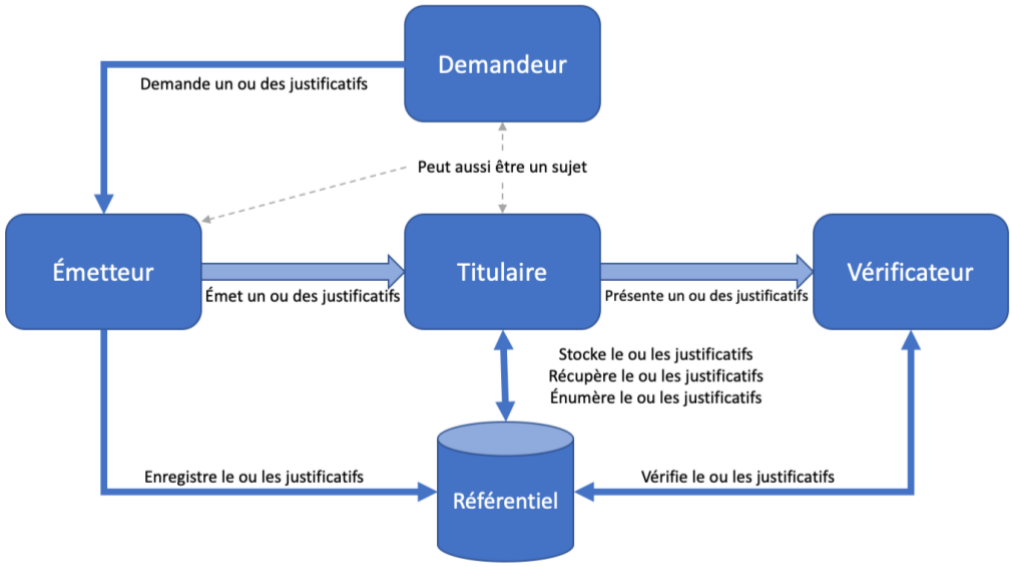

Figure 2. Rôles et relations des justificatifs (relations et attributs) (illustration)

Il est à noter que le modèle de données liées aux justificatifs vérifiables W3C et le profil du secteur public du Cadre de confiance pancanadien incluent d'excellents travaux menés dans ce domaine, qui ont été pris en considération lorsque cette composante a été développée.

Les relations de confiance décrites ci-dessous ne mènent pas toujours directement à des processus techniques ou commerciaux discrets.

Cette composante invite les participants de l'écosystème numérique à tenir compte des exigences essentielles qui suivent pour établir la confiance dans ces relations et qui affectent la fiabilité d'un justificatif :

1. Les participants doivent pouvoir évaluer l'autorité et la fiabilité des émetteurs, et avoir l'assurance que ces émetteurs établissent avec soin l'exactitude des renseignements contenus dans un justificatif.
2. Les participants doivent avoir l'assurance que les émetteurs délivrent des justificatifs avec le consentement des sujets ou d'une entité admissible à agir au nom du sujet, ou lorsque la loi ou règlement l'autorise.
3. Les participants doivent pouvoir déterminer si les justificatifs émis contiennent des renseignements exacts, fiables et à jour.
4. Les participants doivent avoir l'assurance que les émetteurs ont adopté et mis en œuvre des structures de données qui protègent la confidentialité à l'intérieur des justificatifs afin de réduire les risques de corrélation qui pourraient en résulter si une partie dépendante demande plusieurs justificatifs à propos d'un sujet, qu'ils aient été délivrés par un ou plusieurs émetteurs.
5. Les participants doivent avoir l'assurance que les justificatifs compromis ou non valides sont traités d'une manière appropriée et prompte, et qu'ils ne sont rendus inutilisables que dans des circonstances légitimes.
6. Les participants doivent avoir l'assurance que les renseignements qu'ils partagent avec d'autres participants ou qui sont entreposés dans des référentiels ou registres vérifiables

ne sont pas utilisés par le fournisseur de services ou le vérificateur, sauf tel que demandé avec le consentement express du sujet ou d'une entité autorisée à agir en son nom, ou encore lorsque la loi ou un règlement l'autorise. Par exemple, les participants ne doivent pas utiliser des justificatifs qui leur ont été confiés pour représenter les sujets ou s'entendre avec d'autres participants pour regrouper ou partager des renseignements sans un tel consentement.

4. Niveaux d'assurance

Il est essentiel que les participants qui créent ou utilisent des justificatifs comprennent le niveau de confiance qu'ils peuvent leur accorder. La composante « Justificatifs (relations et attributs) du Cadre de confiance pancanadien emploie pour cela une approche basée sur des niveaux d'assurance. La figure 3 donne un aperçu des niveaux d'assurance des justificatifs. L'assurance d'un justificatif fait intervenir le processus qui consiste à associer un justificatif à un ou plusieurs sujets.

Niveau d'assurance	Description de la qualification
Niveau 1 (CAL1)	• Répond à tous les critères de conformité du niveau 1 • Peu ou pas d'assurance nécessaire • Il ne faut avoir guère d'assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 2 (CAL2)	• Répond à tous les critères de conformité du niveau 2 • Une certaine assurance nécessaire • Il faut avoir une certaine assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 3 (CAL3)	• Répond à tous les critères de conformité du niveau 3 • Grand niveau d'assurance nécessaire • Il faut avoir une grande assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 4 (CAL4) Facultatif	• Répond à tous les critères de conformité du niveau 4 • Très grand niveau d'assurance nécessaire • Il faut avoir une très grande assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis

Figure 3. Niveaux d'assurance des justificatifs

Ces niveaux d'assurance sont décrits plus en détail dans le document Profil de conformité « Justificatifs (relations et attributs) » du CCP.

Un justificatif doit, pour atteindre un niveau d'assurance spécifique, doit remplir chaque critère de conformité applicable. Par exemple, si un justificatif a atteint la norme du niveau CAL4 pour neuf critères et celle du niveau CAL1 pour un critère, le niveau établi pour le justificatif ne peut être supérieur à CAL1. Cela est expliqué plus en détail dans le profil de conformité.

5. Processus de confiance

Le CCP favorise la confiance grâce à un ensemble de processus vérifiables.

Un processus est une activité commerciale ou technique, ou un ensemble d'activités, qui transforme une condition d'entrée en condition de sortie dont dépendent souvent d'autres processus. Une condition est un état ou une circonstance spécifique qui s'applique à un Processus de confiance. Une condition peut être une entrée, une sortie ou une dépendance relative à un processus de confiance. Les Critères de conformité spécifient ce qui est requis pour transformer une condition d'entrée en condition de sortie. Ils spécifient, par exemple, ce qui est nécessaire pour que le processus Approuver la relation transforme une condition d'entrée « Relation déclarée » en condition de sortie « Relation approuvée ».

Un processus est désigné comme étant un Processus de confiance lorsqu'il est évalué et certifié conforme aux Critères de conformité définis dans un profil de conformité du CCP. L'intégrité d'un Processus de confiance est fondamentale, car de nombreux participants se fient au résultat du processus, souvent par-delà les frontières territoriales, organisationnelles et sectorielles, et à court et long terme

La composante « Justificatifs (relations et attributs) » du CCP définit cinq processus de confiance rattachés aux relations :

1. Définir la relation
2. Déclarer la relation
3. Approuver la relation
4. Vérifier la relation
5. Réfuter la relation

La composante « Justificatifs (relations et attributs) » du CCP définit quatre processus de confiance rattachés aux attributs :

1. Définir l'attribut
2. Lier l'attribut
3. Maintenir l'attribut
4. Révoquer l'attribut

5.1 Aperçu conceptuel

La figure 4 donne un aperçu conceptuel et montre l'organisation logique des processus rattachés aux relations de confiance de la composante « Justificatifs (relations et attributs) » du CCP. La figure 5 donne un aperçu conceptuel et montre l'organisation logique des processus rattachés aux attributs de confiance de la composante « Justificatifs (relations et attributs) » du CCP.

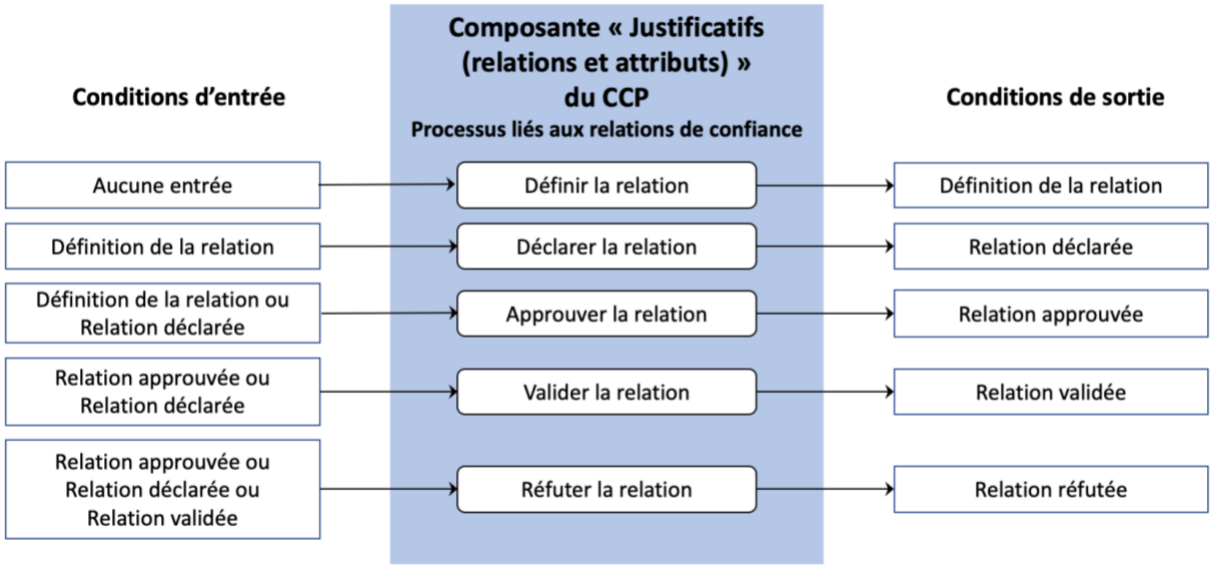

Figure 4. Aperçu conceptuel des relations

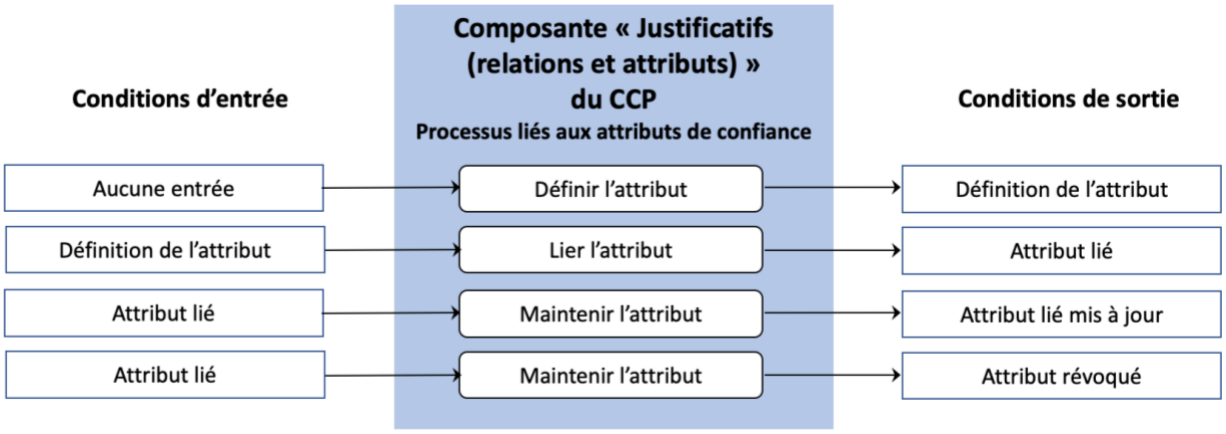

Figure 5. Aperçu conceptuel des attributs

5.2 Descriptions des processus

Les sections qui suivent définissent les processus de confiance de la composante « Justificatifs (relations et attributs) » du CCP. Le profil de conformité « Justificatifs (relations et attributs) » du CCP spécifie les critères de conformité pouvant servir à évaluer la fiabilité de ces processus.

Les processus de confiance « Justificatifs (relations et attributs) » sont définis à l'aide de la structure suivante :

1. Description – Aperçu descriptif du processus
2. Entrées – Données utilisées et/ou suivies par le processus de confiance
3. Sorties – Données créées par le processus
4. Dépendances – Autres processus de confiance devant être exécutés avant le processus décrit dans la section, normalement parce qu'ils produisent une ou plusieurs entrées requises

5.2.1 Définir la relation

Le processus « Définir la relation » décrit un *type* spécifique de relation pouvant exister entre deux sujets ou davantage, ou classe de relation, sous la forme d'une définition de relation. Une Définition de relation ne décrit pas une relation spécifique entre deux entités (p. ex., Fatima a obtenu un doctorat de l'Université de la Colombie-Britannique; Éric est un employé de FictitiousCorp; Diya et Charles sont légalement mariés). Des cas spécifiques de relations sont créés par le processus « Déclarer la relation » qui est décrit plus loin dans ce document. La définition de la relation décrit plutôt les *caractéristiques* de telles relations. La définition de la relation :

- Définit et caractérise un type de relation (p. ex., certificat de mariage, permis de conduire, diplôme);
- Décrit la source de la relation (p. ex., gouvernement provincial, institution d'enseignement);
- Décrit les caractéristiques qui définissent la relation (p. ex., le type de diplôme accordé);
- Indique si une relation doit être approuvée ou non avant de pouvoir lui faire confiance (voir « Approuver les relations » plus loin dans ce document);
- Indique si la relation peut être réfutée (voir « Réfuter les relations » plus loin dans ce document);
- Déclare les risques connus qui devraient être pris en considération pour le type de relation définie (p. ex., si la relation est d'une nature éphémère; conditions ou événements ordinaires pouvant rendre la relation non valide);
- Donne aux parties dépendantes des indications quant aux conditions ou artéfacts à prendre en considération (en plus du niveau d'assurance de la relation) pour évaluer sa fiabilité (p. ex., si des caractérisques spécifiques qui définissent la relation doivent être considérées obligatoires);
- Inclut des définitions juridiques pertinentes, des définitions des relations qui sont des normes de l'industrie, ou des références à elles ou à des schémas pertinents;
- Décrit toute preuve de fiabilité qui existe (p. ex., justificatifs vérifiés ou relations vérifiées connexes) ou déclare qu'il n'y en a pas.

Une entité peut définir une relation incluant, sans s'y limiter, toutes les entités impliquées dans une telle relation, un émetteur, une source qui fait autorité ou une partie dépendante.

Entrées	Aucune entrée
Sorties	Définition de la relation
Dépendances	Aucune dépendance

5.2.2 Déclarer la relation

Le processus « Déclarer la relation » est une assertion faite par une entité selon laquelle il existe une relation entre deux sujets ou davantage. Contrairement au processus « Définir la relation », le processus « Déclarer la relation » décrit une relation *spécifique* entre les sujets (p. ex., Diya et Charles sont mariés légalement dans une province ou un territoire spécifique; Éric est directeur de FictitiousCorp; Fatima a obtenu un doctorat de l'Université de la Colombie-Britannique). Le processus « Déclarer la relation » fait référence à une définition de la relation pour en tirer la structure de la relation qu'il déclare et les attributs obligatoires de la relation.

L'entité qui déclare la relation peut être ou ne pas être un des sujets de la relation (p. ex., un avocat peut déclarer une relation juridique pour le compte de deux partenaires d'affaires; une organisation d'accréditation peut déclarer que Gabriel est l'apprenti-menuisier d'Ali). Chaque sujet d'une relation qui est une personne devrait être une personne vérifiée ou une organisation vérifiée.

Outre son allégation principale, une relation déclarée peut contenir des allégations détaillées supplémentaires concernant ses sujets (p. ex., la date de naissance d'un sujet; le fait qu'un sujet réside à une adresse spécifique). Une allégation peut aussi comporter un prédicat dérivé.

Quand une relation déclarée a été émise, le titulaire – qui est souvent, quoique pas toujours, un sujet – peut la stocker dans un référentiel tel qu'un portefeuille numérique ou un portefeuille de justificatifs vérifiables. Le niveau d'assurance associé au référentiel aura un impact direct sur le niveau d'assurance attribué aux relations déclarées qui y sont stockées.

Entrées	Définition de la relation
Sorties	Relation déclarée
Dépendances	Définir la relation

5.2.3 Approuver la relation

Une entité confirme, par le biais du processus « Approuver la relation », avoir la conviction qu'une relation déclarée est valide. Une relation approuvée peut être approuvée par plus d'une entité. Les parties dépendantes peuvent considérer que les multiples approbations d'une relation sont une indication de la robustesse de sa validité. Les parties dépendantes doivent, lorsqu'elles évaluent la fiabilité d'une relation, tenir compte de la source de l'approbation ou des

approbations, et du fait que ces sources sont des personnes vérifiées ou des organisations vérifiées.

Le résultat du processus « Approuver la relation » peut être une relation approuvée ou une relation approuvée vérifiable. Il y a des cas où une relation approuvée pourrait être créée sans l'existence d'une relation déclarée (p. ex., une province ou un État qui émet un permis de conduire pourrait délivrer un justificatif de relation approuvée). Des relations approuvées ou des relations approuvées vérifiables peuvent être délivrées par n'importe quelle entité, mais elles ne prennent vraiment tout leur sens que lorsqu'elles sont générées par une personne vérifiée ou une organisation vérifiée.

Lorsqu'une relation approuvée a été émise, le titulaire peut la stocker dans un référentiel, p. ex. un référentiel vérifiable, un portefeuille numérique ou un portefeuille de justificatifs vérifiables. Le niveau d'assurance associé au référentiel aura un impact direct sur le niveau d'assurance attribué aux relations qui y sont stockées.

Entrées	Définition de la relation ou relation déclarée
Sorties	Relation approuvée
Dépendances	Déclarer la relation

5.2.4 Valider la relation

Lorsque le titulaire d'une relation (qui est normalement le sujet de la relation, mais pourrait être une tierce partie ayant le consentement du sujet pour partager la relation) est invité par une partie dépendante à faire une ou des allégations, il présente un justificatif de relation contenant ces allégations à un vérificateur sous la forme d'une présentation ou d'une présentation vérifiable. Les présentations et les présentations vérifiables peuvent contenir une combinaison d'allégations détaillées (p. ex., date de naissance, âge, adresse, compétence spécifique) et/ou de prédicats dérivés.

Le vérificateur confirme que la ou les relations présentées sont authentiques en :

1. Confirmant que le statut de la ou des relations est valide (p. ex., non expirée, suspendue ou révoquée);
2. Confirmant que le justificatif est valide, généralement au moyen d'une vérification cryptographique;
3. Confirmant que la ou les relations et/ou présentations sont conformes aux normes ou spécifications pertinentes.

Si le vérificateur est convaincu de l'authenticité des relations, il fournira les données contenues dans la présentation ou la présentation vérifiée à une partie dépendante sous la forme d'une relation vérifiée.

À moins que cela ne soit exigé par un règlement, une politique ou la loi, les vérificateurs ne devraient pas conserver de copies des présentations ou présentations vérifiées afin de limiter l'exposition potentielle des renseignements personnellement identifiables de leur sujet.

Les vérificateurs ne doivent jamais partager des renseignements qui leur sont présentés dans le cadre du processus de vérification avec d'autres Vérificateurs, d'autres participants or ou quelqu'un d'autre que la ou les parties dépendantes sans le consentement express du sujet, à moins que cela ne soit permis ou exigé par la loi ou un règlement. Ce type de collusion pourrait permettre à des auteurs de collusion de regrouper des données et d'en retirer bien plus de renseignements sur le sujet que ce que n'importe lequel de ces auteurs de collusion n'avait en sa possession. Ce genre d'activité peut nuire considérablement à un sujet.

Les relations incluses dans une présentation ou une présentation vérifiable qui est soumise par un vérificateur peuvent être sous la forme d'une relation déclarée ou d'une relation approuvée. Même une Relation déclarée volontairement peut devenir une relation validée dans des circonstances appropriées (p. ex., Christine déclare volontairement qu'elle possède un permis de conduire valide pour la province de la Nouvelle-Écosse, qui peut être vérifié par sa source faisant autorité, c.-à-d. la province); Anderson déclare volontairement qu'il est propriétaire d'une entreprise canadienne enregistrée auprès du gouvernement fédéral, ce qui peut être validé par la source faisant autorité, c.-à-d. le gouvernement du Canada).

Entrées	Relation déclarée ou relation approuvée
Sorties	Relation validée
Dépendances	Approuver la relation ou déclarer la relation

5.2.5 Réfuter la relation

Il existe de nombreuses situations où un émetteur peut vouloir rendre une relation non valide pour s'assurer que le sujet, le titulaire ou quiconque ne puisse pas faire valoir ses allégations. Par exemple :

- Un abonnement peut expirer, ce qui rend les allégations à son sujet non valides;
- La relation et une ou plusieurs de ses allégations peuvent avoir été créées d'une manière frauduleuse;
- Une fraude est commise en utilisant la relation et une nouvelle relation doit être créée pour limiter les torts causés à son sujet;
- Une relation peut avoir été émise par erreur;
- La relation et/ou une ou plusieurs de ses allégations peuvent avoir été rendues non valides par un jugement d'un tribunal;
- Un événement ou un changement dans les circonstances ou les compétences du sujet peut nécessiter la révocation d'une Relation vérifiable et l'émission d'une nouvelle relation vérifiable (p. ex., le permis de conduire d'un sujet passe du statut provisoire au statut pleinement qualifié, un sujet est promu du rang de caporal à celui de sergent, le statut matrimonial d'un sujet change).

Dans de tels cas, les relations doivent être réfutées. Si un sujet a besoin de pouvoir déclarer une ou plusieurs des allégations dans une relation réfutée, il doit demander une nouvelle relation tel que décrit dans les processus \ Déclarer les relations », « Approuver les relations » et/ou « Vérifier les relations ¢ de cet aperçu.

Il peut arriver que des allégations dans une relation réfutée soient acceptées par une partie dépendante, à la discrétion de celle-ci (p. ex., un permis de conduire suspendu *peut* être une preuve d'âge acceptable pour certaines parties dépendantes).

Entrées	Relation déclarée, relation approuvée, relation approuvée vérifiable ou relation validée
Sorties	Relation réfutée
Dépendances	Déclarer la relation, approuver la relation ou valider la relation

5.2.6 Définir l'attribut

Le processus « Définir l'attribut » décrit un *type* spécifique d'attribut qui peut décrire un sujet, ou une classe d'attribut, sous la forme d'une définition d'attribut. Une définition d'attribut ne décrit pas un attribut spécifique (p. ex., date de naissance spécifique de Martina, diplôme spécifique de Hiren). La définition d'un attribut décrit plutôt les *caractéristiques* de cet attribut. La Définition de l'attribut :

- Définit et caractérise un type d'attribut (p. ex., année de fabrication, date, attestation d'études, certifications de l'industrie, qualifications);
- Fournit un contexte pour utiliser l'attribut (p. ex., comment l'utiliser, ce à quoi il est censé servir et son utilisation appropriée et/ou inappropriée);
- Décrit la source de l'attribut, le cas échéant (p. ex., gouvernement provincial, institution d'enseignement);
- Décrit les caractéristiques ou le format qui définissent l'attribut (p. ex., une date sous la forme JJ-MMM-AAAA) et n'est pas assez qualifié de par son seul nom (p. ex., le nom « Date » ne permettrait pas vraiment de dire si 01-02 correspond au 2 janvier, au 1er février, à janvier 2002, à février 1901, etc.);
- Indique s'il s'agit d'une valeur de l'attribut ou d'un prédicat dérivé;
- Inclut un numéro de version et/ou une date d'origine ou un autre identifiant qui permettra aux émetteurs et parties dépendantes de faire la distinction entre les différentes versions de la définition;
- Déclare des risques inhérents connus qui devraient être pris en considération pour le type d'attribut qu'il définit (p. ex., si l'attribut est éphémère par nature; conditions ou événements ordinaires qui pourraient rendre l'attribut non valide);
- Donne des indications aux parties dépendantes quant à sa fiabilité;
- Crée une terminologie et une compréhension communes parmi les émetteurs et les consommateurs de l'attribut;
- Inclut un avis de non-responsabilité ou une déclaration comme quoi il n'y en a pas;
- Inclut des définitions juridiques pertinentes, des définitions de l'attribut qui sont la norme dans l'industrie ou des références à l'attribut ou à des schémas pertinents, ou encore des déclarations comme quoi il n'y en a pas;
- Décrit toute preuve de fiabilité qui existe (p. ex., justificatifs vérifiés ou relations vérifiées connexes) ou déclare qu'il n'y en a pas;
- Décrit l'autorisation en vertu de laquelle l'attribut a été émis ou déclare qu'il n'y en a pas.

Bien que les attributs soient normalement définis par un émetteur ou une partie ayant autorité, n'importe quelle entité peut définir un attribut.

Entrées	Pas d'entrée
Sorties	Définition de l'attribut
Dépendances	Pas de dépendances

5.2.7 Lier l'attribut

Le processus « Lier l'attribut » est une assertion faite par un émetteur selon laquelle un ou plusieurs attributs décrivent avec exactitude un ou plusieurs sujets sous la forme d'un attribut lié. Contrairement au processus « Définir l'attribut », le processus « Lier l'attribut » décrit un attribut *spécifique* qui décrit un ou plusieurs sujets (p. ex., la date de naissance de Martina est le 2 janvier 2020; Éric est un employé de FictitiousCorp; Hiren a une maîtrise en sciences). Un attribut peut aussi consister en un prédicat dérivé.

Le processus « Lier l'attribut » fait référence à une définition d'un attribut pour en extraire la structure de l'attribut et son utilisation et son contexte appropriés.

Le processus « Lier l'attribut » est exécuté par un émetteur qui est une autorité dans le contexte de l'attribut (c.-à-d., une partie ayant autorité) et qui peut vérifier que l'attribut décrit exactement le ou les sujets (p. ex., une société de télécommunications est une partie ayant autorité pour émettre un numéro de téléphone légalement enregistré). Le sujet d'un attribut peut être ou non identifiable d'une manière unique ou encore une personne vérifiée ou une organisation vérifiée.

Les attributs liés doivent pouvoir être vérifiés d'une manière cryptographique.

Quand un Attribut lié a été émis, le titulaire – qui est souvent, quoique pas toujours, un sujet – peut stocker l'attribut lié dans un référentiel, par exemple un référentiel vérifiable, un portefeuille numérique ou un portefeuille de justificatifs vérifiables. Le niveau d'assurance associé au référentiel aura un impact direct sur le niveau d'assurance donné aux attributs liés qui y sont stockés.

Entrées	Définition de l'attribut
Sorties	Lier l'attribut
Dépendances	Définir l'attribut

5.2.8 Maintenir l'attribut

Étant donné la nature de certaines des données qui peuvent être contenues dans les attributs liés, il peut être nécessaire de les mettre à jour. Ces changements peuvent être reliés à des changements apportés à l'attribut comme tel (p. ex., changement d'adresse résidentielle, prolongation d'une date d'expiration, renouvellement d'un abonnement, remise des points d'inaptitude d'un permis de conduire) ou des changements d'état qui affectent un prédicat dérivé (p. ex., le sujet célèbre son 21e anniversaire et est admissible à changer le prédicat dérivé « Plus de 21 ans » pour « Vrai »). Dans ces cas-là, un émetteur peut mettre à jour un attribut lié et le fournir au titulaire.

Dans certains cas, il se peut que ce ne soit pas possible de mettre à jour les renseignements sans changer un justificatif (p. ex., changer un prédicat dérivé en dehors du justificatif comme tel). Dans la plupart des autres cas, il est probable que ce ne soit pas possible, souhaitable ou conseillé de mettre à jour un attribut lié existant. Dans la plupart des cas, un nouvel attribut lié sera donc émis en utilisant les processus « Lier l'attribut ». Quand un nouvel attribut lié est émis, il peut être approprié ou non de révoquer des attributs liés déjà existants en utilisant le processus « Révoquer l'attribut ». Si, par exemple, quelqu'un était le président d'un club local en 2019 et qu'il n'est pas réélu en 2020, il ne serait pas nécessaire de révoquer l'attribut lié indiquant qu'il était président en 2019. Si toutefois l'attribut lié indiquait qu'il est « l'actuel président » et qu'il n'est pas réélu, ce serait censé de révoquer l'attribut.

Entrées	Attribué lié
Sorties	Attribut lié mis à jour
Dépendances	Définir l'attribut, lier l'attribut

5.2.9 Révoquer l'attribut

Il y a beaucoup de situations où un émetteur peut vouloir rendre un attribut définitivement non valide pour s'assurer qu'il ne puisse pas être présenté par une entité comme étant une description actuellement exacte du ou des sujets. Par exemple :

- Un abonnement peut expirer;
- L'attribut peut avoir été lié d'une manière frauduleuse;
- Une fraude est commise en utilisant l'attribut et un nouvel attribut (p. ex., numéro de carte de crédit) doit être créé pour limiter les préjudices à son ou ses sujets;
- Un attribut peut avoir été lié à un sujet par erreur;
- L'attribut peut avoir été rendu non valide par un jugement d'un tribunal;
- Un événement ou un changement dans les circonstances ou les compétences d'un sujet peut nécessiter la révocation d'un attribut lié et l'émission d'un nouvel attribut lié (p. ex., le permis de conduire d'un sujet est suspendu de façon permanente en raison de sa conduite répétée avec facultés affaiblies).

Dans ces cas-là, les attributs liés doivent être révoqués. La révocation vise à rendre un attribut lié définitivement non valide. Si un sujet doit pouvoir présenter une preuve qui dépend d'un attribut révoqué, il doit demander un nouvel attribut lié à l'émetteur tel que décrit dans le processus « Lier des attributs » du présent aperçu.

Entrées	Attribut lié
Sorties	Attribut révoqué
Dépendances	Définir l'attribut, lier l'attribut

6. Introduction au profil de conformité « Justificatifs (relations et attributs) » du CCP

Ce document spécifie les critères de conformité pour la composante « Justificatifs » (relations et Attributs) du Cadre de confiance pancanadien (CCP). Les critères de conformité tiennent une place centrale dans le cadre de confiance, car ils spécifient les exigences essentielles convenues par les participants du cadre de confiance afin d'assurer l'intégrité de leurs processus. Cette intégrité est de la plus haute importance, car elle permet à de nombreux participants de multiples organisations, administrations et secteurs de s'y fier.

Les critères de conformité du CCP visent à compléter les lois et règlements en vigueur sur la protection de la vie privée.

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

6.1 Mots-clés des critères de conformité

Tout au long de ce document, les termes suivants indiquent la priorité et/ou la rigidité générale des critères de conformité et doivent être interprétés tel qu'indiqué ci-dessous.

- **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 que même s'il peut y avoir des raisons valables dans des circonstances particulières pour ignorer l'exigence, toutes les implications devraient être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité ou de choisir une autre option tel que spécifié par les critères de conformité.
- **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.

Remarque : Les mots clés ci-dessus sont écrits en caractères **gras** et en MAJUSCULES dans ce profil de conformité.

7. Niveaux d'assurance

Il est essentiel que les participants qui créent ou utilisent des justificatifs comprennent le niveau de confiance qu'ils peuvent leur accorder. La composante « Justificatifs (relations et attributs) du CCP emploie pour cela une approche basée sur des niveaux d'assurance. La figure 1 donne un aperçu des niveaux d'assurance des justificatifs. L'assurance d'un justificatif fait intervenir le processus qui consiste à associer un ou plusieurs sujets.

Niveau d'assurance du justificatif	Description de la qualification
Niveau 1 (CAL1)	• Répond à tous les critères de conformité du niveau 1 • Peu ou pas d'assurance nécessaire • Il ne faut avoir guère d'assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 2 (CAL2)	• Répond à tous les critères de conformité du niveau 2 • Une certaine assurance nécessaire • Il faut avoir une certaine assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 3 (CAL3)	• Répond à tous les critères de conformité du niveau 3 • Grand niveau d'assurance nécessaire • Il faut avoir une grande assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 4 (CAL4) Facultatif	• Répond à tous les critères de conformité du niveau 4 • Très grand niveau d'assurance nécessaire • Il faut avoir une très grande assurance qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis

Figure 6. Niveaux d'assurance des Justificatifs

Un justificatif doit, pour atteindre un niveau d'assurance spécifique, remplir au moins le niveau d'assurance pour chaque critère de conformité applicable. Par exemple, si un Justificatif a atteint la norme du niveau CAL4 pour neuf critères et celle du niveau CAL1 pour un critère, le niveau d'assurance évalué pour le justificatif ne peut pas être supérieur à CAL1. C'est expliqué plus en détail dans le profil de conformité.

8. Évaluation des risques

La figure 2 contient une énumération des risques couramment utilisée pour évaluer le niveau d'assurance exigé pour une interaction numérique spécifique. Précisons que ce tableau se veut illustratif de par sa nature. Il ne vise pas à être exhaustif ni directif. Les parties dépendantes doivent évaluer les risques et préjudices potentiels qui les attendent, et évaluer les niveaux de risque qu'elles sont disposées à accepter pour une transaction spécifique dans leur contexte opérationnel. Certains critères illustratifs utilisent donc une terminologie qui est sujette à interprétation (p. ex. « élevé », « moyen », « faible »). Cela permet aux praticiens d'établir un profil de risque correspondant à leur ministère, service ou type d'entreprise. Par exemple, une grande institution financière peut considérer le risque de perdre 100 000 $ comme étant « limité » ou « faible », tandis qu'un risque de cette taille peut être « grave » ou « élevé » pour une petite entreprise, une entreprise en démarrage ou un particulier.

Comme les niveaux de risque sont fonction des circonstances propres à une partie dépendante et des politiques, lois et/ou règlements auxquels elles sont assujetties, il incombe à la partie dépendante de documenter d'une façon explicite sa tolérance au risque. Cela permettra de s'assurer que des contrôles des risques sont systématiquement instaurés, qu'ils ne sont pas trop permissifs ni trop rigoureux, peu importe les personnes qui les mettent en place, et qu'ils sont évalués d'une façon équitable lors des audits. Ces risques devraient aussi être documentés de façon à être évidents pour les entités qui interagissent avec et parfaitement compréhensibles pour elles.

La partie utilisatrice doit aussi tenir compte de la fiabilité des entités intervenant dans une transaction et sa vérification pour évaluer la fiabilité d'une transaction, d'une relation ou d'un attribut, tel que documenté dans les composantes « Personne vérifiée », « Organisation vérifiée » et « Authentification » du CCP.

Catégorie d'impact	**Niveau d'assurance requis**			
	CAL1	**CAL2**	**CAL3**	**CAL4**

Désagrément, détresse, préjudice pour la situation ou la réputation	Au pire, désagrément, détresse, embarras ou préjudice limités à court terme pour la situation ou la réputation d'une partie	Au pire, désagrément, détresse ou préjudice grave à court terme ou limités à long terme pour la situation ou la réputation d'une partie	Désagrément, détresse ou préjudice graves ou sérieux à long terme pour la situation ou la réputation d'une partie (ordinairement réservé aux situations qui ont des effets graves ou qui touchent beaucoup de personnes)	Désagrément, détresse ou préjudice graves et permanents pour a situation ou la réputation d'une partie
Perte financière	Au pire, perte financière insignifiante ou sans conséquence pour une partie ou encore responsabilité sans conséquence	Au pire, perte financière sérieuse pour une partie ou responsabilité sérieuse	Grave perte financière pour une partie ou grave responsabilité	Perte financière catastrophique pour une partie ou responsabilité catastrophique

Préjudice pour un programme ou l'intérêt public	Au pire, effet négatif limité sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., diminution de la capacité à mener des missions au point et assez longtemps pour que l'organisation accomplisse ses fonctions principales avec une efficacité nettement réduite; préjudice mineur pour les actifs organisationnels ou les intérêts publics)	Au pire, sérieux effet négatif sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., diminution importante de la capacité à mener des missions au point et assez longtemps pour que l'organisation accomplisse ses fonctions principales avec une efficacité nettement réduite; sérieux préjudice pour les actifs organisationnels ou les intérêts publics)	Grave effet négatif sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., grave diminution ou perte de la capacité à mener des missions au point et assez longtemps pour que l'organisation soit incapable d'accomplir une ou plusieurs de ses fonctions principales; important préjudice pour les actifs organisationnels ou les intérêts publics)	Effet catastrophique sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., diminution ou perte catastrophique de la capacité à mener des missions au point et assez longtemps pour que l'organisation soit incapable d'accomplir ses fonctions principales; préjudice catastrophique pour les actifs organisationnels ou les intérêts publics)

Divulgation non autorisée de renseignements personnels ou commerciaux sensibles	Au pire, divulgation limitée de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée entraînant une perte de confidentialité ayant un faible impact	Au pire, divulgation limitée de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée ayant un impact modéré	Divulgation de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée ayant un impact sérieux	Divulgation de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée ayant un impact catastrophique
Divulgation non autorisée de renseignements gouvernementaux sensibles	Perte de confidentialité ayant peu d'impact	Effet négatif limité sur les opérations et les actifs organisationnels par suite d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées	Effet négatif sérieux sur les opérations et les actifs organisationnels par suite d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées	Effet négatif catastrophique sur les opérations et les actifs organisationnels par suite d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées

Infractions civiles ou pénales	Secteur privé : au pire, risque d'infractions civiles ou pénales d'une nature qui ne serait normalement pas assujettie à des efforts pour faire appliquer la loi Secteur public : tout compromis impliquant une infraction juridique est évalué comme étant au moins de niveau 2	Infraction civile ou pénale qui peut avoir des conséquences mineures et être assujettie à des efforts pour faire appliquer la loi	Infraction civile ou pénale pouvant avoir des conséquences sérieuses qui sont importantes pour les programmes visant à faire appliquer la loi	Infraction pouvant avoir des conséquences exceptionnellement graves qui sont particulièrement importantes pour les programmes visant à faire appliquer la loi
Santé et sécurité du personnel	Secteur privé : au pire, blessure mineure ne nécessitant pas de traitement médical Secteur public : toute atteinte à la santé et la sécurité est évaluée comme étant au moins de niveau 2	Secteur privé : au pire, risque modéré de blessure mineure ou risque limité de blessure nécessitant un traitement médical Secteur public : blessure personnelle mineure ne nécessitant pas de soins médicaux	Secteur privé : au pire, faible risque de blessure grave ou de décès Secteur public : blessure personnelle nécessitant des soins médicaux	Risque de blessure personnelle grave ou de décès

Intérêt national	(Toute atteinte impliquant l'intérêt national est évaluée comme étant au moins de niveau 2)	Un inconvénient pour l'intérêt national	Une atteinte à l'intérêt national	Une atteinte sérieuse ou exceptionnellement grave à l'intérêt national

Figure 7 : Tableau d'évaluation des risques

8.1 Évaluation du niveau de risque

Les risques ci-dessus devraient être évalués comme suit :

Niveau d'assurance requis	Critère
Niveau 1 (CAL1)	Un ou plusieurs risques sont évalués comme étant de niveau 1 et aucun n'est évalué comme dépassant le niveau 1
Niveau 2 (CAL2)	Un ou plusieurs risques sont évalués comme étant de niveau 2 et aucun n'est évalué comme dépassant le niveau 2
Niveau 3 (CAL3)	Un ou plusieurs risques sont évalués comme étant de niveau 3 et aucun n'est évalué comme dépassant le niveau 3
Niveau 4 (CAL4)	Un ou plusieurs risques sont évalués comme étant de niveau 4

Figure 8 : Évaluation des niveaux de risque

8.2 Risques pour les justificatifs

Les Justificatifs fournissent les bases de la confiance dans un écosystème numérique. Outre les évaluations des répercussions sur la protection de la vie privée qu'une entité peut mener, c'est important que les organisations qui participent à un écosystème de confiance comprennent les risques qui pèsent sur les justificatifs qu'elles créent, possèdent et/ou utilisent, et qu'elles prennent des mesures appropriées pour protéger leur intégrité. La figure 4 contient un tableau qui illustre les risques pour les justificatifs et des exemples de stratégies d'atténuation.

Activité	Menace	Exemple	Exemple de stratégie d'atténuation
Stockage des justificatifs	Divulgation	Les noms d'utilisateur et les mots de passe stockés dans un fichier système sont divulgués.	Recourir à des mécanismes de contrôle assurant une protection contre les divulgations non autorisées des justificatifs stockés. Protéger les noms d'utilisateur/les mots de passe au moyen de fonctions sécurisées de salage et de hachage ou de techniques de chiffrement approuvées, de façon à rendre impossible la récupération des mots de passe pouvant résulter de la fuite d'un fichier de mots de passe.
	Trafiquage	Le fichier qui établit la correspondance entre les noms d'utilisateurs et les mots de passe au sein du FJI est piraté, ce qui entraîne une modification des correspondances et le remplacement des mots de passe légitimes par des mots de passe connus d'un auteur de menaces.	Recourir à des mécanismes de contrôle assurant une protection contre le trafiquage des justificatifs et des jetons.
Services de vérification des justificatifs	Divulgation	Un auteur de menaces parvient à visualiser les demandes et les réponses circulant entre un FJI et un vérificateur.	Recourir à un protocole de communication qui offre des fonctions de protection de la confidentialité.

	Trafiquage	Un auteur de menaces parvient à se faire passer pour un FJI et fournit des réponses erronées aux demandes de vérification de mots de passe d'un vérificateur.	Veiller à ce que les vérificateurs authentifient les FJI avant d'accepter une réponse de vérification de la part d'un FJI. Recours à un protocole de communication qui offre des fonctions de protection de l'intégrité.
	Non-disponibilité	Le fichier de mots de passe ou le FJI n'est pas disponible et ne peut donc pas fournir les correspondances entre les mots de passe et les noms d'utilisateur.	Veiller à ce que les FJI disposent d'un plan de contingence perfectionné et éprouvé.
		Les vérificateurs ne peuvent obtenir les certificats de clés publiques des requérants parce que les systèmes annuaires sont en panne (par exemple, aux fins de maintenance ou à la suite d'une attaque par déni de service).	
Émission, renouvellement ou réémission des justificatifs	Divulgation	Le mot de passe d'un abonné est renouvelé par un FJI puis copié par un auteur de menaces pendant que ledit mot de passe est envoyé par le FJI vers l'abonné.	Utiliser un protocole de communication qui protège la confidentialité des données de session.
	Trafiquage	Un nouveau mot de passe créé par un abonné est modifié par un auteur de menaces pendant que ledit mot de passe est acheminé à un FJI pour remplacer un mot de passe expiré.	Utiliser un protocole de communication qui permet à un abonné d'authentifier le FJI avant de s'engager dans des activités de réémissions des jetons et de protéger l'intégrité des données transmises.

	Émission non autorisée	Un FJI est victime de compromission à la suite d'un accès logique ou physique non autorisé rendu possible par l'émission de justificatifs frauduleux.	Mettre en place des contrôles d'accès physiques et logiques empêcher la compromission du FJI.
	Renouvellement ou réémission non autorisés	Un auteur de menaces amène frauduleusement un FJI à réémettre un justificatif pour un abonné légitime. Le nouveau justificatif lie l'identité dudit abonné à un jeton fourni par l'auteur de menaces.	Instaurer une politique exigeant qu'un abonné prouve qu'il est en possession du jeton original afin de négocier avec succès le processus de réémission. Toute tentative pour négocier le processus de réémission, en utilisant un jeton expiré ou révoqué, devrait échouer.
		Un auteur de menaces parvient à tirer avantage d'un protocole faible de renouvellement des justificatifs et à prolonger la période de validité des justificatifs d'un abonné légitime.	
Révocation ou destruction des jetons et des justificatifs	Temporisation de la révocation ou de la destruction de justificatifs	Les listes de révocation de certificats non à jour permettent à l'auteur de menaces d'utiliser des comptes qui auraient dû être verrouillés à la suite de la révocation des justificatifs.	Révoquer ou détruire les justificatifs dès que l'avis de révocation ou de destruction des justificatifs a été signifié.
		Les comptes utilisateur ne sont pas supprimés lorsque des employés quittent une entreprise, ce qui crée le risque que des personnes non autorisées se servent desdits comptes.	
		Un jeton matériel est utilisé après la révocation ou l'expiration des justificatifs correspondants.	Détruire les jetons après la révocation des justificatifs correspondants.

Figure 9 : Risques pour les justificatifs

8.3 Gestion des justificatifs

La façon dont les justificatifs sont gérés aura un impact direct sur leur fiabilité. La figure 5 contient un tableau qui illustre les exigences pour la gestion des justificatifs et l'impact que cela peut avoir sur leur fiabilité. Tel que mentionné dans la discussion préalable de ce document à propos des risques, les parties dépendantes doivent évaluer le niveau de risque qu'elles sont disposées à accepter et ajuster en conséquence leurs propres paramètres de risque. Comme cela a aussi été indiqué, il est important que ces niveaux soient délibérément établis et enregistrés afin d'être mis en œuvre et évalués d'une manière uniforme. Il est également rappelé aux parties dépendantes de tenir compte des lois et règlements, car ils peuvent avoir une incidence sur des aspects spécifiques de la gestion des justificatifs comme les exigences en ce qui concerne leur conservation.

Niveau	Exigences				
	Stockage des justificatifs	**Services de vérification des jetons et des justificatifs**	**Renouvellement /réémission des jetons et des justificatifs**	**Révocation et destruction des jetons et des justificatifs**	**Exigences en matière de conservation des documents**
CAL1	Les fichiers de secrets partagés employés par les vérificateurs seront protégés par des contrôles d'accès afin de limiter l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. Les fichiers de secrets partagés ne doivent pas être stockés en texte clair. Le hachage unidirectionnel ou une autre fonction semblable doit	Les secrets à long terme des jetons ne devraient pas être partagés avec d'autres parties, sauf en cas de nécessité absolue.	Aucune exigence	Aucune exigence	Aucune exigence

	être employé avant le stockage.				
CAL2	Les fichiers de secrets partagés employés par les vérificateurs doivent être protégés par des contrôles d'accès afin de limiter l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. De tels fichiers de secrets partagés ne doivent contenir aucun mot de passe ni aucun secret en texte clair. Ainsi, deux méthodes peuvent être employées pour protéger les secrets partagés : 1. Les mots de passe peuvent être	S'ils sont utilisés, les secrets partagés à long terme aux fins d'authentification ne doivent jamais être révélés à qui que ce soit, sauf aux vérificateurs relevant des FJI. Toutefois, les secrets partagés de sessions (temporaires) peuvent être fournis par les FJI à des vérificateurs indépendants. Des mesures de protection cryptographiques sont	Les FJI doivent instaurer des politiques adéquates de renouvellement et de réémission des jetons et des justificatifs. La preuve de possession d'un jeton encore valide doit être confirmée par le requérant avant qu'un FJI accorde le renouvellement ou la réémission. Les mots de passe ne doivent pas être renouvelés, mais devraient être réémis. À l'expiration d'un jeton et de toute période de grâce, le renouvellement et la réémission ne doivent pas	Les FJI doivent révoquer ou détruire les justificatifs et les jetons dans les 72 heures suivant la réception d'un avis indiquant qu'un justificatif n'est plus valide ou qu'un jeton a été compromis, et ce, pour empêcher l'authentification de requérants qui s'aviseraient d'employer les justificatifs ou les jetons en question. Lorsqu'il émet des justificatifs qui expirent automatiquement après 72 heures (p. ex. émission quotidienne de nouveaux	Le FJI ou son représentant doit tenir dossier de l'inscription, de l'historique et de l'état de chaque jeton et justificatif (y compris leur révocation). Les dossiers doivent être conservés sept ans en ce qui concerne les donnes pour les justificatifs de niveau 2 et six mois après l'expiration ou la révocation du justificatif, selon l'échéance la plus tardive.

	concaténés à une variable de salage (variable distribuée dans un groupe de mots de passe stockés ensemble) puis hachés au moyen d'un algorithme approuvé, faisant ainsi que les calculs informatiques employés pour exécuter une attaque par dictionnaire ou une attaque exhaustive visant un fichier de mots de passe volé ne sont pas utiles pour attaquer d'autres fichiers de mots de passe similaires. Les mots de passe hachés sont ensuite stockés dans le fichier de mots de passe. Les variables de salage peuvent consister en une fonction de salage	requises pour tous les messages échangés entre un FJI et un vérificateur, qui contiennent des justificatifs privés ou qui confirment la validité des justificatifs faiblement liés ou possiblement révoqués. Les justificatifs privés ne devraient être acheminés que par des sessions protégées à une partie obligatoirement authentifiée, de façon à garantir la confidentialité et à contrer le trafiquage.	être permis. Lors de la réémission, les secrets des jetons ne doivent pas être réglés à une valeur par défaut ni réutilisés de quelque façon que ce soit. Toutes les transactions devraient se faire dans le cadre d'une session protégée comme SSL ou par TSL.	certificats valides pour 24 heures) un FJI n'est pas tenu de fournir un mécanisme particulier pour révoquer les justificatifs. Les FJI qui enregistrent des mots de passe devraient veiller à ce que la révocation ou la radiation de ceux-ci s'exécute dans les 72 heures.	

	global (commune à un groupe de mots de passe) et le nom d'utilisateur (un par mot de passe) ou une autre technique visant à assurer l'unicité du salage dans le groupe de mots de passe. 2. Les secrets partagés peuvent être chiffrés et enregistrés au moyen de procédures et d'algorithmes approuvés. Les secrets ne doivent être déchiffrés qu'au moment voulu, soit dès lors que l'authentification l'exige. De plus, toute méthode devant servir à la protection des secrets partagés de niveau 3 ou 4 peut également être employée au niveau 2.				

CAL3	Les fichiers de secrets partagés employés par les vérificateurs devraient être protégés par des contrôles d'accès dans le but de réserver l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. Les fichiers contenant des secrets partagés doivent être chiffrés. Voici les exigences minimales en ce qui concerne le chiffrement : 1. La clé de chiffrement pour le secret partagé est elle-même chiffrée selon une clé conservée dans un module cryptographique matériel FIPS 140-2 de niveau 2 ou supérieur ou encore dans un module cryptographique FIPS 140-2 de niveau 3 ou 4; elle n'est déchiffrée qu'au besoin,	Les FJI doivent fournir un mécanisme sécurisé permettant aux vérificateurs et aux PC de vérifier la validité des justificatifs. Ce type de mécanisme peut inclure des serveurs de validation en ligne ou des serveurs FJI ayant accès aux enregistrements de statut pendant les transactions d'authentification. Au nombre des services de vérification offerts par les FJI, des clés temporaires d'authentification de session peuvent être générées par ces FJI à partir de clés de secrets partagés à long terme, puis distribuées à de tiers vérificateurs. Toutefois, les	Le renouvellement et la réémission ne devraient avoir lieu qu'avant l'expiration des justificatifs concernés. Dans les cas de renouvellement ou de réémission des justificatifs, les requérants devraient être authentifiés auprès des FJI au moyen des jetons et des justificatifs existants. Toutes les transactions devraient se faire par voie de session protégée, notamment par SSL ou par TSL.	Les FJI devraient disposer d'une procédure permettant de révoquer les justificatifs et les jetons dans les 24 heures. Les vérificateurs doivent veiller à ce que les jetons employés soient ou bien fraîchement émis (depuis au plus 24 heures) ou bien encore valides. Les systèmes d'authentification fondés sur les secrets partagés peuvent simplement supprimer, dans la base de vérification, les noms d'utilisateurs dont l'accès a été révoqué.	Aucune exigence additionnelle par rapport au niveau 2.

	lorsqu'elle doit faire partie de mesures d'authentification. 2. Les secrets partagés sont protégés en tant que clés dans un module cryptographique matériel FIPS 140-2 de niveau 2 ou supérieur ou encore dans un module cryptographique FIPS 140-2 de niveau 3 ou 4; ils ne sont jamais exportés en texte clair depuis le module en question.	secrets partagés à long terme ne devraient pas partagés avec des tierces parties, y compris des vérificateurs tiers.			

CAL4	Aucune exigence additionnelle par rapport au niveau 3.	Aucune exigence additionnelle par rapport au niveau 3.	Les transferts de données sensibles doivent être authentifiés par voie cryptographique, au moyen de clés liées au processus d'authentification. Toutes les clés temporaires ou à court terme qui sont produites pendant l'authentification initiale doivent expirer et une nouvelle authentification doit être effectuée dans les 24 heures de l'authentification initiale.	Les FJI doivent avoir une procédure permettant de révoquer les justificatifs dans les 24 heures suivant l'authentification. Les vérificateurs ou les PC doivent s'assurer que les justificatifs employés sont fraîchement émis (depuis au plus 24 heures) ou encore valides.	Toutes les stipulations relevant des niveaux 2 et 3 s'appliquent. La période minimale de conservation des données constituant les justificatifs de niveau 4 est de 10 ans et six mois suivant l'expiration ou la révocation de ces justificatifs.

Figure 10 : Gestion des justificatifs

9. Critères de conformité

Les critères de conformité sont catégorisés par élément de confiance. Pour faciliter la référence, on peut se référer à un critère de conformité spécifique par son numéro de catégorie et de référence. Exemple : « RABS1 » fait référence au « critère de conformité de base n^{o} 1 ».

Remarques :

- Les critères de conformité de base sont également inclus dans ce profil de conformité.
- Les critères de conformité spécifiés dans d'autres composantes du CCP peuvent aussi s'appliquer à la composante « Justificatifs (relations et attributs) » du CCP.

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
RABS	**Ces critères de base s'appliquent à tous les processus rattachés aux relations et aux attributs**				
1	Ces critères de conformité ne remplacent ou n'annulent pas les règlements existants; on s'attend à ce que les organisations et les personnes se conforment aux lois, aux politiques et aux règlements en vigueur dans leur province ou territoire.	X	X	X	X
RDEF	**Définir une relation**				
1	L'émetteur **NE DEVRAIT PAS** inclure des renseignements à propos d'un cas spécifique du type de relation défini.	X	X	X	X
2	L'émetteur **DEVRAIT** inclure des renseignements qui identifient clairement la partie qui définit.	X	X		
3	L'émetteur **DOIT** inclure des renseignements qui identifient clairement la partie qui définit.			X	X
4	L'émetteur **DEVRAIT** indiquer l'autorité sous laquelle la relation peut être divulguée (p. ex., un certificat de mariage ne peut être divulgué légitimement que par une partie appropriée faisant autorité comme un tribunal ou un organisme d'État; l'appartenance à une association communautaire peut être légitimement réfutée d'une manière volontaire ou être réfutée par la direction de l'association).	X			
5	L'émetteur **DOIT** indiquer l'autorité en vertu de laquelle la relation peut être réfutée (p. ex., un certificat de mariage ne peut être divulgué légitimement que par une partie appropriée faisant autorité comme un tribunal ou un organisme d'État; l'appartenance à une association communautaire peut être légitimement réfutée d'une manière volontaire ou être réfutée par la direction de l'association).		X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
6	L'émetteur **DEVRAIT** déclarer si le type de Relation décrite doit être approuvé pour être considéré fiable (voir le processus de confiance « Approuver la relation » dans l'aperçu les critères énumérés sous REND pour les détails).	X			
7	L'émetteur **DOIT** déclarer si le type de Relation décrite doit être approuvé pour être considéré fiable (voir le processus de confiance « Approuver la relation » dans l'aperçu les critères énumérés sous REND pour les détails).		X	X	X
8	Dans la mesure du possible, et si approprié, l'Émetteur **PEUT** utiliser des définitions juridiques pertinentes, des définitions des normes de l'industrie ou des références à des schémas pertinents.	X			
9	Dans la mesure du possible, et si approprié, l'Émetteur **DEVRAIT** utiliser des définitions juridiques pertinentes, des définitions des normes de l'industrie ou des références à des schémas pertinents.		X	X	X
RDEC	**Déclarer une relation**				
1	L'émetteur **PEUT** utiliser une définition de la relation comme base pour la relation déclarée et y faire référence dans la relation déclarée.	X			
2	L'émetteur **DOIT** utiliser une définition de la relation comme base pour la relation déclarée et y faire référence dans la relation déclarée.		X	X	X
3	L'émetteur **PEUT** fournir aux participants un résumé de son mandat et son autorité reliés aux relations qu'il déclare.	X			
4	L'émetteur **DOIT** fournir aux participants un résumé de son mandat et son autorité reliés aux relations qu'il déclare.		X	X	X
5	Le cas échéant, l'émetteur **DEVRAIT** fournir aux participants la preuve qu'il remplit toutes les exigences juridiques et réglementaires s'appliquant aux types de relations qu'il émet.	X			

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
6	Le cas échéant, l'émetteur **DOIT** fournir aux participants la preuve qu'il remplit toutes les exigences juridiques et réglementaires s'appliquant aux types de relations qu'il émet.		X	X	X
7	L'émetteur **PEUT** fournir aux participants les conditions générales régissant l'utilisation légitime ou interdite des relations déclarées qu'il émet (p. ex., il y a des cas où la carte d'assurance maladie provinciale ou le numéro d'assurance sociale devraient être utilisés, et des cas où ils ne devraient pas être utilisés ou leur utilisation est interdite par un règlement, une loi ou une politique).	X			
8	L'émetteur **DEVRAIT** fournir aux participants les conditions générales régissant l'utilisation légitime ou interdite des relations déclarées qu'il émet (p. ex., il y a des cas où la carte d'assurance maladie provinciale ou le numéro d'assurance sociale devraient être utilisés, et des cas où ils ne devraient pas être utilisés ou leur utilisation est interdite par un règlement, une loi ou une politique).		X	X	
9	L'émetteur **DOIT** fournir aux participants les conditions générales régissant l'utilisation légitime ou interdite des relations déclarées qu'il émet (p. ex., il y a des cas où la carte d'assurance maladie provinciale ou le numéro d'assurance sociale devraient être utilisés, et des cas où ils ne devraient pas être utilisés ou leur utilisation est interdite par un règlement, une loi ou une politique).				X
10	L'émetteur **PEUT** fournir aux participants un point de contact leur permettant d'obtenir de l'information sur ses relations et processus connexes.	X			
11	L'émetteur **DOIT** fournir aux participants un point de contact leur permettant d'obtenir de l'information sur ses relations et processus connexes.		X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
12	Le cas échéant, l'Émetteur **DOIT** permettre au Sujet de spécifier l'endroit (c.-à-d., référentiel de justificatifs local ou hébergé) où la Relation sera fournie, à moins que ce ne soit interdit par un règlement, une politique ou une loi.	X	X	X	X
13	L'émetteur **PEUT** fournir aux participants des détails concernant la preuve et les processus spécifiques sur lesquels il s'est fié pour vérifier et valider les renseignements sur le sujet contenus dans une relation.	X			
14	L'émetteur **DEVRAIT** fournir aux participants des détails concernant la preuve et les processus spécifiques sur lesquels il s'est fié pour vérifier et valider les renseignements sur le sujet contenus dans une relation.		X		
15	L'émetteur **DOIT** fournir aux participants des détails concernant la preuve et les processus spécifiques sur lesquels il s'est fié pour vérifier et valider les renseignements sur le sujet contenus dans une relation.			X	X
16	L'émetteur **PEUT** fournir des références aux justificatifs de tierces parties (c.-à-d., des justificatifs émis par d'autres entités) dont il s'est servi pour vérifier et valider les renseignements contenus dans une relation qu'il a émise.	X			
17	L'émetteur **DEVRAIT** fournir des références aux justificatifs de tierces parties (c.-à-d., des justificatifs émis par d'autres entités) dont il s'est servi pour vérifier et valider les renseignements contenus dans une relation qu'il a émise.		X		
18	L'émetteur **DOIT** fournir des références aux justificatifs de tierces parties (c.-à-d., des justificatifs émis par d'autres entités) dont il s'est servi pour vérifier et valider les renseignements contenus dans une relation qu'il a émise.			X	X
19	Les renseignements contenus dans une relation **DOIVENT** concorder avec ceux qui sont contenus dans les dossiers de l'émetteur.	X	X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
20	L'émetteur **DEVRAIT** fournir des renseignements indiquant la confiance qu'il faisait à l'exactitude des renseignements contenus dans la relation quand celle-ci a été émise. Ce serait normalement fait en communiquant le niveau d'assurance associé au justificatif, mais pourrait inclure d'autres renseignements ou mises en garde.		X	X	X
21	L'émetteur **DEVRAIT** fournir des renseignements indiquant la confiance qu'il faisait à l'identité du sujet ou celle de l'entité agissant pour le compte du sujet quand la relation déclarée a été émise. Ce serait normalement fait en communiquant le niveau d'assurance associé au justificatif, mais pourrait inclure d'autres renseignements ou mises en garde.	X	X		
22	L'émetteur **DOIT** fournir des renseignements indiquant la confiance qu'il faisait à l'identité du sujet ou celle de la personne agissant pour le compte du sujet quand la relation déclarée a été émise. Ce serait normalement fait en communiquant le niveau d'assurance associé au justificatif, mais pourrait inclure d'autres renseignements ou mises en garde.			X	X
23	L'émetteur **PEUT** être capable de démontrer qu'une relation déclarée émanait de l'émetteur et qu'elle n'a pas été altérée pendant la transmission à un autre participant (sujet, détenteur, partie utilisatrice, etc.).Ce serait normalement fait sous la forme d'une relation déclarée vérifiable.	X			
24	L'émetteur **DEVRAIT** être capable de démontrer qu'une relation déclarée émanait de l'émetteur et qu'elle n'a pas été altérée pendant la transmission à un autre participant (sujet, détenteur, partie utilisatrice, etc.).Ce serait normalement fait sous la forme d'une relation déclarée vérifiable.		X		

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
25	L'émetteur **DOIT** être capable de démontrer qu'une relation déclarée émanait de l'émetteur et qu'elle n'a pas été altérée pendant la transmission à un autre participant (sujet, détenteur, partie utilisatrice, etc.).Ce serait normalement fait sous la forme d'une relation déclarée vérifiable.			X	X
26	Un justificatif de relation déclarée **DOIT** inclure des renseignements qui identifient l'émetteur.		X	X	X
27	L'émetteur **DOIT** inclure la date à laquelle la relation a été émise, et étiquetée comme telle sans ambiguïté.		X	X	X
28	L'émetteur **PEUT** fournir une date d'expiration pour toutes les relations qu'il déclare ou indiquer que la relation n'a pas de date d'expiration.	X			
29	L'émetteur **DOIT** fournir une date d'expiration pour toutes les relations qu'il déclare ou indiquer que la relation n'a pas de date d'expiration.		X	X	X
30	En déclarant une relation, l'émetteur **PEUT** indiquer qu'elle est entièrement ou partiellement contestée. En pareil cas, l'émetteur **DEVRAIT** inclure une référence à d'autres relations déclarées qui contiennent des renseignements contestés et/ou faisant l'objet d'un examen.	X	X	X	X
31	L'émetteur **DEVRAIT** fournir aux participants des conditions générales en vertu desquelles les relations qu'il déclare deviendront inutilisables ou non fiables.	X			
32	L'émetteur **DOIT** fournir aux participants des conditions générales en vertu desquelles les relations qu'il déclare deviendront inutilisables ou non fiables.		X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
33	Le titulaire **DOIT** s'assurer que le référentiel où il entrepose une relation déclarée est adéquatement sécurisé, trouvé d'une manière légitime et situé dans une province ou un territoire tel qu'exigé par la loi, une politique et/ou un règlement.		X	X	X
REND	**Approuver une relation**				
1	Une partie qui approuve **PEUT** être une source faisant autorité qui est une personne vérifiée ou une organisation vérifiée.	X			
2	Une partie qui approuve **DEVRAIT** être une source faisant autorité qui est une personne vérifiée ou une organisation vérifiée.		X		
3	Une partie qui approuve **DOIT** être une source faisant autorité qui est une personne vérifiée ou une organisation vérifiée.			X	X
RVAL	**Valider une relation**				
1	Les vérificateurs **DEVRAIENT** fournir assez de renseignements à la partie dépendante pour lui permettre d'évaluer convenablement le niveau d'assurance qui peut être associé à chaque relation.	X	X		
2	Les vérificateurs **DOIVENT** fournir assez de renseignements à la partie dépendante pour lui permettre d'évaluer convenablement le niveau d'assurance qui peut être associé à chaque relation.			X	X
3	Les vérificateurs **PEUVENT** confirmer que la partie qui approuve ou qui déclare est une source faisant autorité et que le ou les sujets sont des personnes ou des organisations vérifiées.	X			
4	Les vérificateurs **DEVRAIENT** confirmer que la partie qui approuve ou qui déclare est une source faisant autorité et que le ou les sujets sont des personnes ou des organisations vérifiées.		X		

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
5	Les vérificateurs **DOIVENT** confirmer que la partie qui approuve ou qui déclare est une source faisant autorité et que le ou les sujets sont des personnes ou des organisations vérifiées.			X	X
6	Les vérificateurs **PEUVENT** informer la partie dépendante si la partie qui approuve ou qui déclare est une source faisant autorité et si le ou les sujets sont des personnes ou des organisations vérifiées.	X			
7	Les vérificateurs **DEVRAIENT** informer la partie dépendante si la partie qui approuve ou qui déclare est une source faisant autorité et si le ou les sujets sont des personnes ou des organisations vérifiées.		X		
8	Les vérificateurs **DOIVENT** informer la partie dépendante si la partie qui approuve ou qui déclare est une source faisant autorité et si le ou les sujets sont des personnes ou des organisations vérifiées.			X	X
9	La partie qui approuve ou qui déclare **PEUT** être une personne vérifiée ou une organisation vérifiée.	X			
10	La partie qui approuve ou qui déclare **DEVRAIT** être une personne vérifiée ou une organisation vérifiée.		X		
11	La partie qui approuve ou qui déclare **DOIT** être une personne vérifiée ou une organisation vérifiée.			X	X
12	Le vérificateur **DEVRAIT** être une personne vérifiée ou une organisation vérifiée.	X			
13	Le vérificateur **DOIT** être une personne vérifiée ou une organisation vérifiée.		X	X	X
14	Le vérificateur **NE DEVRAIT PAS** garder des copies des présentations ou des présentations vérifiées qu'il vérifie, ni des données qu'elles contiennent ni des données dérivées de ces données, à moins qu'un règlement, une politique ou une loi ne l'exige.	X	X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
15	Les vérificateurs **NE DOIVENT PAS** partager les renseignements qui leur sont présentés dans le cadre du processus de vérification avec d'autres vérificateurs, d'autres participants ou qui que ce soit d'autre que la ou les parties dépendantes sans le consentement express du sujet, à mois que cela ne soit exigé par un règlement, une politique ou la loi.	X	X	X	X
16	Les relations incluses dans une présentation ou une présentation vérifiable qui est soumise à un vérificateur **DEVRAIENT** être sous la forme d'une relation déclarée, approuvée ou validée.	X	X	X	X
RDIS	**Réfuter une relation**				
1	La partie qui réfute **DOIT** réfuter, ou rendre inutilisable ou non fiable, une Relation si elle décèle des indices d'une Relation compromise ou non valide.	X	X	X	X
2	La partie qui réfute **DOIT** mettre à la disposition des participants le statut de toutes les Relations autrement inutilisables ou non fiables qu'elle a émises.	X	X	X	X
3	La partie qui réfute **DOIT** saisir les détails suivants à propos des relations que l'émetteur a rendues inutilisables ou non fiables : date à laquelle la mesure a été prise, raison de la mesure, indication générale de qui a initié la mesure (p. ex., sujet ou émetteur).	X	X	X	X
4	La partie qui réfute **DOIT** uniquement réfuter les détails saisis à propos de relations inutilisables ou non fiables à des participants connus qui ont un besoin raisonnable d'avoir l'information, et dans les limites des règlements, politiques ou lois applicables.	X	X	X	X
5	La partie qui réfute **DOIT** divulguer la raison pour laquelle elle réfute la relation au ou aux sujets.	X	X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
6	La partie qui réfute **NE DOIT PAS** réfuter arbitrairement des relations. Les relations réfutées devraient être le résultat de politiques, procédures, lois ou règlements pertinents ou encore d'activités malveillantes confirmées ou suspectées, comme de la fraude, qui présenteraient un risque indu si la relation était acceptée.	X	X	X	X
7	La partie qui approuve **DEVRAIT** fournir aux sujets la capacité d'amorcer un processus pour réfuter, ou autrement rendre inutilisable ou non fiable, une relation quand le sujet décèle des indications d'une relation compromise ou invalide.	X	X	X	X
ADEF	**Définir un attribut**				
1	L'Émetteur **NE DEVRAIT PAS** inclure des renseignements à propos d'un cas spécifique de type d'attribut défini.	X	X	X	X
2	L'Émetteur **DEVRAIT** inclure des renseignements qui identifient clairement l'émetteur.	X	X		
3	L'Émetteur **DOIT** inclure des renseignements qui identifient clairement l'émetteur.			X	X
4	Dans la mesure du possible, et si approprié, l'Émetteur **PEUT** utiliser des définitions juridiques pertinentes, des définitions standard de l'industrie ou des références à des schémas pertinents.	X	X		
5	Dans la mesure du possible, et si approprié, l'Émetteur **DEVRAIT** utiliser des définitions juridiques pertinentes, des définitions standard de l'industrie ou des références aux schémas pertinents.			X	X
ABND	**Lier un attribut**				
1	L'émetteur **PEUT** utiliser une définition de l'attribut comme base pour l'attribut lié et y faire référence dans l'attribut lié.	X			

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
2	L'émetteur **DOIT** utiliser une définition de l'attribut comme base pour l'attribut lié et y faire référence dans l'attribut lié.		X	X	X
3	L'émetteur **PEUT** fournir aux participants un résumé de son mandat et de son autorité, car ils sont reliés aux attributs qu'il émet.	X			
4	L'émetteur **DOIT** fournir aux participants un résumé de son mandat et de son autorité, car ils sont reliés aux attributs qu'il émet.		X	X	X
5	L'émetteur **DEVRAIT** fournir aux participants la preuve qu'il répond à toutes les exigences juridiques et réglementaires applicables aux types d'attributs qu'il émet.	X			
6	L'émetteur **DOIT** fournir aux participants la preuve qu'il répond à toutes les exigences juridiques et réglementaires applicables aux types d'attributs qu'il émet.		X	X	X
7	L'émetteur **PEUT** fournir aux participants les conditions générales qui régissent l'émission et l'utilisation des attributs qu'il émet.	X			
8	L'émetteur **DEVRAIT** fournir aux participants les conditions générales qui régissent l'émission et l'utilisation des attributs qu'il émet.		X		
9	L'émetteur **DOIT** fournir les conditions spécifiques qui régissent l'émission et l'utilisation d'un attribut spécifique qu'il émet.			X	X
10	L'émetteur **DOIT** donner aux sujets qui demandent l'émission d'un attribut un avis stipulant que le fait de faire des déclarations ou de fournir des informations fausses ou trompeuses peut entraîner une violation des conditions régissant son émission et son utilisation.		X	X	X
11	L'émetteur **DOIT** confirmer que les sujets comprennent et acceptent l'avis précisant que toute déclaration fausse ou trompeuse peut entraîner une violation des conditions générales régissant l'émission et l'utilisation des justificatifs.		X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
12	L'émetteur **PEUT** fournir aux participants un point de contact pour obtenir des renseignements à propos de ses justificatifs et processus associés.	X			
13	L'émetteur **DOIT** fournir aux participants un point de contact pour obtenir des renseignements à propos de ses justificatifs et processus associés.		X	X	X
14	Le cas échéant, l'émetteur **DOIT** permettre au sujet de spécifier l'endroit (c.-à-d. un référentiel de justificatifs local ou hébergé) où l'attribut sera livré, à moins qu'un règlement, une politique ou la loi ne l'interdise.	X	X	X	X
15	L'émetteur **PEUT** fournir aux participants les détails des preuves et processus auxquels il s'est fié pour vérifier et valider les renseignements sur le sujet contenus dans un attribut.	X			
16	L'émetteur **DEVRAIT** fournir aux participants les détails des preuves et processus auxquels il s'est fié pour vérifier et valider les renseignements sur le sujet contenus dans un attribut.		X		
17	L'émetteur **DOIT** fournir aux participants les détails des preuves et processus auxquels il s'est fié pour vérifier et valider les renseignements sur le sujet contenus dans un attribut.			X	X
18	L'émetteur **PEUT** fournir des références aux justificatifs ou attributs de tierces parties (c.-à-d., les justificatifs ou attributs émis par d'autres entités) qu'il a utilisés pour vérifier et valider les renseignements contenus dans un attribut qu'il a émis.	X			
19	L'émetteur **DEVRAIT** fournir des références aux justificatifs ou attributs de tierces parties (c.-à-d., les justificatifs ou attributs émis par d'autres entités) qu'il a utilisés pour vérifier et valider les renseignements contenus dans un attribut qu'il a émis.		X		

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
20	L'émetteur **DOIT** fournir des références aux justificatifs ou attributs de tierces parties (c.-à-d., les justificatifs ou attributs émis par d'autres entités) qu'il a utilisés pour vérifier et valider les renseignements contenus dans un attribut qu'il a émis.			X	X
21	Les renseignements contenus dans un justificatif **DOIVENT** correspondre à ceux qui sont contenus dans les dossiers de l'émetteur.	X	X	X	X
22	L'émetteur **DEVRAIT** fournir des renseignements indiquant qu'il s'est fié à l'exactitude des renseignements contenus dans l'attribut lorsque celui-ci a été émis. Ce serait normalement fait en communiquant le niveau d'assurance associé au justificatif, quoiqu'il pourrait inclure d'autres renseignements ou mises en garde.		X	X	X
23	L'émetteur **DOIT** émettre un attribut uniquement à la demande ou avec le consentement du sujet ou d'une personne admissible à agir pour le compte du sujet, sauf lorsqu'une politique, un règlement ou une loi le permet.	X	X	X	X
24	L'émetteur **DOIT** prendre des mesures raisonnables pour s'assurer que des attributs liés sont émis à la demande et/ou avec le consentement du sujet en droit de le faire ou d'une personne autorisée à agir pour le compte du sujet, sauf là où cela est permis par une politique, un règlement ou la loi.	X	X	X	X
25	L'émetteur **DEVRAIT** fournir des renseignements indiquant qu'il s'est fié à l'identité du sujet ou de la personne agissant pour le compte du sujet quand l'attribut lié a été émis.	X	X		
26	L'émetteur **DOIT** fournir des renseignements indiquant qu'il s'est fié à l'identité du sujet ou de la personne agissant pour le compte du sujet quand l'attribut lié a été émis.			X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
27	L'émetteur **PEUT** démontrer qu'un attribut provenait de lui et qu'il n'a pas été altéré pendant la transmission à un autre participant (sujet, titulaire, partie dépendante, etc.). Ce serait généralement fait sous la forme d'un attribut lié vérifiable.	X			
28	L'émetteur **DEVRAIT** pouvoir démontrer qu'un attribut provenait de lui et qu'il n'a pas été altéré pendant la transmission à un autre participant (sujet, titulaire, partie dépendante, etc.). Ce serait généralement fait sous la forme d'un attribut lié vérifiable.		X		
29	L'émetteur **DOIT** pouvoir démontrer qu'un attribut provenait de lui et qu'il n'a pas été altéré pendant la transmission à un autre participant (sujet, titulaire, partie dépendante, etc.). Ce serait généralement fait sous la forme d'un attribut lié vérifiable.			X	X
30	Un attribut lié **DOIT** inclure des renseignements qui identifient l'émetteur de cet attribut.		X	X	X
31	L'émetteur **DOIT** inclure la date à laquelle l'attribut a été émis et étiqueté comme tel d'une façon non ambiguë.		X	X	X
32	L'émetteur **PEUT** fournir une date d'expiration pour tous les attributs qu'il émet ou indiquer que l'attribut n'a pas de date d'expiration.	X			
33	L'émetteur **DOIT** fournir une date d'expiration pour tous les attributs qu'il émet ou indiquer que l'attribut n'a pas de date d'expiration.		X	X	X
34	Lorsqu'il émet un attribut, l'émetteur **PEUT** indiquer que cet attribut est contesté en tout ou en partie. En pareil cas, l'émetteur **DEVRAIT** inclure une référence à d'autres attributs qui contiennent des renseignements contestés et/ou en cours d'examen.	X	X	X	X
35	L'émetteur **DEVRAIT** fournir aux participants les conditions générales en vertu desquelles les attributs seront rendus inutilisables ou non fiables.	X			

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
36	L'émetteur **DOIT** fournir aux participants les conditions générales en vertu desquelles les attributs seront rendus inutilisables ou non fiables.		X	X	X
37	L'émetteur **DOIT** s'assurer que le référentiel auquel il envoie un attribut est adéquatement sécurisé, trouvé d'une manière légitime et situé dans une province ou un territoire comme l'exige la loi, une politique et/ou un règlement.		X	X	X
AMNT	**Maintenir un attribut**				
1	L'émetteur **DEVRAIT** établir, maintenir et faire connaître à d'autres participants un processus pour régler les différends à propos de l'exactitude des renseignements contenus dans les attributs qu'il a émis.	X	X		
2	L'émetteur **DOIT** établir, maintenir et faire connaître à d'autres participants un processus pour régler les différends à propos de l'exactitude des renseignements contenus dans les attributs qu'il a émis.			X	X
3	L'émetteur **DOIT** fournir au sujet la raison pour laquelle un attribut est mis à jour.	X	X	X	X
4	L'émetteur **DOIT** informer le ou les sujets de tout changement apporté à un attribut.	X	X	X	X
5	L'autorité qui révoque **DOIT** révoquer, mettre à jour ou rendre autrement inutilisable ou non fiable un attribut si elle décèle des indications comme quoi cet attribut est compromis ou non valide.	X	X	X	X
6	L'émetteur **DOIT** saisir les détails suivants concernant les attributs qu'il a mis à jour : date de l'intervention, raison de l'intervention, indication générale de qui a initié l'intervention (p. ex., sujet ou émetteur).	X	X	X	X
7	Les Participants **DOIVENT** divulguer uniquement les détails relevés à propos des Attributs inutilisables ou non fiables à d'autres Participants connus ayant un besoin raisonnable d'avoir ces renseignements.	X	X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
8	L'émetteur **NE DOIT PAS** changer arbitrairement des attributs. Les changements devraient être le résultat de politiques, procédures, lois ou règlements pertinents ou d'activités malveillantes confirmées ou suspectées, comme la fraude, qui indiqueraient un risque indu si l'attribut était accepté.	X	X	X	X
9	L'émetteur **DEVRAIT** fournir au sujet la capacité d'amorcer un processus pour révoquer, mettre à jour ou autrement rendre inutilisable ou non fiable un attribut qu'il a émis à ce sujet lorsque ce dernier décèle des indications comme quoi l'attribut est compromis ou non valide.	X	X	X	X
AREV	**Révoquer un attribut**				
1	L'autorité qui révoque **DOIT** initier un processus pour révoquer, mettre à jour ou autrement rendre inutilisable ou non fiable un attribut si elle décèle des indications comme quoi l'attribut est compromis ou non valide.	X	X	X	X
2	L'autorité qui révoque **DOIT** fournir le statut de tous les attributs révoqués ou autrement inutilisables ou non fiables qu'elle a émis (p. ex., si un attribut est un « attribut révoqué ») aux participants qui ont un besoin raisonnable d'avoir l'information.	X	X	X	X
3	L'autorité qui révoque **DOIT** saisir les détails suivants à propos des Attributs que l'émetteur a rendus inutilisables ou non fiables : date de l'intervention, raison de l'intervention, indication générale de qui a amorcé l'intervention (p. ex., sujet ou émetteur).	X	X	X	X
4	L'autorité qui révoque **DOIT** divulguer uniquement les détails saisis à propos des attributs inutilisables ou non fiables à des participants connus ayant un besoin raisonnable d'avoir l'information.	X	X	X	X
5	L'autorité qui révoque **DOIT** fournir au sujet la raison de la révocation.	X	X	X	X

Référence	Critères de conformité	Niveau d'assurance			
		CAL1	CAL2	CAL3	CAL4
6	L'autorité qui révoque **NE DOIT PAS** révoquer arbitrairement des attributs. La révocation devrait être le résultat de politiques, procédures, lois ou règlements pertinents ou d'activités malveillantes confirmées ou suspectées, comme la fraude, qui indiqueraient un risque indu si l'attribut était accepté.	X	X	X	X
7	L'autorité qui révoque **DEVRAIT** fournir au sujet la capacité d'initier un processus pour révoquer, mettre à jour ou autrement rendre inutilisable ou non fiable un attribut qu'il a émis à ce sujet quand le sujet décèle des indications comme quoi l'attribut est compromis ou non valide.	X	X	X	X
8	L'Autorité qui révoque **DEVRAIT** établir, maintenir et faire connaître aux autres participants un processus pour résoudre les différends à propos de l'exactitude de l'information contenue dans les attributs qu'elle a révoqués.	X	X		
9	L'Autorité qui révoque **DOIT** établir, maintenir et faire connaître aux autres participants un processus pour résoudre les différends à propos de l'exactitude de l'information contenue dans les attributs qu'elle a révoqués.			X	X

10. Références

Cette section énumère l'ensemble des normes, lignes directrices et autres documents externes auxquels il est fait référence dans cette composante du CCP.

Remarque : Le cas échéant, seul le numéro de version spécifié ici s'applique à cette composante du CCP.

Cette composante du CCP met à profit les compétences et l'expérience d'autres organisations et les leçons qu'elles ont apprises en s'efforçant d'améliorer ce domaine, et elle a pris en considération le matériel provenant des sources suivantes :

- W3C : Verifiable Credentials Data Model 1.0 <https://www.w3.org/TR/vc-data-model/>
- Gouvernement du Canada, *Secrétariat du Conseil du Trésor du Canada : Profil du secteur public du Cadre de confiance pancanadien, version 1.1* <https://canada-ca.github.io/PCTF-CCP/>

11. Historique des révisions

Version	Date de diffusion	Auteur(s)	Description
0.01	2020-01-20	Équipe de rédaction du CCP	Ébauche de discussion initiale
0.02	2020-03-18	Équipe de rédaction du CCP	Traitement des commentaires initiaux du TFEC
0.03	2020-04-08	Équipe de rédaction du CCP	Ajout des processus axés sur les relations
0.04	2020-04-22	Équipe de rédaction du CCP	Ajout des processus axés sur les attributs
1.0	2020-05-13	Équipe de rédaction du CCP	Ébauche de recommandations V1.0
1.1	2020-07-29	Équipe de rédaction du CCP	Ébauche de recommandations V1.1
1.0	2020-09-16	Équipe de rédaction du CCP	Approuvé en tant que recommandation finale V1.0 par vote du membre de soutien du CCIAN