Aperçu de la composante « Portefeuille numérique » du CCP

Statut du document : Recommandation finale V1.0

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

Ce document donne un aperçu de la composante « Portefeuille numérique » du CCP, une composante du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale sur le CCP, veuillez vous référer à l'aperçu du modèle de CCP, lequel décrit les buts et objectifs du CCP et donne un aperçu général du CCP.

Chaque composante du CCP est décrite dans deux documents :

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

Cet aperçu fournit des renseignements reliés au profil de conformité de la composante « Justificatifs (relations et attributs) » du CCP, qui sont nécessaires pour l'interpréter d'une manière uniforme.

1.1 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 évaluer dans quelle mesure les portefeuilles numériques qui font partie de leurs écosystèmes respectifs accomplissent ce qui suit :

1. Fournir aux citoyens et aux consommateurs un portefeuille numérique qui se conforme aux principes des droits de la personne consistant à préserver la vie privée des gens et le contrôle de leurs renseignements.
2. Introduire une métaphore identitaire et une expérience automatisée axée sur le consentement qui soient uniformisées parmi tous les participants à l'écosystème afin de réduire l'impact de la transformation numérique sur les utilisateurs.
3. Contribuer à une infrastructure stable, dotée d'une longévité et d'une interopérabilité mondiale, en adoptant et en soutenant des normes pertinentes selon ce qui est approprié (p. ex., normes W3C pour les justificatifs vérifiables et les identifiants décentralisés (DID)).
4. Lutter contre la cybervulnérabilité et la cyberextorsion en permettant aux fournisseurs de services de remplacer graduellement les mécanismes de connexion existants, dont certains peuvent être exploitables, sans impacts négatifs sur les activités.

5. Établir un environnement de confiance dans lequel le titulaire du portefeuille peut interagir avec d'autres participants à l'écosystème tels que émetteurs, vérificateurs et autres parties dépendantes.

1.2 Contexte

Le portefeuille physique est un conteneur privé pour l'argent, les cartes de paiement, la preuve d'identité et autres documents du titulaire. Les portefeuilles d'identité numérique sont analogues à des portefeuilles physiques du fait qu'ils contiennent des versions numériques des preuves d'identité et actifs connexes du titulaire du portefeuille. Ces actifs contiennent habituellement des versions numériques des cartes et documents physiques qui nous sont familiers (p. ex., permis de conduire, preuve d'assurance, cartes de santé, etc.). Les actifs numériques sont souvent entreposés sous forme de justificatifs (généralement des justificatifs vérifiables) – et ce terme est utilisé dans tout le présent document pour faire référence au contenu du portefeuille. Un portefeuille d'identité numérique peut aussi entreposer des clés cryptographiques utilisées par le titulaire du portefeuille. Ce sont habituellement de petites applications logicielles qui résident dans les appareils informatiques personnels.

Un portefeuille d'identité numérique bien conçu assure la sécurité de son contenu sensible et confidentiel, tout en faisant en sorte que ce soit facile pour le titulaire du portefeuille d'utiliser des preuves et des justificatifs d'identité numériques en ligne et pour les interactions en personne. Un portefeuille d'identité numérique bien conçu peut protéger davantage la vie privée en permettant au titulaire du portefeuille de contrôler quand, où et comment le contenu du portefeuille est divulgué à de tierces parties et ce qui est divulgué.

Les portefeuilles numériques peuvent servir à fournir à leurs utilisateurs la responsabilité et le contrôle de l'utilisation de leurs données et leurs justificatifs, de sorte qu'une attention particulière a été apportée pendant l'élaboration et l'examen de cette composante aux questions d'usabilité, d'accessibilité, d'abordabilité, de diversité, d'équité, d'inclusions et d'intersectionnalité. Il est fortement recommandé que les fournisseurs de portefeuilles numériques envisagent une façon de limiter leur potentiel pour ce qui est de limiter ou d'exclure l'accès par des segments de la société à des services numériques.

Le concept des portefeuilles numériques en tant de façon pour les titulaires de stocker, de gérer et d'utiliser des identités numériques et des actifs connexes a fait son apparition lorsque les systèmes d'identité sont passés des mécanismes d'authentification des utilisateurs spécifiques aux applications à des systèmes sophistiqués qui partagent et vérifient les actifs identitaires parmi de multiples entités (applications, fournisseurs de services, autres personnes, etc.) dans divers arrangements de fédération et de confiance.

Voici certains facteurs spécifiques qui ont favorisé l'émergence des portefeuilles d'identité numériques :

1. **Hausse des craintes à propos de l'invasion de la vie privée** – La surveillance des utilisateurs par les acteurs commerciaux et étatiques est devenue visible et est à présent un facteur politique qui mène les politiques publiques. Les fabricants de navigateurs et les fournisseurs de logiciels ont fait des efforts pour réduire les possibilités de suivre les utilisateurs en ligne. Mais l'utilisation des adresses de courriel et des numéros de téléphone (qui sont des renseignements personnellement identifiables) comme identifiants universels demeure une pratique courante.
2. **Limitations des solutions d'identité traditionnelles –** Pour les organisations qui s'efforcent de numériser un service important et précieux, la réduction de la redondance, de la duplication et des chevauchements qui peuvent résulter de la prolifération des solutions d'identité chez et entre les fournisseurs de service est une considération commerciale majeure, voire un défi colossal. Lorsque cela arrive, les utilisateurs se retrouvent à devoir gérer de multiples identités numériques et actifs connexes. L'utilisation à grande échelle de gestionnaires de mots de passe pour alléger le fardeau que pose la sécurité de chaque relation de service en est la preuve. Les portefeuilles numériques peuvent aider leurs titulaires à gérer un nombre croissant d'actifs d'identité, et à contrôler le partage et l'utilisation de ces actifs dans leurs relations et interactions numériques.
3. **Expérience utilisateur fragmentée –** Les fournisseurs de services procurent aux utilisateurs des expériences qui sont optimisées pour leurs propres processus. Les expériences utilisateurs numériques tiennent rarement compte de la pleine portée des relations et interactions numériques d'une personne. Beaucoup de personnes se retrouvent alors à naviguer parmi des services numériques largement dissimilaires et qui prêtent souvent à confusion. Les portefeuilles numériques peuvent fournir une expérience utilisateur fiable, uniforme et familière pour les aspects essentiels des interactions impliquant des identités numériques (c.-à-d., entreposage, récupération et présentation des renseignements d'identité).
4. **Professionnalisation et militarisation des cyberattaques** – Étant donné les expériences utilisateurs fragmentées, l'existence de nombreuses identités numériques à vocation unique et la prolifération des renseignements personnels dans tous les systèmes reliés à Internet, il est facile pour des acteurs malveillants qui sont doués et déterminés de compromettre les renseignements personnels et la vie privée. Les portefeuilles d'identité numériques peuvent aider à atténuer quantité de vecteurs d'attaques (avant tout le hameçonnage et d'autres attaques basées sur l'obtention de renseignements personnels). De plus, les titulaires de portefeuilles d'identité numériques peuvent aider à améliorer globalement la cybersécurité en partageant d'une manière sélective uniquement les renseignements nécessaires pour une fin ou une interaction spécifique (p. ex., au moyen d'une preuve à divulgation nulle de connaissance ou d'un prédicat dérivé).

5. **Normes de l'industrie pour les justificatifs et les renseignements personnels vérifiables** – Le besoin de revenir à des processus chronophages nécessitant du personnel pour valider les identités et les renseignements personnels est un obstacle important à l'interaction numérique presque en temps réel. Ces validations sont nécessaires pour maintenir l'intégrité des processus pour les services de grande valeur, mais elles érodent l'efficacité et l'expérience utilisateur. Lorsqu'il y a possibilité d'automatiser la vérification des données (p. ex., une connexion entre le fournisseur de services et l'ARC pour confirmer le revenu imposable), les mécanismes de sécurité des renseignements et de protection de la vie privée peuvent être difficiles à mettre en place sans compromettre l'expérience utilisateur ou contrevenir aux lois existantes. Les justificatifs portables et vérifiables d'une manière cryptographique, qui sont utilisés avec les portefeuilles numériques, sont de plus en plus acceptés comme moyen pour les fournisseurs de services d'obtenir des données qui apportent une grande assurance, tout en procurant une sécurité et une transparence au titulaire du portefeuille. Le modèle de données de justificatifs vérifiables 1.0 du Wide Web Consortium (W3C) a suscité un intérêt et un soutien à grande échelle en tant que norme de données essentielle pour faciliter les justificatifs vérifiables interopérables.

1.3 Portée

Les sujets qui sont considérés comme étant inclus dans la portée et exclus de celle-ci définissent la portée de cette composante du CCP. Les types de portefeuilles numériques et leurs contenus habituels sont aussi un déterminant essentiel de la portée de la composante.

Remarque : Les autres composantes du CCP devraient être prises en considération dans le cadre de n'importe quelle évaluation. Les exigences qui sont directement couvertes par d'autres composantes ne sont pas dupliquées ici. Il est recommandé en particulier que les composantes Authentification, Respect de la vie privée, Avis et consentement, Personne vérifiée et Organisation vérifiée soient incluses dans n'importe quelle évaluation d'un portefeuille numérique.

1.3.1 Types de portefeuilles numériques et mises en œuvre

Le terme « portefeuille numérique », qui est utilisé partout dans ce document, est un indicateur de la portée de cette composante du CCP. Cette composante met l'accent sur les portefeuilles numériques qui contiennent des identités numériques et des actifs connexes. Ces portefeuilles numériques sont conçus de façon à être optimisés pour aider leurs titulaires à gérer et à utiliser :

1. Les documents et attributs d'identité personnels (p. ex., preuve d'identité essentielle, numéros d'assurance sociale, passeports, permis de conduire,

cartes de santé publique, preuve de citoyenneté, preuve de résidence, preuve d'âge, etc.);
2. Les renseignements personnels à propos d'autres personnes proches et les relations avec elles (p. ex., preuve de relation conjugale avec une autre personne, preuve de garde de mineurs, preuve de statut d'emploi dans une organisation);
3. Les clés de chiffrement et de signature pour soutenir la vérification des attributs et la signature des documents numériques.

Les portefeuilles numériques peuvent aussi contenir et faciliter l'utilisation de :

1. Renseignements sur les paiements numériques (p. ex., cartes de crédit) pour divers services et sites Web;
2. Détails d'authentification (p. ex., noms d'utilisateurs/mots de passe) pour divers services et sites Web.

Étant donné ce chevauchement entre les portefeuilles numériques et les applications conçues exclusivement pour les paiements et les transactions financières numériques (p. ex., un portefeuille de cryptomonnaie en bitcoins), il se pourrait que certains critères de conformité spécifiés pour cette composante du CCP s'appliquent aux portefeuilles et applications utilisés exclusivement pour des paiements numériques. Toutefois, ce profil ne traitera pas explicitement de ces types de portefeuilles. De même, les applications qui fonctionnent strictement comme des gestionnaires de mots de passe ou des utilitaires pour remplir des formulaires ne sont pas considérées comme étant inclus dans la portée de cette composante du CCP.

La portée de cette composante du CCP n'est pas limitée à un modèle de mise en œuvre en particulier pour les portefeuilles d'identité numérique et elle spécifie les critères de conformité qui s'appliquent généralement à tous les portefeuilles numériques, qu'ils soient instaurés comme :

1. Des applications en mode naturel sur des téléphones intelligents et d'autres appareils mobiles,
2. Des applications Web progressives qui sont exécutées sur d'autres appareils,
3. Des applications traditionnelles hébergées sur le Web qui sont exécutées sur des serveurs.

La portée de cette composante du CCP n'est pas limitée aux portefeuilles numériques utilisés par un particulier. Elle inclut :

1. Les portefeuilles numériques conçus pour être utilisés par des personnes qui agissent pour leur propre compte ou des membres de leur famille ou encore qui représentent une entreprise ou un autre type d'organisation;

2. Les organisations qui ont besoin de contrôler les portefeuilles numériques d'entreprise que leurs employés et représentants peuvent utiliser à des fins autorisées.

1.3.2 Sujets inclus dans la portée

Cette composante du CCP inclut les sujets suivants :

1. Qualité des produits et services : du point de vue de la confiance, les processus de développement, de distribution et de soutien du titulaire utilisés pour mettre en place et soutenir un portefeuille numérique sont des aspects essentiels. L'essai et la validation des portefeuilles numériques par de tierces parties et l'attribution de marques de confiance peuvent améliorer la fiabilité des portefeuilles numériques. Pour les applications Web progressives et les portefeuilles hébergés sur le Web, la composante « Infrastructure » (technologie et opérations) du CCP devrait s'appliquer à ces services d'hébergement.
2. Les capacités fonctionnelles suivantes des portefeuilles numériques et des normes sont incluses dans la portée :
    1. Authentification du titulaire pour ouvrir et utiliser un portefeuille numérique, et lui donner un consentement, notamment l'authentification biométrique et du NIP d'un téléphone mobile, les mécanismes d'authentification multifacteurs, et les mécanismes de nom d'utilisateur et de mot de passe.
    2. Capacité pour les portefeuilles numériques d'authentifier les émetteurs et vérificateurs de justificatifs, ainsi que les registres de données associés.
    3. Normes technologiques de gestion essentielles pour gérer et entreposer en sécurité des clés publiques et privées, notamment la capacité facultative d'exporter, d'importer et de sauvegarder/récupérer des clés.
    4. Normes technologiques pour la gestion des justificatifs pour gérer et entreposer d'une manière sécuritaire les justificatifs des portefeuilles numériques, notamment la capacité facultative d'exporter, d'importer et de sauvegarder/récupérer des justificatifs, et de soutenir l'image de marque et les politiques des émetteurs.
    5. Capacité pour les portefeuilles numériques d'entreposer et de présenter des jetons d'attestation provenant d'émetteurs établis ou existants.
    6. Normes technologiques pour les demandes et la prestation aux émetteurs, notamment les signatures numériques.
    7. Normes technologiques pour la présentation des justificatifs aux vérificateurs, notamment les signatures numériques.
    8. Soutien d'une divulgation minimale.
    9. Dialogue avec le titulaire pour soutenir des décisions éclairées de divulguer ou non, incluant le dialogue de consentement.
3. Normes d'accessibilité et d'inclusivité applicables aux portefeuilles numériques.
4. Format d'affichage en langage clair et standard (c.-à-d., représentation du portefeuille et des cartes).
5. Capacité multilingue.

6. Consentement informé et traçable, et consignation et signalement des activités et de l'historique.

Remarque : L'aperçu et 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 territoire.

1.3.3 Sujets exclus de la portée

Les sujets suivants sont considérés comme étant exclus de la portée de cette composante :

1. Normes, processus et politiques technologiques applicables aux émetteurs et aux vérificateurs de justificatifs, sauf lorsqu'ils sont directement reliés à la fonctionnalité du portefeuille.
2. Normes, processus et politiques technologiques applicables aux registres de données vérifiables, sauf lorsqu'ils sont directement reliés à la fonctionnalité du portefeuille.
3. Normes, processus et politiques technologiques applicables aux essais et à la validation par des tierces parties des portefeuilles numériques pour les besoins de l'émission de marques de confiance.

1.4 Relation avec le Cadre de confiance pancanadien

Le Cadre de confiance pancanadien consiste en une série de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées d'une manière indépendante pour être prises en considération comme composantes de confiance. Le CCP, qui tire parti d'une approche pancanadienne, permet aux secteurs public et privé de collaborer pour protéger les identités numériques en uniformisant les processus et pratiques dans tout l'écosystème numérique canadien.

Remarque : La composante « Portefeuille numérique » recoupe partiellement les composantes « Authentification », « Avis et consentement » et « Justificatifs (relations et attributs) ». Cette composante du CCP représente donc un point d'intersection entre plusieurs autres composantes et élargit les critères de conformité pour inclure un outil spécifique qui est mis à la disposition des participants aux écosystèmes de l'identité numérique.

La figure 1 est une illustration des composantes de l'ébauche du Cadre de confiance pancanadien.

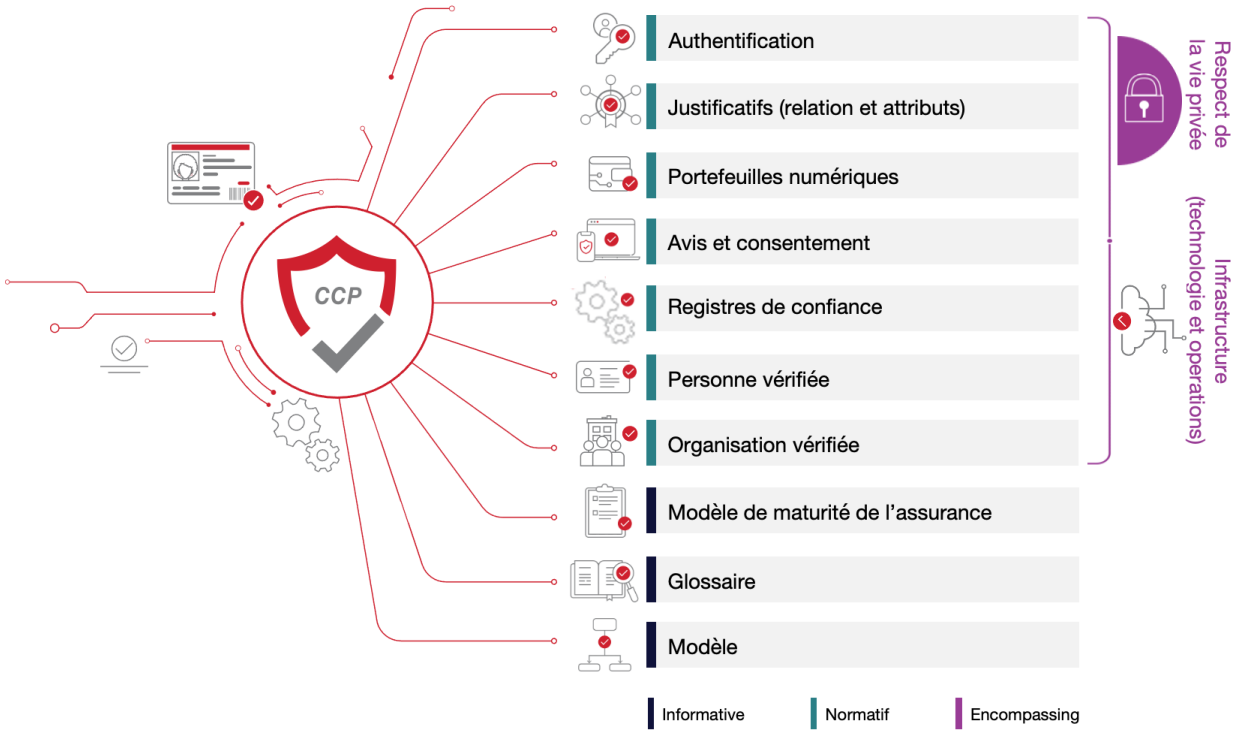

Figure 1. Composantes du Cadre de confiance pancanadien

2. Conventions

Cette section décrit et définit les termes et notions essentiels utilisés dans la composante « Portefeuille numérique » du CCP. Ces renseignements sont fournis pour assurer une utilisation et une interprétation uniformes des termes qui apparaissent dans cet aperçu et dans le profil de conformité « Justificatifs (relations et attributs) » du CCP.

Remarques :

- Les conventions peuvent varier entre les composantes du CCP. Les lecteurs sont invités à examiner les conventions de chacune des composantes du CCP qu'ils consultent.
- Les principaux termes et concepts décrits et définis dans cette section, la section sur les processus de confiance et le glossaire du CCP sont écrits avec une majuscule tout au long de ce document.
- Il se pourrait que des liens hypertextes soient intégrés dans les versions électroniques de ce document. Tous les liens étaient accessibles lors de la rédaction.

2.1 Termes et définitions

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

Attestation

- Vérification de confiance comme quoi une chose est véridique ou authentique.

Attribut

- Un attribut est de l'information reliée à une partie caractéristique ou inhérente d'une entité (p. ex. le prénom ou l'adresse résidentielle d'un sujet). Les attributs sont parfois appelés des « propriétés » ou « revendications ». Les attributs sont entreposés dans les justificatifs.

CLUF ou contrat de licence d'utilisateur final

- Contrat entre un producteur de logiciel et l'éventuel utilisateur du produit, qui spécifie les conditions d'utilisation.

Divulgation sélective

- Un justificatif peut contenir de multiples revendications comme paires de valeurs clés. Par exemple, le vocabulaire citoyen proposé par le W3C inclut le prénom, le nom de famille, le sexe, l'image et la date de naissance entre autres éléments de données dans le schéma des justificatifs. Par principe, la minimisation des données devrait être utilisée chaque fois que possible pour limiter le partage des renseignements personnels. Une preuve d'âge avec minimum de données fournie à un vérificateur, dans l'exemple ci-dessus, pourrait inclure uniquement la date de naissance du titulaire et possiblement une photo.
- Des techniques cryptographiques à divulgation nulle de connaissance peuvent être employées pour créer une preuve de divulgation sélective basée sur le justificatif d'origine avec des éléments de données aveuglés que le titulaire ne veut pas ou n'a pas besoin de partager avec un vérificateur et/ou une partie dépendante. La preuve est agencée de façon que le titulaire puisse encore prouver au vérificateur que le justificatif a été signé par l'émetteur et que les données présentées n'ont pas été falsifiées. Les mécanismes de signature ordinaires incluent les signatures CL, les signatures BBS+ et les mécanismes basés sur SNARK.
- Une utilisation puissante de la divulgation sélective est aveugle à l'identifiant de liaison qui est commun à un groupe de justificatifs émis. Cela réduit le risque de suivi de l'activité du titulaire, car le secret qui fait le lien n'est pas divulgué au vérificateur.

Remarque : La divulgation sélective peut être faite par d'autres méthodes comme l'émission juste à temps des justificatifs ou l'utilisation d'un courtier de confiance. Ces

méthodes ne sont pas recommandées, car on peut retracer toute l'activité d'un utilisateur jusqu'à une source unique – l'émetteur ou le courtier.

Entrepôt sécurisé

- L'entrepôt sécurisé est un endroit utilisé pour assurer la sécurité, la confidentialité et l'intégrité des données qui y sont gardées. Cet endroit peut dépendre de la protection physique du matériel dans lequel les données sont entreposées, ainsi que du logiciel de sécurité. Les données gardées dans un entrepôt sécurisé ne peuvent en être retirées ou peuvent être uniquement récupérées par des parties autorisées.
- *Voir aussi* https://www.techopedia.com/definition/29701/secure-data-storage.

Jeton

- Représentation numérique d'une attestation ou d'un conteneur pour une ou des revendications.

Justificatif

- Un justificatif est un ensemble d'une ou de plusieurs revendications faites par une seule entité à propos d'un sujet (p. ex., le sujet a un permis de conduire; le sujet réside à une adresse spécifique; le sujet a une certification spécifique). Dans ce document, le terme « justificatifs » n'inclut pas les justificatifs d'authentification, sauf si le terme « justificatifs d'authentification » est employé explicitement (voir aussi Justificatif vérifiable).

Justificatif vérifiable

- Un justificatif vérifiable est un justificatif inviolable qui est codé de manière à ce que son intégrité et sa paternité (c.-à-d., source) soient confirmées par vérification cryptographique. Les justificatifs vérifiables doivent être sûrs du point de vue cryptographique et vérifiables à l'aide de machines.

Liaison cryptographique (voir aussi Liaison forte)

- Association de deux éléments d'information ou davantage à l'aide de techniques cryptographiques.

Liaison forte (voir aussi Liaison cryptographique)

- Association étroite d'un titulaire avec des éléments de données vérifiées entreposées dans un portefeuille à l'aide d'un authentificateur.

Portefeuille d'identité numérique (portefeuille, portefeuille numérique)

- Un portefeuille numérique est un référentiel de justificatifs basé sur un logiciel qui entrepose d'une manière sécuritaire des renseignements pour un titulaire. Selon la nature du portefeuille, celui-ci peut contenir, entre autres, des justificatifs, des justificatifs vérifiables, des renseignements sur des paiements et/ou des mots de passe. Un portefeuille sert à entreposer d'une manière sécuritaire des justificatifs et/ou attributs d'identité, et à permettre au titulaire d'assembler et de préparer des présentations vérifiables. Il arrive que certains portefeuilles aient des moyens de prouver l'identité et/ou des agents pour faciliter le partage des justificatifs qu'ils gèrent.

Prédicat dérivé (voir aussi Preuves à divulgation nulle de connaissance)

- Un prédicat dérivé est une assertion booléenne vérifiable à propos d'un sujet qui est basée sur la valeur d'un autre attribut décrivant ce sujet. Prenons, par exemple, un sujet qui souhaite prouver qu'il est admissible à des services uniquement disponibles pour des personnes qui sont âgées d'au moins 21 ans et qui possèdent un justificatif contenant un attribut qui renferme leur date de naissance. Plutôt que de fournir sa date de naissance comme preuve d'admissibilité, le sujet pourrait présenter un prédicat dérivé comme « plus de 21 ans » qui contient une valeur « Vrai » ou « Faux » indiquant si le sujet est âgé de plus de 21 ans. L'utilisation de prédicats dérivés protège mieux la vie privée d'un sujet en ne divulguant pas de renseignements personnellement identifiables, tout en permettant à un vérificateur de valider l'admissibilité d'un sujet à un service.

Présentation

- Une présentation est un ensemble de données, représentant généralement une ou plusieurs revendications à propos d'un sujet, qui sont dérivées d'un ou de plusieurs justificatifs, justificatifs vérifiables, relations endossées ou relations vérifiables et partagées avec un vérificateur.

Présentation vérifiable

- Une présentation vérifiable est une présentation inviolable qui est codée de manière à ce que son intégrité et sa paternité (c.-à-d., source) soient confirmées par vérification cryptographique.

Preuves à divulgation nulle de connaissance

- Une preuve à divulgation nulle de connaissance est une technique cryptographique qui permet au titulaire de prouver à un vérificateur qu'il connaît une valeur sans la partager en fait.

- Une preuve à divulgation nulle de connaissance peut être utilisée dans le contexte de l'identité numérique pour soutenir les fonctionnalités essentielles de préservation de la vie privée suivantes :
    - Divulgation sélective – divulgation d'un sous-ensemble d'attributs d'un justificatif à un émetteur.
    - Prédicats – calculs sur des attributs comme étant égal ou supérieur à (p. ex., prouver que votre salaire est supérieur à x ou que votre âge est plus grand que y) où les valeurs réelles ne sont pas partagées avec le vérificateur.
    - Aveuglement de la signature – randomisation de la signature de l'émetteur avant de la partager avec le vérificateur pour éliminer la signature en tant que facteur de corrélation y) où les valeurs réelles ne sont pas partagées avec le vérificateur.
    - Aveuglement du titulaire privé – l'identifiant de corrélation n'est pas exposé au vérificateur.

Référentiel / référentiel de justificatifs

- Un référentiel est un système logiciel (application) tel qu'une base de données, voûte d'entreposage ou portefeuille de justificatifs vérifiable qui entrepose les justificatifs vérifiables d'un titulaire et en contrôle l'accès.

Registre de données vérifiables

- Rôle qu'un système peut jouer en faisant la médiation dans la création et la vérification des identifiants, clés et autres données pertinentes, comme des schémas de justificatifs vérifiables, registres de révocation, clés publiques d'émetteurs et ainsi de suite, qui peuvent être nécessaires pour utiliser des justificatifs vérifiables.
- (Référence : https://www.w3.org/TR/vc-data-model/#dfn-verifiable-data-registries)

Relation

- Une relation est un type spécifique de justificatif qui décrit la façon dont deux entités ou plus sont reliées entre elles (p. ex., Fatima est doctorante à l'Université de la Colombie-Britannique; Éric travaille pour FictitiousCorp; Sheila est un membre en règle de la Société de droit).

Rendu de justificatif

- La stylisation de la présentation visuelle de divers types et données d'entités (p. ex., justificatifs) est un besoin commun qui existe dans bien des cas d'utilisation. Afin de fournir une série prévisible d'indices de stylisation et d'affichage de données aux agents utilisateurs, émetteurs, vérificateurs et autres participants

qui rendent l'IU associée à des entités et données, cette spécification s'efforce d'uniformiser un modèle de données ordinaire pour décrire des indices de style et données génériques qui peuvent être utilisés avec n'importe quelle formulation d'éléments IU.

Revendication

- Une revendication est une assertion faite à propos d'un sujet (p. ex., le sujet a un permis de conduire; le sujet est âgé de plus de 21 ans; le sujet a été incorporé dans la province de l'Ontario).

Vérification des justificatifs

- La vérification des justificatifs est l'évaluation qui consiste à déterminer si un justificatif vérifiable ou une présentation vérifiable représente d'une manière authentique l'émetteur ou le sujet. Cela inclut la vérification comme quoi la preuve est satisfaite (normalement au moyen d'une validation cryptographique), la confirmation que le justificatif ou la présentation est valide (p. ex., elle n'est pas suspendue, révoquée ou expirée) et que le justificatif ou la présentation se conforme aux spécifications et/ou aux normes pertinentes.

2.2 Abréviations

Les abréviations et acronymes suivants apparaissent tout au long de cet aperçu et dans le profil de conformité « Justificatifs (relations et attributs) » du CCP :

- **CCP :** Cadre de confiance pancanadien
- **NAJ :** Niveau d'assurance des justificatifs
- **DID :** Identifiant décentralisé
- **PDNC :** Preuves à divulgation nulle de connaissance

2.3 Rôles

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

Remarques

- Une entité peut assumer un ou plusieurs rôles, selon le cas d'utilisation. Par exemple, une entité qui est la partie dépendante dans une transaction peut aussi être le vérificateur de cette transaction.
- Les définitions des rôles n'impliquent ou ne nécessitent pas une solution, une architecture, une mise en œuvre ou un modèle de gestion spécifique.

Autorité qui révoque

- Une autorité qui révoque est une entité avec une responsabilité exclusive ou principale pour révoquer des justificatifs et maintenir des renseignements à propos des justificatifs révoqués. L'autorité qui révoque peut être l'émetteur du justificatif révoqué, mais ce n'est pas obligatoire.

Demandeur

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

Émetteur

- Un émetteur est une entité qui fournit de l'information concernant un sujet en créant et en émettant un justificatif, un jeton d'attestation ou un justificatif vérifiable (p. ex., une province ou un territoire qui délivre un permis de conduire).

Remarque : Cette définition permet à une entité de créer et d'émettre des justificatifs, y compris le sujet.

Partie dépendante

- Une partie dépendante est une entité qui consomme de l'information, des attributs, des relations ou autres justificatifs reliés à l'identité numérique pour effectuer des transactions numériques (p. ex., un magasin d'alcools ou un propriétaire de commerce qui a besoin de s'assurer qu'un client est assez âgé pour acheter de l'alcool). Voir Vérificateur ci-dessous.

Titulaire

- Un titulaire est une entité qui possède un ou plusieurs justificatifs. Le titulaire est habituellement le sujet du justificatif, mais il n'a pas besoin de l'être (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 entreposer les justificatifs qu'ils possèdent dans un référentiel.

Vérificateur

- Un vérificateur est une entité qui reçoit un ou plusieurs jetons d'attestation et justificatifs vérifiables, et qui détermine si le ou les justificatifs représentent d'une manière authentique et exacte l'émetteur ou le sujet (voir Vérification des justificatifs). Un vérificateur est une partie dépendante qui consomme et vérifie

les renseignements d'identité numériques sous la forme de jetons d'attestation ou de justificatifs vérifiables.

3. Relations de confiance

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

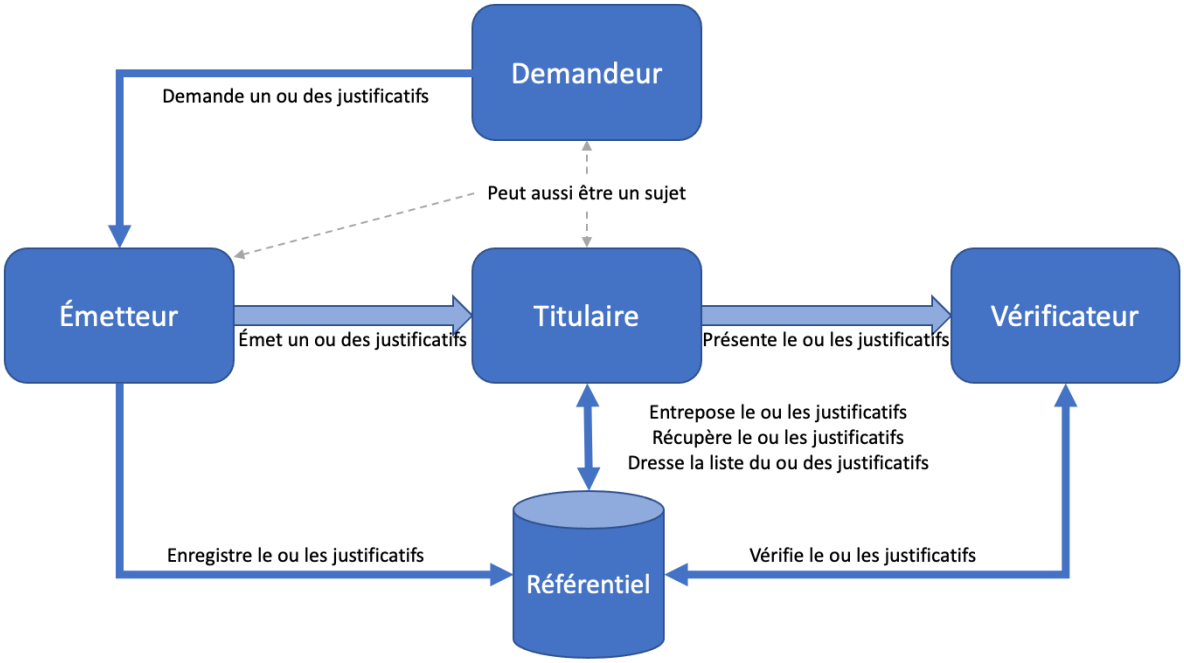

Figure 2. Rôles et relations dans le portefeuille numérique (illustration)

Il est à noter que cette composante a été élaborée en tenant compte du travail qui a donné lieu au modèle de données des justificatifs vérifiables W3C, au profil du secteur public du Cadre de confiance pancanadien et au projet Hyperledger Aries.

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

Cette composante conseille aux participants à l'écosystème numérique de 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 s'assurer qu'ils sont méticuleux lorsqu'ils déterminent l'exactitude des renseignements inclus 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 c'est autorisé par la loi ou les règlements.
3. Les participants doivent pouvoir déterminer si les justificatifs émis contiennent des renseignements exacts qui sont fiables et à jour.
4. Les participants doivent avoir l'assurance que les émetteurs ont adopté et mis en place à l'intérieur des justificatifs des structures de données qui protègent la vie privée pour réduire le risque de corrélation qui pourrait résulter si un vérificateur demande plusieurs justificatifs à propos d'un sujet, qu'ils soient délivrés par un ou plusieurs émetteurs de justificatifs.
5. Les participants doivent avoir l'assurance qu'on s'occupe d'une manière appropriée et opportune des justificatifs compromis ou non valides, et que les justificatifs 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 des registres vérifiables, ne sont pas utilisés par un fournisseur de services ou un vérificateur sauf :
    1. comme signifié par le consentement express du sujet, ou
    2. comme signifié par le consentement express d'une entité autorisée à agir pour le compte du sujet, ou
    3. lorsque la loi ou un règlement l'autorise.

Par exemple, les participants ne doivent pas utiliser les justificatifs qui leur ont été confiés pour :

- représenter les sujets, ou
- s'entendre avec d'autres participants pour agréger ou partager des renseignements sans avoir un tel consentement.

4. 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 d'autres processus dépendent souvent. Une condition est un état ou une circonstance en particulier qui sont pertinents à un processus de confiance. Une condition peut être un intrant, un extrant ou une dépendance relative à un processus de confiance. Les critères de conformité spécifient ce qui est nécessaire pour transformer une condition d'entrée en condition de sortie. Les critères de conformité spécifient, par exemple, ce qui est nécessaire pour que le processus d'enregistrement du portefeuille d'identité numérique transforme une condition d'entrée du portefeuille d'identité numérique vérifiable en condition de sortie du portefeuille d'identité numérique.

Un processus est désigné comme étant de confiance quand 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 peuvent dépendre du résultat du processus, souvent par-delà les frontières territoriales, organisationnelles et sectorielles, et souvent à court et long terme.

La composante « Portefeuille numérique » du CCP définit les processus de confiance suivants en trois grandes catégories :

Processus d'instanciation et de sécurité du portefeuille

1. Création du portefeuille numérique
2. Enregistrement du portefeuille numérique
3. Authentification

Processus de gestion et d'utilisation des justificatifs

1. Demande de justificatif vérifiable
2. Entreposage du justificatif vérifiable
3. Gestion du justificatif vérifiable
4. Présentation du justificatif vérifiable
5. Rendu du justificatif vérifiable
6. Présentation de la preuve

Processus de gestion du consentement

1. Inclus dans le processus de présentation de la preuve

4.1 Aperçu conceptuel

Les figures 3 et 4 donnent un aperçu conceptuel, et l'organisation logique, des processus de confiance du portefeuille numérique du CC.

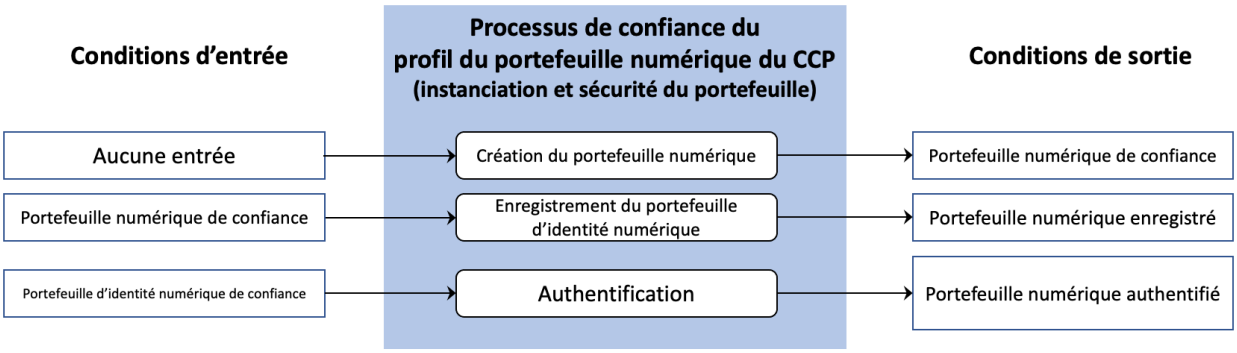

Figure 3 : Processus de confiance pour l'instanciation et la sécurité du portefeuille numérique

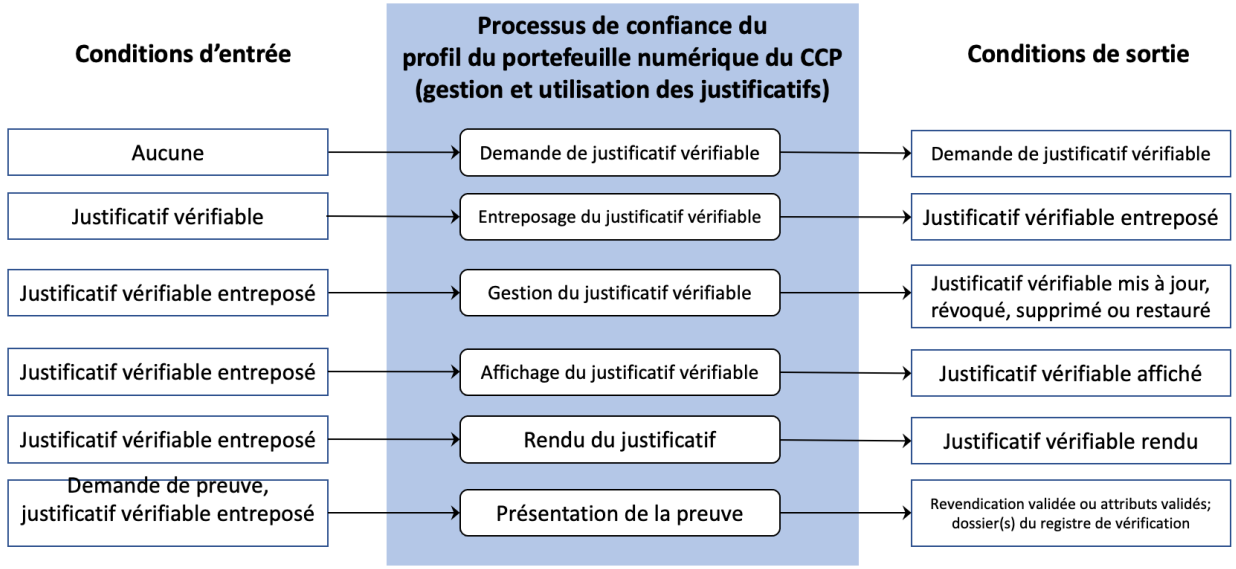

Figure 4 : Processus de confiance pour la gestion et l'utilisation des justificatifs du portefeuille numérique

4.2 Descriptions des processus

Les sections qui suivent définissent les processus de confiance de la composante « Portefeuille d'identité numérique » du CCP. Le profil de conformité du portefeuille d'identité numérique du CCP spécifie les critères de conformité d'après lesquels ces processus peuvent être évalués.

Les processus de confiance sont définis en utilisant la structure suivante :

1. **Description :** Aperçu descriptif du processus
2. **Intrants :** Données qui sont consommées et/ou exploitées par le processus

3. **Extrants :** Données qui sont créées par le processus
4. **Dépendances :** Autres processus qui doivent être exécutés avant celui qui est décrit dans la section, normalement parce qu'ils produisent un ou plusieurs intrants requis

4.2.1 Processus d'instanciation et de sécurité du portefeuille

Création du portefeuille numérique

La création du portefeuille numérique est le processus qui consiste à créer un portefeuille pouvant être vérifié par un vérificateur. La création peut impliquer l'installation d'un logiciel sur un appareil mobile ou non mobile ou à générer une instance de portefeuille sur un serveur.

Intrants	Aucun
Extrants	Portefeuille numérique de confiance
Dépendances	Aucune dépendance

Enregistrement du portefeuille numérique

L'enregistrement du portefeuille numérique est le processus selon lequel le titulaire d'un portefeuille établit une relation (ou « se connecte ») avec un émetteur, un vérificateur ou un registre de données vérifiables. Une fois ce processus terminé, le titulaire aura un portefeuille numérique enregistré qui peut être géré d'une façon persistante par le service d'enregistrement de l'émetteur, du vérificateur ou du registre de données vérifiable.

Cet enregistrement vise à faire en sorte que tous les participants puissent choisir ce qu'ils sont disposés à soutenir et à accepter. Exemples :

1. Un titulaire peut choisir d'enregistrer (« connecter ») un portefeuille avec un émetteur, un vérificateur ou un registre de données vérifiables.
2. Un vérificateur peut choisir d'accepter un tel enregistrement (« connexion ») venant d'un portefeuille.
3. Un émetteur peut choisir d'accepter un enregistrement d'un portefeuille qui se qualifie selon certains critères prédéfinis.

Remarque : Cet enregistrement peut survenir de nombreuses fois, car il peut se faire entre un portefeuille et un certain nombre d'autres parties. Cet enregistrement peut être un processus assez léger. Par exemple, il peut s'agir de quelque chose aussi simple qu'un échange de clés entre deux parties qui se connectent pour la première fois.

Intrants	Portefeuille numérique de confiance
Extrants	Portefeuille numérique enregistré
Dépendances	Création d'un portefeuille numérique

Authentification

Ce processus établit un contrôle de l'authentification qui permet à un propriétaire de lier des justificatifs à un portefeuille numérique. Cette liaison assure que le propriétaire contrôle le portefeuille numérique et est autorisé à posséder, contrôler et présenter les justificatifs qui sont liés à ce portefeuille.

L'extrant de ce processus doit être vérifiable du point de vue cryptographique.

Intrants	Portefeuille numérique de confiance
Extrants	Portefeuille numérique authentifié
Dépendances	Aucune dépendance

4.2.2 Processus de gestion et d'utilisation des justificatifs

Demande de justificatif vérifiable

Dans le cadre de ce processus, un titulaire de portefeuille demande un justificatif à un émetteur. L'assurance de la demande peut être améliorée en vérifiant les attributs du portefeuille d'identité numérique, un dossier de personne vérifiée et le dossier du lien comme prérequis à la demande de justificatif.

Remarque : Cette définition du processus permet intentionnellement à un portefeuille de demander un justificatif vérifiable qui est émis par le sujet, lequel peut être l'utilisateur du portefeuille. De tels justificatifs sont décrits comme étant « auto-émis » ou « auto-attestés ».

Intrants	Aucun
Extrants	Demande de justificatif vérifiable
Dépendances	Création d'un portefeuille numérique

Entreposage d'un justificatif vérifiable

Dans le cadre de ce processus, un justificatif vérifiable est obtenu et entreposé par un portefeuille numérique. Dans les cas où des niveaux d'assurance élevés sont

nécessaires, des processus et technologies peuvent être mis en place comme prérequis pour obtenir le justificatif.

Intrants	Justificatif vérifiable
Extrants	Justificatif vérifiable entreposé
Dépendances	Création du portefeuille numérique, demande de justificatif vérifiable

Gestion des justificatifs vérifiables

Le CCP reconnaît la nature dynamique des justificatifs qui peuvent être entreposés dans un portefeuille numérique. Le processus de gestion des justificatifs vérifiables assure que les justificatifs et les attributs entreposés dans les portefeuilles numériques contiennent des renseignements exacts et opportuns. Dans le cadre du processus de gestion des justificatifs vérifiables, un justificatif vérifiable qui est obtenu et accessible par un portefeuille d'identité numérique peut être :

1. Mis à jour : Les attributs d'un justificatif vérifiable sont actualisés par l'intermédiaire de l'émetteur du justificatif
2. Révoqué : La procédure déclenchée par un émetteur pour révoquer un justificatif vérifiable et aviser le titulaire du justificatif vérifiable
3. Expiré : La procédure déclenchée par un émetteur pour l'avis, et l'expiration, d'un justificatif expiré
4. Restauré : La procédure utilisée par un émetteur ou un titulaire de portefeuille d'identité numérique pour restaurer un justificatif vérifiable
5. Supprimé : La procédure utilisée par un titulaire de portefeuille d'identité numérique pour supprimer un justificatif vérifiable

Ces fonctions ne devraient être mises à la disposition que du titulaire légitime des justificatifs (c.-à-d., le propriétaire lié au portefeuille d'identité numérique).

Intrants	Justificatif vérifiable entreposé
Extrants	Justificatif vérifiable mis à jour, révoqué, supprimé ou restauré
Dépendances	Entreposage du justificatif vérifiable

Présentation du justificatif vérifiable

Ce processus récupère un justificatif dans un portefeuille numérique et le présente pour le titulaire.

Intrants	Justificatif vérifiable entreposé

Extrants	Justificatif vérifiable présenté
Dépendances	Entreposage du justificatif vérifiable, rendu du justificatif vérifiable

Rendu du justificatif vérifiable

Ce processus établit un état ou une condition en particulier pour un justificatif obtenu et le présente dans un format qui peut être lu et compris par une personne.

Intrants	Justificatif vérifiable entreposé
Extrants	Justificatif vérifiable rendu
Dépendances	Entreposage du justificative vérifiable

Présentation de la preuve

Un portefeuille numérique doit être capable de présenter la preuve des revendications (justificatifs signés) du titulaire (c.-à-d., le titulaire du portefeuille) à un vérificateur dans un format compatible pour satisfaire une demande de preuve d'un vérificateur. Les principales considérations de compatibilité incluent le format des justificatifs, le mécanisme de signature, l'émetteur acceptable pour chaque revendication demandée et si la divulgation sélective est soutenue ou non. Idéalement, le portefeuille (et l'émetteur) soutiendra un processus de négociation bilatéral qui satisfait les politiques du portefeuille et du vérificateur contrairement à un échange unique fixe.

Une preuve est une présentation inviolable des revendications demandées que le vérificateur peut valider au moyen du processus cryptographique approprié. Si la divulgation sélective est soutenue, seules les revendications spécifiques demandées par le vérificateur peuvent alors être partagées. Sinon, la série complète de justificatifs nécessaires pour répondre à la demande de preuve peut être partagée. Celle-ci présente le risque que des renseignements personnels dont le vérificateur n'a pas besoin du point de vue commercial soient partagés.

Avant d'accepter une demande de preuve, le titulaire doit consentir à envoyer les renseignements demandés au vérificateur. Un registre d'audit, accessible par le titulaire, doit enregistrer l'heure de la transaction, les revendications demandées et présentées, les détails du vérificateur, l'état de réussite et le reçu, s'il est fourni. Le registre d'audit peut aussi persister et présenter une méthode pour examiner et révoquer le consentement.

Intrants	Demande de preuve, justificatif vérifiable entreposé
Extrants	Présentation vérifiable, register(s) d'audit

Dépendances	Entreposage du justificatif vérifiable

4.2.3 Processus de consentement

La composante « Avis et consentement » du CCP est la source qui fait autorité pour les critères de conformité de l'avis et du consentement. Les critères de conformité de l'avis et du consentement ne seront pas fournis dans le cadre des critères de conformité du portefeuille numérique, sauf s'ils sont uniques à l'interaction avec les portefeuilles numériques. La demande de consentement pour présenter une preuve de justificatif à un vérificateur est incluse dans le présent processus de preuve.

5. Références

Cette section fournit la liste des normes, lignes directrices et autres documents auxquels il est fait référence dans cette composante du CCP.

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

Cette composante du CCP tire parti des compétences, de l'expérience et des leçons apprises d'autres organisations qui œuvrent à améliorer ce domaine, et elle a pris en considération le matériel provenant des sources suivantes :

- Conseil stratégique des DPI : CAN/CIOSC 103-1:2020 Confiance et identité numériques – Partie 1 : Fondamentaux
- Gouvernement du Canada, Secrétariat du Conseil du Trésor du Canada : Profil du secteur public du Cadre de confiance pancanadien version 1.1
- W3C : Modèle de données de justificatifs vérifiables 1.0
- W3C : Identifiant décentralisés (DID)

6. Historique des révisions

Version	Date	Auteur(s)	Commentaire
0.01	01-17-2022	Équipe de conception du portefeuille numérique du CCP	Ébauche de discussion initiale créée par l'équipe de conception du portefeuille numérique du CCP
0.02	02-28-2022	Équipe de conception du portefeuille numérique du CCP	Version mise à jour pour incorporer la rétroaction du TFEC

0.03	2022-03-10	Équipe de conception du portefeuille numérique du CCP	Duplication du niveau d'assurance supprimée de l'aperçu, voir le profil de conformité
1.0	2022-03-30	Équipe de conception du portefeuille numérique du CCP	Le TFEC l'approuve comme recommandation préliminaire V1.0
1.1	2022-01-11	Équipe de conception du portefeuille numérique du CCP	Révisions initiales provenant de l'examen de l'utilisation des commentaires.
1.0	2023-01-18	Équipe de conception du portefeuille numérique du CCP	Le TFEC l'approuve comme candidat pour la recommandation finale V1.0
1.0	2023-04-19	Équipe de conception du portefeuille numérique du CCP	Approuvé en tant que recommandation finale V1.0 par vote du membre de soutien du CCIAN