« Registres de confiance » 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

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.

2. Raison d’être, contexte et portée

2.1 Raison d’être

Un registre de confiance vise à donner aux participants d’un écosystème de l’identité numérique les moyens de vérifier que les participants numériques de l’écosystème sont dignes de confiance. Les participants inscrits dans le registre de confiance incluent des émetteurs, vérificateurs, fournisseurs de portefeuilles et autres registres de confiance. Par exemple, si un émetteur figure dans un registre de confiance, cela indique aux parties intéressées (p. ex., les vérificateurs et titulaires) qu’ils peuvent faire confiance (dans une certaine mesure) à un émetteur en tant que fournisseur de justificatifs. Si un vérificateur figure dans un registre de confiance, cela indique aux titulaires qu’ils peuvent lui faire confiance pour recevoir des preuves de justificatifs. Si un fournisseur de portefeuille est un registre de confiance (peut-être comme émetteur de justificatifs de portefeuilles), cela indique alors aux participants (émetteurs, vérificateurs et titulaires) que le portefeuille numérique est digne de confiance. Les écosystèmes d’identité numérique et leurs registres de confiance associés utilisent un cadre de confiance (comme le CCP) pour déterminer la façon dont les émetteurs, les vérificateurs, les titulaires et les portefeuilles numériques devraient ou doivent fonctionner pour être considérés comme dignes de confiance.

Remarque : un écosystème d’identité numérique peut exploiter un registre de données vérifiables ou une technologie équivalente qui fournit des renseignements lisibles à la machine sur les justificatifs de l’écosystème pour permettre le traitement des justificatifs vérifiables et des présentations vérifiables. Les exigences relatives à un registre de données vérifiables ou une technologie équivalente n’entrent pas dans la portée de cette composante.

2.2 Contexte

Un registre de confiance est une composante essentielle de l’architecture de l’identité numérique décentralisée nouvelle et émergente. Dans une architecture décentralisée (ou autosouveraine), un portefeuille numérique reçoit des justificatifs vérifiables de la part d’émetteurs, après quoi il fournit des présentations de ces justificatifs aux

vérificateurs. Dans cette architecture, un registre de confiance fournit aux émetteurs, aux vérificateurs, aux titulaires et autres registres de confiance les renseignements nécessaires pour vérifier l'identité et le statut des autres parties dans l'écosystème.

Remarque : un émetteur, un vérificateur ou un titulaire peut faire partie de n'importe quel écosystème de l'identité numérique. Le diagramme conceptuel ci-dessous montre les parties avec lesquelles un registre de confiance interagit, mais il n'est pas conçu pour montrer les transferts de données d'une mise en œuvre technique spécifique. De même, les participants à un écosystème peuvent assumer un ou plusieurs rôles comme émetteurs, vérificateur et titulaire.

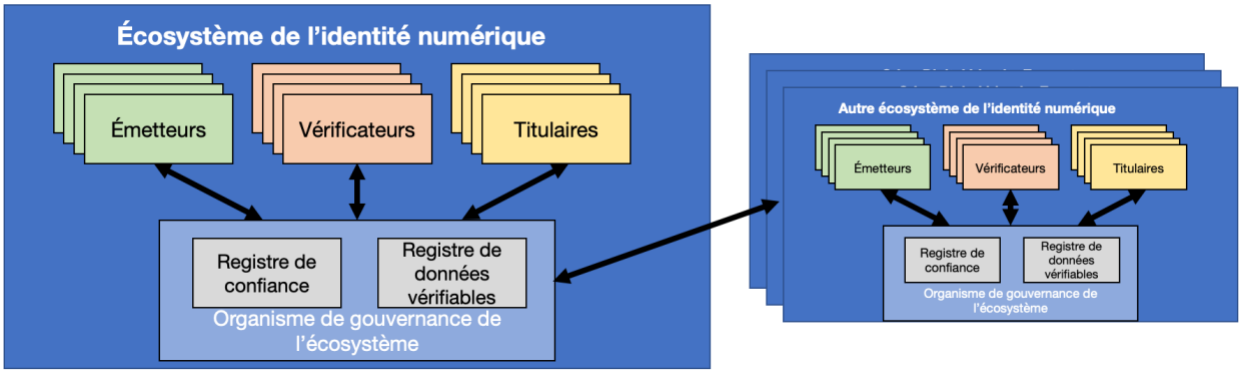

Figure 1. Écosystèmes de l'identité numérique

Les registres de confiance doivent à leur tour dépendre de sources d'identité numérique reconnues comme des organismes professionnels, des registres d'entreprises, des permis de conduire et des fournisseurs de cartes de santé. D'autres composantes du CCP définissent la façon dont ces sources fondamentales d'identité numérique devraient ou doivent être utilisées pour enregistrer des services numériques à l'intérieur du registre de confiance (voir la section 3 ci-dessous).

2.2.1 Exemple d'écosystèmes et de participants

Les exemples suivants d'écosystèmes de l'identité numérique sont énumérés afin de fournir au lecteur un contexte supplémentaire.

- Partout au Canada, les établissements d'enseignement postsecondaire peuvent mettre sur pied un organisme de gouvernance pour tenir un registre de confiance. Le registre de confiance pourrait avoir des établissements d'enseignement comme émetteurs des justificatifs du rôle et des études des étudiants et des professeurs (p. ex., relevés de notes et diplômes). Les entités qui ont besoin de valider un justificatif de rôle ou des études délivré par un établissement d'enseignement postsecondaire canadien seraient capables de consulter ce registre de confiance pour confirmer que l'émetteur du justificatif

était valide. Dans cet écosystème, les étudiants, les candidats aux études, les professeurs et les employés des établissements d'enseignement seraient les titulaires des justificatifs.

- Les secteurs des soins de santé peuvent mettre sur pied un organisme de gouvernance pour tenir un registre de confiance. Le registre de confiance pourrait avoir des organes professionnels (p. ex., Conseil médical du Canada) comme émetteurs de justificatifs professionnels pour les fournisseurs de soins de santé et les hôpitaux, laboratoires, pharmacies et organismes de soins de santé privés comme vérificateurs. Dans cet écosystème, les patients, les fournisseurs de soins de santé et les employés des services de soins de santé seraient les titulaires des justificatifs.
- Les associations professionnelles, comme le Barreau d'une province, peuvent établir un registre de confiance pour permettre à leurs membres d'accéder en sécurité à des services hébergés par des vérificateurs enregistrés qui sont reliés à leur profession.

Remarque : dans ces exemples, on s'attendrait à ce que ces écosystèmes dépendent à leur tour d'autres écosystèmes (et de leurs registres de confiance), qui incluent des justificatifs personnels et commerciaux délivrés par les émetteurs d'identité gouvernementaux.

2.2.2 Besoin d'interopérabilité

Étant donné qu'ils sont une exigence essentielle dans l'architecture d'identité décentralisée, avec son interrelation avec de nombreux titulaires, portefeuilles numériques, émetteurs, vérificateurs et autres registres de confiance, les écosystèmes doivent faire des efforts d'interopérabilité (au niveau local, régional et international). La conformité aux normes de l'industrie reconnues doit être un objectif important pour les organismes de gouvernance des écosystèmes et cela se reflète dans bien des critères de conformité pour les registres de confiance. En outre, le suivi des développements technologiques émergents sera une activité importante pour les organismes de gouvernance des écosystèmes afin de se préparer pour l'interopérabilité future.

2.3 Portée

2.3.1 Sujets inclus dans la portée

- Gouvernance des registres de confiance
  - Structure d'affaires – cadre juridique, objectifs commerciaux, frais, contrats et résolution des différends.
  - Portée de l'écosystème (émetteurs, vérificateurs, fournisseurs de portefeuilles, autres registres de confiance) – types et industries de services numériques soutenus par le registre.

    - Processus de gouvernance – qui exploite le processus de gouvernance et façon dont les décisions de gouvernance sont prises, communiquées et appliquées.
    - Politique et normes (cadre de confiance) – règles des services numériques soutenues par le registre et pour le registre comme tel, incluant l'autorisation d'émettre des justificatifs.
- Opérations du registre de confiance
    - Gestion de la technologie et de l'infrastructure – façon dont l'infrastructure technique d'un registre de confiance devrait être gérée (voir la composante Infrastructure du CCP (technologie et infrastructure)).
    - Services techniques – interfaces technologiques du registre qui sont fournies, schémas des inscrits, schémas des justificatifs et renseignements sur le statut des justificatifs qui sont fournis par le registre.
- Gestion de l'inscription et de la certification
    - Services de certification, de vérification et de marque de confiance – processus pour s'assurer que l'inscrit se conforme aux politiques et aux normes de l'écosystème.
    - Inscription – façon dont les inscrits sont identifiés et authentifiés/autorisés pour utiliser le registre (voir les composantes Personne vérifiée et Organisation vérifiée du CCP).
    - Certification et inscription de registres de confiance tiers.
    - Processus pour suspendre ou révoquer une inscription.

2.3.2 Sujets non inclus dans la portée

- Cette composante ne traite pas des exigences des registres d'identité essentielle dont dépendent les registres de confiance pour l'identification des identités, comme les registres d'entreprises, les permis de conduire et les registres de naissances.
- Les écosystèmes de l'identité numérique peuvent
    - limiter la portée de leur adhésion à un segment particulier de l'industrie. Cette composante ne fournit pas d'instructions sur la façon dont l'écosystème ou les écosystèmes pourraient choisir ou limiter la portée de leur adhésion.
    - avoir des politiques qui déterminent si les vérificateurs, les émetteurs, les produits des portefeuilles ou d'autres registres de confiance seront inscrits dans leur registre de confiance. Cette composante ne donne pas de consignes comme quoi ils devraient ou non être inscrits, mais seulement qu'ils peuvent être inclus au besoin et la façon dont ils devraient ou doivent être inscrits.
    - avoir des politiques qui régissent les justificatifs que les émetteurs enregistrés sont autorisés à fournir. Cette composante ne fournit pas d'orientation quant au fait qu'ils devraient ou non les fournir; elle indique

uniquement que ces politiques peuvent être incluses au besoin, y compris la façon dont cette autorisation serait vérifiée.
    - avoir des politiques qui permettent un accès anonyme (ou non) au registre de confiance. Cette composante ne donne pas de consignes comme quoi cela devrait être permis ou non, mais seulement qu'un accès anonyme peut être permis au besoin.
- Les exigences pour les registres de données vérifiables et les technologies équivalentes ne sont pas incluses dans la portée.

3. Relation avec le cadre de confiance pancanadien

Le CCP consiste en un ensemble de composantes modulaires ou fonctionnelles pouvant 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 préserver les identités numériques en uniformisant les processus et les pratiques à l'échelle de l'écosystème numérique canadien.

Cette composante fait référence à d'autres composantes du CCP pour définir la technologie, les opérations et les processus de gestion attendus du registre de confiance comme suit :

- La composante Authentification du CCP définit la façon dont le registre de confiance devrait/doit authentifier les utilisateurs des services numériques du registre de confiance.
- La composante Avis et consentement du CCP définit la façon dont le registre de confiance devrait fournir l'avis et le consentement concernant la gestion des renseignements.
- La composante Portefeuille numérique du CCP définit la façon dont le portefeuille numérique devrait/doit utiliser un registre de confiance.
- La composante Personne vérifiée du CCP définit la façon dont le registre de confiance devrait identifier les parties qui s'enregistrent et les autres utilisateurs des services numériques du registre de confiance.
- La composante Organisation vérifiée du CCP définit la façon dont le registre de confiance devrait identifier les organisations (et les parties autorisées à s'enregistrer) qui sont en train d'être enregistrées.

Comme pour les autres composantes du CCP, cette composante ne spécifie pas une infrastructure technologique en particulier.

La figure 2 est une illustration des composantes du cadre de confiance pancanadien.

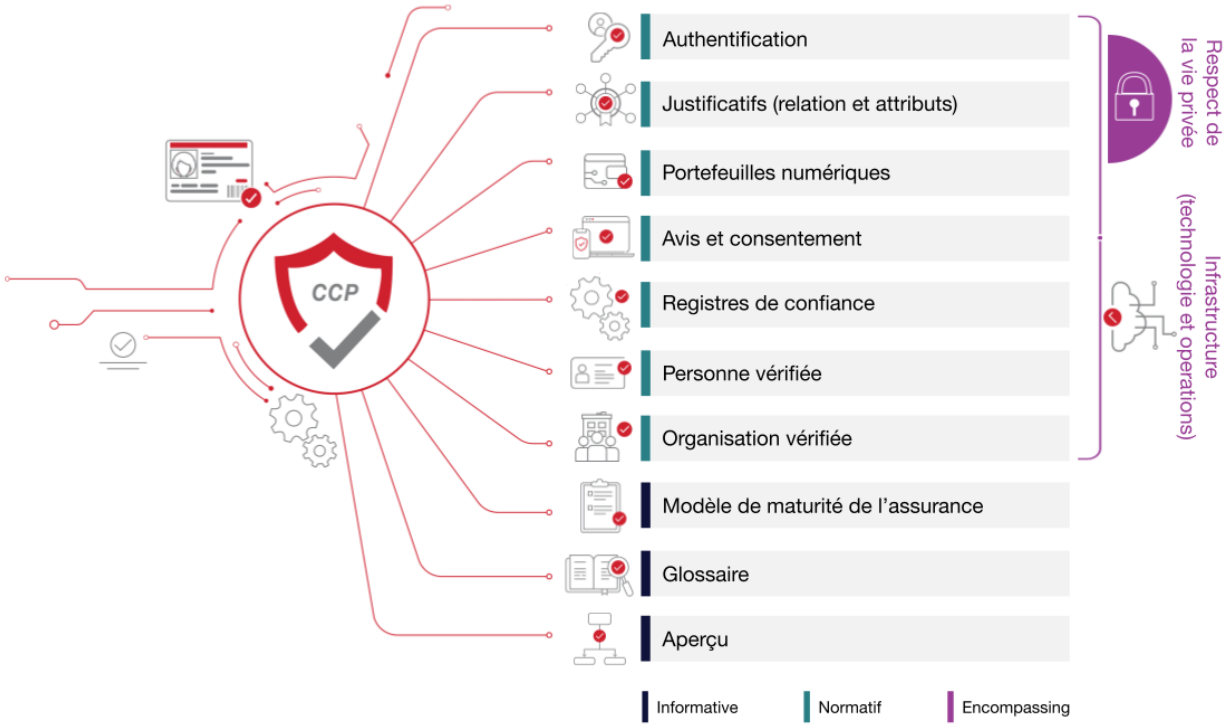

Figure 2. Composantes du cadre de confiance pancanadien

4. Conventions

Cette section décrit et définit les principaux termes et notions utilisés dans la composante « Registres de confiance » 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 des registres de confiance du CCP.

Remarques :

- Les conventions peuvent varier entre les composantes du CCP. Les lecteurs sont invités à examiner les conventions de chaque composante du CCP qu'ils lisent.
- Les principaux termes et notions décrits et définis dans cette section et le glossaire du CCP sont écrits avec une majuscule initiale dans tout le document.
- Il se pourrait que des liens hypertextes soient intégrés dans les versions électroniques de ce document. Tous les liens étaient accessibles au moment de la rédaction.

4.1 Abréviations

L'acronyme ci-dessous apparaît dans cet aperçu :

- **CCP :** Cadre de confiance pancanadien

4.2 Termes et définitions

Écosystème de l'identité numérique (aussi appelé réseau)

- Organisation officielle de participants à l'identité numérique (entités) qui exploitent un registre de confiance. Comme défini dans la Recommandation finale du glossaire du CCP V1.0, il s'agit d'un réseau interrelié pour l'échange et la vérification des renseignements d'identité numérique impliquant des organisations des secteurs public et privé qui se conforment à un cadre de confiance commun pour la gestion et l'utilisation des identités numériques, et les sujets de ces identités numériques.

Émetteur

- Inscrit qui peut affirmer des revendications à propos des titulaires, créer des justificatifs à partir de ces revendications et envoyer ces justificatifs aux titulaires.

Entité

- Comme défini dans la Recommandation finale du glossaire du CCP V1.0, chose qui a une existence séparée et distincte, et qui peut être identifiée dans un contexte. Dans ce contexte, une entité est un écosystème de l'identité numérique, un émetteur, un titulaire ou un vérificateur (et une entité peut remplir un ou plusieurs de ces rôles dans l'écosystème).

Fournisseur de portefeuille numérique

- Entité qui développe des produits de portefeuilles numériques destinés à être utilisés par les titulaires. Les fournisseurs de portefeuilles numériques peuvent être des émetteurs de justificatifs destinés à des portefeuilles numériques pour prouver l'authenticité du portefeuille aux émetteurs et aux vérificateurs.

Gouvernance du registre de confiance (gouvernance de l'écosystème)

- Processus de gestion qui définissent la mission, les politiques, les procédures et les normes d'un écosystème et de son registre de confiance.

Inscrit

- Entité qui est enregistrée dans un registre de confiance. Les inscrits sont des émetteurs, des vérificateurs, des fournisseurs de portefeuilles numériques et autres registres de confiance.

Justificatif

- Un justificatif est un ensemble d'une ou de plusieurs revendications faites à propos d'un sujet par un émetteur. On parle aussi de justificatifs vérifiables. La provenance d'un justificatif vérifiable peut être vérifiée d'une manière cryptographique. Les présentations des justificatifs vérifiables peuvent aussi être vérifiées d'une manière cryptographique.

Opérations du registre de confiance

- Processus commerciaux et technologiques utilisés pour gérer le contenu de l'infrastructure et de l'information du registre de confiance, ainsi que pour certifier/inscrire des entités dans le registre de confiance. Le registre de confiance et ses opérations se conforment à un cadre de confiance comme le CCP.

Partie qui inscrit

- Entité (habituellement une vraie personne) qui est autorisée à inscrire une entité auprès d'un registre de confiance (p. ex. un administrateur d'une entreprise ou un employé à qui cette autorité a été déléguée).

Portefeuille numérique

- Un portefeuille numérique est un système de référentiel de justificatifs basé sur un logiciel qui entrepose d'une manière sécuritaire des renseignements pour un titulaire. Selon la nature du portefeuille, il peut contenir des renseignements tels que des justificatifs, des justificatifs vérifiables, des renseignements sur des paiements et/ou des mots de passe. Le but d'un portefeuille est d'entreposer d'une manière sécuritaire les justificatifs et/ou les attributs de l'identité, et de permettre au titulaire d'assembler et de préparer des présentations vérifiables. Certains portefeuilles peuvent avoir des capacités pour prouver l'identité et/ou des agents pour faciliter le partage des justificatifs qu'ils gèrent. Pour en savoir plus sur les exigences du portefeuille numérique, voir les critères de conformité du portefeuille numérique.

Présentation vérifiable

- Une présentation vérifiable correspond à des données qui représentent habituellement une ou plusieurs revendications à propos d'un sujet, qui est

dérivé d'un ou de plusieurs justificatifs vérifiables, et est fournie par les titulaires aux vérificateurs.

Registre de confiance

- Service numérique exploité par un réseau d'identité numérique qui fournit de l'information à propos des inscrits. L'information peut être lue par des personnes et/ou des machines de sorte que des personnes et des organisations (services technologiques opérationnels) puissent prendre des décisions en connaissance de cause à propos de la fiabilité des services d'un inscrit (p. ex., niveau d'assurance, transparence et statut d'audit conformément à un cadre de confiance). Par exemple, les titulaires peuvent prendre des décisions en connaissance de cause avant d'interagir avec des émetteurs et des vérificateurs, et les vérificateurs peuvent en faire autant pour l'acceptation de présentations de justificatifs vérifiables par les titulaires (et les émetteurs des justificatifs).

Registre de données vérifiables

- Rôle qu'un système peut jouer en servant de médiateur dans la création et la vérification des identifiants, clés et autres données pertinentes comme des schémas de justificatifs vérifiables, des registres de révocation, des clés publiques d'émetteurs et ainsi de suite, qui peuvent être nécessaires pour utiliser des justificatifs vérifiables (à partir de W3C).

Titulaire

- Entité qui reçoit des justificatifs des émetteurs, qui les garde en sa possession et qui présente des justificatifs aux vérificateurs. Les titulaires utilisent les portefeuilles numériques pour recevoir, conserver et présenter des justificatifs. Les portefeuilles numériques présentent aux titulaires l'information provenant du registre de confiance sur les émetteurs et les vérificateurs (comme leur identité légale, leur capacité en matière d'assurances et leurs politiques de gestion de l'information), afin que les titulaires puissent prendre des décisions en connaissance de cause à propos de la sécurité des interactions avec les émetteurs et les vérificateurs.

Vérificateur (aussi appelé partie dépendante)

- Inscrit ou entité qui demande des présentations vérifiables provenant des titulaires, et qui vérifie les présentations vérifiables. Les vérificateurs utilisent les renseignements à propos des émetteurs des justificatifs vérifiables associés provenant d'un registre de confiance et/ou d'un registre de données vérifiables pour effectuer la vérification des présentations vérifiables.

5. Introduction au profil de conformité de la composante « Registres de confiance » du CCP

Ce document spécifie les critères de conformité de la composante « Registres de confiance » du Cadre de confiance pancanadien (CCP). Les critères de conformité sont fondamentaux pour le cadre de confiance, car ils spécifient les exigences essentielles convenues par les participants à ce cadre de confiance afin d'assurer l'intégrité de leurs processus. Cette intégrité est fondamentale, car de nombreux participants à travers les frontières organisationnelles, territoriales et sectorielles peuvent s'y fier.

Les critères de conformité du CCP visent à compléter les lois et les règlements existants sur le respect de la vie privée.

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 personnes se conforment aux lois, aux politiques et aux règlements pertinents en vigueur dans leur territoire.

Le CCP consiste en une série de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées indépendamment afin d'être prises en considération en tant que composantes de confiance. Le CCP, qui tire parti d'une approche pancanadienne, permet aux secteurs public et privé de collaborer afin de préserver les identités numériques en uniformisant les processus et les pratiques à l'échelle de l'écosystème numérique canadien.

5.1 Mots clés des critères de conformité

Dans ce document, les mots clés suivants sont utilisés dans les critères de conformité pour indiquer leur priorité et/ou leur rigidité générale, et doivent être interprétés de la façon suivante :

- **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de conformité.
- **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de conformité.
- **DEVRAIT** signifie que bien qu'il existe des raisons valables dans des circonstances particulières pour ignorer l'exigence, toutes les implications doivent être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité ou de choisir une option différente spécifiée

par les critères de conformité. La raison pour laquelle un critère de conformité n'est pas rempli devrait être documentée.

- **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 en **caractères gras** et en MAJUSCULES tout au long de ce profil de conformité.

6. Niveaux d'assurance

C'est essentiel que les participants à l'écosystème de l'identité numérique (l'Écosystème) aient une façon d'évaluer la robustesse et la fiabilité des transactions à l'intérieur de cet écosystème. Pour ce faire, les participants doivent partager un vocabulaire commun qui décrit le niveau de confiance qu'ils peuvent associer à une entité ou transaction, ainsi qu'une façon commune de déterminer ce niveau de confiance.

Dans le CCP, un niveau d'assurance représente le niveau de confiance qu'une entité peut accorder aux processus et autres critères de conformité définis dans n'importe quelle composante du CCP. Les niveaux d'assurance sont fondamentaux pour créer des réseaux de confiance. Les modèles de niveaux d'assurance ne fonctionnent que si tous les participants d'un écosystème sont capables de les interpréter d'une manière uniforme. Il est donc essentiel que tous les participants d'un écosystème s'entendent sur un ensemble minimum de critères pour chaque niveau d'assurance. Ce n'est alors seulement qu'une partie dépendante dans cet écosystème sera capable d'évaluer adéquatement les risques inhérents dans une relation ou une transaction, et le niveau d'assurance qui peut être mis dans les participants, les justificatifs et ces transactions. Les composantes du CCP décrivent les critères de conformité détaillés qui devraient être utilisés pour évaluer de tels niveaux d'assurance dans le contexte d'une composante donnée du CCP.

Pour obtenir des indications vraiment à jour sur les niveaux d'assurance, veuillez vous référer à la recommandation préliminaire du modèle de maturité de l'assurance V1.0 du CCP.

7. Critères de conformité

Les critères de conformité sont catégorisés par groupes fonctionnels de registres de confiance. Pour faciliter les choses, on peut faire référence à un critère de conformité spécifique d'après sa catégorie et son numéro de référence. Exemple : « BASE1 » correspond à la « référence nº 1 des critères de conformité de base ».

Remarque : Les critères de conformité de base sont également inclus dans le présent profil de conformité.

Référence	Critères de conformité	Niveau d'assurance			
BASE	**Ces critères de base s'appliquent à <u>tous</u> les processus des registres de confiance**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Ces critères de conformité 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 qui existent dans leurs territoires.	X	X	X	X
GOV	**Exigences en matière de gouvernance (structure commerciale, portée de l'écosystème, processus de gouvernance, et politiques et normes)**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Une organisation de gouvernance de l'écosystème de l'identité numérique (écosystème) **DOIT** établir des politiques d'accès à l'information pour le registre de confiance et les documents connexes publiés décrits dans ce document. Cette composante ne fournit pas d'orientation quant au fait qu'un écosystème devrait fournir un accès ouvert ou non; elle indique simplement que cette politique doit être définie et que des contrôles d'accès doivent être mis en place au besoin.	X	X	X	X

2	Une organisation de gouvernance de l'écosystème de l'identité numérique (écosystème) **DEVRAIT** être une entreprise enregistrée légalement (p. ex., société, partenariat, etc.) dans le ou les territoires où elle mène ses activités ou, si l'écosystème est un organe public, il **DEVRAIT** alors y avoir une législation qui l'autorise et, dans l'un ou l'autre des cas, l'écosystème **DEVRAIT** publier ces renseignements.	X			
3	Une organisation de gouvernance de l'écosystème de l'identité numérique (l'écosystème) **DOIT** être une entreprise enregistrée légalement (p. ex., société, partenariat, etc.) dans le ou les territoires où elle mène ses activités ou, si l'écosystème est un organe public, il **DOIT** alors y avoir une législation qui l'autorise et, dans l'un ou l'autre des cas, l'écosystème **DOIT** publier ces renseignements.		X	X	X
4	Un écosystème **DEVRAIT** documenter et publier sa propriété bénéficiaire le cas échéant (p. ex., pas d'organes publics).	X			
5	Un écosystème **DOIT** documenter et publier sa propriété bénéficiaire le cas échéant (p. ex., pas d'organes publics).		X	X	X
6	Un écosystème **DEVRAIT** documenter et publier sa structure de gestion et ses coordonnées.	X			
7	Un écosystème **DOIT** documenter et publier sa structure de gestion et ses coordonnées.		X	X	X
8	Un écosystème **DEVRAIT** documenter et publier ses processus opérationnels et d'élaboration de politiques, ses comités et autres processus connexes.	X			
9	Un écosystème **DOIT** documenter et publier ses processus opérationnels et d'élaboration de politiques, ses comités et autres processus connexes.		X	X	X

10	Un écosystème **PEUT** documenter et publier chaque année un plan d'affaires qui est examiné et approuvé par l'organe de gouvernance sur une base annuelle.	X	X	X	X
11	Un écosystème **DEVRAIT** documenter et publier les types d'entités qu'il va enregistrer (émetteurs, vérificateurs, fournisseurs de portefeuilles, autres registres de confiance) et d'autres critères tels que l'industrie, l'association ou la profession.	X			
12	Un écosystème **DOIT** documenter et publier les types d'entités qu'il va enregistrer (émetteurs, vérificateurs, fournisseurs de portefeuilles, autres registres de confiance) et d'autres critères tels que l'industrie, l'association ou la profession.		X	X	X
13	Un écosystème **DEVRAIT** documenter et publier la politique et le processus pour vérifier l'autorité juridique des inscrits pour émettre des justificatifs ou accepter les présentations de justificatifs.	X			
14	Un écosystème **DOIT** documenter et publier la politique et le processus pour vérifier l'autorité juridique des inscrits pour émettre des justificatifs ou accepter les présentations de justificatifs.		X	X	X
15	Un écosystème **DEVRAIT** documenter et rendre disponible son statut financier et d'assurance aux inscrits. Les exigences en matière de rapports financiers et de documents d'assurance varieront selon le modèle d'affaires de l'écosystème et son type d'organisation (p. ex., elles pourraient ne pas être pertinentes en ce qui concerne les organes publics).	X	X	X	X
16	Un écosystème **DEVRAIT** documenter et rendre disponible sa politique de souscription, le cas échéant.	X	X	X	X

17	Un écosystème **DEVRAIT** se conformer à un cadre de confiance reconnu comme le CCP ou un équivalent.	X			
18	Un écosystème **DOIT** se conformer à un cadre de confiance reconnu comme le CCP ou un équivalent.		X	X	X
19	Un écosystème **DEVRAIT** maintenir un cadre de confiance, une marque de confiance ou un processus de vérification équivalent reconnu sur une base annuelle et publier son statut.	X			
20	Un écosystème **DOIT** maintenir un cadre de confiance, une marque de confiance ou un processus de vérification équivalent reconnu sur une base annuelle et publier son statut.		X	X	X
21	Un écosystème **DEVRAIT** documenter et publier des descriptions et des niveaux de service pour tous les processus opérationnels et services technologiques.	X			
22	Un écosystème **DOIT** documenter et publier des descriptions et des niveaux de service pour tous les processus opérationnels et services technologiques.		X	X	X
23	Un écosystème **DEVRAIT** documenter et publier une déclaration de la façon dont il ne fait pas de discrimination injuste envers une partie quelconque et dont il maintient son impartialité dans ses processus opérationnels.	X	X	X	X
24	Un écosystème **DEVRAIT** exploiter un programme de gestion des risques, maintenir un registre des risques, et avoir un examen et une approbation annuels par l'organe de gouvernance.	X			
25	Un écosystème **DOIT** exploiter un programme de gestion des risques, maintenir un registre des risques, et avoir un examen et une approbation annuels par l'organe de gouvernance.		X	X	X

OPS	Opérations liées aux registres de confiance (services techniques et de gestion liés à la technologie et à l'infrastructure)	LOA1	LOA2	LOA3	LOA4
1	Un registre de confiance (registre) **DEVRAIT** se conformer à un cadre de l'industrie reconnu pour ses opérations reliées à l'infrastructure technologique comme la composante Infrastructure (technologie et opérations) du CCP) ou la norme ISO/IEC 20000-1:2018.	X			
2	Un registre de confiance (registre) **DOIT** se conformer à un cadre de l'industrie reconnu pour ses opérations reliées à l'infrastructure technologique comme la composante Infrastructure (technologie et opérations) du CCP) ou la norme ISO/IEC 20000-1:2018.		X	X	X
3	Un registre **DEVRAIT** maintenir un référentiel accessible (p. ex., site Web) pour héberger tous les documents publiés dont il est fait mention dans cette composante.	X	X	X	X
4	Un registre **DEVRAIT** démontrer l'authenticité de tous les documents publiés, comme le fait d'utiliser des signatures numériques.	X	X		
5	Un registre **DOIT** démontrer l'authenticité de tous les documents publiés, comme le fait d'utiliser des signatures numériques.			X	X
6	Un registre **DOIT** fournir des versions lisibles par des personnes des documents publiés dans cette composante.	X	X	X	X
7	Un registre **DEVRAIT** fournir des versions lisibles par des machines des documents appropriés dans des formats et des protocoles reconnus par l'industrie.	X	X		
8	Un registre **DOIT** fournir des versions lisibles par des machines des documents appropriés dans des formats et des protocoles reconnus par l'industrie.			X	X

9	Un registre **DEVRAIT** fournir de l'information lisible par des machines d'une manière qui empêche le suivi et la corrélation de l'utilisation par les émetteurs et les vérificateurs des titulaires et des portefeuilles numériques.	X	X	X	X
10	Un registre **DEVRAIT** fournir de l'information à propos de son identité dans un format conforme aux normes reconnues de l'industrie comme la composante Organisation vérifiée du CCP.	X			
11	Un registre **DOIT** fournir de l'information à propos de son identité dans un format conforme aux normes reconnues de l'industrie comme la composante Organisation vérifiée du CCP.		X	X	X
12	Un registre **DEVRAIT** fournir aux titulaires, aux vérificateurs et aux émetteurs des données du registre dans des formats et normes de l'industrie reconnus pour permettre des transactions hors ligne entre les titulaires, les émetteurs ou les vérificateurs.	X	X		
13	Un registre **DOIT** fournir aux titulaires, aux vérificateurs et aux émetteurs des données du registre dans des formats et normes de l'industrie reconnus pour permettre des transactions hors ligne entre les titulaires, les émetteurs ou les vérificateurs.			X	X
14	Un registre **DEVRAIT** fournir de l'information sur les inscrits et leur statut dans des formats et protocoles standard de l'industrie.	X			
15	Un registre **DOIT** fournir de l'information sur les inscrits et leur statut dans des formats et protocoles standard de l'industrie.		X	X	X

16	Un écosystème **PEUT** permettre aux inscrits de publier directement de l'information sur ses services numériques dans un registre en utilisant des méthodes et des processus d'assurance des cadres qui sont standard dans l'industrie, comme les composantes Authentification et Justificatifs (relations et attributs) du CCP.	X	X	X	X
17	Un registre **PEUT** fournir de l'information sur le statut des justificatifs ou des liens menant à des renseignements sur le statut des justificatifs.	X	X	X	X
18	Un registre de confiance **DOIT** documenter et publier des renseignements techniques pour les émetteurs, les vérificateurs et les fournisseurs de portefeuilles numériques afin de soutenir le développement de produits qui sont reliés au registre.	X	X	X	X
19	Un registre **DEVRAIT** fournir des environnements de développement et d'essai aux émetteurs, vérificateurs et fournisseurs de portefeuilles numériques pour développer et tester leur utilisation du registre avec des produits numériques.	X	X	X	X
REG	**Gestion des inscriptions et des certifications (services de certification/vérification/marques de confiance, processus d'inscription, de suspension et de révocation)**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Un écosystème **DEVRAIT** identifier les inscrits qui utilisent des processus d'assurance reconnus comme la composante Organisation vérifiée du CCP.	X			
2	Un écosystème **DOIT** identifier les inscrits qui utilisent des processus d'assurance reconnus comme la composante Organisation vérifiée du CCP.		X	X	X

3	Un écosystème **DEVRAIT** mettre en place des processus et des contrôles pour s'assurer que les renseignements sur les inscrits sont à jour et conformes aux enregistrements juridiques, lois et/ou certifications.	X	X		
4	Un écosystème **DOIT** mettre en place des processus et des contrôles pour s'assurer que les renseignements sur les inscrits sont à jour et conformes aux enregistrements juridiques, lois et/ou certifications.			X	X
5	Un écosystème **DEVRAIT** identifier et authentifier les parties qui s'inscrivent et les propriétaires bénéficiaires qui utilisent des processus d'assurance des cadres comme les composantes Personne vérifiée et Justificatifs (relations et attributs) du CCP.	X			
6	Un écosystème **DOIT** identifier et authentifier les parties qui s'inscrivent et les propriétaires bénéficiaires qui utilisent des processus d'assurance des cadres comme les composantes Personne vérifiée et Justificatifs (relations et attributs) du CCP.		X	X	X
7	Un écosystème **DEVRAIT** exiger que les inscrits se conforment à un cadre de confiance reconnu comme le CCP.	X			
8	Un écosystème **DOIT** exiger que les inscrits se conforment à un cadre de confiance reconnu comme le CCP.		X	X	X
9	Un écosystème **DEVRAIT** exiger que les inscrits aient une certification de conformité à un cadre de confiance à l'aide de services de certification de la confiance reconnus comme le Programme de marque de confiance Voilà Vérifié ou utiliser un processus de certification ou de vérification équivalent.	X	X		

10	Un écosystème **DOIT** exiger que les inscrits aient une certification de conformité à un cadre de confiance à l'aide de services de certification de la confiance reconnus comme le Programme de marque de confiance Voilà Vérifié ou utiliser un processus de certification ou de vérification équivalent.			X	X
11	Un écosystème **DEVRAIT** documenter et publier les processus et services d'inscription et de certification à la disposition des inscrits, comme le programme de marque de confiance Voilà Vérifié.	X	X	X	X
12	Un écosystème **DEVRAIT** vérifier que les inscrits sont autorisés à émettre des justificatifs ou à recevoir des présentations de justificatifs conformément aux politiques de l'écosystème et à inclure cette autorisation dans le registre de confiance.	X			
13	Un Écosystème **DOIT** vérifier que les inscrits sont autorisés à émettre des justificatifs ou à recevoir des présentations de justificatifs conformément aux politiques de l'écosystème et à inclure cette autorisation dans le registre de confiance.		X	X	X

8. Références

Cette section fournit la liste des normes, cadres, lignes directrices, registres et autres documents auxquels il est fait référence dans 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 :

- Trust Over IP (ToIP) https://trustoverip.org/ e
- Groupe de travail sur les justificatifs de la Decentralized Identity Foundation (DIF)
- https://trustoverip.github.io/essiflab/glossary (https://essif-lab.eu)
- World Wide Web Consortium (W3C)
- Norme ISO/IEC 20000-1:2018

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.

9. Historique des révisions

Version	Date	Auteur(s)	Commentaire
0.01	2022-07-19	Équipe de conception des registres de confiance du CCP	Ébauche de discussion initiale créée par l'équipe de conception des registres de confiance du CCP
0.02	2022-08-22	Équipe de conception des registres de confiance du CCP	Version mise à jour pour incorporer la rétroaction de l'équipe de conception
1.0	2023-03-01	Équipe de conception des registres de confiance du CCP	Le TFEC l'approuve comme ébauche de recommandations V1.0
1.1	2023-05-23	Équipe de conception des registres de confiance du CCP	Version mise à jour pour incorporer la rétroaction reçue de l'appel à commentaires public et de la période d'examen des DPI
1.0	2023-08-30	Équipe de conception des registres de confiance du CCP	Approbation du TFEC comme candidate pour une recommandation finale V1.0
1.0	2023-11-10	Équipe de conception des registres de confiance du CCP	Approuvé en tant que recommandation finale V1.0 par vote du membre de soutien du CCIAN