Aperçu de la composante « 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 préparé par le Comité d'experts du Cadre de confiance pancanadien (TFEC) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN). Le TFEC est régi par les politiques du CCIAN qui le contrôlent. 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 DIACC.ca.

Table des matières

1. Introduction

Ce document donne un aperçu de la composante « Registres de confiance » 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 « Registres de confiance » du CCP et nécessaires pour l'interpréter d'une manière uniforme.

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.

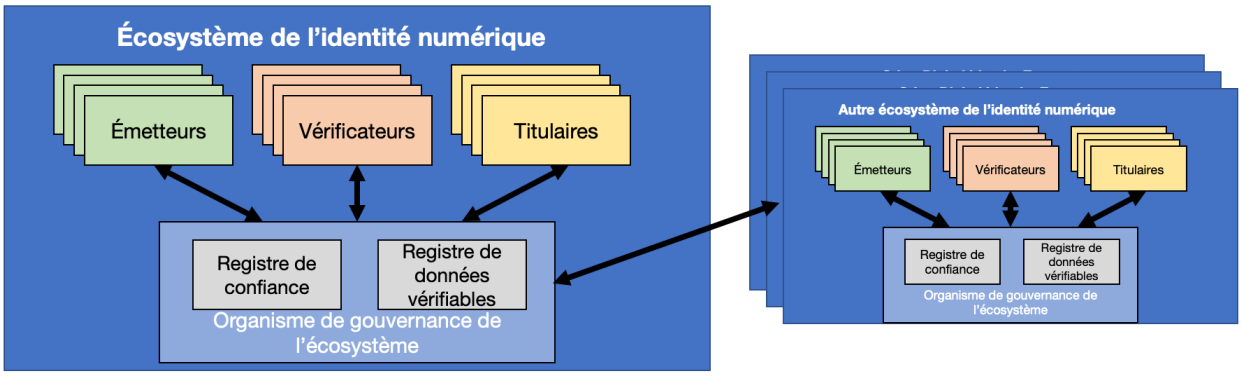

Figure 1. Écosystèmes de l'identité numérique

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 1 est une illustration des composantes du cadre de confiance pancanadien.

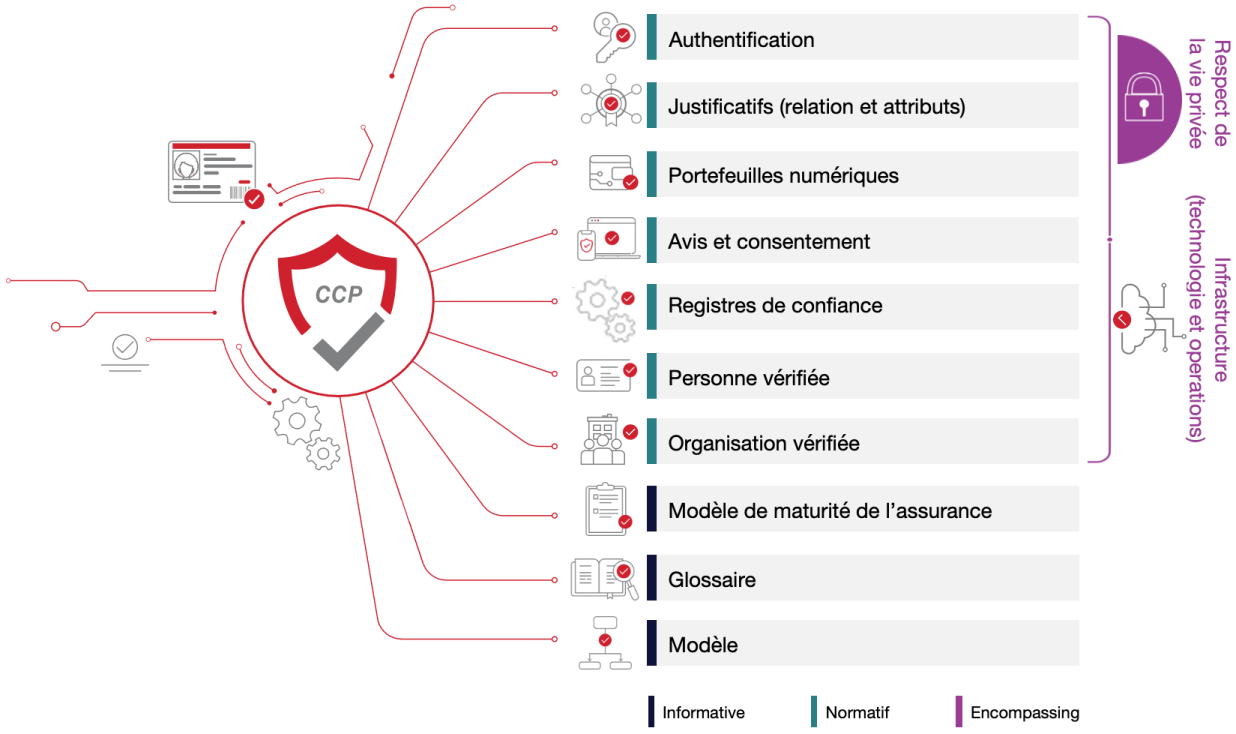

Figure 1. Composantes du cadre de confiance pancanadien

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. 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.

6. 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