Aperçu de la composante « Infrastructure (technologie et opérations) » du CCP

Statut du document : Recommandation finale V1.2

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

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

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

Droits de propriété intellectuelle : Droits de propriété intellectuelle du CCIAN V1.0 PDF | © 2023

Table des matières

1. Introduction de la composante « Infrastructure (technologie et opérations) »

Ce document donne un aperçu de la composante « Infrastructure (technologie et opérations) » du CCP, une composante du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale sur le CCP, veuillez vous référer au modèle de CCP, lequel décrit les buts et objectifs du CCP et donne un aperçu de haut niveau du CCP.

Les composantes du CCP comprennent habituellement deux documents :

1. **Aperçu de la composante** – 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 de la composante** – Il spécifie les critères de conformité utilisés pour uniformiser et évaluer l'intégrité des processus de confiance qui font partie de la composante.

Cet aperçu fournit des renseignements reliés à la composante « Évaluation » du CCP et nécessaires pour l'interpréter d'une manière uniforme.

1.1 Raison d'être et avantages anticipés

La composante « Infrastructure (technologie et opérations) » du CCP vise à recenser les politiques, plans, et exigences relatives à la technologie et aux opérations technologiques pour soutenir la mise en œuvre des principes des profils du CCP dans le contexte de l'écosystème de l'identité numérique.

Un processus certifié est un processus de confiance auquel d'autres participants du CCP peuvent se fier. Les critères de conformité du CCP visent à compléter les lois et règlements existants sur la protection de la vie privée; on s'attend à ce que les participants à l'écosystème de l'identité numérique certifiés par le CCIAN satisfassent aux exigences et aux règlements prévus par la loi qui sont applicables dans leurs territoires.

La composante « Infrastructure (technologie et opérations) » du CCP définit :

- Les artéfacts officiels en matière de politiques et plans qui forment la base d'une installation technologique conforme et de ses opérations de soutien technologique.
- Les capacités de haut niveau en termes de technologie et d'outils technologiques requises pour soutenir une infrastructure technologique qui dessert un écosystème de l'identité numérique.
- Les outils et caractéristiques opérationnels de soutien technologique pour soutenir une infrastructure technologique installée qui dessert un écosystème de l'identité numérique.

1.2 Portée

Cette section définit la portée de la composante « Infrastructure (technologie et opérations) » du CCP. Les exigences incluses dans la portée sont identifiées à un haut niveau pour illustrer la portée; les exigences détaillées sont élaborées dans le profil de conformité de la composante « Infrastructure (technologie et opérations) » du CCP.

1.2.1 Inclus dans la portée

Cette composante du CCP va spécifier les critères de conformité qui fournissent les exigences et lignes directrices générales concernant la fiabilité de l'infrastructure TI qui permet la mise en œuvre et la prestation de processus de confiance définis dans d'autres composantes du CCP. Les principaux domaines de la composante sont la sécurité et l'intégrité des composantes techniques. À l'intérieur de ces domaines d'intérêt, la portée de la composante inclut :

- La sécurité TI (en tant que considération générale).
- La supervision de la collecte, la validation, l'entreposage et l'accessibilité des données.
- Les audits et l'enregistrement.
- La prévention des événements TI qui compromettent la fiabilité de l'écosystème de l'identité numérique et la réaction à ceux-ci.
- Les politiques et plans qui soutiennent la gestion de la fiabilité de la technologie et des opérations technologiques.

1.2.2 Exclus de la portée

La portée de cette composante du CCP n'inclut pas :

- Le caractère adéquat des produits spécifiques pour soutenir un processus de confiance donné.

- Le caractère adéquat des normes, processus, technologies ou protocoles technologiques qui peuvent être spécifiques à ou imposés par un écosystème de l'identité numérique en particulier.
- L'obligation d'utiliser un ensemble spécifique de pratiques ou cadres standards pour gouverner les opérations technologiques (p. ex. IT Infrastructure Library <<ITIL>>, Control Objectives for Information Technology <<COBIT>>).

1.3 Relations avec le CCP

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.

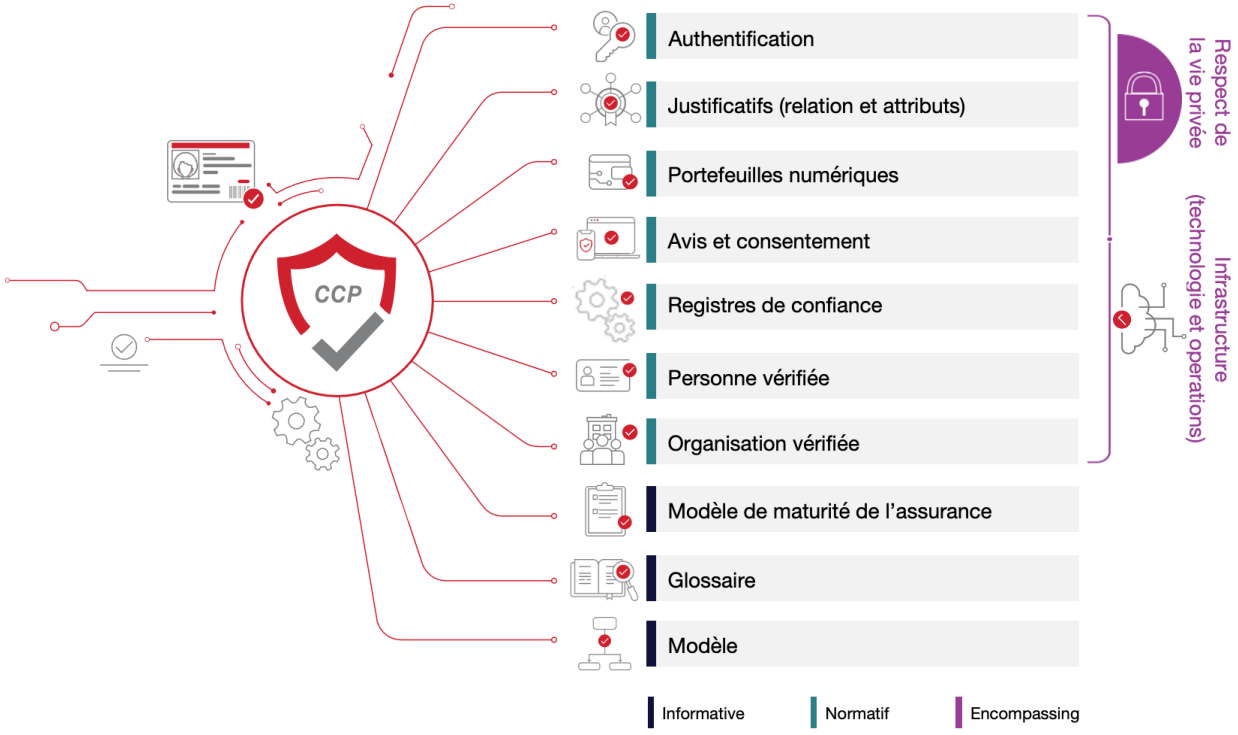

Figure 1 - Composantes du Cadre de confiance pancanadien

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

2. Conventions de la composante « Infrastructure (technologie et opérations) »

Cette section décrit et définit les principaux termes et notions utlisés dans la composante « Infrastructure (technologie et opérations) » du CCP. Ces renseignements sont fournis pour assurer une utilisation et une interprétation uniformes des termes dans toute cette composante.

Remarques :

- Les conventions peuvent varier entre les composantes du CCP. Les lecteurs sont encouragés à passer en revue les conventions de chaque composante du CCP qu'ils lisent.
- Termes définis – les principaux termes et notions décrits et définis dans cette section et le glossaire du CCP sont écrits avec une majuscule dans ce document.
- Liens hypertextes – il se pourrait que des liens hypertextes soient intégrés dans les versions électroniques de ce document comme référence pour le lecteur. Tous les liens étaient accessibles au moment de la rédaction.

2.1 Termes et définitions

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

Critères de conformité

Exigences développées pour chacune des composantes du CCP et servant de base pour évaluer la conformité.

Écosystème de l'identité numérique

Écosystème interconnecté pour l'échange et la vérification de l'information sur l'identité numérique, qui implique des organisations des secteurs public et privé qui se conforment à un cadre de confiance commun pour la gestion et l'utilisation d'identités numériques, et les sujets de ces identités numériques.

Renseignements personnels

Tout renseignement factuel ou subjectif, consigné ou non, concernant une personne identifiable (Source : Survol de la LPRPDE, Commissariat de protection de la vie privée du Canada – Qu'entend-on par « renseignements personnels?).

2.2 Abréviations

Les abréviations et acronymes qui suivent apparaissent tout au long de cette composante du CCP :

- CCIAN – Conseil canadien de l'identité et de l'authentification numériques
- COBIT - Control Objectives for Information Technology
- ENISA – Agence de l'Union européenne pour la cybersécurité
- FEDRAMP - Federal Risk and Authorization Management Program
- ITIL - IT Infrastructure Library
- NIST - National Institute of Standards and Technology
- CCP – Cadre de confiance pancanadien

3. Couverture des critères de conformité

Les critères de conformité sont élaborés en détail dans le profil de conformité de la composante « Infrastructure (technologie et opérations) » du CCP. Les exigences ont été conçues pour refléter les capacités et les caractéristiques trouvées dans les opérations technologiques et les normes de gouvernance (p. ex., ITIL, COBIT) sans être aussi prescriptives qu'une norme spécifique l'exige.

De même, les organismes de normalisation du secteur public et les orientations concernant la mise en œuvre ont été mis à contribution pour aider à définir certaines exigences détaillées dans les critères de conformité. C'est notamment le cas du National Institute of Standards and Technology (NIST) et du Federal Risk and Authorization Management Program (FEDRAMP) aux États-Unis, de l'Agence de l'Union européenne pour la cybersécurité (ENISA) en Europe et de diverses directives du gouvernement fédéral au Canada. L'approche a consisté à s'inspirer de certaines orientations communes pour la mise en œuvre et la gestion technologiques tout en s'assurant que les critères de conformité du CCP étaient assez génériques pour coexister dans un domaine du secteur public ou privé.

Cela vaut la peine de souligner que les critères de conformité de la composante « Infrastructure (technologie et opérations) » du CCP sont décrits d'une manière générique, en mettant davantage l'accent sur les capacités nécessaires pour avoir une infrastructure de confiance comme plateforme pour fournir d'autres services conformes à l'intérieur du CCP. On s'attend à ce que les organisations désirant participer à un écosystème de l'identité numérique spécifique aient des exigences spécifiques en ce

qui concerne la technologie et les opérations technologiques qui leur sont imposées par l'écosystème de l'identité numérique. L'identification d'un produit technologique, d'un protocole ou d'une norme opérationnelle tierce dans un écosystème particulier de l'identité numérique n'est pas inclus dans la portée de ce profil.

Les critères sont organisés en trois grandes catégories :

- Politiques et plans – saisit les principaux artéfacts officiels qui peuvent définir l'approche uniforme de l'organisation pour instancier et gérer les composantes technologiques et systèmes qui remplissent le rôle que l'organisation joue dans l'écosystème de l'identité numérique.
- Technologie – identifie les caractéristiques et capacités des composantes technologiques requises.
- Opérations – identifie les caractéristiques et capacités requises du cadre et de l'ensemble d'outils opérationnels utilisés pour jouer un rôle défini au sein de l'écosystème de l'identité numérique.

3.1 Politique et plans

La base de la composante technologique d'une architecture d'entreprise est un ensemble complet de politiques et plans organisationnels clairement cartographiés selon les objectifs commerciaux identifiés dans les composantes commerciales de l'architecture d'entreprise. Ce profil identifie les exigences concernant les artéfacts officiels et leur gestion continue dans les domaines suivants :

- Évaluation des risques;
- Audit et imputabilité;
- Évaluation de la sécurité;
- Planification des désastres ou des situations d'urgence;
- Identification et authentification;
- Protection des systèmes et des communications;
- Intervention en cas d'incident;
- Intégrité des systèmes et de l'information;
- Gestion de la configuration;
- Gestion de l'information;
- Maintenance des systèmes;
- Contrôle de l'accès technique;
- Contrôle de l'accès physique;
- Sécurité du personnel.

D'une façon générale, on retient surtout de cet ensemble de critères le besoin d'avoir une planification ordonnée qui commence par la détermination des objectifs dans les

énoncés de politique, et est soutenue par des plans officiels qui régissent la mise en œuvre et le fonctionnement de la technologie.

3.2 Critères technologiques

Ces critères mettent l'accent sur l'identification des outils et des capacités technologiques génériques nécessaires pour soutenir une infrastructure opérationnelle qui fournit des services conformes au CCP. Les produits ou protocoles spécifiques ne sont pas précisés, car ils tendent à varier selon le processus de confiance spécifique fourni à un écosystème de l'identité numérique en particulier. On s'attend à ce que les organisations aient des exigences spécifiques supplémentaires dans ce domaine qui sont imposées par l'écosystème de l'identité numérique dans lequel elles veulent fonctionner.

Les capacités qui sont spécifiques à d'autres processus de confiance du CCP (authentification, respect de la vie privée, personne vérifiée, etc.) ne sont pas élaborées dans ce profil. Ces critères sont identifiés dans les profils de conformité du CCP spécifiques au sujet. Il y a plusieurs références croisées à d'autres profils de conformité lors c'est approprié.

3.3 Critères des opérations technologiques

La troisième catégorie de critères de conformité identifie les opérations technologiques et les capacités de soutien nécessaires pour exploiter une infrastructure conforme au CCP. Ces capacités, qui s'alignent sur les politiques et les plans indiqués plus tôt, représentent les caractéristiques technologiques, opérationnelles et en matière de soutien permanentes qui sont requises pour respecter les capacités d'entreprise identifiées dans les politiques et les plans associés à une architecture d'entreprise globale.

4. Références

Ce profil a été influencé par les normes ou les organes de normalisation indiqués ci-dessous. Chacune des organisations mentionnées inclut un référentiel qui contient de multiples documents ayant trait à l'établissement et au fonctionnement d'une infrastructure technique requise pour soutenir la prestation du service, dans ce cas-ci, un écosystème de l'identité numérique.

Remarque : Lorsque c'est applicable, l'unique numéro de version spécifié dans ce document s'applique à cette composante du CCP.

Les profils de conformité des composantes du CCP (les versions publiques seront publiées une fois rendues au stade final au www.diacc.ca) ont été mentionnés au stade d'ébauche :

- Profil de conformité de la composante « Authentification »
- Profil de conformité de la composante « Justificatifs (relations et attributs) »
- Profil de conformité de la composante « Avis et consentement »
- Profil de conformité de la composante « Respect de la vie privée »
- Profil de conformité de la composante « Organisation vérifiée »
- Profil de conformité de la composante « Personne vérifiée »

Gouvernement du Canada. *Directive du Conseil du Trésor du gouvernement du Canada sur les services et le numérique.* https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32601

Gouvernement du Canada. *Version 1.1 du profil du CCP lié à la fonction publique.* https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_1

United States Department of Commerce. National Institute of Standards and Technology. *Digital Identity Guidelines (NIST Special Publication 800-63 – 5 documents).* 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html

United States Department of Commerce. National Institute of Standards and Technology. *Assessing Security and Privacy Controls (NIST Special Publication 800-53 Rev. 5).* September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

ISACA. *Control Objectives for Information Technology (COBIT)*. www.isaca.org

Axelos. *IT Infrastructure Library (ITIL)*. www.axelos.com

Organisation internationale de normalisation (ISO). *Critères d'évaluation pour la sécurité TI*. https://www.iso.org/standard/50341.html

US Federal Government, *Federal Risk and Authorization Management Program (FedRAMP). Voir le lien menant au référentiel*. www.fedramp.gov

Agence de l'Union européenne pour la cybersécurité (ENISA). *Voir le lien menant vers le référentiel.* https://www.enisa.europa.eu/

5. Historique des révisions

Version	Date	Auteur	Commentaire
0.01	2019-12-15	Équipe de rédaction du CCP	Ébauche initiale du cadre
0.02	2020-02-14	Équipe de rédaction du CCP	Ébauche initiale avec tout le contenu
0.03	2020-03-03	Équipe de rédaction du CCP	Ajustements basés sur une étude et un examen supplémentaires des ébauches des composantes du CCP
0.04	2020-03-30	Équipe de rédaction du CCP	Ajustements finaux pour la publication de la version préliminaire
0.05	2020-06-05	Équipe de rédaction du CCP	Mises à jour basées sur les commentaires des membres du TFEC
0.06	2020-06-29	Équipe de rédaction du CCP	Mises à jour faisant suite à une brève période d'examen supplémentaire du TFEC
1.0	2020-07-08	Équipe de rédaction du CCP	Approbation du TFEC comme recommandation préliminaire V1.0
1.1	2020-09-18	Équipe de rédaction du CCP	Mises à jour d'après les commentaires reçus pendant la période d'examen public de l'ébauche de recommandation
1.0	2020-09-30	Équipe de rédaction du CCP	Approbation du TFEC comme candidat pour une recommandation finale V1.0
1.1	2022-08-09	Rédacteur et équipe de conception de l'infrastructure du CCP	Recommandation finale V1.1 destinée à incorporer la rétroaction des essais alpha
1.1	2022-09-14	Rédacteur et équipe de conception de l'infrastructure du CCP	Approbation du TFEC comme recommandation finale V1.1
1.1.1	2023-01-19	Rédacteur et équipe de conception de l'infrastructure du CCP	Mises à jour d'après les commentaires reçus pendant la période d'examen public de la recommandation finale V1.1
1.2	2023-02-01	Rédacteur et équipe de conception de l'infrastructure du CCP	Approbation du TFEC comme candidat pour une recommandation finale V1.2

1.2	2023-04-19	Rédacteur et équipe de conception de l'infrastructure du CCP	Approuvé en tant que recommandation finale V1.0 par vote du membre de soutien du CCIAN