Profil de conformité du « 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 aux critères de conformité du portefeuille numérique du CCP

Ce document spécifie les critères de conformité pour le profil du portefeuille numérique 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 au cadre de confiance pour assurer l'intégrité de leurs processus. Cette intégrité est de la plus haute importance, car de nombreux participants à travers les frontières organisationnelles, territoriales et sectorielles peuvent se fier aux extrants ou au résultat d'un processus de confiance.

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

Remarque : Les critères de conformité du CCP ne remplacent ou 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 dans leur propre territoire.

Le profil du portefeuille numérique a été décrit dans l'aperçu de la composante « Portefeuille numérique » du CCP. Un portefeuille numérique est un outil qu'une personne peut utiliser pour créer et gérer ses propres identités, obtenir auprès d'entités de confiance des « justificatifs vérifiables » (JV) attestant qui elle est et ce à quoi elle a droit, et déterminer si et comment elle veut présenter ces justificatifs vérifiables à des vérificateurs.

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 fiables. Le CCP, qui s'appuie sur une approche pancanadienne, permet aux secteurs public et privé de collaborer pour protéger les identités numériques en uniformisant les processus et les pratiques dans tout l'écosystème numérique canadien.

Le profil du portefeuille d'identité numérique recoupe partiellement certaines composantes du CCP, notamment les composantes « Authentification », « Avis et consentement » et « Justificatifs (relations et attributs) ». Même s'il y a un recoupement avec d'autres composantes du CCP, les critères de conformité inclus visent à couvrir la pleine portée de la création d'un portefeuille d'identité numérique de confiance.

Ce profil est organisé selon les processus de confiance qui sont nécessaires pour avoir un portefeuille numérique fiable. L'intégrité d'un processus de confiance est de la plus

haute importance, car de nombreux participants peuvent dépendre du résultat du processus, qui déborde souvent des frontières territoriales, organisationnelles et sectorielles, et à court et long terme. Un processus est considéré de confiance lorsqu'il est évalué et certifié conforme à ces critères de conformité.

Le présent document inclut une discussion et des détails sur les risques pour la conformité du portefeuille numérique. Lorsqu'une entité cherche à démontrer la conformité à ce cadre, il faudrait tenir compte de la tolérance au risque de la partie dépendante et du fait que les contrôles des risques sont systématiquement appliqués d'une manière ni trop permissive ni trop rigoureuse.

Les critères de conformité sont une série d'énoncés et d'exigences qui fourniront les considérations fondamentales à l'entité cherchant à évaluer son portefeuille numérique. Ces énoncés sur les critères de conformité forment la base de l'évaluation de toutes les composantes du Cadre de confiance pancanadien.

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

1.1 Processus d'instanciation et de sécurité du portefeuille

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

1.2 Processus de gestion et d'utilisation des justificatifs

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

1.3 Processus de gestion du consentement

1. Expression du consentement

2. Mots-clés des critères de conformité

Les termes suivants, qui sont utilisés dans ce document, indiquent la priorité et/ou la rigidité générale des critères de conformité, et doivent être interprétés tel qu'indiqué ci-dessous.

- **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de

conformité.

- **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de conformité.
- **DEVRAIT** signifie que, même s'il peut y avoir des raisons valides 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 autre option comme spécifié par les critères de conformité. La raison pour ne pas respecter un critère devrait être documentée dans les cas où les critères de conformité ne sont pas respectés.
- **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 dans ce profil de conformité.

3. Niveaux d'assurance

Dans le CCP, un niveau d'assurance représente le niveau de confiance qu'une entité peut placer dans les processus et autres critères de conformité définis dans une composante du CCP. Comme défini dans la recommandation finale du glossaire du CCP V1.0, les niveaux d'assurance représentent un niveau de confiance auxquels d'autres peuvent se fier. Dans le CCP, il est appliqué comme mesure de certitude qu'un sujet est la personne ou la chose qu'il revendique être, ou qu'un sujet a gardé le contrôle d'un authentificateur et que l'authentificateur n'a pas été compromis. Dans le contexte du CCP, les niveaux d'assurance s'appuient sur la Directive du gouvernement du Canada sur la gestion de l'identité – Annexe A : Norme sur l'assurance de l'identité et des justificatifs. Les portefeuilles contribuent à l'assurance de l'authentification et des justificatifs.

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 avoir les consignes les plus à jour en ce qui concerne les niveaux d'assurance, veuillez vous référer à l'ébauche recommandation pour le modèle de maturité du CCP V1.0.

4. Risques liés au portefeuille numérique

Les portefeuilles numériques jouent un rôle important dans les fondements de la confiance dans un écosystème numérique. Outre les évaluations d'impacts sur la protection de la vie privée qu'une entité peut effectuer ou être tenue d'effectuer, il est important que les organisations qui participent à un écosystème de confiance comprennent les risques que pose l'utilisation de portefeuilles numériques. La figure 3 contient un tableau illustratif des risques pour les portefeuilles numériques et des exemples de stratégies d'atténuation.

Type de risque	Catégorie de menace	Scénario de menaces / vulnérabilité aux menaces	Renseignements supplémentaires	Agent de menace	Impact	Protections proposées (p. ex., apport aux exigences de conformité)
Sécurité des renseignements / du portefeuille → torts causés au titulaire	Risque pour la qualité du portefeuille	Le portefeuille contient des vulnérabilités logicielles qui peuvent être exploitées par un acteur malveillant.	Intention accidentelle ou malveillante	Pirate / agresseur	Torts causés aux participants de l'écosystème - confiance dans l'écosystème; risque pour la réputation de l'écosystème dans son ensemble ou la marque de confiance, s'il en a une. Torts causés au titulaire : • Vol d'identité • Torts financiers • Perte de privilèges / d'accès / d'utilisation • Torts causés à la réputation	Le portefeuille suit le processus de certification et a la marque de confiance prouvant que le réalisateur suit un processus de développement de produits acceptable tout au long du cycle de vie du portefeuille : • R et D / lancement du portefeuille • Utilisation (inclut l'instanciation / la personnalisation du portefeuille par le titulaire) • Temporisation • Considérations pour la validation de l'intégrité de la chaîne d'approvisionnement, sécurité dans la SDLC, évaluations de sécurité des tierces parties, processus de gestion des vulnérabilités. • Montre le besoin d'avoir une évaluation / certification continue
Sécurité des renseignements / gestion du	Risque pour la qualité du	Le portefeuille n'est plus soutenu et est		S.O.	Le titulaire est incapable d'effectuer les	• Le titulaire acquiert un autre portefeuille qui se conforme aussi aux

cycle de vie → inconvénients pour l'utilisateur	portefeuille	obsolète.			transactions requises.	normes de l'industrie comme le prouve la marque de confiance. • [Prendre en considération] Portefeuille représenté dans des registres de confiance (p. ex., liste de portefeuilles certifiés du CCIAN). • Le titulaire choisit le portefeuille à partir d'un registre de confiance. • Le portefeuille suit le processus de certification et a la marque de confiance prouvant que le réalisateur suit un processus de développement de produits acceptable tout au long du cycle de vie du portefeuille : o R et D / lancement du portefeuille o Utilisation (inclut l'instanciation / la personnalisation du portefeuille par le titulaire) o Temporisation • Considérations pour la validation de l'intégrité de la chaîne d'approvisionnement, sécurité dans la SDLC, évaluations de sécurité des tierces parties, processus de gestion des vulnérabilités • Montre le besoin d'avoir une évaluation / certification continue
Sécurité des renseignements / gestion du cycle de vie →	Risque pour la qualité du portefeuil	Le portefeuille n'est plus soutenu et est obsolète.	Le portefeuille est incapable d'interopérer avec un	S.O.	Le titulaire est incapable d'effectuer les transactions	• Le titulaire acquiert un autre portefeuille qui se conforme aussi à la certification de la

inconvénients pour l'utilisateur	le		émetteur ou le titulaire a besoin d'un vérificateur.		voulues.	marque de confiance du CCP.
Sécurité des renseignements / du portefeuille → torts causés au titulaire	Risque pour la qualité du portefeuille	Des acteurs malveillants développent le portefeuille avec l'intention de nuire au titulaire ou de se faire passer pour lui.	Des acteurs malveillants placent le portefeuille dans l'Apple Store et le Google Store.	Développeur de portefeuille malveillant	• Hameçonnage • Déguisement ou autre tort causé au titulaire	• Le titulaire peut identifier et authentifier un portefeuille certifié. • Montre le besoin d'avoir des registres pour que l'utilisateur puisse vérifier la certification.
Sécurité des renseignements / gestion du cycle de vie → inconvénients pour l'utilisateur	Risque pour la qualité du portefeuille	Le portefeuille n'applique pas / ne suit pas les normes de l'industrie.	Le portefeuille est incapable d'interopérer avec un émetteur ou le titulaire a besoin d'un vérificateur.	Développeur de portefeuille	• Le service est refusé au titulaire. • Le titulaire est incapable d'effectuer les transactions voulues. • L'émetteur est incapable d'émettre. • Le vérificateur n'arrive pas à s'engager dans une transaction avec le titulaire.	• Le portefeuille applique les normes de l'industrie comme le prouve la marque de confiance. • La marque de confiance doit vérifier les exigences de conformité aux normes de l'industrie. • Le portefeuille doit respecter / appliquer les normes de l'industrie pertinentes (p. ex., justificatifs vérifiables W3C, DIF, DID, cadre de gouvernance, etc.).
Sécurité des renseignements / sécurité de l'émetteur / du vérificateur → torts causés au titulaire	Risque pour la qualité du produit de l'émetteur / du vérificateur	La plateforme hébergée / en nuage (émetteurs, vérificateurs, etc.) a des contrôles de sécurité techniques et des pratiques de gestion inadéquats.		Pirate	Le système est facilement compromis, ce qui pourrait exposer les données entreposées dans le portefeuille ou permettre à un attaquant sophistiqué d'émettre de faux documents.	• Tous les participants à l'écosystème suivent un processus de certification et ont une marque de confiance prouvant la conformité à la norme. • Considérations pour la validation de l'intégrité de la chaîne d'approvisionnement, sécurité dans la SDLC, évaluations de sécurité des tierces parties, processus de gestion des vulnérabilités.

						• Montre le besoin d'avoir une évaluation / certification continue.
Sécurité des renseignements / sécurité de la gestion des clés → torts causés au titulaire	Risques pour la sécurité de l'appareil / la gestion des clés	L'appareil ne soutient pas les fonctions de sécurité nécessaires pour le ou les niveaux d'assurance spécifiques / ciblés.	L'appareil manque d'une capacité de gestion essentielle adéquate.	Acteur malveillant (local ou à distance)	Majeur Clés compromises / portefeuille compromis / atteinte à la vie privée / usurpation d'identité	• Le portefeuille soutient explicitement les appareils et les versions OS ayant une capacité de gestion des clés adéquate / évaluée. *Remarques :* • *Cela inclut les fonctions de gestion des clés et de sécurité à grand impact gérées sur le même appareil que le logiciel du portefeuille, ainsi que l'appareil externe au logiciel du portefeuille.* • *Le caractère « adéquat » (FIPS pour le matériel, NIST pour le logiciel) dépendra du niveau d'assurance.*
Sécurité des renseignements / sécurité de la gestion des clés → torts causés	Risques pour la sauvegarde / récupération / risques pour la gestion des clés	Processus de sauvegarde / récupération faible	Un acteur malveillant vole les clés secrètes à l'aide d'un mécanisme de sauvegarde / récupération	Acteur malveillant (local ou à distance)	Majeur : Clés compromises / portefeuille compromis / atteinte à la vie privée / usurpation d'identité	• Les processus de sauvegarde et récupération doivent être définis pour le niveau d'assurance correspondant et évalués dans le cadre du processus de certification. • Les sauvegardes doivent avoir les mêmes protections du niveau d'assurance que les protections d'origine.
Sécurité des renseignements / sécurité de la gestion des clés →	Risques pour la sécurité du portefeuil	Le logiciel du portefeuille ne soutient pas les fonctions de sécurité	• Le logiciel du portefeuille n'a pas de protections	Acteur malveillant (local ou à distance)	Majeur : Clés compromises / portefeuille compromis / atteinte à la vie	• Le portefeuille utilise un logiciel de gestion des clés adéquat / évalué et/ou du matériel avec des clés non

torts causés au titulaire	le / la gestion des clés	requises pour le ou les niveaux d'assurance spécifiques / ciblés.	adéquates pour la gestion des clés. • Un acteur malveillant vole les clés secrètes (p. ex., il vole la clé de la mémoire, déplombe le cryptage de la boîte blanche, analyse de puissance).		privée / usurpation d'identité	exportables. *Remarque : Le caractère « adéquat » (NIST pour le logiciel) dépendra du niveau d'assurance.*
Sécurité des renseignements / contrôles de l'authentification → torts causés au titulaire	Utilisation non autorisée du portefeuille	Le logiciel du portefeuille ne soutient pas les fonctions de sécurité requises pour le ou les niveaux d'assurance spécifiques.	L'appareil manque d'une capacité d'authentification adéquate de l'utilisateur.	Accès par un non titulaire	Prise en charge du compte / atteinte à la vie privée / usurpation d'identité	Le portefeuille interdit des appareils et des versions OS spécifiques – exigences dictées par le niveau d'assurance.
Sécurité des renseignements / analyse des données → torts causés au titulaire	Analyse des données dans le portefeuille	Renseignements sensibles transmis lors de la collecte des analyses de données	Non intentionnel ou intentionnel	Acteur malveillant	• Fuite de données sensibles dans les données d'analyse • Atteinte à la vie privée / usurpation d'identité	• Si des données sensibles sont requises dans l'analyse, il faut s'assurer qu'elles sont anonymisées avant d'être envoyées – y compris avant d'être enregistrées pour être entreposées localement en mode hors ligne et dans des dossiers du portefeuille. • La marque de confiance pour assurer l'évaluation des risques pour la vie privée est attribuée en ajoutant / modifiant l'analyse des données – lorsque l'évaluation inclut un risque d'utilisation indésirable des

						données d'analyse. • Marque de confiance pour que les exigences relatives au contrôle de l'accès s'appliquent à l'accès aux données d'analyse.
Sécurité des renseignements / sécurité de l'environnement du portefeuille → torts causés au titulaire	Risques pour la sécurité des appareils	L'appareil n'est pas mis à jour avec les dernières mises à jour de sécurité.	Vulnérabilités exploitables	• Logiciel malveillant • Privilège de haut niveau • Attaque de l'homme du milieu	Atteinte à la vie privée / usurpation d'identité	• Le portefeuille vérifiera la version OS au moment du lancement, avisera le titulaire et (selon le niveau d'assurance) empêchera d'utiliser le portefeuille jusqu'à ce que la mise à jour soit terminée. • Le portefeuille interdit des appareils et versions OS spécifiques – exigences en fonction du niveau d'assurance.
Sécurité des renseignements / sécurité de l'environnement du portefeuille → torts causés au titulaire	Risques pour la sécurité des appareils	Les fonctionnalités de sécurité de l'appareil ne sont pas activées.	P. ex., verrou d'écran	Accès par un non-titulaire	Atteinte à la vie privée / usurpation d'identité	• Le portefeuille vérifie les vulnérabilités connues au lancement, avise le titulaire des vulnérabilités spécifiques et des mesures correctives requises avant d'utiliser le portefeuille. • Exigences en fonction du niveau de sécurité.
Sécurité des renseignements / Lien et authentification → torts causés au titulaire	Utilisation non autorisée du portefeuille	La personne qui utilise le portefeuille n'est pas le titulaire autorisé.	Quand les utilisateurs partagent des appareils, cela permettrait à d'autres d'émettre des assertions et de partager le document du titulaire autorisé sans son contentement.	• Pirates • Connaissances • Membres de la famille	Des assertions sont faites au nom de l'utilisateur sans son consentement.	• Inclure la formulation spécifique dans le CLU pour s'assurer que les utilisateurs autorisés comprennent leur responsabilité. • Authentification au niveau du portefeuille (par opposition à / en plus de l'autorisation de l'appareil). • Lien fort entre le portefeuille /

						l'authentification du portefeuille et la personne vérifiée. • Ajout de techniques antileurrage et de détection du vivant (ISO-30107)
Vie privée → suivi de l'utilisateur	Suivi de l'utilisateur	Le vérificateur suit le titulaire et partage avec d'autres vérificateurs qui peuvent faire le lien à l'aide des identifiants.	Le portefeuille numérique utilise des identifiants ordinaires avec de nombreux vérificateurs.	Invasion de la vie privée	Liaison des identifiants avec les vérificateurs; suivi de l'utilisateur; agrégation des données	• Le portefeuille utilise des technologies standard d'identifiants uniques comme : • URI (p. ex., diverses méthodes DID) • UUID • GUID
Vie privée→ suivi de l'utilisateur	Suivi de l'utilisateur	L'émetteur suit les interactions du titulaire avec les vérificateurs ou les émetteurs (l'émetteur est le courtier ici – modèle fédéré).	L'émetteur, le portefeuille et les vérificateurs établissent des protocoles de fédération (p. ex., SAML).	Invasion de la vie privée.	Liaison des identifiants par émetteur; suivi de l'utilisateur; agrégation des données	• Le portefeuille utilise des protocoles d'autosouveraineté / décentralisés qui sont la norme de l'industrie. • Transparence – l'avis relatif à la protection de la vie privée contient un langage clair et se conforme aux exigences des lois, politiques et règlements des territoires.
Vie privée → partage excessif	Partage excessif	Le portefeuille numérique ne soutient pas la minimisation des données (p. ex., le vérificateur demande une preuve à divulgation nulle de connaissance, le portefeuille numérique ne la soutient pas).	Le titulaire fournit au vérificateur plus de renseignements qu'il convient.	• Vérificateur indésirable ciblant l'utilisateur de portefeuilles numériques spécifiques qui n'offrent pas des capacités minimisation des données. • Vérificateur indésirable qui reçoit plus d'information	• Le titulaire fournit au vérificateur plus de renseignements qu'il convient. • Atteinte à la vie privée / usurpation d'identité. • Non-conformité du vérificateur avec la réglementation de la protection de la vie privée	• Le portefeuille va soutenir les capacités de minimisation des données (p. ex., divulgation sélective, preuve à divulgation nulle de connaissance).

				que demandé / nécessaire.	en ce qui concerne la réception de données pour lesquelles il n'avait pas un besoin commercial. • Impossibilité d'utiliser le vérificateur gouvernemental, car le gouvernement n'a peut-être pas l'autorisation de recevoir des renseignements supplémentaires qu'il n'a pas demandés.	
Vie privée → partage excessif	Partage excessif	Le portefeuille ne divulgue pas complètement l'information à partager au vérificateur ou ne permet pas au titulaire de contrôler.	Avis incomplet, pas clair ou ambigu	• Développeur de portefeuille (introduit la menace) – problème avec la qualité du portefeuille • Vérificateur indésirable ciblant l'utilisateur de portefeuille numériques spécifiques qui ne fournit pas un avis adéquat	• Le titulaire fournit au vérificateur plus de renseignements qu'il n'aurait voulu; les décisions prises par le vérificateur sur la base de ces renseignements pourraient avoir un impact négatif pour cet utilisateur. • Le titulaire n'est pas capable d'évaluer avec exactitude le risque de divulgation de	• Le portefeuille divulgue efficacement les renseignements à partager au titulaire et permet au titulaire de les contrôler. • Les données qui pourraient ne pas être « compréhensibles » (c.-à-d. données codées) devraient être décrites en langage clair comme étant impossibles à rendre.

					renseignements.	
Conformité → vie privée	Vie privée	Le portefeuille numérique ne se conforme pas à la composante « Respect de la vie privée » du CCP.		S.O.	• Non-conformité du respect de la vie privée	Marque de confiance pour assurer la conformité à la composante « Respect de la vie privée » du CCP dans le cadre de la certification du portefeuille.
Accessibilité	Utilisation du portefeuille numérique	Le portefeuille numérique ne se conforme pas aux normes d'accessibilité de l'industrie.		S.O.	• Le titulaire est incapable d'utiliser le portefeuille en raison de déficiences physiques; cela assujetti la population vulnérable à des processus de portefeuilles non numériques qui peuvent comporter plus de risques de usurpation d'identité. • Abandon; risque pour la réputation. • Manque de service; partage excessif des données.	• Le portefeuille instaure des capacités d'accessibilité standard de l'industrie.
Utilisabilité	Utilisation du portefeuille numérique	Le titulaire ne comprend pas la formulation du portefeuille.	• Les instructions du portefeuille ne sont pas claires pour le titulaire.	S.O.	• Le titulaire utilise le portefeuille d'une façon non prévue qui lui cause des torts.	• Le portefeuille utilise un langage clair et a une apparence uniforme. • Conception robuste du portefeuille : empêche l'accès ou le partage sans valider les entités

			• L'avis n'est pas clair ou est ambigu. • Expérience utilisateur médiocre.		• Divulgation de renseignements personnellement identifiables à un destinataire non prévu (atteinte accidentelle à la vie privée; hameçonnage).	avec qui les renseignements sont partagés.
Sécurité des renseignements / sécurité du registre de données → torts causés au titulaire	Qualité du registre de données de confiance	Le registre de données a des contrôles de sécurité et des pratiques de gestion inadéquates.	L'acteur malveillant insère ses clés publiques dans le registre de données (c'est un risque non pour le portefeuille, mais pour l'écosystème).	Acteur malveillant	• Les utilisateurs prennent des décisions non intentionnelles / mal informées sur le partage. • Atteinte à la vie privée / usurpation d'identité.	• Le portefeuille authentifie le registre de données comme étant de confiance; là où l'authentification implique une capacité à s'assurer qu'il est « légitime ».
Sécurité des renseignements / sécurité du registre de données → torts causés au titulaire	Qualité du portefeuille	Le portefeuille utilise le registre de données fourni par l'acteur malveillant.	Le portefeuille numérique fait confiance à la clé publique de l'acteur malveillant.	L'acteur malveillant qui établit un registre de données indésirable.	• Les utilisateurs prennent des décisions non intentionnelles / mal informées sur le partage. • Atteinte à la vie privée / usurpation d'identité.	• Le portefeuille authentifie le registre de données comme étant de confiance; là où l'authentification implique une capacité à s'assurer qu'il est « légitime ».
Accessibilité	Qualité du portefeuille	Le portefeuille ne soutient pas la langue du titulaire.	P. ex., le portefeuille ne soutient pas le chinois mandarin.	S.O.	Limites d'accessibilité / de marché adressable	• Le portefeuille instaure un soutien multilingue et/ou adopte des symboles ordinaires pour rendre la signification.

Sécurité des renseignements / contrôles de l'authentification → torts causés au titulaire	Confiance dans l'écosystème	Le titulaire interagit avec l'émetteur malveillant.	Le portefeuille : • N'authentifie pas l'émetteur pour le titulaire, ce qui cause des torts au titulaire. • N'informe pas efficacement le titulaire de l'identité vérifiée de l'émetteur.	Émetteur malveillant	Atteinte à la vie privée / usurpation d'identité	• Le portefeuille authentifie l'émetteur et instaure une communication efficace avec le titulaire; là où l'authentification implique une capacité à s'assurer qu'il est « légitime » (p. ex., clé publique de l'émetteur dans un registre de données certifié; la certification TLS concorde avec le DNS de l'émetteur).

Figure 3 : Risques liés au portefeuille numérique

5. Critères de conformité

Les critères de conformité sont catégorisés par élément de confiance. Pour faciliter la référence, un critère de conformité spécifique mentionné selon sa catégorie et son numéro de référence. Exemple : « BASE1 » correspond à la « référence nº 1 des critères de conformité de base »).

Remarques

- Les critères de conformité de base sont également inclus comme faisant partie de ce profil de conformité.
- Les critères de conformité spécifiés dans d'autres composantes du CCP s'appliqueront aussi aux justificatifs de la composante « Justificatifs (relations et attributs) » du CCP dans certaines circonstances.
- Pour avoir les indications les plus à jour en ce qui concerne les niveaux
- d'assurance, veuillez vous référer à l'ébauche de recommandation du modèle de maturité de l'assurance du CCP V1.0.

Référence	Critères de conformité	Niveau d'assurance			
BASE	**Ces critères de base s'appliquent à <u>tous</u> les processus du portefeuille numérique**	**LOA1**	**LOA2**	**LOA3**	**LOA4**

1	Ces critères de conformité ne remplacent ou 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 dans leur propre territoire.	X	X	X	X
2	Là où c'est applicable, les critères relatifs aux justificatifs, aux justificatifs vérifiables, aux relations et/ou aux attributs **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 1 de la composante « Justificatifs (relations et attributs) » du CCP.	X			
3	Là où c'est applicable, les critères relatifs aux justificatifs, aux justificatifs vérifiables, aux relations et/ou aux attributs **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 2 de la composante « Justificatifs (relations et attributs) » du CCP.		X		
4	Là où c'est applicable, les critères relatifs aux justificatifs, aux justificatifs vérifiables, aux relations et/ou aux attributs **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 3 de la composante « Justificatifs (relations et attributs) » du CCP.			X	
5	Là où c'est applicable, les critères relatifs aux justificatifs, aux justificatifs vérifiables, aux relations et/ou aux attributs **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 4 de la composante « Justificatifs (relations et attributs) » du CCP.				X
6	Là où c'est applicable, les critères relatifs à l'avis et au consentement **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 1 de la composante « Avis et consentement » du CCP.	X			
7	Là où c'est applicable, les critères relatifs à l'avis et au consentement **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 2 de la composante « Avis et consentement » du CCP.		X		

8	Là où c'est applicable, les critères relatifs à l'avis et au consentement **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 3 de la composante « Avis et consentement » du CCP.			X	
9	Là où c'est applicable, les critères relatifs à l'avis et au consentement **DOIVENT** se conformer aux critères de conformité du niveau d'assurance 4 de la composante « Avis et consentement » du CCP.				X
CREA	**Création du portefeuille numérique**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Dans le cadre de l'installation, l'application du portefeuille **DEVRAIT** s'assurer qu'elle est bien installée dans un environnement d'exécution soutenu par le fournisseur actuel (p. ex., le téléphone ou le système d'exploitation n'est plus soutenu par le fournisseur).	X			
2	Dans le cadre de l'installation, l'application du portefeuille **DOIT** s'assurer qu'elle est bien installée dans un environnement d'exécution soutenu par le fournisseur actuel (p. ex., le téléphone ou le système d'exploitation n'est plus soutenu par le fournisseur).		X	X	X
3	Dans le cadre de l'installation, l'application du portefeuille **DEVRAIT** s'assurer que le système d'exploitation est à jour et corrigé selon les exigences de sécurité minimales qui prévalent (p. ex., corrections de sécurité du fournisseur ou correctifs de sécurité essentiels).	X	X		
4	Dans le cadre de l'installation, l'application du portefeuille **DOIT** s'assurer que le système d'exploitation est à jour et corrigé selon les exigences de sécurité minimales qui prévalent (p. ex., corrections de sécurité du fournisseur ou correctifs de sécurité essentiels).			X	X

5	Le portefeuille **DEVRAIT** aviser et encourager le titulaire à faire une mise à jour/mise à niveau à la version certifiée minimale du portefeuille.	X			
6	Le portefeuille **DOIT** aviser et encourager le titulaire à passer à faire une mise à jour/mise à niveau à la version certifiée minimale du portefeuille.		X	X	X
7	Le portefeuille **PEUT** identifier la version du portefeuille aux émetteurs et aux vérificateurs, et leur permettre ainsi de gérer leurs propres risques associés à l'utilisation d'une version particulière d'un portefeuille.	X	X	X	X
8	Le processus de mise à jour du portefeuille **DEVRAIT** être fait à partir d'une source de confiance et s'assurer que la mise à jour n'a pas été compromise pendant le transfert ou l'installation (p. ex. par des signatures numériques).	X			
9	Le processus de mise à jour du portefeuille **DOIT** être fait à partir d'une source de confiance et s'assurer que la mise à jour n'a pas été compromise pendant le transfert ou l'installation (p. ex. par des signatures numériques).		X	X	X
10	Le portefeuille **DEVRAIT** utiliser le processeur d'entreposage et de cryptage de clés le plus sécuritaire disponible sur la plateforme hébergeant le portefeuille (p. ex., téléphone mobile, navigateurs) au niveau d'assurance opérationnel ciblé du portefeuille.	X	X		
11	Le portefeuille **DOIT** utiliser le processeur d'entreposage et de cryptage de clés le plus sécuritaire disponible sur la plateforme hébergeant le portefeuille (p. ex., téléphone mobile, navigateurs) au niveau d'assurance opérationnel ciblé du portefeuille.			X	X
12	Le portefeuille **DEVRAIT** amorcer la création de clés cryptographiques uniques.	X	X		

13	Le portefeuille **DOIT** amorcer la création de clés cryptographiques uniques.			X	X
14	Le portefeuille **DEVRAIT** faire l'essai des clés cryptographiques qui ont été créées.	X	X		
15	Le portefeuille **DOIT** faire l'essai des clés cryptographiques qui ont été créées.			X	X
16	Le portefeuille **PEUT** être capable de démontrer sa fiabilité au titulaire, à l'émetteur et au vérificateur (p. ex., un lien vers les résultats de l'audit du profil de conformité ou l'affichage d'une marque de confiance).	X			
17	Le portefeuille **DEVRAIT** être capable de démontrer sa fiabilité au titulaire, à l'émetteur et au vérificateur (p. ex., un lien vers les résultats de l'audit du profil de conformité ou l'affichage d'une marque de confiance).		X	X	X
18	Un portefeuille mobile **DEVRAIT** être capable de s'assurer que l'appareil dans lequel il réside n'a pas été enraciné ou compromis d'une manière similaire, ou encore qu'il est certifié ou évalué comme étant capable de fonctionner d'une façon sécuritaire dans un environnement ayant été compromis d'une manière similaire.	X			
19	Un portefeuille mobile **DOIT** être capable de s'assurer que l'appareil dans lequel il réside n'a pas été enraciné ou compromis d'une manière similaire, ou encore qu'il est certifié ou évalué comme étant capable de fonctionner d'une façon sécuritaire dans un environnement ayant été compromis d'une manière similaire.		X	X	X
20	Pour un portefeuille hébergé, le ou les fournisseurs de services **DEVRAIENT** être capables d'assurer ou de certifier (d'une manière continue) que l'environnement n'a pas de CVE non résolues ou « non atténuées » pour ce système.	X			

21	Pour un portefeuille hébergé, le ou les fournisseurs de services **DOIVENT** être capables d'assurer ou de certifier (d'une manière continue) que l'environnement n'a pas de CVE non résolues ou « non atténuées » pour ce système.		X	X	X
REGI	**Enregistrement du portefeuille numérique**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Le portefeuille **DEVRAIT** fournir une façon de vérifier d'une manière programmatique et de confirmer d'une manière cryptographique son statut « fiable ».	X			
2	Le portefeuille **DOIT** fournir une façon de vérifier d'une manière programmatique et de confirmer d'une manière cryptographique son statut « fiable ».		X	X	X
3	Le portefeuille **DOIT** permettre à une personne vérifiée ou à une organisation vérifiée d'identifier d'une manière unique et persistante une instance de portefeuille.			X	X
4	Le portefeuille **PEUT** avoir un mécanisme qui empêche un suivi non autorisé de ses activités par de multiples entités avec lesquelles il interagit (p. ex., il doit empêcher les entités d'agréger l'information concernant les justificatifs, les sujets, les titulaires ou d'autres renseignements partagés au moyen du portefeuille).	X			
5	Le portefeuille **DEVRAIT** avoir un mécanisme qui empêche un suivi non autorisé de ses activités par de multiples entités avec lesquelles il interagit (p. ex., il doit empêcher les entités d'agréger l'information concernant les justificatifs, les sujets, les titulaires ou d'autres renseignements partagés au moyen du portefeuille).		X		

6	Le portefeuille **DOIT** avoir un mécanisme qui empêche un suivi non autorisé de ses activités par de multiples entités avec lesquelles il interagit (p. ex., il doit empêcher les entités d'agréger l'information concernant les justificatifs, les sujets, les titulaires ou d'autres renseignements partagés au moyen du portefeuille).			X	X
7	Le portefeuille **DEVRAIT** maintenir une liste des entités auprès desquelles il est enregistré.	X	X	X	X
8	Le portefeuille **DEVRAIT** offrir au titulaire de se désenregistrer auprès d'une entité auprès de laquelle il s'est enregistré.	X	X	X	X
AUTH	**Authentification**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Le portefeuille **DOIT** authentifier le titulaire conformément aux critères de conformité de la composante « Authentification » du CCP pour le niveau d'assurance 1.	X			
2	Le portefeuille **DOIT** authentifier le titulaire conformément aux critères de conformité de la composante « Authentification » du CCP pour le niveau d'assurance 2.		X		
3	Le portefeuille **DOIT** authentifier le titulaire conformément aux critères de conformité de la composante « Authentification » du CCP pour le niveau d'assurance 3.			X	
4	Le portefeuille **DOIT** authentifier le titulaire conformément aux critères de conformité de la composante « Authentification » du CCP pour le niveau d'assurance 4.				X
5	Le portefeuille **DEVRAIT** mettre le titulaire au défi de s'authentifier quand il accomplit des interventions qui partagent, modifient, ajoutent ou suppriment des renseignements personnellement identifiables.	X			

6	Le portefeuille **DOIT** mettre le titulaire au défi de s'authentifier au niveau d'assurance voulu quand il accomplit des interventions qui partagent, modifient, ajoutent ou suppriment des renseignements personnellement identifiables.		X	X	X
7	Le portefeuille **DEVRAIT** garder des clés et des secrets privés dans un entreposage sécuritaire. REMARQUE : Veuillez vous référer à la section Entreposage des justificatifs d'authentification de la composante « Authentification » - CDIS 17 - 21.	X			
8	Le portefeuille **DOIT** garder des clés et des secrets privés dans un entreposage sécuritaire. REMARQUE : Veuillez vous référer à la section Entreposage des justificatifs d'authentification de la composante « Authentification » - CDIS 17 - 21.		X	X	X
9	Le portefeuille **DEVRAIT** enregistrer et entreposer en sécurité les renseignements (p. ex., heure, date, identification de l'utilisateur) à propos des événements d'authentification. Le portefeuille doit se conformer aux critères de conformité 1 et 5 de la composante « Authentification » du CCP.	X			
10	Le portefeuille **DOIT** enregistrer et entreposer en sécurité les renseignements (p. ex., heure, date, identification de l'utilisateur) à propos des événements d'authentification. Le portefeuille doit se conformer aux critères de conformité 2, 3, 4 et 5 de la composante « Authentification » du CCP.		X	X	X
REQU	**Demande de justificatif vérifiable**	**LOA1**	**LOA2**	**LOA3**	**LOA4**

1	Le portefeuille **PEUT** fournir une liste d'organisations et/ou de réseaux d'émetteurs vérifiés ou encore d'écosystèmes de confiance soutenus dans lesquels il peut fonctionner.	X	X	X	X
3	Le portefeuille **PEUT** autoriser un utilisateur à initier la demande du flux de justificatifs vérifiables.	X	X	X	X
4	Le portefeuille **PEUT** soutenir la demande d'un ou de plusieurs attributs d'une entité.	X	X	X	X
5	Le portefeuille **PEUT** soutenir la demande d'un ou de plusieurs attributs d'un justificatif vérifiable d'un autre titulaire.	X	X	X	X
6	Le portefeuille **PEUT** permettre à l'utilisateur de vérifier le statut d'une demande de justificatif vérifiable.	X	X	X	X
7	Le portefeuille **DEVRAIT** conserver un historique des demandes de justificatifs vérifiables que le titulaire peut consulter et est capable de gérer.	X	X	X	X
STOR	**Entreposage des justificatifs vérifiables**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Le portefeuille **DEVRAIT** fournir une capacité d'entreposage sécuritaire qui est conforme aux normes et pratiques exemplaires actuellement acceptées pour un entreposage sûr (p. ex., les pratiques exemplaires actuellement acceptées pour le cryptage).	X			
2	Le portefeuille **DOIT** fournir une capacité d'entreposage sécuritaire qui est conforme aux normes et pratiques exemplaires actuellement acceptées pour un entreposage sûr (p. ex., les pratiques exemplaires actuellement acceptées pour le cryptage).		X	X	X
3	Le portefeuille **PEUT** entreposer la clé de cryptage du stockage dans un entrepôt local.	X	X		
4	Le portefeuille **DEVRAIT** accéder à la clé de cryptage du stockage en utilisant une authentification robuste.	X			

5	Le portefeuille **DOIT** accéder à la clé de cryptage du stockage en utilisant une authentification robuste.		X	X	X
6	Le portefeuille **DEVRAIT** fournir des options d'authentification multifacteurs aux titulaires qui accèdent à leur entrepôt sécurisé.	X			
7	Le portefeuille **DOIT** fournir des options d'authentification multifacteurs aux titulaires qui accèdent à leur entrepôt sécurisé.		X	X	X
8	Le portefeuille **DEVRAIT** exiger une authentification multifacteurs pour les titulaires qui accèdent à l'entrepôt sécurisé.	X			
9	Le portefeuille **DOIT** exiger une authentification multifacteurs pour les titulaires qui accèdent à l'entrepôt sécurisé.		X	X	X
MANA	**Gestion des justificatifs vérifiables**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Le portefeuille **DEVRAIT** soutenir l'affichage de tous les attributs d'un justificatif vérifiable.	X			
2	Le portefeuille **DOIT** soutenir l'affichage de tous les attributs d'un justificatif vérifiable.		X	X	X
3	Le portefeuille **DOIT** permettre au titulaire de supprimer des justificatifs du portefeuille.	X	X	X	X
4	Le portefeuille **DEVRAIT** consigner les événements de gestion des justificatifs dans un registre d'audit. Le portefeuille doit se conformer aux critères 1 et 5 de la composante « Authentification » du CCP.	X			
5	Le portefeuille **DOIT** consigner les événements de gestion des justificatifs dans un registre d'audit. Le portefeuille doit se conformer aux critères 2, 3, 4 et 5 de la composante « Authentification » du CCP.		X	X	X
6	Le portefeuille **DOIT** consigner les événements de gestion des justificatifs dans un registre d'audit gardé dans une zone de stockage sécuritaire**.**			X	X

7	Le portefeuille **DEVRAIT** indiquer au titulaire le statut actuel, dans la mesure où le portefeuille possède de tels renseignements, des justificatifs (p. ex., si le justificatif a expiré ou été révoqué).	X			
8	Le portefeuille **DOIT** indiquer au titulaire le statut actuel, dans la mesure où le portefeuille possède de tels renseignements, des justificatifs (p. ex., si le justificatif a expiré ou été révoqué).		X	X	X
9	Le portefeuille **PEUT** permettre au titulaire de demander la révocation d'un justificatif.	X	X	X	X
DISP	**Affichage des justificatifs vérifiables**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Le portefeuille **DOIT** permettre au titulaire de naviguer dans une liste de tous les justificatifs qui y sont entreposés et d'afficher les détails de tout justificatif sélectionné par un titulaire.	X	X	X	X
2	Le portefeuille **DOIT** permettre à son titulaire de sélectionner un justificatif spécifique et d'afficher ses détails et attributs.	X	X	X	X
3	Le portefeuille **PEUT** consigner qu'un titulaire a affiché un ou des justificatifs et lesquels ont été affichés et quand.	X	X	X	
4	Le portefeuille **DEVRAIT** consigner qu'un titulaire a affiché un ou des justificatifs et lesquels ont été affichés et quand.				X
5	Le portefeuille **DEVRAIT** instaurer des pratiques exemplaires pour prévenir l'enregistrement d'écran non intentionnel ou malveillant pendant l'affichage des attributs ou détails des justificatifs.	X	X		
6	Le portefeuille **DOIT** instaurer des pratiques exemplaires pour prévenir l'enregistrement d'écran non intentionnel ou malveillant pendant l'affichage des attributs ou détails des justificatifs.			X	X
REND	**Rendu d'un justificatif vérifiable**	**LOA1**	**LOA2**	**LOA3**	**LOA4**

1	Le portefeuille **DEVRAIT** soutenir les normes d'accessibilité en rendant les justificatifs.	X	X	X	X
2	Le portefeuille **DEVRAIT** donner au titulaire la capacité de révéler ou masquer des attributs spécifiques.	X	X	X	X
3	Le portefeuille **DEVRAIT** donner au titulaire la capacité de rendre des justificatifs dans un format reconnaissable par des humains.	X	X	X	X
4	Le portefeuille **DEVRAIT** soutenir la localisation en rendant le justificatif.	X	X	X	X
PRES	**Présentation de la preuve**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Le portefeuille **DOIT** demander au titulaire du portefeuille la permission de présenter une preuve lorsqu'elle est demandée.	X	X	X	X
2	Le portefeuille **DOIT** afficher le nom de l'attribut demandé et toute valeur correspondante sélectionnée pour la réponse fournie comme preuve.	X	X	X	X
3	Le portefeuille **DOIT** permettre au titulaire d'autoriser qu'aucune preuve ou davantage de preuves soient envoyées quand plus d'une preuve est réclamée par une entité dans une seule demande.	X	X	X	X
4	Le portefeuille **PEUT** permettre au titulaire de sélectionner les attributs qui sont fournis dans une preuve avant qu'elle ne soit envoyée au demandeur.	X	X	X	X
5	Le portefeuille **DEVRAIT** permettre à un titulaire de présenter une preuve sans demande explicite.	X	X	X	X
6	Le portefeuille **DEVRAIT** permettre une divulgation sélective des attributs des preuves provenant d'un justificatif.	X	X	X	X
7	Le portefeuille **DEVRAIT** soutenir les preuves à divulgation nulle de connaissance et les prédicats dérivés.	X	X	X	X

8	Le titulaire du portefeuille **DOIT** être avisé des demandes de preuves.	X	X	X	X
9	Le portefeuille **PEUT** permettre au titulaire d'établir l'approbation ou le rejet préalable des demandes de preuve spécifique provenant d'entités spécifiques.	X	X	X	
10	Le portefeuille **DEVRAIT** conserver un historique des demandes de preuves pour une période prédéterminée appropriée à la mise en œuvre. Cette période doit être communiquée au titulaire avant qu'il n'utilise le portefeuille.	X	X		
11	Le portefeuille **DOIT** conserver un historique des demandes de preuves pour une période prédéterminée appropriée à la mise en œuvre. Cette période doit être mise à la disposition du titulaire avant qu'il n'utilise le portefeuille.			X	X
12	Le portefeuille **DEVRAIT** conserver un historique de la présentation des preuves.	X	X		
13	Le portefeuille **DOIT** conserver un historique de la présentation des preuves pour une période prédéterminée appropriée à la mise en œuvre. Cette période doit être mise à la disposition du titulaire avant qu'il n'utilise le portefeuille.			X	X
14	Le titulaire **DEVRAIT** avoir l'option de supprimer l'historique des événements maintenu par un portefeuille.	X			
15	Le titulaire **DOIT** avoir l'option de supprimer l'historique des événements maintenu par un portefeuille.		X	X	X
EXPR	**Consentement express**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Le portefeuille **DOIT** demander le consentement à partager les renseignements ou justificatifs du titulaire (c.-à-d. le titulaire) conformément aux critères établis dans la composante « Avis et consentement » du CCP.	X	X	X	X

2	Le portefeuille **DOIT** permettre au titulaire d'approuver ou de rejeter la demande de consentement.	X	X	X	X
3	Le portefeuille **DEVRAIT** enregistrer un historique des demandes de consentement, notamment les renseignements indiquant si une approbation a été accordée ou rejetée. Cela devrait être conservé pendant une période prédéterminée appropriée à la mise en œuvre. Cette période doit être mise à la disposition du titulaire avant qu'il n'utilise le portefeuille.	X			
4	Le portefeuille **DOIT** conserver un historique des demandes de consentement, notamment les renseignements indiquant si l'approbation a été accordée ou rejetée.		X	X	X
5	Les conditions d'entreposage et/ou de rétention des avis et les renseignements sur les consentements **DOIVENT** se conformer aux lois et règlements du ou des territoires où le consentement en dossier est appliqué et **DOIVENT** se conformer aux critères de conformité établis dans la composante « Avis et consentement » du CCP.	X	X	X	X
6	Le portefeuille **DEVRAIT** aviser le demandeur de l'avis de consentement du consentement affirmatif du titulaire.	X			
7	Le portefeuille **DOIT** aviser le demandeur de l'avis de consentement du consentement affirmatif du titulaire.		X	X	X

6. Historique des révisions

Version	Date	Auteur(s)	Commentaires
0.01	2022-01-17	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	2022-02-28	Équipe de conception du portefeuille numérique du CCP	Version mise à jour pour incorporer la rétroaction du TFEC
1.0	2022-03-30	Équipe de conception du portefeuille numérique du CCP	Le TFEC l'approuve comme ébauche de recommandation V1.0
1.1	2022-01-11	Équipe de conception du portefeuille numérique du CCP	Corrections initiales découlant de l'examen de la disposition des commentaires.
1.0	2023-01-18	Équipe de conception du portefeuille numérique du CCP	Le TFEC l'approuve comme candidat pour une 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