



1
2 **Profil de conformité de la composante**
3 **« Authentification » du CCP**

4 Statut du document : Recommandation finale V1.1

5 Conformément aux [procédures opérationnelles du CCIAN](#), une recommandation finale
6 est un livrable qui représente les conclusions d'un comité d'experts du Conseil canadien
7 de l'identification et de l'authentification numériques (CCIAN) ayant été approuvées par
8 un comité d'experts et ratifiées par un vote des membres bienfaiteurs du CCIAN.

9 Ce document a été préparé par le [Comité d'experts du Cadre de confiance](#)
10 [pancanadien](#) (TFEC) du CCIAN. On s'attend à ce que le contenu de ce document soit
11 examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise
12 en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois,
13 règlements et politiques. Les avis concernant les changements apportés à ce document
14 seront partagés sous la forme de communications électroniques, notamment le courriel
15 et les réseaux sociaux. Les notifications seront également consignées dans
16 le [programme de travail du Cadre de confiance pancanadien](#).

17 consignées dans le [programme de travail du Cadre de confiance pancanadien](#).

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

24 Droits de propriété intellectuelle : [Droits de propriété intellectuelle du CCIAN V1.0 PDF](#) |
25 © 2023

26

27

28

29

30

31
32
33
34
35
36
37
38
39
40
41

42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57

Table des matières

1. Introduction aux critères de conformité de la composante « Authentification » du CCP	3
1.1 À propos des critères de conformité du CCP.....	3
2. Conventions d’authentification.....	4
2.1 Mots clés des critères de conformité.....	4
3. Risques de l’authentification	5
4. Critères de conformité de la composante « Authentification »	19

58

59 **1. Introduction aux critères de conformité de la** 60 **composante « Authentification » du CCP**

61 Ce document spécifie les critères de conformité de la composante « Authentification »
62 du Cadre de conformité pancanadien (CCP). Pour avoir une introduction générale au
63 CCP, veuillez consulter l'aperçu du modèle de CCP. Cet aperçu fournit les buts et les
64 objectifs du CCP, une présentation générale du CCP et des renseignements
65 contextuels.

66 Chaque composante du CCP comporte deux documents :

- 67 1. **Aperçu** – Il introduit le sujet de la composante. L'aperçu fournit des
68 renseignements essentiels pour comprendre les critères de conformité de la
69 composante, à savoir des définitions des termes clés, des concepts et les
70 processus de confiance qui font partie de la composante.
- 71 2. **Profil de conformité** – Il spécifie les critères de conformité utilisés pour
72 uniformiser et évaluer l'intégrité des processus de confiance qui font partie de la
73 composante.

74 Les critères de conformité spécifiés dans le présent document peuvent être utilisés pour
75 assurer l'intégrité continue des processus de connexion et d'authentification de façon à
76 représenter un sujet unique en assurant qu'il s'agit du même sujet à chaque connexion
77 réussie auprès d'un fournisseur de services d'authentification.

78 **1.1 À propos des critères de conformité du CCP**

79 Le CCP favorise la confiance grâce à une série d'exigences commerciales et
80 techniques vérifiables pour divers processus.

81 Un processus est une activité commerciale ou technique (ou un ensemble de ces
82 activités) qui transforme une condition d'entrée en condition de sortie – un extrant dont
83 dépendent souvent d'autres processus. Les critères de conformité sont les exigences et
84 les spécifications qui forment une norme pour ces processus. Ils peuvent servir à
85 évaluer l'intégrité d'un processus. Dans le contexte du CCP, un processus est qualifié
86 de confiance quand il est vérifié et certifié conforme aux critères de conformité définis
87 dans un profil de conformité du CCP.

88 L'intégrité d'un processus est essentielle, car de nombreux participants—d'une diversité
89 de provinces et territoires, d'organisations et de secteurs, à court et à long terme—
90 dépendent de l'extrant de ce processus. Les critères de conformité sont donc

91 fondamentaux pour le cadre de confiance, car ils spécifient les exigences qui assurent
92 l'intégrité du processus.

93
94 **Remarque** : Les critères de conformité du CCP ne remplacent et ne substituent pas les
95 règlements existants; on s'attend à ce que les organisations et les particuliers se
96 conforment aux lois, politiques et règlements pertinents dans leur province ou territoire.

97 2. Conventions d'authentification

98 Chaque composante du CCP comporte des conventions qui assurent une utilisation et
99 une interprétation uniformes des termes et notions apparaissant dans la composante.

100 **L'aperçu de la composante « Authentification » du CCP fournit les conventions**
101 **pour cette composante.** Ces conventions incluent des définitions et descriptions des
102 éléments suivants auxquels il est fait référence dans ce profil de conformité :

- 103 • Principaux termes et notions
- 104 • Abréviations et acronymes
- 105 • Rôles
- 106 • Niveaux d'assurance
- 107 • Processus de confiance et conditions connexes

108
109 **Remarque**

- 110 • Les conventions peuvent varier selon les composantes du CCP. Les lecteurs
111 sont invités à examiner les conventions propres à chacune de ces composantes.
- 112 • Termes définis – Pour les besoins de ce profil de conformité, les termes et
113 définitions figurant dans l'aperçu de la composante « Authentification » et le
114 glossaire du CCP s'appliquent. Les principaux termes et notions décrits et définis
115 dans la présente section, ou dans l'aperçu de la composante « Authentification »
116 du CCP, sont indiqués en majuscules dans ce document.
- 117 • Liens hypertextes – Il se pourrait que des liens hypertextes soient intégrés dans
118 les versions électroniques de ce document. Tous les liens étaient accessibles au
119 moment de la rédaction.
- 120 • Toutes les mentions du terme « justificatif » dans le présent document font
121 référence à un « justificatif d'authentification ». La version raccourcie est utilisée
122 ici pour améliorer la lecture.

123 2.1 Mots-clés des critères de conformité

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

- 127 • **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de
- 128 conformité.
- 129 • **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de
- 130 conformité.
- 131 • **DEVRAIT** signifie que bien qu'il existe des raisons valables dans des
- 132 circonstances particulières pour ignorer l'exigence, toutes les implications
- 133 doivent être comprises et considérées avec soin avant de décider de ne pas
- 134 respecter les critères de conformité ou de choisir une option différente spécifiée
- 135 par les critères de conformité.
- 136 • **NE DEVRAIT PAS** signifie qu'il peut exister une raison valable dans des
- 137 circonstances particulières pour que l'exigence soit acceptable ou même utile,
- 138 mais que toutes les implications devraient être comprises et le cas devrait être
- 139 bien pris en considération avant de choisir de ne pas se conformer aux
- 140 exigences telles que décrites.
- 141 • **PEUT** signifie que l'exigence est discrétionnaire mais recommandée.
- 142

143 **Remarque** : les mots clés ci-dessus sont en **caractères gras** et en MAJUSCULES tout
 144 au long de ce profil de conformité.

145 3. Risques de l'authentification

136a	Type de risque	Catégorie de menace	Scénario de menace / vulnérabilité à la menace	Renseignements supplémentaires	Agent de menace	Impact	Protections proposées (p. ex., commentaires relatifs aux exigences de conformité)
136b	Sécurité de l'information → préjudices pour le titulaire/les parties dépendantes	Risque pour la qualité du produit ou du service	Le produit ou service contient des vulnérabilités logicielles	Intention accidentelle ou malveillante	<ul style="list-style-type: none"> • Pirate/ agresseur • Conséquences non intentionnelles des failles logicielles 	Préjudices pour les participants à l'écosystème : <ul style="list-style-type: none"> • Confiance dans l'écosystème • Risque pour la réputation de tout l'écosystème Préjudices pour le titulaire :	<ul style="list-style-type: none"> • Le produit est soumis à un processus de certification et, le cas échéant, à un processus de recertification, et il a une marque de confiance prouvant que la personne effectuant la mise en application suit les processus de développement des produits qui sont une pratique courante de l'industrie pendant

					<ul style="list-style-type: none"> • Vol d'identité • Préjudice financier • Perte de privilèges /d'accès/ d'usage • Atteinte à la réputation <p>Préjudices pour les parties dépendantes :</p> <ul style="list-style-type: none"> • Préjudices financiers • Perte de privilèges /d'accès/ d'usage • Atteinte à la réputation • Atteinte à la vie privée 	<p>tout le cycle de vie.</p> <ul style="list-style-type: none"> • Considérations pour la validation de l'intégrité de la chaîne d'approvisionnement, la sécurité du protocole SDLC, les évaluations de la sécurité des tierces parties, le processus de gestion de la vulnérabilité 	
136c	Gestion du cycle de vie de la sécurité de l'information → désagréments pour l'utilisateur	Risque pour la qualité du produit ou du service	Le produit ou le service n'est plus soutenu et est désuet	<ul style="list-style-type: none"> • Failles non corrigées • Manque d'interopérabilité/d'utilité 	<ul style="list-style-type: none"> • Acteurs malveillants ciblant des logiciels non corrigés • Logiciels inutilisables (incompatibles) 	<ul style="list-style-type: none"> • Le titulaire est incapable d'exécuter les transactions voulues • Justificatifs ou accès compromis 	<ul style="list-style-type: none"> • Le produit et/ou service devrait être mis à jour ou remplacé par un autre plus sécuritaire et un régime de gestion des correctifs devrait être maintenu
136d	Sécurité de l'information	Risque pour l'intégrité	Des acteurs malicieux fournissent	Des acteurs malicieux	Fournisseur de produits ou	<ul style="list-style-type: none"> • Personnalisation 	Le client évalue convenablement les fournisseurs de

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

	n → préjudices pour le titulaire	du fournisseur de produits ou de services/la chaîne d'approvisionnement	un produit ou service dans l'intention de nuire aux clients	fournissent un produit ou service qui peut sembler bien connu.	services malveillant	du titulaire <ul style="list-style-type: none"> • Atteinte à la vie privée du titulaire • Atteinte à la réputation du titulaire 	produits ou services; les clients peuvent se fier aux certifications et/ou marques de confiance
136e	Gestion du cycle de vie de la sécurité de l'information → désagréments pour l'utilisateur	Risque pour la qualité du produit ou du service	Le produit ou le service n'applique pas les normes de l'industrie ou ne s'y conforme pas	Le produit ou service est incapable d'interopérer avec des applications ou d'autres systèmes	Fournisseur de produits ou services	<ul style="list-style-type: none"> • Déni de service au client • Le titulaire est incapable d'effectuer les transactions requises • L'émetteur est incapable d'attribuer • Le vérificateur est incapable de vérifier 	<ul style="list-style-type: none"> • Le produit ou service applique les normes de l'industrie comme le prouve une marque de confiance ou un programme de certification appropriés • Vérifier l'interopérabilité avec des normes de l'industrie reconnues comme X.509, TOTP, SAML, la famille OIDC, des justificatifs vérifiables du W3C, etc.
135f	Sécurité de l'information → préjudices pour le titulaire	Risque pour la qualité du produit ou du service	Le produit ou le service a des pratiques de gestion ou des contrôles de sécurité techniques inadéquats	La mise en œuvre du produit ou service n'a pas été surveillée d'une	Pirate	Le système est facilement compromis, ce qui pourrait exposer des données ou	<ul style="list-style-type: none"> • Le fournisseur de produits ou services passe par un processus de certification et à une marque de confiance qui prouve sa

			manière appropriée		permettre à un agresseur sophistiqué d'attribuer des justificatifs non autorisés ou de contourner les contrôles d'accès	conformité aux pratiques standards de l'industrie. <ul style="list-style-type: none"> • Considérations pour la validation de l'intégrité de la chaîne d'approvisionnement, sécurité du SDLC, évaluations de la sécurité des tierces parties, processus de gestion de la vulnérabilité
136g	Sécurité de l'information : gestion des clés → préjudices pour les sujets	Risque d'un accès non autorisé aux données	L'environnement opérationnel ne soutient pas les fonctions de sécurité voulues pour les niveaux d'assurance spécifiques ou ciblés	Les outils et processus de gestion standards des clés de l'industrie ne sont pas utilisés ou pas utilisés efficacement	Acteur malveillant (local ou à distance)	Clés compromises/non-respect de la vie privée/vol d'identité/accès non autorisés aux données <ul style="list-style-type: none"> • Le fournisseur de produits ou services soutient explicitement une capacité de gestion des clés adéquate/évaluée Remarque <ul style="list-style-type: none"> • Cela inclut les fonctions de gestion des clés et les fonctions de sécurité à fort impact gérées sur l'infrastructure du produit ou service et/ou l'équipement de l'utilisateur final • Le protocole « adéquat » (FIPS pour le matériel, NIST pour le logiciel) dépendra du

						niveau d'assurance	
136h	Sécurité de l'information : gestion des clés → préjudices pour les sujets	Risques pour la sauvegarde et la récupération/risques pour la gestion des clés	Le produit ou service a des contrôles de sauvegarde et de récupération inadéquats	Un acteur malveillant vole des clés secrètes en utilisant des mécanismes de sauvegarde/récupération	Acteur malveillant (local ou à distance)	Clés compromise s'accès non autorisé aux données/non-respect de la vie privée/vol d'identité	<ul style="list-style-type: none"> • Les processus de sauvegarde et de récupération seront 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 ou de « service en temps réel »
136i	Sécurité de l'information : gestion des clés → préjudices pour les sujets	Risques de sécurité liés à l'infrastructure, aux logiciels ou aux appareils/risques pour la gestion des clés	Le produit ou service ne soutient pas les fonctions de sécurité requises pour le ou les niveaux d'assurance spécifiques ou ciblés.	<ul style="list-style-type: none"> • Le logiciel du produit ou service n'a pas de protections adéquates pour la gestion des clés. • Un acteur malveillant vole les clés secrètes 	Acteur malveillant (local ou à distance)	Clés compromise s'accès non autorisé aux données/non-respect de la vie privée/vol d'identité	<ul style="list-style-type: none"> • Le produit ou service utilise un logiciel et/ou du matériel de gestion des clés qui est adéquat/évalué avec des clés non exportables • Remarque : Le protocole « adéquat » (NIST pour le logiciel) dépendra du niveau d'assurance

			s (p. ex., il vole la clé de la mémoire, perce le cryptage de la boîte blanche, l'analyse de la puissance)			
136j	Sécurité de l'information : analyse des données → préjudices pour les sujets	Analyse des données dans le produit ou service	Le produit ou service permet (ou n'interdit pas adéquatement) de partager des renseignements sensibles (p. ex., renseignements sensibles transmis lors de la collecte d'analyse de données)	Non intentionnel ou intentionnel	Acteur malveillant ou effectif insuffisamment formé	<ul style="list-style-type: none"> • Fuite de données sensibles dans les données d'analyse • Non-respect de la vie privée/vol d'identité <ul style="list-style-type: none"> • Si des données sensibles sont nécessaires dans l'analyse, il faut s'assurer qu'elles sont anonymisées ou segmentées en unités et chiffrées avant d'être envoyées, y compris avant d'être enregistrées pour être entreposées localement dans des modes et des sauvegardes hors réseau • La marque de confiance pour assurer l'évaluation des risques pour la vie privée est terminée en

						<p>ajoutant/modifiant l'analyse des données lorsque l'évaluation inclut le risque d'une utilisation non intentionnelle des données d'analyse</p> <ul style="list-style-type: none"> • Marque de confiance pour assurer les exigences relatives au contrôle de l'accès aux données d'analyse • Formation de la main-d'œuvre sur les pratiques standard de confidentialité des données 	
136k	Sécurité de l'information : sécurité de l'environnement → préjudices pour les sujets	Risques pour la sécurité des initiés	Le personnel du fournisseur de produits ou services est compromis	Ingénierie sociale	Accès non autorisé aux données/a ccès hors sujet	Non-respect de la vie privée/vol d'identité	<ul style="list-style-type: none"> • Le fournisseur de produits ou services vérifie s'il y a des vulnérabilités connues au lancement, et avise les sujets/clients des vulnérabilités spécifiques et des mesures correctives nécessaires avant l'utilisation du produit ou service • Exigences dictées par le niveau d'assurance

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

136l

Sécurité de l'information : sécurité de l'environnement → préjudices pour le sujet	Risques pour la sécurité des initiés	Le titulaire du justificatif est compromis	Ingénierie sociale	Accès non autorisé aux données/a ccès hors sujet	Non-respect de la vie privée/vol d'identité	<ul style="list-style-type: none"> Le fournisseur de produits ou services vérifie s'il y a des vulnérabilités connues au moment du lancement, avise les sujets/clients des vulnérabilités spécifiques et des mesures correctives nécessaires avant d'utiliser le produit ou service Exigences dictées par le niveau d'assurance
--	--------------------------------------	--	--------------------	--	---	---

136m

Sécurité de l'information : obligation et authentification → préjudices pour le sujet	Utilisation non autorisée du produit ou service	Authentifiant compromis	Quand les utilisateurs partagent des services, des authentifiants sans contrôles appropriés de l'accès pourraient permettre à d'autres de partager des renseignements du titulaire autorisé sans son consentement	<ul style="list-style-type: none"> Pirates Connaissances Membres de la famille 	Des assertions sont faites de la part de l'utilisateur sans son consentement	<ul style="list-style-type: none"> Inclut un langage spécifique dans les conditions générales d'utilisation pour s'assurer que les utilisateurs autorisés comprennent leur responsabilité. Fournit des expériences en matière d'autorisation qui ne dépendent pas exclusivement de la possession et du contrôle d'un seul appareil. Applique des techniques supplémentaires
---	---	-------------------------	---	---	--	--

						d'anti-intrusion et de détection de spontanéité (ISO-30107)	
136n	Respect de la vie privée → suivi des utilisateurs	Suivi des utilisateurs	Identification de la corrélation des renseignements sans avis ou consentement	Le produit ou service utilise des identifiants communs à de multiples vérificateurs	Invasion de la vie privée	<ul style="list-style-type: none"> • Liaison des identifiants de multiples vérificateurs • Suivi des utilisateurs • Agrégation des données 	<ul style="list-style-type: none"> • Le produit ou service utilise des technologies d'identifiants uniques telles que : <ul style="list-style-type: none"> ○ URI (p. ex., diverses méthodes DID) ○ UUID ○ GUID
136o	Vie privée → partage excessif	Partage excessif	Le produit ou service ne soutient pas la minimisation des données	Le sujet fournit plus de renseignements au vérificateur que c'est approprié	<ul style="list-style-type: none"> • Vérificateur indésirable ciblant l'utilisateur d'un produit ou service spécifique qui n'offre pas de capacité de minimiser les données • Vérificateur non intentionnel qui reçoit plus de 	<ul style="list-style-type: none"> • Le titulaire fournit au vérificateur plus de renseignements que ce qui est approprié • Non-respect de la vie privée/vol d'identité • Non-conformité du vérificateur aux règlements qui régissent la vie 	Produit ou service pour soutenir les capacités de minimisation des données (p. ex., divulgation sélective, preuve à divulgation nulle de connaissance)

				renseignements qu'il n'en demande ou en a besoin	privée pour la réception de données dont il n'avait pas besoin pour ses affaires	
136p	Vie privée → partage excessif	Partage excessif	Le choix du justificatif et/ou des revendications par l'utilisateur final peut entraîner la	Avis incomplet, pas clair ou ambigu	<ul style="list-style-type: none"> • Incapacité pour un vérificateur gouvernemental de les utiliser car le gouvernement n'a peut-être pas l'autorisation de recevoir des renseignements supplémentaires qu'il n'a pas demandés 	<ul style="list-style-type: none"> • Fournisseur de produit ou service (introduit une menace • Le titulaire fournit au vérificateur plus de renseignements • Le produit ou service divulgue efficacement les renseignements à partager avec le titulaire et permet à celui-ci

		divulgateurs de renseignements qui ne sont pas strictement exigés		<p>e) – problème de qualité</p> <ul style="list-style-type: none"> • Vérificateur escroc ciblant l'utilisateur de produits ou services spécifiques qui n'offrent pas de mise en garde appropriée 	<p>ements ce qu'il aurait autrement accepté de faire; les décisions prises par le vérificateur concernant ces renseignements pourraient avoir des répercussions négatives pour cet utilisateur</p> <ul style="list-style-type: none"> • Le titulaire est incapable d'évaluer avec exactitude le risque que pose la divulgation de l'information 	<p>d'exercer un contrôle</p> <ul style="list-style-type: none"> • Les données qui peuvent ne pas être « compréhensibles » (c.-à-d., données codées) devraient être décrites dans un langage clair
--	--	---	--	---	--	--

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

136q

Vie privée → partage excessif	Partage excessif	Le produit ou service recueille plus de revendication s que ce qui est strictement nécessaire	Le sujet fournit au vérificateur plus de renseigne ments que ce qui est approprié. Avis incomplet, pas clair ou ambigu	Le fournisseur de produits ou services fait courir des risques à des renseigne ments supplémen taires	Le titulaire n'est pas capable d'évaluer avec exactitude le risque de divulgarion de l'information	<ul style="list-style-type: none"> Le produit ou service limite efficacement les renseignements qu'il recueille Le produit ou service fournit un avis complet et exhaustif au titulaire.
-------------------------------------	---------------------	---	---	--	---	--

136r

Conformité → vie privée	Vie privée	Le produit ou service ne se conforme pas à la composante « Respect de la vie privée » du CCP	S.O.	S.O.	Non-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 produit ou service
-------------------------------	------------	---	------	------	------------------------------------	---

136s

Accessibilit é	Expérien ce utilisateur	Le produit ou service ne se conforme pas aux normes d'accessibilité de l'industrie	S.O.	S.O.	<ul style="list-style-type: none"> Le titulaire est incapable d'utiliser le produit ou service en raison de sa situation de handicap ; il faut soumettre la population vulnérable à des processus 	Le produit ou service instaure des capacités d'accessibilité standards de l'industrie
-------------------	-------------------------------	---	------	------	--	---

					s ou outils de rechange qui peuvent comporter des risques différents pour la vie privée <ul style="list-style-type: none"> • Abandon ; risque pour la réputation • Manque de service; partage excessif de données 	
136t	Utilisabilité	Expérience utilisateur	Les instructions du produit ou service ne sont pas claires <ul style="list-style-type: none"> • Les instructions du produit ou service ne sont pas claires pour le titulaire • L'avis est vague ou ambigu • Expérience utilisateur 	S.O.	<ul style="list-style-type: none"> • Le titulaire utilise le produit ou service d'une manière non prévue qui lui porte préjudice • Divulgateion de renseignements personnels à un destinataire non 	<ul style="list-style-type: none"> • Le produit ou service utilise un langage clair, et a un aspect et une convivialité uniformes • Conception robuste du produit ou service : empêche l'accès ou le partage sans valider les entités avec qui les renseignements sont échangés

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

			médiocre		prévu (atteinte accidentelle à la vie privée; hameçonnage)		
136u	Sécurité de l'information : sécurité du registre de données → préjudice pour le sujet	Gouvernance	Le produit ou service dépend (fait confiance) d'une autorité en matière de justificatifs qui n'est pas (ou n'est plus) appropriée	Le produit ou service fait confiance à la clé publique de l'acteur malveillant	Acteur malveillant qui établit un registre de données ou une rubrique de registre indésirable	<ul style="list-style-type: none"> • Les utilisateurs prennent des décisions non intentionnelles ou mal informées sur le partage. • Atteinte à la vie privée/vol d'identité 	Le produit ou service authentifie le registre de données comme étant de confiance; l'authentification implique une capacité à assurer qu'elle « est légitime » ou « convient pour les fins définies »
136v	Sécurité de l'information : compromission des canaux → risques pour le sujet	Authentification manquante	<ul style="list-style-type: none"> • Le canal d'authentification n'est pas sûr ou est compromis (c.-à-d., agresseur au milieu) • Gestion de session non sécuritaire ou piratage de session 	S.O.	Tierce partie malveillante	<ul style="list-style-type: none"> • Accès aux données non autorisé, vie privée • Vol d'identité • Interventions non autorisées 	<ul style="list-style-type: none"> • Le produit ou service met en place des contrôles appropriés pour offrir le niveau d'assurance sélectionné • Le produit ou service a les contrôles qu'il a mis en place, vérifiés et/ou testés activement pour en assurer l'efficacité

136w

Sécurité de l'information : information stockée compromise	Clés compromises	Stockage de justificatifs : le stockage non sécuritaire de justificatifs peut mener à un accès non autorisé si les données stockées sont compromises	<ul style="list-style-type: none"> • Sauvegarde sécuritaire • Stockage de clés sécuritaire 	Tierce partie malveillante	<ul style="list-style-type: none"> • Atteinte à la vie privée • Vol d'identité • Accès autorisé aux données et/ou à une activité 	<ul style="list-style-type: none"> • Le produit ou service met en place des contrôles appropriés pour offrir le niveau d'assurance sélectionné • Le produit ou service a les contrôles qu'il a mis en place, vérifiés et/ou testés activement pour en assurer l'efficacité
--	------------------	--	--	----------------------------	---	--

146 4. Critères de conformité de la composante 147 « Authentification »

148 Les sections qui suivent définissent les critères de conformité qui sont des conditions
149 essentielles pour les processus de confiance de la composante « Authentification ». Les
150 processus de confiance de l'authentification sont les suivants :

- 151 1. Délivrance des justificatifs
- 152 2. Authentification
- 153 3. Début de session authentifiée
- 154 4. Fin de session authentifiée
- 155 5. Suspension des justificatifs
- 156 6. Récupération des justificatifs
- 157 7. Maintenance des justificatifs
- 158 8. Révocation des justificatifs

159 Les critères de conformité sont catégorisés par processus de confiance et profilés selon
160 les niveaux d'assurance. Ils sont groupés par sujet à l'intérieur de chaque catégorie.
161 Pour faciliter la référence, un critère de conformité spécifique peut être mentionné
162 d'après sa catégorie et son numéro de référence. Exemple : « **BASE-1** » fait référence
163 au « critère de conformité de base n° 1 ».

164 Remarques

- 166 • Les critères de conformité de base sont aussi inclus dans le présent profil de
167 conformité.

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

- 168 • Les critères de conformité spécifiés dans d'autres composantes du CCP peuvent
 169 aussi s'appliquer dans certaines circonstances aux processus de confiance de
 170 l'authentification.
- 171 • Les critères de conformité des notifications spécifiés dans le présent profil de
 172 conformité représentent uniquement les notifications spécifiques aux processus
 173 dans le contexte de la composante « Authentification » du CCP. Voir la
 174 composante « Avis et consentement » du CCP pour obtenir d'autres critères de
 175 conformité reliés aux notifications.
- 176 • Le niveau d'assurance 4 déborde du champ d'application de la présente version.
 177 La référence est conservée pour être intégrée dans des développements futurs.
- 178 • D'autres consignes sur les politiques et contrôles opérationnels soutenant le profil
 179 de conformité « Authentification » peuvent être consultées dans le profil de
 180 conformité « Infrastructure (technologie et opérations) » du CCP.

181

170a

170b

170c

170d

170e

170f

170g

Référence	Critères de conformité	Niveau d'assurance			
BASE	Critères de base	Nivea u 1	Nivea u 2	Nivea u 3	Nivea u 4
CONSIGNATION DES ÉVÉNEMENTS					
1	L'utilisation des justificatifs PEUT être consignée et conservée pendant une période prédéfinie en guise de preuve.	X			
2	L'utilisation des justificatifs DEVRAIT être consignée et conservée pendant une période prédéfinie en guise de preuve.		X		
3	L'utilisation des justificatifs DOIT être consignée et conservée pendant une période prédéfinie en guise de preuve.			X	
4	La gestion et l'utilisation des justificatifs DOIVENT être : <ul style="list-style-type: none"> • Retraçables jusqu'à un justificatif spécifique, et inclure le résultat, la date et l'heure de l'événement consigné; • Protégées par des contrôles pour limiter l'accès uniquement à 		X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		ceux qui en ont besoin (voir NIST Special Publication 800-92 pour des recommandations concernant la gestion des registres de sécurité).				
170h	5	Les registres de gestion et d'utilisation des justificatifs DOIVENT avoir un mécanisme de détection des tentatives frauduleuses pour déceler les modifications non autorisées.		X	X	
170i	6	Les renseignements personnels et les secrets d'authentification (p. ex., mots de passe, valeurs des mots de passe à usage unique, questions et réponses de sécurité) NE DOIVENT PAS être consignés dans le service.	X	X	X	
170j	SÉCURITÉ DE L'INFORMATION					
170k	7	Le fournisseur de services de justificatifs ou d'authentification PEUT assurer i) l'intégrité, ii) la confidentialité et iii) la disponibilité des services en suivant une série de consignes et de contrôles de sécurité de l'information (p. ex., CSEC ITSG-33) qui soutiennent ces efforts.	X			
170l	8	Le fournisseur de services de justificatifs ou d'authentification DOIT assurer i) l'intégrité, ii) la confidentialité et iii) la disponibilité des services en suivant une série de consignes et de contrôles de sécurité de l'information		X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		(p. ex., CSEC ITSG-33) qui soutiennent ces efforts.				
170m	9	Le fournisseur de services de justificatifs ou d'authentification DOIT avoir un rapport de contrôle vérifié d'une manière indépendante pour démontrer la conformité à une série de lignes directrices et de contrôles de sécurité de l'information.			X	
170n	GESTION DES SERVICES TI					
	10	Le fournisseur de services de justificatifs ou d'authentification DEVRAIT avoir une pratique de gestion des services documentée pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP.	X			
170o	11	Le fournisseur de services de justificatifs ou d'authentification DOIT établir et maintenir une pratique de gestion des services documentée pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP.		X		
170p	12	Le fournisseur de services de justificatifs ou d'authentification DOIT : <ul style="list-style-type: none"> • établir et maintenir une pratique de gestion des services documentée pour tous les aspects des services qu'il fournit en lien avec les 			X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		<p>processus de confiance de la composante « Authentification » du CCP.</p> <ul style="list-style-type: none"> avoir une pratique de gestion des services documentée et vérifiée de façon indépendante pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP. 				
170q	13	Le fournisseur de services de justificatifs ou d'authentification DEVRAIT se conformer à un cadre de gestion des services standard de l'industrie (p. ex., ITIL).	X	X		
170r	14	Le fournisseur de services de justificatifs ou d'authentification DOIT se conformer à un cadre de gestion des services standard de l'industrie (p. ex., ITIL).			X	
170s	SURVEILLANCE					
170t	15	Le fournisseur de services de justificatifs ou d'authentification DEVRAIT avoir des contrôles pour déceler l'utilisation malveillante ou la compromission des justificatifs.	X			
170u	16	Le fournisseur de services de justificatifs ou d'authentification DOIT avoir des contrôles pour déceler		X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		l'utilisation malveillante ou la compromission des justificatifs.				
170v	17	Le fournisseur de services de justificatifs DEVRAIT amorcer le processus de suspension, de maintenance ou de révocation des justificatifs quand il découvre des indications d'utilisation malveillante ou de compromission des justificatifs donnant lieu à des poursuites.	X			
170w	18	Le fournisseur de services de justificatifs DOIT amorcer le processus de suspension, de maintenance ou de révocation des justificatifs quand il découvre des indications d'utilisation malveillante ou de compromission des justificatifs donnant lieu à des poursuites.		X	X	
170x	RESPECT DE LA VIE PRIVÉE					
170y	19	Le fournisseur de services de justificatifs ou d'authentification DEVRAIT se conformer aux pratiques de gestion des risques pour la confidentialité de la composante « Respect de la vie privée » du CCP et de tous les profils pertinents du CCP applicables aux services d'identité numérique.	X			
170z	20	Le fournisseur de services de justificatifs ou d'authentification DOIT se conformer aux pratiques de gestion des risques pour la confidentialité de la		X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		composante « Respect de la vie privée » du CCP et de tous les profils pertinents du CCP applicables aux services d'identité numérique.				
170aa	21	Le fournisseur de services de justificatifs ou d'authentification DOIT se conformer aux pratiques de gestion des risques pour le respect de la vie privée qui sont acceptées par et applicables à toutes les parties participant au service d'identité numérique.		X	X	
170ab	NOTIFICATIONS					
170ac	22	Le fournisseur de services de justificatifs PEUT aviser sans délai le sujet (p. ex., notification immédiate par courriel, messagerie texte ou comme prescrit par une politique de ce fournisseur) de tout changement aux renseignements sur des justificatifs individuels (p. ex., mise à jour de mot de passe, ajout ou suppression d'authentifiants).	X			
170ad	23	Le fournisseur de services de justificatifs DOIT aviser sans délai le sujet (p. ex., notification immédiate par courriel, messagerie texte ou comme prescrit par une politique de ce fournisseur) de tout changement aux renseignements sur des justificatifs individuels (p. ex., mise à jour de mot de passe, ajout ou suppression d'authentifiants).		X	X	

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

	CDIS	Attribution de justificatifs	Niveau 1	Niveau 2	Niveau 3	Niveau 4
170ae	LIER UN SUJET					
170af						
170ag	1	Le fournisseur de services de justificatifs DEVRAIT imposer que le justificatif soit uniquement lié à un sujet.	X			
170ah	2	Le fournisseur de services de justificatifs DOIT imposer que le justificatif soit uniquement lié à un sujet.		X	X	
170ai	3	Le fournisseur de services de justificatifs PEUT documenter ou avoir un processus documenté pour démontrer le niveau d'assurance de l'identité du sujet quand le justificatif a été attribué.	X			
170aj	4	Le fournisseur de services de justificatifs DOIT documenter ou avoir un processus documenté pour démontrer le niveau d'assurance de l'identité du sujet quand le justificatif a été attribué.		X	X	
170ak	5	Le fournisseur de services de justificatifs DOIT mettre à la disposition des fournisseurs de services d'authentification des renseignements sur l'état actuel de tous les justificatifs qu'il a attribués, à moins que les contraintes du respect de la vie privée n'empêchent de partager ces renseignements (p. ex., si un justificatif est « inaccessible » ou « révoqué », le minimum de renseignements nécessaires sur l'état doit être mis à la	X	X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		disposition des fournisseurs de services d'authentification, si permis).				
170al	LIER DES AUTHENTIFIANTS					
170am	6	Le fournisseur de services de justificatifs PEUT donner la capacité de lier un authentifiant fourni par le sujet au justificatif.	X	X	X	
170an	7	Le fournisseur de services de justificatifs DOIT lier au moins un authentifiant au justificatif (p. ex., mot de passe, Foire aux questions ou mot de passe à usage unique).	X			
170ao	8	Le fournisseur de services de justificatifs DOIT lier deux authentifiants ou plus au justificatif (p. ex., mot de passe, Foire aux questions ou mot de passe à usage unique).		X	X	
170ap	9	Au moins deux authentifiants différents DEVRAIENT être liés au justificatif de sorte qu'il soit possible d'en récupérer un (qui a été perdu ou volé) en utilisant un autre authentifiant (p. ex., un compte d'authentifiant pourrait être récupéré avec un code de récupération à usage unique).		X		
170aq	10	Au moins deux authentifiants différents DOIVENT être liés au justificatif de sorte qu'il soit possible d'en récupérer un (qui a été perdu ou volé) en utilisant un autre authentifiant (p. ex., un compte d'authentifiant pourrait être récupéré avec			X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		un code de récupération à usage unique).				
170ar	11	Les authentifiants supplémentaires, qui pourraient servir à des fins de récupération, DOIVENT avoir un niveau d'assurance identique ou supérieur à celui d'un authentifiant à récupérer.		X	X	
170as	12	Le fournisseur de services de justificatifs PEUT documenter ou avoir un processus documenté pour démontrer le niveau d'assurance de l'identité du sujet quand le justificatif a été récupéré.	X			
170at	13	Le fournisseur de services de justificatifs DOIT documenter ou avoir un processus documenté pour démontrer le niveau d'assurance de l'identité du sujet quand le justificatif a été récupéré.		X	X	
170au	CRÉATION D'UN AUTHENTIFIANT					
170av	14	Quand l'authentifiant est créé (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le créateur DOIT avoir un système ou des processus de gestion de la qualité vérifiables.		X		
170aw	15	Quand l'authentifiant est créé (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le créateur DOIT avoir un système ou des processus de gestion de la qualité vérifiables.			X	
170ax	16	Quand l'authentifiant utilise des renseignements		X		

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		intégrés par un fabricant (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le fournisseur de services de justificatifs DOIT s'assurer qu'il y a un processus de gestion de la sécurité vérifiable qui empêche les renseignements d'être compromis de la fabrication à la livraison au fournisseur de services de justificatifs.				
170ay	17	Quand l'authentifiant utilise des renseignements intégrés par un fabricant (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le fournisseur de services de justificatifs DOIT s'assurer qu'il y a un processus de gestion de la sécurité vérifié d'une manière indépendante qui empêche les renseignements d'être compromis de la fabrication à la livraison au fournisseur de services de justificatifs.			X	
170az	ENTREPOSAGE DE JUSTIFICATIFS					
170ba	18	Le fournisseur de services de justificatifs ou d'authentification DOIT imposer des contrôles pour empêcher l'accès non autorisé aux renseignements sur les justificatifs.	X	X	X	
170bb	19	Les secrets liés au justificatif DOIVENT être entreposés comme du hash salé ou chiffrés.		X	X	
170bc	20	Les attributs des justificatifs qui contiennent des renseignements personnels	X	X	X	

		entreposés dans le service DOIVENT être sécurisés (p. ex., chiffrés et/ou hashés).				
170bd	21	Les sauvegardes des renseignements liés aux justificatifs DOIVENT être chiffrées avant d'être entreposées à long terme et DOIVENT rester chiffrées tant qu'elles sont entreposées.		X	X	
170be	22	Les modules cryptographiques DOIVENT satisfaire une norme de validation reconnue de l'industrie (p. ex., <u>FIPS 140-2</u>).		X	X	
170bf	AUTH	Authentification	LOA1	LOA2	LOA3	LOA4
170bg	AUTHENTIFIANTS					
170bh	1	Le fournisseur de services d'authentification DOIT exiger au moins un authentifiant des types suivants : <ul style="list-style-type: none"> • Chose que le sujet connaît; • Chose que le sujet a; • Chose que le sujet est ou fait. 	X	X		
170bi	2	Si un seul authentifiant est requis, l'authentifiant DOIT être du type « chose que le sujet connaît » ou « chose que le sujet a ». Un authentifiant du type « chose que le sujet est ou fait » NE DOIT ÊTRE utilisé que comme authentifiant secondaire.		X		
170bj	3	Le fournisseur de services d'authentification DOIT exiger au moins deux authentifiants différents qui :			X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		<ul style="list-style-type: none"> fournissent des facteurs d'authentification différents; ne sont pas susceptibles aux mêmes vecteurs de menaces. 				
170bk	4	<p>Parmi les différents authentifiants exigés par le fournisseur de services d'authentification selon les critères de la section AUTH :</p> <ul style="list-style-type: none"> un des authentifiants DOIT être du type « chose que le sujet a »; les autres authentifiants PEUVENT être du type « chose que le sujet connaît » ou « chose que le sujet est ou fait ». 			X	
170bl	5	Le fournisseur de services d'authentification DOIT consulter les renseignements fournis par le fournisseur de services de justificatifs pour déterminer l'état actuel d'un justificatif.	X	X	X	
170bm	6	Une biométrie NE DEVRAIT PAS être utilisée, à moins que sa nécessité ne soit démontrée et qu'il s'agisse du meilleur mécanisme pour répondre à un besoin d'authentification spécifique compte tenu de l'éventuelle perte correspondante de confidentialité.	X	X	X	
170bn	TYPE D'AUTHENTIFIANT					

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

170bo	6	N'importe quel type d'authentifiant PEUT être utilisé.	X			
170bp	7	Le fournisseur de services d'authentification DOIT utiliser une norme ou une pratique exemplaire de l'industrie pour l'authentification (p. ex., normes développées et approuvées par Kantara, W3C, IETF ou FIDO Alliance).		X	X	
170bq	8	Le fournisseur de services d'authentification DOIT utiliser des types d'authentifiants qui résistent aux menaces énumérées dans les critères d' ATTÉNUATION DES MENACES pour le niveau d'assurance 3.			X	
170br	ATTÉNUATION DES MENACES					
170bs	9	Le fournisseur de services d'authentification DOIT avoir des processus de contrôle efficaces pour prévenir et déceler au moins les types d'attaques suivants et s'en remettre : <ul style="list-style-type: none"> • Devinette des secrets des authentifiants; • Rejeu. Cela PEUT être inclus dans la portée des lignes directrices décrites dans les critères de la section BASE .	X			
170bt	10	Le fournisseur de services d'authentification DOIT avoir des processus de contrôle efficaces pour prévenir et déceler au moins les types d'attaques suivants et s'en remettre :		X		

		<ul style="list-style-type: none"> • Devinette des secrets des authentifiants; • Rejeu; • Écoute illicite; • Piratage de session. <p>Cela DOIT être inclus dans la portée des lignes directrices décrites dans les critères de la section BASE.</p>				
170bu	11	<p>Le fournisseur de services d'authentification DOIT avoir des processus de contrôle efficaces pour prévenir et déceler au moins les types d'attaques suivants et s'en remettre :</p> <ul style="list-style-type: none"> • Devinette des secrets des authentifiants; • Rejeu; • Écoute illicite; • Piratage de session; • Usurpation d'identité/hameçonnage; • Homme du milieu (p. ex., utilisation d'un TLS mutuellement authentifié). <p>Cela DOIT être inclus dans la portée du processus de vérification indépendante exigé dans les critères de la section BASE.</p>			X	
170bv	RISQUE D'ADAPTATION					
170bw	12	<p>Le fournisseur de services d'authentification PEUT offrir la capacité d'authentifier le risque d'adaptation.</p>	X			
170bx	13	<p>Le fournisseur de services d'authentification DEVRAIT offrir la capacité</p>		X		

		d'authentifier le risque d'adaptation.				
170by	14	Le fournisseur de services d'authentification DOIT déceler et atténuer les interactions qui représentent un risque élevé, en se basant sur les renseignements provenant du contexte de l'authentification (comme les transactions provenant d'un endroit ou d'un canal imprévu pour un sujet, ou qui indiquent une configuration matérielle ou logicielle imprévue). -ou- Le fournisseur de services d'authentification DOIT traiter chaque interaction comme représentant un risque élevé.			X	
170bz	MODULE CRYPTOGRAPHIQUE					
170ca	15	Les modules cryptographiques utilisés dans l'authentification côté client DOIVENT respecter une norme de validation reconnue de l'industrie (p. ex., <u>FIPS 140-2</u> ou l'équivalent).		X	X	
170cb	RÉSULTAT DE L'AUTHENTIFICATION					
170cc	16	Le fournisseur de services d'authentification DOIT déclarer une réussite seulement si le sujet a effectué avec succès sa tentative d'authentification.	X	X	X	
170cd	17	Le fournisseur de services d'authentification DOIT déclarer un échec à une tentative d'authentification si	X	X	X	

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

		le justificatif présenté est suspendu ou révoqué ou encore si l'on décèle une utilisation malveillante ou la compromission du justificatif.				
170ce	18	Le fournisseur de services d'authentification DOIT fournir un mécanisme qui : <ul style="list-style-type: none"> • Confirme que le résultat de l'authentification provient du fournisseur de services d'authentification; • N'a pas été altéré pendant le transit; • Ne peut être utilisé que par la partie dépendante. 		X	X	
170cf	19	Le résultat de l'authentification DOIT être valide pour une période maximale qui est : <ul style="list-style-type: none"> • spécifiée par le fournisseur de services d'authentification; • connue de la partie dépendante. 		X	X	
170cg	INSE	Lancement de session authentifiée	Niveau 1	Niveau 2	Niveau 3	Niveau 4
170ch	LANCEMENT DE SESSION					
170ci	1	Le fournisseur de services d'authentification DEVRAIT offrir la capacité de maintenir une session qui lie toutes les parties dépendantes, le lancement de session authentifiée étant un processus soutenu.	X			
170cj	2	Le fournisseur de services d'authentification DOIT offrir la capacité de maintenir une		X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		session qui lie toutes les parties dépendantes, le lancement de session authentifiée étant un processus soutenu.				
170ck	3	Si un sujet est authentifié à un niveau d'assurance donné, la session qui en résulte DOIT être considérée comme étant du même niveau d'assurance (p. ex., si le sujet est authentifié au niveau d'assurance 2, la session DOIT être considérée comme étant du niveau d'assurance 2), le lancement de session authentifiée étant un processus soutenu.	X	X	X	
170cl	RÉAUTHENTIFICATION					
170cm	4	Le fournisseur de services d'authentification DEVRAIT exiger que le sujet s'authentifie de nouveau après une période ou un événement prédéterminés selon une approche basée sur les risques (p. ex., quand une seule tentative de connexion est effectuée avec une autre partie dépendante dans une fédération).	X			
170cn	5	Le fournisseur de services d'authentification DOIT exiger que le sujet s'authentifie de nouveau après une période ou un événement prédéterminés selon une approche basée sur les risques (p. ex., quand une seule tentative de connexion est effectuée avec une autre partie		X	X	

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

		dépendante dans une fédération ou quand une partie dépendante demande une réauthentification).				
170co	6	Le fournisseur de services d'authentification PEUT rallonger les périodes d'inactivité des sessions.	X			
170cp	7	Si la réauthentification est au niveau d'assurance 2 ou 3, les périodes d'inactivité des sessions PEUVENT être prolongées mais DOIVENT correspondre au niveau d'assurance initial et remplir tous les critères d'authentification indiqués plus haut.		X	X	
170cq	TESE	Fin de la session authentifiée	Niveau 1	Niveau 2	Niveau 3	Niveau 4
170cr	SESSION INACTIVE					
170cs	1	Le fournisseur de services d'authentification DEVRAIT imposer une durée de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.	X			
170ct	2	Le fournisseur de services d'authentification DOIT imposer une durée de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.		X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

170cu	3	Le fournisseur de services d'authentification DEVRAIT imposer une durée d'inactivité de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.	X			
170cv	4	Le fournisseur de services d'authentification DOIT imposer une durée d'inactivité de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.		X	X	
170cw	5	Les valeurs de la durée et d'inactivité de session maximales au niveau d'assurance 3 DEVRAIENT être plus courtes que celles pour le niveau d'assurance 2.			X	
170cx	6	Une session inactive en raison d'un dépassement de la durée ou de la durée d'inactivité de session maximale au niveau d'assurance 3 PEUT entraîner une fin de session ou une baisse à une session de niveau d'assurance 2.			X	
170cy	7	En cas de passage à une session de niveau inférieur : <ul style="list-style-type: none"> Le fournisseur de services d'authentification 			X	

		<p>DOIT aviser toutes les parties dépendantes associées à la session de niveau d'assurance 3;</p> <ul style="list-style-type: none"> Les sessions inactives en raison d'un dépassement de la durée de session ou de la durée d'inactivité de session maximale <p>PEUVENT être prolongées jusqu'aux valeurs du niveau d'assurance 2 (moins le temps déjà passé).</p>				
170cz	FIN DE SESSION					
170da	8	Le fournisseur de services d'authentification DEVRAIT aviser toutes les parties dépendantes que la session est terminée.	X			
170db	9	Le fournisseur de services d'authentification DOIT aviser toutes les parties dépendantes que la session est terminée.		X	X	
170dc	CRSP	Suspension de justificatifs	Niveau 1	Niveau 2	Niveau 3	Niveau 4
170dd	PAR UN SUJET					
170de	1	Le fournisseur de services de justificatifs DEVRAIT donner à un sujet la capacité de procéder à la suspension d'un justificatif.	X	X	X	
170df	PAR UN ADMINISTRATEUR					
170dg	2	Le fournisseur de services de justificatifs PEUT donner au personnel autorisé la capacité de suspendre l'utilisation d'un justificatif.	X	X	X	
170dh	3	Le fournisseur de services de justificatifs DEVRAIT	X			

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

		imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.				
170di	4	Le fournisseur de services de justificatifs DOIT imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.		X	X	
170dj	5	Le fournisseur de services de justificatifs DOIT demander au personnel autorisé de fournir un niveau d'assurance 3 ou un justificatif supérieur afin de suspendre l'utilisation d'un justificatif.			X	
170dk	CRVY	Récupération des justificatifs	Niveau 1	Niveau 2	Niveau 3	Niveau 4
170dl	PAR UN SUJET					
170dm	1	Le fournisseur de services de justificatifs DEVRAIT donner au sujet la capacité de demander la récupération d'un justificatif suspendu, la récupération des justificatifs étant un processus soutenu.	X			
170dn	2	Le fournisseur de services de justificatifs DEVRAIT exiger que le sujet s'authentifie avec un niveau d'assurance équivalent à celui du justificatif récupéré, la récupération des justificatifs étant un processus soutenu.	X			
170do	3	Le fournisseur de services de justificatifs DOIT donner au sujet la capacité de demander la récupération d'un justificatif suspendu, la récupération des justificatifs étant un processus soutenu.		X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

170dp	4	Le fournisseur de services de justificatifs DOIT exiger que le sujet s'authentifie avec un niveau d'assurance équivalent à celui du justificatif récupéré, la récupération des justificatifs étant un processus soutenu.		X	X	
170dq	PAR UN ADMINISTRATEUR					
170dr	5	Le fournisseur de services de justificatifs PEUT donner au personnel autorisé la capacité d'entreprendre la récupération d'un justificatif pour le sujet.	X	X	X	
170ds	6	Le fournisseur de services de justificatifs DEVRAIT imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus, la récupération des justificatifs étant un processus soutenu.	X			
170dt	7	Le fournisseur de services de justificatifs DOIT imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus, la récupération des justificatifs étant un processus soutenu.		X	X	
170du	8	Le fournisseur de services de justificatifs DOIT obliger le personnel autorisé à fournir un justificatif de niveau d'assurance 3 ou supérieur pour récupérer un justificatif, la récupération des justificatifs étant un processus soutenu.			X	
170dv	PAR UN SYSTÈME					
170dw	9	Le fournisseur de services de justificatifs PEUT offrir la capacité de récupérer automatiquement un	X	X	X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		justificatif suspendu (p. ex., réactiver automatiquement un justificatif préalablement suspendu à la suite d'un trop grand nombre de tentatives de connexion ratées).				
170dx	CRMA	Maintenance des justificatifs	Niveau 1	Niveau 2	Niveau 3	Niveau 4
170dy	PAR UN SUJET					
170dz	1	Le fournisseur de services de justificatifs DEVRAIT donner la possibilité de mettre à jour les authentifiants liés au justificatif lorsque c'est possible (p. ex., changer de mot de passe, lier un nouvel authentifiant).	X			
170ea	2	Le fournisseur de services de justificatifs DEVRAIT donner la possibilité de modifier les attributs des justificatifs (p. ex., mot de passe, Foire aux questions, codes de récupération).	X			
170eb	3	Le fournisseur de services de justificatifs DOIT donner la possibilité de mettre à jour les authentifiants liés au justificatif lorsque c'est possible (p. ex., changer de mot de passe, changer de NIP, rafraîchir la photo du visage en dossier par une image plus récente ou changer une clé privée).		X	X	
170ec	4	Le fournisseur de services de justificatifs DOIT donner la possibilité de modifier les attributs des justificatifs (p. ex., mot de passe, Foire aux questions, codes de récupération clés		X	X	

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

		cryptographiques, biométrie, alias, DID).				
170ed	5	Le fournisseur de services de justificatifs DOIT exiger une authentification à un niveau d'assurance équivalent ou supérieur à celui de l'attribut du justificatif qui est modifié (p. ex., mot de passe, Foire aux questions, codes de récupération clés cryptographiques, biométrie, alias, DID). Par exemple, un sujet connecté à l'aide d'un mot de passe à un seul facteur ne devrait pas pouvoir modifier des codes de récupération et des valeurs de mots de passe à usage unique.		X	X	
170ee	PAR UN ADMINISTRATEUR					
170ef	6	Le fournisseur de services de justificatifs PEUT permettre au personnel autorisé de mettre à jour les authentifiants liés au justificatif (p. ex., supprimer un authentifiant ou entreprendre un changement de mot de passe).	X	X	X	
170eg	7	Le fournisseur de services de justificatifs PEUT permettre au personnel autorisé de mettre à jour les attributs des justificatifs.	X	X	X	
170eh	8	Le fournisseur de services de justificatifs DOIT imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.	X	X	X	
170ei	9	Le fournisseur de services de justificatifs DOIT exiger			X	

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		que le personnel autorisé donne un justificatif de niveau 3 ou supérieur pour effectuer la maintenance des justificatifs.				
170ej	10	Le fournisseur de services de justificatifs DEVRAIT exiger que le sujet termine les activités liées aux justificatifs amorcées par un administrateur (p. ex., un administrateur ne peut pas changer le mot de passe d'un sujet, seulement amorcer une réinitialisation).	X			
170ek	11	Le fournisseur de services de justificatifs DOIT exiger que le sujet termine les activités liées aux justificatifs amorcées par un administrateur (p. ex., un administrateur ne peut pas changer le mot de passe d'un sujet, seulement amorcer une réinitialisation).		X	X	
170el	PAR UN SYSTÈME					
170em	12	Le fournisseur de services de justificatifs DEVRAIT imposer des exigences en matière de contrôle et de protection des authentifiants (p. ex., Foire aux questions, exigences en matière de complexité, mises à jour des mots de passe, mises à jour des mots de passe à usage unique) appropriées à l'authentifiant (voir NIST Special Publication 800-53 (Rev. 4) et la page Orientation sur les mots de passe du gouvernement du Canada pour avoir des exemples et des références).	X			

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

170en	13	Le fournisseur de services de justificatifs DOIT imposer des exigences en matière de contrôle et de protection des authentifiants (p. ex., Foire aux questions, exigences en matière de complexité, mises à jour des mots de passe, mises à jour des mots de passe à usage unique) appropriées à l'authentifiant (voir NIST Special Publication 800-53 (Rev. 4) et la page Orientation sur les mots de passe du gouvernement du Canada pour avoir des exemples et des références).		X	X	
170eo	CRVX	Révocation de justificatifs	Niveau 1	Niveau 2	Niveau 3	Niveau 4
170ep	PAR UN SUJET					
170eq	1	Le fournisseur de services de justificatifs DEVRAIT permettre à un sujet de révoquer son propre justificatif.	X			
170er	2	Le fournisseur de services de justificatifs DOIT permettre à un sujet de révoquer son propre justificatif.		X	X	
170es	PAR UN ADMINISTRATEUR					
170et	3	Le fournisseur de services de justificatifs PEUT permettre au personnel autorisé de révoquer un justificatif.	X			
170eu	4	Le fournisseur de services de justificatifs DOIT pouvoir permettre au personnel autorisé de révoquer un justificatif.		X	X	
170ev	5	Le fournisseur de services de justificatifs DOIT imposer	X	X	X	

Cadre de confiance pancanadien
Composante « Authentification » du CCP – Recommandation finale V1.1
CCIAN / CCP03

		des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.				
170ew	6	Le fournisseur de services de justificatifs DOIT obliger le personnel autorisé à fournir un justificatif ayant un niveau d'assurance 3 ou supérieur afin de révoquer un justificatif.			X	

182 **Tableau 1. Critères de conformité de la composante « Authentification » du CCP**

183

184 Historique des révisions

173a	Version	Date de publication	Auteur(s)	Description
173b	.01	2018-04-10	TFEC	Ébauche de travail initiale
173c	.02	2018-07-31	Rédacteur du CCIAN	Changements suggérés en fonction des commentaires d'examen en suspens.
173d	.03	2019-04-30	Rédacteur du CCIAN	<ul style="list-style-type: none"> • Modifications au formatage • Mise à jour des liens vers les normes mentionnées
173e	.04	2019-07-08	Rédacteur du CCIAN	<ul style="list-style-type: none"> • Uniformisation de la priorité des modalités des exigences • Mise à jour de l'image du modèle de CCP
173f	.05	2019-10-21	TFEC et équipe de rédaction du CCP	Révision du contenu basée sur les commentaires concernant l'ébauche de discussion.
173g	1.0	2019-10-30	TFEC	Approbation comme recommandation préliminaire V1.0
173h	1.1	S.O.	Équipe de rédaction du CCP	Mises à jour apportées en fonction des commentaires reçus pendant la période d'examen des recommandations préliminaires.
173i	1.0	2020-05-11	Équipe de rédaction du CCP	Recommandation finale V1.0
173j	1.1	2023-11-15	Équipe de conception de	Mises à jour apportées en fonction de la rétroaction reçue dans le cadre des

Cadre de confiance pancanadien
 Composante « Authentification » du CCP – Recommandation finale V1.1
 CCIAN / CCP03

		l'authentification du CCP	essais alpha du CCP et des commentaires reportés lors d'itérations antérieures.
173k	1.1	2023-12-01	Équipe de conception de l'authentification du CCP
			Approbation du TFEC comme recommandation finale V1.1

185