Profil de conformité de l'authentification du CCP

Statut du document : Recommandation finale version 1.0

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

Ce document a été préparé par le Comité d'experts du Cadre de confiance pancanadien du CCIAN avec l'apport du public recueilli et traité par le biais d'un processus d'examen ouvert mené par des 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 au moyen 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). Les changements apportés à ce document qui pourraient se répercuter sur l'état des certifications et des marques de confiance seront définis dans la composante « Évaluation » du CCP.

Table des matières

1 Introduction aux critères de conformité de la composante « Authentification » du CCP

Ce document spécifie l'ensemble de critères de conformité pour la composante « Authentification » du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale au CCP, veuillez consulter l'aperçu du modèle de CCP. Cet aperçu fournit les buts et objectifs du CCP, une présentation de haut niveau du modèle de cadre de confiance pancanadien et des renseignements contextuels.

Chaque composante du CCP comporte deux documents :

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

Les critères de conformité spécifiés dans le présent document peuvent être utilisés pour assurer l'intégrité constante des processus de connexion et d'authentification de façon à ce qu'ils donnent la représentation d'un sujet unique à un niveau d'assurance qu'il s'agit du même sujet à chaque connexion réussie auprès d'un fournisseur de services d'authentification.

1.1 À propos des critères de conformité du CCP

Le cadre de confiance pancanadien favorise la confiance grâce à une série d'exigences commerciales et techniques vérifiables pour divers processus.

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

L'intégrité d'un processus est essentielle, car de nombreux participants—de divers provinces et territoires, organisations et secteurs, et à court et long terme—dépendent de l'extrant de ce processus. Les critères de conformité sont donc fondamentaux pour le cadre de confiance, car ils spécifient les exigences qui assurent l'intégrité des processus.

Remarque

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

2 Conventions d'authentification

Chaque composante du CCP comporte des conventions qui assurent une utilisation et une interprétation uniformes des termes et notions apparaissant dans la composante. L'aperçu de la composante « Connexion vérifiée » du CCP fournit les conventions pour cette composante. Ces conventions incluent des définitions et descriptions des éléments suivants auxquels il est fait référence dans ce profil de conformité :

- Principaux termes et notions
- Abréviations et acronymes
- Rôles
- Niveaux d'assurance
- Processus de confiance et conditions connexes

Remarque

- Les conventions peuvent varier entre les composantes du CCP. Les lecteurs sont invités à examiner les conventions propres à chacune de ces composantes.
- Termes définis – Pour les besoins de ce profil de conformité, les termes et définitions figurant dans l'aperçu de la composante « Authentification » et le glossaire du CCP s'appliquent. Les principaux termes et notions décrits et définis dans la présente section, ou dans l'aperçu de la composante « Authentification » du CCP, sont indiqués en majuscules dans le document.
- Liens hypertextes – Il se pourrait que des liens hypertextes soient intégrés dans les versions électroniques de ce document. Tous les liens étaient accessibles au moment de la rédaction.

2.1 Mots clés des critères de conformité

Tout au long de ce document, les termes suivants 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 valables dans des circonstances particulières pour ignorer l'exigence, toutes les implications devraient être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité ou de choisir une autre option tel que spécifié par les critères de conformité.
- **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 apparaissent en caractères **gras** et en MAJUSCULES dans ce profil de conformité.

3 Critères de conformité de la composante « Authentification »

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

1. Délivrance des justificatifs d'authentification
2. Authentification
3. Début de session authentifiée
4. Fin de session authentifiée
5. Suspension des justificatifs d'authentification
6. Récupération des justificatifs d'authentification
7. Maintenance des justificatifs d'authentification
8. Révocation des justificatifs d'authentification

Les critères de conformité sont catégorisés par processus de confiance et profilés selon les niveaux d'assurance. Ils sont groupés par sujet à l'intérieur de chaque catégorie. Pour faciliter la référence, un critère de conformité spécifique peut être mentionné d'après sa catégorie et son numéro de référence. Exemple : « BASE1 » fait référence au « critère de conformité de base n° 1 ».

Remarque

- Les critères de conformité de base sont aussi inclus dans le présent profil de conformité.
- Les critères de conformité spécifiés dans d'autres composantes du CCP peuvent aussi s'appliquer dans certaines circonstances aux processus de confiance de l'authentification.
- Les critères de conformité des notifications spécifiés dans le présent profil de conformité représentent uniquement les notifications spécifiques aux processus dans le contexte de la composante « Authentification » du CCP. Voir la composante « Avis et consentement » du CCP pour obtenir d'autres critères de conformité reliés aux notifications.
- Le niveau d'assurance 4 déborde du champ d'application de la présente version. La référence est conservée pour être intégrée dans des développements futurs.

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	Niveau 2	Niveau 3	Niveau 4
BASE	**Critères de base**				
CONSIGNATION D'ÉVÉNEMENTS					
1	La gestion et l'utilisation des justificatifs d'authentification **PEUVENT** être consignées et conservées. Si elles sont conservées, des registres des évènements de gestion et d'utilisation des justificatifs d'authentification **DOIVENT** être conservés pendant une période prédéfinie en guise de preuve.	O			
2	La gestion et l'utilisation des justificatifs d'authentification **DOIVENT** être consignées et conservées pendant une période prédéfinie en guise de preuve.		O	O	
3	La gestion et l'utilisation des justificatifs d'authentification **DOIVENT** être : 1. Retraçables jusqu'à un justificatif d'authentification spécifique, et inclure le résultat, la date et l'heure de l'événement consigné; 2. Protégés par des contrôles pour limiter l'accès uniquement à ceux qui en ont besoin (voir NIST Special Publication 800-92 pour des recommandations concernant la gestion des registres de sécurité informatique).		O	O	
4	La gestion et l'utilisation des justificatifs d'authentification **DOIVENT** avoir un mécanisme de détection des tentatives frauduleuses pour déceler les modifications non autorisées.			O	
5	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.	O	O	O	
SÉCURITÉ DE L'INFORMATION					

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
6	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.	O			
7	Le fournisseur de services de justificatifs ou d'authentification **DOIT** : 1. assurer i) l'intégrité, ii) la confidentialité et iii) la disponibilité des services en suivant une série de lignes directrices et de contrôles de sécurité de l'information (p. ex., CSEC ITSG-33) qui soutiennent ces efforts; 2. avoir un processus vérifiable pour démontrer la conformité à une série de lignes directrices et contrôles de sécurité de l'information.		O	O	
8	Le fournisseur de services de justificatifs ou d'authentification **DOIT** avoir un processus vérifié d'une manière indépendante pour démontrer la conformité à une série de lignes directrices et contrôles de sécurité de l'information.			O	
GESTION DES SERVICES TI					
9	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** avoir une pratique de la 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.	O			

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
10	Le fournisseur de services de justificatifs ou d'authentification **DOIT** : 1. établir et maintenir une pratique de la 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; 2. avoir un processus vérifiable pour démontrer la conformité d'une pratique de gestion des services pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP.		O		
11	Le fournisseur de services de justificatifs ou d'authentification **DOIT:** 1. établir et maintenir une pratique de la 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; 2. 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.			O	
12	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** se conformer à un cadre de gestion des services standard de l'industrie, comme ITIL.	O	O		
13	Le fournisseur de services de justificatifs ou d'authentification **DOIT** se conformer à un cadre de gestion des services standard de l'industrie, comme ITIL.			O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
SURVEILLANCE					
14	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** pouvoir surveiller les services pour avoir des indices ou preuves d'une possible utilisation malveillante ou compromission des justificatifs d'authentification.	O			
15	Le fournisseur de services de justificatifs ou d'authentification **DOIT** pouvoir surveiller les services pour avoir des indications ou preuves d'une possible utilisation malveillante ou compromission des justificatifs d'authentification.		O	O	
16	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** prendre des mesures pour déceler l'utilisation malveillante des justificatifs d'authentification.	O			
17	Le fournisseur de services de justificatifs ou d'authentification **DOIT** prendre des mesures pour déceler l'utilisation malveillante des justificatifs d'authentification.		O	O	
18	Le fournisseur de services de justificatifs **DEVRAIT** amorcer le processus de suspension, de maintenance ou de révocation des justificatifs d'authentification quand il découvre des indications d'utilisation malveillante ou de compromission des justificatifs donnant lieu à des poursuites.	O			
19	Le fournisseur de services de justificatifs ou d'authentification **DOIT** amorcer le processus de suspension, de maintenance ou de révocation des justificatifs d'authentification quand il découvre des indications d'utilisation malveillante ou de compromission des justificatifs donnant lieu à des poursuites.		O	O	
CONFIDENTIALITÉ					

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
20	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.	O			
21	Le fournisseur de services de justificatifs ou d'authentification **DOIT** 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.		O	O	
22	Le fournisseur de services de justificatifs ou d'authentification **DOIT** se conformer aux pratiques de gestion des risques pour la confidentialité qui sont acceptées par et applicables à toutes les parties participant au service d'identité numérique.		O	O	
NOTIFICATIONS					
23	Le fournisseur de services de justificatifs **PEUT** aviser le sujet de tout changement apporté aux renseignements sur les justificatifs d'authentification (p. ex., mise à jour de mots de passe, ajout ou suppression d'authentifiants).	O			
24	Le fournisseur de services de justificatifs **DOIT** aviser le sujet de tout retard indu de tout changement apporté aux renseignements sur les justificatifs d'authentification (p. ex., mise à jour de mots de passe, ajout ou suppression d'authentifiants).		O	O	
CDIS	**Attribution de justificatifs**				
LIER UN SUJET					

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
1	Le fournisseur de services de justificatifs **DEVRAIT** imposer que le justificatif d'authentification soit uniquement lié à un sujet.	O			
2	Le fournisseur de services de justificatifs **DOIT** imposer que le justificatif d'authentification soit uniquement lié à un sujet.		O	O	
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 d'authentification a été attribué.	O			
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 d'authentification a été attribué.		O	O	
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 d'authentification qu'il a attribués (p. ex., si un justificatif est « inaccessible » ou « révoqué », ces renseignements sur l'état **DOIVENT** être mis à la disposition des fournisseurs de services d'authentification).	O	O	O	
LIER DES AUTHENTIFIANTS					
6	Le fournisseur de services de justificatifs **PEUT** donner la capacité de lier un authentifiant fourni par le sujet au justificatif d'authentification.	O	O	O	
7	Le fournisseur de services de justificatifs **DOIT** lier au moins un authentifiant au justificatif d'authentification (p. ex., mot de passe, Foire aux questions ou mot de passe à usage unique).	O	O	O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
8	Au moins deux authentifiants différents **DEVRAIENT** être liés au justificatif d'authentification de sorte qu'il soit possible d'en récupérer un (qui a été perdu ou volé) en utilisant un autre authentifiant.		O		
9	Au moins deux authentifiants différents **DOIVENT** être liés au justificatif d'authentification de sorte qu'il soit possible d'en récupérer un (qui a été perdu ou volé) en utilisant un autre authentifiant.			O	
10	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.		O	O	
11	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 d'authentification a été récupéré.	O			
12	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 d'authentification a été récupéré.		O	O	
CRÉATION D'UN AUTHENTIFIANT					
13	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.		O		
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 vérifiés d'une manière indépendante.			O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
15	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 vérifiable qui empêche les renseignements d'être compromis de la fabrication à la livraison au fournisseur de services de justificatifs.		O		
16	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.			Y	
ENTREPOSAGE DES IDENTIFIANTS					
17	Le fournisseur de services de justificatifs ou d'authentification **DOIT** imposer des contrôles pour empêcher l'accès non autorisé aux renseignements sur les justificatifs d'authentification.	O	O	O	
18	Les secrets liés au justificatif d'authentification **DOIVENT** être entreposés comme du hash salé ou chiffrés.		O	O	
19	Les attributs des justificatifs d'authentification qui contiennent des renseignements personnels entreposés dans le service **DOIVENT** être sécurisés (p. ex., chiffrés et/ou hashés).	O	O	O	
20	Les sauvegardes des renseignements liés aux justificatifs d'authentification **DOIVENT** être chiffrées avant d'être entreposées à long terme et **DOIVENT** rester chiffrées tant qu'elles sont entreposées.		O	O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
21	Les modules cryptographiques **DOIVENT** satisfaire une norme de validation reconnue de l'industrie (p. ex., FIPS 140-2).			O	
AUTH	**Authentification**				
AUTHENTIFIANTS					
1	Le fournisseur de services d'authentification **DOIT** exiger qu'au moins un authentifiant soit lié à un justificatif d'authentification.	O	O		
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.		O		
3	Le fournisseur de services d'authentification **DOIT** exiger au moins deux authentifiants différents qui : 1. fournissent des facteurs d'authentification différents 2. ne sont pas susceptibles aux mêmes vecteurs de menaces.			O	
4	Parmi les différents authentifiants exigés par le fournisseur de services d'authentification conformément à AUTH3 : 1. Un des authentifiants **DOIT** être du type « chose que le sujet a » 2. Les autres authentifiants **PEUVENT** être du type « chose que le sujet connaît » ou « chose que le sujet est ou fait ».			O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
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 d'authentification.	O	O	O	
TYPE D'AUTHENTIFIANT					
6	Tout type d'authentifiant est acceptable.	O			
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).		O	O	
8	Le fournisseur de services d'authentification **DOIT** utiliser des types d'authentifiants qui résistent aux menaces indiquées en **AUTH13**.			O	
ATTÉNUATION DES MENACES					
9	Le fournisseur de services d'authentification **DOIT** être capable de se défendre au moins contre les attaques suivantes : devinette des secrets des authentifiants et attaques par rejeu. Cela **PEUT** être inclus dans la portée des lignes directrices décrites dans **BASE6**.	O			
10	Le fournisseur de services d'authentification **DOIT** être capable de se défendre au moins contre les attaques suivantes : devinette des secrets des authentifiants, rejeu, écoute illicite et piratage de cession. Cela **DOIT** être inclus dans la portée du processus vérifiable décrit dans **BASE7.**		O		

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
11	Le fournisseur de services d'authentification **DOIT** être capable de se défendre au moins contre les attaques suivantes : devinette des secrets des authentifiants, rejeu, écoute illicite, piratage de cession, usurpation d'identité/hameçonnage et homme du milieu (p. ex., utilisation d'un TLS mutuellement authentifié). Cela **DOIT** être inclus dans la portée du processus de vérification indépendante exigé dans **BASE8**.			O	
RISQUE D'ADAPTATION					
12	Le fournisseur de services d'authentification **PEUT** fournir la capacité de faire une authentification du risque d'adaptation.	O			
13	Le fournisseur de services d'authentification **DEVRAIT** fournir la capacité de faire une authentification du risque d'adaptation.		O		
14	Le fournisseur de services d'authentification **DOIT** déceler et atténuer les interactions qui représentent un risque plus grand que d'ordinaire, 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 le plus grand risque possible que le fournisseur de services d'authentification peut soutenir pour une telle interaction.			O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
MODULE CRYPTOGRAPHIQUE					
15	Les modules cryptographiques utilisés dans l'authentification côté client **DOIVENT** respecter une norme de validation reconnue de l'industrie (p. ex., FIPS 140-2 ou l'équivalent).		O	O	
RÉSULTAT DE L'AUTHENTIFICATION					
16	Le fournisseur de services d'authentification **DOIT** déclarer une réussite seulement si le sujet a effectué avec succès sa tentative d'authentification.	O	O	O	
17	Le fournisseur de services d'authentification **DOIT** déclarer un échec à une tentative d'authentification si le justificatif d'authentification présenté est suspendu ou révoqué ou encore si l'on décèle une utilisation malveillante ou la compromission du justificatif d'authentification.	O	O	O	
18	Le fournisseur de services d'authentification **DOIT** fournir un mécanisme qui : 1. Confirme que le résultat de l'authentification provient du fournisseur de services d'authentification; 2. N'a pas été altéré pendant le transit; 3. Ne peut être utilisé que par la partie dépendante.		O	O	
19	L'authentification **DOIT** être valide pour une période maximale qui est i) spécifiée par le fournisseur de services d'authentification et ii) connue de la partie dépendante.		O	O	
INSE	**Lancement de session authentifiée**				
LANCEMENT DE SESSION					

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
1	Le fournisseur de services d'authentification **DEVRAIT** offrir la capacité de maintenir une session qui lie toutes les parties dépendantes.	O			
2	Le fournisseur de services d'authentification **DOIT** offrir la capacité de maintenir une session qui lie toutes les parties dépendantes.		O	O	
3	Si le sujet est authentifié à un niveau d'assurance donné, la session qui en résulte **DOIT** être considérée comme étant du même (p. ex., si le sujet est authentifié au niveau d'assurance 2, la session DOIT être considérée comme étant du niveau d'assurance 2).	O	O	O	
RÉAUTHENTIFICATION					
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).	O			
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 dépendante dans une fédération ou quand une partie dépendante demande une nouvelle authentification).		O	O	
6	Le fournisseur de services d'authentification **PEUT** rallonger les périodes d'inactivité des sessions.	O			

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	Niveau 2	Niveau 3	Niveau 4
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.		O	O	
TESE	**Fin de la session d'authentification**				
SESSION INACTIVE					
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.	O			
2	Le fournisseur de services d'authentification **DOIT** imposer une durée de session maximale pour former la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie		O	O	
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.	O			
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.		O	O	
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.			O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
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** découler d'une fin de session ou d'une baisse à une session de niveau d'assurance 2.			O	
7	En cas de passage à une session de niveau inférieur : 1. Le fournisseur de services d'authentification **DOIT** aviser toutes les parties dépendantes associées à la session de niveau d'assurance 3; et 2. Les sessions inactives en raison d'un dépassement de la durée de session ou de la durée d'inactivité de session maximale **PEUVENT** être prolongées jusqu'aux valeurs du niveau d'assurance 2 (moins le temps déjà passé).			O	
FIN DE SESSION					
8	Le fournisseur de services d'authentification **DEVRAIT** aviser toutes les parties dépendantes que la session est terminée.	O			
9	Le fournisseur de services d'authentification **DOIT** aviser toutes les parties dépendantes que la session est terminée.		O	O	
CRSP	**Suspension de justificatifs d'authentification**				
PAR UN SUJET					
1	Le fournisseur de services de justificatifs **DEVRAIT** donner à un sujet la capacité de suspendre l'utilisation de son justificatif d'authentification.	O	O	O	
PAR UNE PERSONNE					

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
2	Le fournisseur de services de justificatifs **PEUT** donner à du personnel autorisé la capacité de suspendre l'utilisation d'un justificatif d'authentification.	O	O	O	
3	Le fournisseur de services de justificatifs **DEVRAIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.	O			
4	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.		O	O	
5	Le fournisseur de services de justificatifs **DOIT** demander au personnel autorisé de fournir un niveau d'assurance 3 ou un justificatif d'authentification supérieur afin de suspendre l'utilisation d'un justificatif d'authentification.			O	
CRVY	**Récupération des justificatifs d'authentification**				
PAR UN SUJET					
1	Le fournisseur de services de justificatifs **DEVRAIT** donner la capacité de récupérer un justificatif d'authentification perdu ou suspendu.	O			
2	Le fournisseur de services de justificatifs **DEVRAIT** exiger que le sujet s'authentifie avec un niveau d'assurance équivalent à celui du justificatif d'authentification récupéré.	O			
3	Le fournisseur de services de justificatifs **DOIT** donner la capacité de récupérer un justificatif d'authentification perdu ou suspendu.		O	O	
4	Le fournisseur de services de justificatifs **DOIT** exiger que le sujet s'authentifie avec un niveau d'assurance équivalent à celui du justificatif d'authentification récupéré.		O	O	
PAR UN ADMINISTRATEUR					

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
5	Le fournisseur de services de justificatifs **PEUT** donner à du personnel autorisé la capacité d'entreprendre la récupération d'un justificatif d'authentification pour le compte du sujet.	O	O	O	
6	Le fournisseur de services de justificatifs **DEVRAIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.	O			
7	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.		O	O	
8	Outre les exigences spécifiées pour le niveau d'assurance 2, le fournisseur de services de justificatifs **DOIT** obliger le personnel autorisé à fournir un justificatif d'authentification de niveau d'assurance 3 ou supérieur pour récupérer un justificatif d'authentification.			Y	
PAR UN SYSTÈME					
9	Le fournisseur de services de justificatifs **PEUT** offrir la capacité de récupérer automatiquement un justificatif d'authentification suspendu (p. ex., réactiver automatiquement un justificatif d'authentification préalablement suspendu à la suite d'un trop grand nombre de tentatives de connexion ratées).	O	O	O	
CRMA	**Maintenance des justificatifs d'authentification**				
PAR LE SUJET					
1	Le fournisseur de services de justificatifs **DEVRAIT** donner la possibilité de mettre à jour les authentifiants liés au justificatif d'authentification lorsque c'est possible (p. ex., changer de mot de passe, lier un nouvel authentifiant).	O			

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
2	Le fournisseur de services de justificatifs **DEVRAIT** donner la possibilité de modifier les attributs des justificatifs d'authentification (p. ex., mot de passe, Foire aux questions, codes de récupération).	O			
3	Le fournisseur de services de justificatifs **DOIT** donner la possibilité de mettre à jour les authentifiants liés au justificatif d'authentification 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).		O	O	
4	Le fournisseur de services de justificatifs **DOIT** donner la possibilité de modifier les attributs des justificatifs d'authentification (p. ex., mot de passe, Foire aux questions, codes de récupération clés cryptographiques, biométrie, alias, DID).		O	O	
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 d'authentification 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.		O	O	
PAR UNE ADMINISTRATION					
6	Le fournisseur de services de justificatifs **PEUT** fournir la possibilité de permettre au personnel autorisé de mettre à jour les authentifiants liés au justificatif d'authentification (p. ex., supprimer un authentifiant ou entreprendre un changement de mot de passe).	O	O	O	

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
7	Le fournisseur de services de justificatifs **PEUT** fournir la possibilité de permettre au personnel autorisé de mettre à jour les attributs des justificatifs d'authentification.	O	O	O	
8	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès afin que seul le personnel autorisé a accès à ce processus.	O	O	O	
9	Le fournisseur de services de justificatifs **DOIT** exiger que le personnel autorisé donne un justificatif d'authentification de niveau 3 ou supérieur pour effectuer la maintenance des justificatifs d'authentification.			O	
10	Le fournisseur de services de justificatifs **DEVRAIT** exiger que le sujet termine les activités liées aux justificatifs d'authentification amorcées par un administrateur (p. ex., un administrateur ne peut pas changer le mot de passe d'un sujet, seulement initier une réinitialisation).	O			
11	Le fournisseur de services de justificatifs **DOIT** exiger que le sujet termine les activités liées aux justificatifs d'authentification amorcées par un administrateur (p. ex., un administrateur ne peut pas changer le mot de passe d'un sujet, seulement initier une réinitialisation).		O	O	
PAR UN SYSTÈME					
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).	O			

Référence	Critères de conformité	Niveau d'assurance			
		Niveau 1	Niveau 2	Niveau 3	Niveau 4
13	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).		O	O	
CRVX	**Révocation de justificatifs**				
PAR UN SUJET					
1	Le fournisseur de services de justificatifs **DEVRAIT** permettre à un sujet de révoquer son propre justificatif d'authentification.	O			
2	Le fournisseur de services de justificatifs **DOIT** permettre à un sujet de révoquer son propre justificatif.		O	O	
PAR UNE ADMINISTRATION					
3	Le fournisseur de services de justificatifs **PEUT** avoir la capacité de permettre au personnel autorisé de révoquer un justificatif d'authentification.	O			
4	Le fournisseur de services de justificatifs **DOIT** avoir la capacité de permettre au personnel autorisé de révoquer un justificatif d'authentification.		O	O	
5	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.	O	O	O	
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 d'authentification.			O	

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

4 Contrôle des versions du document

Numéro de version	Date de publication	Auteurs	Description
.01	2018-04-10	TFEC	Ébauche de travail initiale
.02	2018-07-31	Rédacteur du CCIAN	Changements suggérés pour donner suite aux commentaires d'examen en suspens
.03	2019-04-30	Rédacteur du CCIAN	Modifications au formatage. Mise à jour des liens vers les normes mentionnées
.04	2019-07-08	Rédacteur du CCIAN	Uniformisation de la priorité des modalités des exigences Mise à jour de l'image du modèle de CCP
.05	2019-10-21	TFEC et équipe de rédaction du CCP	Révision du contenu basée sur les commentaires concernant l'ébauche de discussion
1.0	2019-10-30	Équipe de rédaction du CCP	Approbation comme ébauche de recommandations V1.0
1.1	N/A	Équipe de rédaction du CCP	Mises à jour apportées à la suite des commentaires reçus pendant la période d'examen de l'ébauche de recommandations
1.0	2020-05-11	Équipe de rédaction du CCP	Recommandation finale V1.0