Document de travail sur le profil de conformité de la connexion vérifiée - version 0.03

Ce document de travail a été préparé par le Comité d'experts du cadre de confiance (TFEC) du Digital ID & Authentication Council of Canada (DIACC). Le TFEC est régi par les politiques du DIACC en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'entente de contributeur du DIACC.

Le DIACC prévoit modifier et améliorer ce document de travail en fonction des commentaires du public. Les commentaires ouverts ont pour but d'assurer la transparence de l'élaboration et la diversité d'un apport véritablement pancanadien. Les commentaires effectués pendant l'examen seront pris en considération en vue d'être incorporés dans la prochaine ébauche. Le DIACC va regrouper les commentaires afin de montrer d'une façon transparente comment chacun a été traité.

Les prochaines versions du cadre de confiance pancanadien vont étoffer, clarifier et peaufiner le contenu de ce document. L'auditoire ciblé inclut des décideurs qui peuvent être ou non des experts dans la technologie des domaines.

En examinant cette ébauche, veuillez tenir compte de ce qui suit :

1. Est-ce que les normes dont il est question dans le document (c.-à-d. ITSP.30.031 V3 du Centre de la sécurité des télécommunications, NIST 800-63-3 des É.-U. et GPG-44 du R.-U.) continuent d'être celles auxquelles il est fait référence dans la connexion vérifiée. Y a-t-il est solutions de rechange ou des normes et directives plus récentes auxquelles on devrait faire référence en plus ou à la place de celles qui sont indiquées?
2. Êtes-vous d'accord avec le nom « connexion vérifiée » actuellement utilisé ou y a-t-il un autre nom comme « justificatif vérifié » qui serait plus approprié?
3. Êtes-vous d'accord avec la liste des processus de confiance pour la connexion vérifiée?
4. La description des processus de confiance est-elle claire et exacte?
5. Les critères de conformité sont-ils clairs et mesurables/peuvent-ils être évalués?
6. Êtes-vous d'accord avec les termes utilisés pour décrire la connexion vérifiée tels qu'ils sont présentés dans le document?

Table des matières

1 Introduction aux critères de conformité de la connexion vérifiée

Ce document spécifie la série de critères de conformité convenus pour le volet connexion vérifiée, un élément du cadre de confiance pancanadien. Le profil de conformité de la connexion vérifiée correspond aux critères convenus qui servent à s'assurer que les processus de confiance représentent un sujet unique et un niveau d'assurance comme quoi il s'agit du même sujet à chaque connexion réussie au fournisseur de services de justificatifs. Les parties utilisatrices peuvent alors avoir l'assurance d'identifier d'une manière unique le sujet dans le cadre d'une application ou d'un programme.

Les critères de conformité sont fondamentaux pour le cadre de confiance, car ils spécifient les exigences essentielles convenues par les participants au cadre de confiance afin d'assurer l'intégrité de leurs processus. Cette intégrité est fondamentale, car beaucoup de participants se fient à l'extrant ou au résultat d'un processus de confiance – à la longue et par-delà les frontières organisationnelles, juridictionnelles et sectorielles.

1.1 Relation avec le cadre de confiance pancanadien

Le cadre de confiance pancanadien consiste en une série de composantes modulaires ou fonctionnelles pouvant être évaluées et certifiées indépendamment pour être considérées comme des éléments de confiance. Le cadre de confiance pancanadien, qui mise sur une approche pancanadienne, permet au public et au secteur privé de collaborer pour préserver les identités numériques en uniformisant les processus et les pratiques dans tout l'écosystème numérique canadien.

La figure 1 illustre l'ébauche visuelle du modèle de cadre de confiance pancanadien. Les processus du volet connexion vérifiée sont exécutés par les participants dans les catégories « Créer et gérer des identités numériques » et « Utiliser l'identité numérique ».

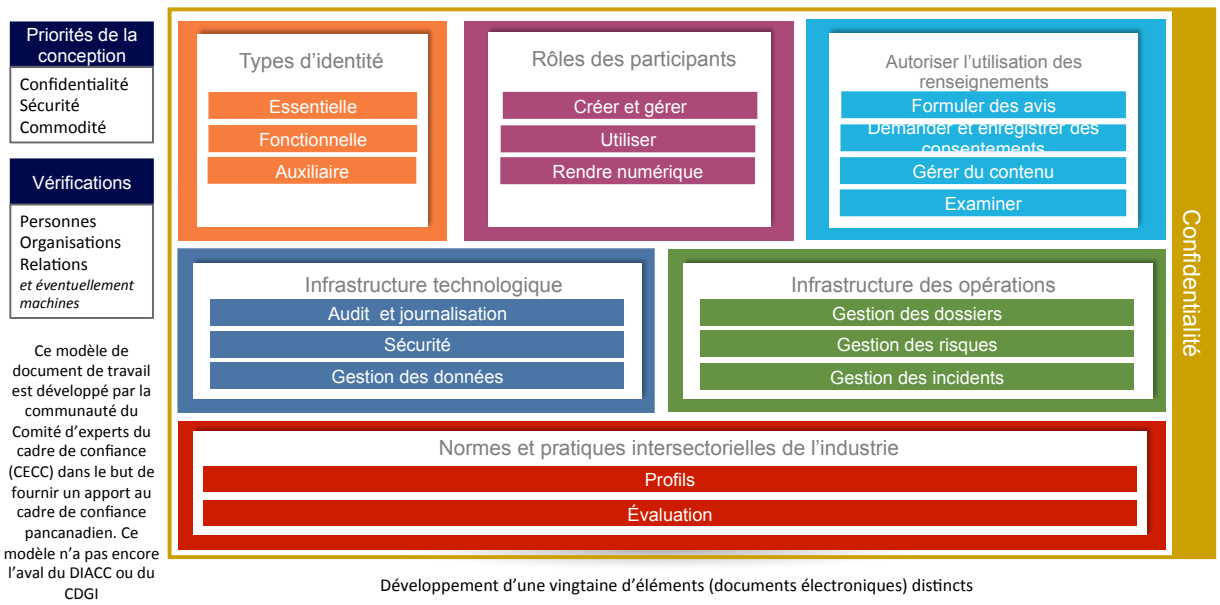

Figure 1. Ébauche visuelle du modèle de cadre de confiance pancanadien

1.2 Mots clés et définitions

Afin d'assurer une application uniforme, les mots clés en **gras** dans les critères de conformité doivent être interprétés comme suit :

- **DOIT**, **EST EXIGÉ** or **DEVRA** signifie que l'exigence est impérative en ce qui concerne les critères de conformité.
- **NE DOIT PAS** ou **NE DEVRA PAS** signifie que l'exigence est une interdiction absolue des critères de conformité.
- **DEVRAIT** ou **EST RECOMMANDÉ** 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** ou **N'EST PAS RECOMMANDÉ** signifie qu'il peut exister une raison valable dans des circonstances particulières pour que l'exigence soit acceptable ou même utile, mais toutes les implications devraient être comprises et le cas devrait être considéré avec soin avant de choisir de ne pas se conformer aux exigences telles que décrites.
- **PEUT** ou **FACULTATIF** signifie que l'exigence est discrétionnaire mais recommandée.

D'autres mots clés, comme des définitions normatives dans des normes et spécifications connexes, seront également indiqués en **gras**.

1.3 Normes connexes et documents de référence

Le cadre de confiance pancanadien, et tout particulièrement la connexion vérifiée, a pour but d'élaborer des normes canadiennes qui permettront aux citoyens et aux consommateurs d'interagir avec confiance et assurance auprès des organisations des secteurs privé et public. Des démarches similaires sont en cours, ou achevées, ailleurs dans le monde et au sein du secteur public canadien s'occupant des normes d'authentification. Au lieu de réinventer de nouvelles normes, la connexion vérifiée devrait chercher à tirer parti de l'expérience d'autres gouvernements et organisations et des leçons qu'ils ont tirées en développant et en faisant évoluer activement ces processus et normes. La connexion vérifiée s'aligne et est basée sur les normes et documents d'orientation suivants :

- ITSP.30.031 v3 Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031)
- NIST 800-63-3 Digital Identity Guidelines (800-63-3, 800-63A, 800-63B et 800-63C)
- Good Practice Guide No. 44 Authentication and Credentials for use with HMG Online Service (GPG-44)

Le lecteur est invité à lire ces documents pour mieux comprendre les processus et normes d'authentification et les critères de conformité qui ont été élaborés dans d'autres territoires de compétence.

À propos de la biométrie : Étant donné le manque inhérent de révocabilité qui la caractérise, la biométrie est généralement considérée dans les normes ci-dessus comme un moyen de déverrouiller un authentificateur dans un appareil local pour faciliter l'authentification à distance d'un service. C'est ce qui se passe notamment lorsqu'on utilise Apple TouchID pour déverrouiller l'accès à un mot de passe temporaire pour mobile ou à un autre authentificateur pour mobile enregistré et généré localement.

La norme NIST 800-63 décrit l'utilisation de la biométrie de la façon suivante : « La biométrie n'est pas non plus un secret. Par conséquent, ces lignes directrices ne permettent d'utiliser la biométrie à des fins d'authentification que lorsqu'elle est étroitement liée à un authentificateur physique. »

La norme ITSP.30.031 décrit l'utilisation de la biométrie de la façon suivante : « Il s'agit de ce qu'un utilisateur est ou fait et qui peut être reproduit. Un auteur malveillant peut obtenir une copie de l'empreinte du propriétaire du jeton et construire une réplique – en tenant pour acquis que le ou les systèmes biométriques utilisés ne bloquent pas de telles attaques grâce à l'utilisation de robustes techniques de détection du caractère vivant » et « Reconnaissance automatisée des personnes basée sur leurs caractéristiques comportementales et biologiques. Dans ce document, la biométrie peut être utilisée pour déverrouiller des jetons d'authentification et empêcher le rejet de l'inscription. »

Compte tenu des consignes ci-dessus émanant du NIST et de l'ITSP, la connexion vérifiée va pour l'instant envisager l'authentification biométrique uniquement pour déverrouiller l'accès à un autre authentificateur, l'exemple le plus courant consistant à déverrouiller l'accès biométrique à un authentificateur mobile.

1.4 Définitions

Pour les besoins des documents sur le volet connexion vérifiée, voici les définitions qui sont utilisées :

- **Risque adaptatif –** mesure dynamique du risque associé à l'accès à une transaction ou un service en fonction du contexte et du comportement.
- **Authentification du risque adaptatif –** ajustement dynamique des étapes d'authentification spécifiques en fonction du risque adaptatif.
- **Authentificateur** – ce qu'un sujet possède et contrôle (habituellement un module cryptographique ou un mot de passe) et qui sert à authentifier l'identité du sujet. Les authentificateurs servent à prouver, avec le niveau d'assurance spécifié, qu'un justificatif fait référence au même sujet initialement lié au justificatif (p. ex., mot de passe, Foire aux questions ou mot de passe temporaire. Remarque : On parle de jeton dans le glossaire ITSP.30.031.
- **Justificatifs** – une structure d'objets ou de données qui relie d'une manière décisive une identité (ou des attributs supplémentaires) à un authentificateur (aussi appelé un jeton) qui est possédé et contrôlé par un sujet. Un justificatif inclut un ou plusieurs identifiants qui peuvent être des pseudonymes et peuvent contenir des attributs vérifiés par l'émetteur du justificatif. Remarque : basé sur le glossaire de la norme ITSP.30.031.

1.5 Rôles

Les rôles qui suivent sont définis pour couvrir la portée des critères de conformité de l'avis et du consentement. Selon le cas d'utilisation, différentes organisations peuvent jouer un ou plusieurs rôles.

- **Sujet –** dans le contexte de la connexion vérifiée, un sujet peut être une personne naturelle, une organisation, une application ou un appareil liés à un justificatif.
- **Fournisseur de services de justificatifs –** entité qui exploite un service mettant en œuvre les processus de confiance de la connexion vérifiée. (Pour les cas d'utilisation où le secteur privé fournit des services au secteur public, il s'agit d'une entité du secteur privé.)
- **Partie utilisatrice –** dans le contexte de la connexion vérifiée, une entité qui dépend d'une mise en œuvre conforme des processus de confiance de la connexion vérifiée. (Pour les cas d'utilisation où le secteur privé fournit des services au secteur public, il s'agit d'une activité, d'un service ou d'un programme du secteur public.)

Ces rôles aident à isoler les différentes fonctions et responsabilités à l'intérieur des processus de connexion vérifiée de bout en bout. Ils ne visent pas à impliquer une solution, architecture ou mise en œuvre en particulier.

2 Processus de confiance et critères de conformité

2.1 Processus de confiance

Le profil de conformité de la connexion vérifiée définit les critères de conformité comme des exigences essentielles des processus de confiance définis dans l'aperçu du volet connexion vérifiée, à savoir :

1. **Émission du justificatif –** processus au cours duquel un justificatif est créé et lié à un ou plusieurs authentificateurs contrôlés par un sujet.

2. **Authentification –** processus qui établit la certitude, ou le niveau d'assurance, qu'un sujet contrôle le justificatif qui lui a été attribué et que celui-ci est actuellement valide (c.-à-d., qu'il n'est pas suspendu ou révoqué).
3. **Début de la session d'authentification –** processus qui permet une interaction persistante entre un sujet et un point ultime, comme un fournisseur de services de justificatifs ou une partie utilisatrice, tout en éliminant le besoin de répéter continuellement le processus d'authentification entre les interactions.
4. **Fin de la session d'authentification –** expiration de la session, qui est une déconnexion explicite, en raison d'une inactivité ou d'une durée maximale ou encore par d'autres moyens.
5. **Suspension du justificatif –** processus qui rend inaccessible un justificatif émis.
6. **Récupération du justificatif –** processus qui fournit un moyen de rendre utilisable un justificatif inaccessible.
7. **Entretien du justificatif –** processus qui fournit des activités liées au cycle de vie du justificatif, comme le fait de lier de nouveaux authentificateurs (p. ex., lier un nouveau justificatif de mot de passe temporaire pour du matériel), de supprimer des authentificateurs (p. ex., supprimer un mot de passe temporaire de logiciel précédemment enregistré) et de mettre à jour des authentificateurs (p. ex., changement de mot de passe, mise à jour des questions et réponses de sécurité).
8. **Révocation du justificatif –** processus consistant à faire en sorte qu'un justificatif ne puisse plus être utilisé.

Une description complète des processus de confiance est fournie dans le document Aperçu du volet connexion vérifiée.

2.2 Niveaux d'assurance

Le profil des critères de conformité est défini en termes de niveaux d'assurance. Un niveau d'assurance reflète la rigueur relative des critères de conformité et sert à rendre un degré relatif de confiance qu'une partie utilisatrice peut accepter d'utiliser. Le tableau 1 indique les quatre niveaux d'assurance définis dans les cadres de confiance existants.

	Niveau d'assurance	Description de la qualification
184-b	Niveau 1 (LOA1)	• Peu ou pas de degré de confiance nécessaire • Conforme aux critères de conformité de niveau 1
184-c	Niveau 2 (LOA2)	• Certain degré (raisonnable) de confiance nécessaire • Conforme aux critères de conformité de niveau 2
184-d	Niveau 3 (LOA3)	• Degré élevé de confiance nécessaire • Conforme aux critères de conformité de niveau 3
184-e	Niveau 4 (LOA4)	• Degré très élevé de confiance nécessaire • Conforme aux critères de conformité de niveau 4

Tableau 1. Niveaux d'assurance

2.3 Critères de conformité de la connexion vérifiée

Les critères de conformité sont organisés par les processus de confiance définis dans le volet connexion vérifiée et profilés d'après les niveaux d'assurance [1]. Dans chaque catégorie, les critères de conformité sont ensuite groupés par sujet. Pour faciliter la consultation, un critère de conformité spécifique peut être désigné par son numéro de catégorie et de référence (p. ex., « **BASE-1** » correspond à la « référence n° 1 des critères de conformité de base »).

***Remarque** : Les critères de notification spécifiés dans ces critères de conformité ne correspondent qu'aux notifications spécifiques aux activités des justifiants dans le contexte de la connexion vérifiée. Il est probable que les futurs critères de notification, avec toutes les exigences de base, seront transférés dans un profil de conformité distinct comme l'infrastructure de confiance. Le cas échéant, ces critères spécifiques seront déplacés au besoin et la connexion vérifiée sera révisée en conséquence.*

Référence	Critères de conformité	Niveau d'assurance			
BASE	**Base**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
CONSIGNATION DES ÉVÉNEMENTS					
1	Les événements de gestion et d'utilisation des justificatifs **PEUVENT** être consignés et **PEUVENT** être conservés pour une période prédéfinie en guise de preuve.	O			
2	Les événements de gestion et d'utilisation des justificatifs **DOIVENT** être consignés et conservés pour une période prédéfinie en guise de preuve. Le journal **DOIT** permettre de retrouver un justifiant spécifique et inclure le résultat ainsi que la date et l'heure de l'événement. Les journaux **DOIVENT** être protégés par des contrôles d'accès pour limiter l'accès à ceux qui en ont besoin.		O	O	
3	En plus des exigences du niveau LOA2, les journaux **DOIVENT** avoir un mécanisme de détection des altérations pour déceler les modifications non autorisées.			O	
4	Les renseignements personnels et les authentificateurs secrets (p. ex., mots de passe, valeurs des mots de passe temporaires ou questions de sécurité) **NE DOIVENT PAS** être consignés dans le service.	O	O	O	
SÉCURITÉ DE L'INFORMATION					
5	Le fournisseur de services de justificatifs **PEUT** se conformer à un ensemble de lignes directrices sur la sécurité des renseignements et de contrôles de sécurité pour protéger l'intégrité, la confidentialité et la disponibilité des services (p. ex., CSEC ITSG-33).	O			

206	6	Le fournisseur de services de justificatifs **DOIT** se conformer à une série de lignes directrices sur la sécurité des renseignements et de contrôles de sécurité pour protéger l'intégrité, la confidentialité et la disponibilité des services (p. ex., CSEC ITSG-33). Le fournisseur de services de justificatifs **DOIT** avoir un processus vérifiable pour démontrer la conformité.		O		
207	7	Outre les exigences du niveau LOA2, le fournisseur de services de justificatifs **DOIT** avoir un processus vérifié de façon indépendante pour démontrer la conformité.			O	
208	**GESTION DES SERVICES DE TI**					
209	8	Le fournisseur de services de justificatifs **DEVRAIT** avoir une pratique documentée en matière de gestion des services pour tous les aspects des services.	O			
210	9	Le fournisseur de services de justificatifs **DOIT** avoir une pratique de gestion des services documentée et vérifiable pour tous les aspects des services.		O		
211	10	Le fournisseur de services de justificatifs **DOIT** avoir une pratique de gestion des services documentée et vérifiée de façon indépendante pour tous les aspects des services.			O	
212	11	Le fournisseur de services de justificatifs **DEVRAIT** se conformer à un cadre de gestion des services qui est une norme de l'industrie, comme l'Information Technology Infrastructure Library (ITIL).	O	O		
213	12	Le fournisseur de services de justificatifs **DOIT** se conformer à un cadre de gestion des services qui est une norme dans l'industrie, comme l'ITIL.			O	
214	**SURVEILLANCE**					
215	13	Le fournisseur de services de justificatifs **DEVRAIT** être capable de surveiller les services pour voir s'il y a des indications comme quoi les justificatifs sont utilisés d'une façon malveillante ou compromis.	O			
216	14	Le fournisseur de services de justificatifs **DOIT** avoir une surveillance en temps réel des services donnant des indications comme quoi les justificatifs sont utilisés d'une façon malveillante ou compromis.		O	O	

217	15	Le fournisseur de services de justificatifs **DEVRAIT** prendre des mesures pour déceler l'utilisation malveillante d'un justificatif.	O			
218	16	Le fournisseur de services de justificatifs **DOIT** prendre des mesures pour déceler l'utilisation malveillante d'un justificatif.		O	O	
219	**CONFIDENTIALITÉ**					
220	17	Le fournisseur de services de justificatifs **DOIT** se conformer aux pratiques de gestion des risques pour le respect de la vie privée du cadre de confiance et des profils de conformité sélectionnés.		O	O	
221	18	Le fournisseur de services de justificatifs **DOIT** se conformer aux pratiques de gestion des risques pour le respect de la vie privée des parties utilisatrices.		O	O	
222	19	Le fournisseur de services de justificatifs **DOIT** se conformer aux lois et règlements applicables sur le respect de la vie privée pour les territoires de compétence où ses services sont offerts.	O	O	O	
223	**NOTIFICATIONS**					
224	20	Le fournisseur de services de justificatifs **PEUT** notifier le sujet des changements apportés aux renseignements sur les justificatifs (p. ex., mise à jour du mot de passe, ajout ou suppression d'authentificateurs).	O			
225	21	Le fournisseur de services de justificatifs **DEVRAIT** notifier le sujet des changements apportés aux renseignements sur les justificatifs (p. ex., mise à jour du mot de passe, ajout ou suppression d'authentificateurs).		O		
226	22	Le fournisseur de services de justificatifs **DOIT** notifier le sujet des changements apportés aux renseignements sur les justificatifs (p. ex., mise à jour du mot de passe, ajout ou suppression d'authentificateurs).			O	
227	**CDIS**	**Attribution de justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
228	**LIEN AVEC UN SUJET**					
229	1	Le fournisseur de services de justificatifs **DEVRAIT** insister sur le fait que le justificatif est uniquement lié à un sujet.	O			

230	2	Le fournisseur de services de justificatifs **DOIT** insister sur le fait que le justificatif est uniquement lié à un sujet.		O	O	
231	**LIEN AVEC DES AUTHENTIFICATEURS**						
232	3	Le fournisseur de services de justificatifs **PEUT** offrir la capacité d'établir un lien avec un authentificateur fourni par le sujet.	O	O	O	
233	4	Au moins un authentificateur (p. ex., mot de passe, Foire aux questions ou mot de passe temporaire) **DOIT** être lié au justificatif.	O	O	O	
234	5	Au moins deux authentificateurs différents **DEVRAIENT** être liés au justificatif pour la récupération après la perte ou le vol de l'authentificateur principal.		O		
235	6	Au moins deux authentificateurs différents **DOIVENT** être liés au justificatif pour la récupération après la perte ou le vol de l'authentificateur principal			O	
236	7	Des authentificateurs supplémentaires, qui pourraient être utilisés aux fins de récupération, **DOIVENT** avoir un niveau d'assurance identique ou supérieur à celui de l'authentificateur principal		O	O	
237	**CRÉATION D'UN AUTHENTIFICATEUR**						
238	8	Quand l'authentificateur est créé (p. ex., appareil avec mot de passe temporaire pour le matériel OU mot de passe temporaire pour le logiciel), le créateur **DOIT** avoir un processus de gestion de la qualité vérifiable.		O		
239	9	Quand l'authentificateur est créé (p. ex., appareil avec mot de passe temporaire pour le matériel OU mot de passe temporaire pour le logiciel), le créateur **DOIT** avoir un processus de gestion de la qualité vérifié de manière indépendante.			O	
240	10	Quand l'authentificateur utilise l'information intégrée par un fabricant (p. ex., appareil avec mot de passe temporaire pour le matériel OU mot de passe temporaire pour le logiciel), le fabricant **DOIT** avoir un processus de gestion de la sécurité vérifiable qui empêche ces renseignements d'être compromis de la fabrication à la livraison au vérificateur de l'authentification.		O		

241	11	Quand l'authentificateur utilise l'information intégrée par un fabricant (p. ex., appareil avec mot de passe temporaire pour le matériel OU mot de passe temporaire pour le logiciel), le fabricant **DOIT** avoir un processus de gestion de la sécurité vérifié d'une manière indépendante qui empêche ces renseignements d'être compromis de la fabrication à la livraison au vérificateur de l'authentification.			O	
242	**ENTREPOSAGE DES JUSTIFICATIFS**					
243	12	Le fournisseur de services de justificatifs **DEVRAIT** appliquer les contrôles d'accès pour empêcher l'accès non autorisé aux renseignements sur les justificatifs.	O			
244	13	Le fournisseur de services de justificatifs **DOIT** appliquer les contrôles d'accès pour empêcher l'accès non autorisé aux renseignements sur les justificatifs.		O	O	
245	14	Les secrets liés aux justificatifs **DOIVENT** être entreposés sous forme de hachage salé ou chiffrée.		O	O	
246	15	Les attributs des justificatifs contenant des renseignements personnels qui sont entreposés dans le service **DOIVENT** être sécurisés, par exemple, en étant chiffrés et/ou hachés.	O	O	O	
247	16	Les sauvegardes de renseignements sur les justificatifs **DOIVENT** être chiffrées avant d'être entreposées à long terme.		O	O	
248	17	Les modules cryptographiques doivent satisfaire une norme de validation reconnue par l'industrie (p. ex., FIPS 140-2).			O	
249	**CRAU**	**Authentification des justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
250	**AUTHENTIFICATEURS**					
251	1	Le fournisseur de services de justificatifs **DOIT** exiger qu'au moins un authentificateur soit lié à un justificatif.	O	O		

252	2	Si un seul authentificateur est nécessaire, il **DOIT** fournir « quelque chose que le sujet connaît » ou « quelque chose que le sujet a » en guise de facteur d'authentification. Les authentificateurs qui fournissent « quelque chose que le sujet est ou fait » comme facteur d'authentification **DOIVENT** être utilisés uniquement comme deuxième authentificateur.		O		
253	3	Le fournisseur de services de justificatifs **DOIT** exiger au moins deux authentificateurs différents, fournissant différents facteurs d'authentification, qui ne sont pas sujets aux mêmes vecteurs de menaces.			O	
254	4	Un des authentificateurs **DOIT** fournir « quelque chose que le sujet a » comme facteur d'authentification. L'autre authentificateur **PEUT** fournir « quelque chose que le sujet connaît » ou « quelque chose que le sujet est ou fait » comme facteur d'authentification.			O	
255	**TYPE D'AUTHENTIFICATEUR**					
256	6	Tout type d'authentificateur est acceptable.	O			
257	7	Le fournisseur de services de justificatifs **DOIT** utiliser une norme ou une pratique exemplaire de l'industrie pour l'authentification, comme des normes développées et approuvées par Kantara, W3C, IETF ou FIDO.		O	O	
258	8	Le fournisseur de services de justificatifs **DOIT** utiliser des types d'authentificateur qui résistent aux menaces indiquées dans **CRAU11**.			O	
259	**ATTÉNUATION DES MENACES**					
260	9	Le fournisseur de services de justificatifs **DOIT** être capable d'atténuer un minimum d'attaques visant à percer et à rejouer les secrets des authentificateurs. Cela **PEUT** être inclus dans la portée des lignes directrices décrites dans **BASE5.**	O			
261	10	Le fournisseur de services de justificatifs **DOIT** être capable d'atténuer un minimum d'attaques visant à percer, rejouer et écouter les secrets, et à pirater les sessions des authentificateurs. Cela **DOIT** être inclus dans la portée du processus vérifiable décrit dans **BASE6**.		O		

262	11	Le fournisseur de services de justificatifs **DOIT** être capable d'atténuer un minimum d'attaques visant à percer, rejouer et écouter les secrets, à pirater les sessions, à personnifier et à hameçonner des authentificateurs, et d'attaques de l'homme du milieu (p. ex., en utilisant la sécurité de la couche de transport mutuellement authentifiée). Cela **DOIT** être inclus dans la portée du processus de vérification indépendante exigée par **BASE7**.			O	
263	**RISQUE ADAPTATIF**						
264	12	Le fournisseur de services de justificatifs **PEUT** offrir la capacité d'effectuer une authentification des risques adaptatifs.	O			
265	13	Le fournisseur de services de justificatifs **DEVRAIT** offrir la capacité d'effectuer une authentification des risques adaptatifs.		O		
266	14	Le fournisseur de services de justificatifs **DOIT** offrir la capacité d'effectuer une authentification des risques adaptatifs, à moins que les niveaux d'authentification les plus robustes soient toujours utilisés pour le service en question.			O	
267	**MODULE CRYPTOGRAPHIQUE**						
268	15	Les modules cryptographiques utilisés pour l'authentification du côté du client doivent satisfaire une norme de validation reconnue par l'industrie (p. ex., FIPS 140-2).			O	
269	**RÉSULTAT DE L'AUTHENTIFICATION**						
270	16	Le fournisseur de services de justificatifs **DOIT** retourner un succès uniquement lorsque le sujet a effectué avec succès sa tentative d'authentification.	O	O	O	
271	17	Le fournisseur de services de justificatifs **DOIT** retourner un échec à une tentative d'authentification quand le justificatif présenté est suspendu ou révoqué ou une utilisation malveillante ou une compromission est détectée.	O	O	O	
272	18	Le fournisseur de services de justificatifs **DOIT** signer et chiffrer d'une façon numérique le résultat de l'authentification pour la partie utilisatrice visée.		O	O	

273	19	Le résultat de l'authentification **DOIT** être valide pour une période spécifiée.		O	O	
274	**INSE**	**Lancer la session**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
275	**LANCER LA SESSION**					
276	1	Le fournisseur de services de justificatifs **DEVRAIT** offrir la capacité de maintenir une session qui lie toutes les parties utilisatrices.	O			
277	2	Le fournisseur de services de justificatifs **DOIT** offrir la capacité de maintenir une session qui lie toutes les parties utilisatrices.		O	O	
278	3	Si le sujet s'authentifie au niveau LOA2, la session **DOIT** être considérée au niveau LOA2.		O		
279	4	Si le sujet s'authentifie au niveau LOA3, la session **DOIT** être considérée au niveau LOA3.			O	
280	**RÉAUTHENTIFICATION**					
281	5	Le fournisseur de services de justificatifs **DEVRAIT** exiger que le sujet se réauthentifie après une période ou un événement prédéfini, par exemple quand une seule tentative d'ouverture de session est faite avec une autre partie utilisatrice appartenant à la fédération.	O			
282	6	Le fournisseur de services de justificatifs **DOIT** exiger que le sujet se réauthentifie après une période ou un événement prédéfini, par exemple quand une seule tentative d'ouverture de session est faite avec une autre partie utilisatrice appartenant à la fédération ou quand une partie utilisatrice demande une réauthentification.		O	O	
283	7	Le fournisseur de services de justificatifs **PEUT** prolonger les délais d'expiration des sessions.	O			
284	8	Si la réauthentification est au moins au niveau LOA2, les délais d'expiration des sessions **PEUVENT** être prolongés mais doivent correspondre au niveau initial et remplir tous les critères d'authentification énumérés plus haut.		O		
285	9	Si la réauthentification est au moins au niveau LOA3, les délais d'expiration des sessions **PEUVENT** être prolongés mais doivent correspondre au niveau initial et remplir tous les critères d'authentification énumérés plus haut.			O	
286	**TESE**	**Terminer la session**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**

287	**EXPIRATION DE LA SESSION**					
288	1	Le fournisseur de services de justificatifs **DEVRAIT** appliquer un délai de session maximal pour forcer la réauthentification dans un scénario de connexion unique après le délai de session prédéfini.	O			
289	2	Le fournisseur de services de justificatifs **DOIT** appliquer un délai de session maximal pour forcer la réauthentification dans un scénario de connexion unique fédérée après le délai de session prédéfini.		O	O	
290	3	Les valeurs d'expiration de la session au niveau LOA3 **DEVRAIENT** être plus courtes que celles du niveau LOA2.			O	
291	4	Une expiration de la session au niveau LOA3 **PEUT** entraîner une fin de session ou une rétrogradation à une session de niveau LOA2.			O	
292	5	En cas de rétrogradation : • le fournisseur de services de justificatifs **DOIT** notifier toutes les parties utilisatrices associées à la session de niveau LOA3; • l'expiration des sessions **PEUT** être étendue à leurs valeurs LOA2 (moins le temps déjà passé).			O	
293	**FIN DE SESSION**					
294	6	Le fournisseur de services de justificatifs **DEVRAIT** aviser toutes les parties utilisatrices que la session a été interrompue.	O			
295	7	Le fournisseur de services de justificatifs **DOIT** aviser toutes les parties utilisatrices que la session a été interrompue.		O	O	
296	**CRSP**	**Suspension des justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
297	**INITIÉE PAR LE SUJET**					
298	1	Le fournisseur de services de justificatifs **PEUT** offrir la capacité à un sujet de suspendre l'utilisation de son justificatif ou de le révoquer.	O			
299	2	Le fournisseur de services de justificatifs **DEVRAIT** offrir la capacité à un sujet de suspendre l'utilisation de son justificatif ou de le révoquer.		O	O	
300	**INITIÉE PAR UN ÊTRE HUMAIN**					

301	3	Le fournisseur de services de justificatifs **PEUT** offrir à du personnel autorisé la capacité de suspendre l'utilisation d'un justificatif ou de le révoquer.	O	O	O	
302	4	Le fournisseur de services de justificatifs **DEVRAIT** appliquer des contrôles d'accès pour s'assurer que seul le personnel autorisé a accès à ce processus.	O			
303	5	Le fournisseur de services de justificatifs **DOIT** appliquer des contrôles d'accès pour s'assurer que seul le personnel autorisé a accès à ce processus.		O	O	
304	6	Outre les exigences du niveau LOA2, le fournisseur de services de justificatifs **DOIT** exiger que le personnel autorisé fournisse un justificatif de niveau LOA3 ou supérieur.			O	
305	**INITIÉE PAR UN SYSTÈME**					
306	**CRVY**	**Récupération des justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
307	**INITIÉE PAR UN SUJET**					
308	1	Le fournisseur de services de justificatifs **DEVRAIT** offrir la capacité de récupérer un justificatif perdu ou suspendu.	O			
309	2	Le fournisseur de services de justificatifs **DEVRAIT** exiger que le sujet s'authentifie avec un niveau d'assurance équivalent à celui du justificatif en train d'être récupéré.	O			
310	3	Le fournisseur de services de justificatifs **DOIT** offrir la capacité de récupérer un justificatif perdu ou suspendu.		O	O	
311	4	Le fournisseur de services de justificatifs **DOIT** exiger que le sujet s'authentifie avec un niveau d'assurance équivalent à celui du justificatif en train d'être récupéré.		O	O	
312	**INITIÉE PAR UN ÊTRE HUMAIN**					
313	5	Le fournisseur de services de justificatifs **PEUT** offrir à du personnel autorisé la capacité d'initier la récupération d'un justificatif pour le compte du sujet.	O	O	O	
314	6	Le fournisseur de services de justificatifs **DEVRAIT** appliquer des contrôles d'accès pour s'assurer que seul le personnel autorisé a accès à ce processus.	O			

315	7	Le fournisseur de services de justificatifs **DOIT** appliquer des contrôles d'accès pour s'assurer que seul le personnel autorisé a accès à ce processus.		O	O	
316	8	Outre les exigences du niveau LOA2, le fournisseur de services de justificatifs **DOIT** exiger que le personnel autorisé fournisse un justificatif de niveau LOA3 ou supérieur.			O	
317	**INITIÉE PAR UN SYSTÈME**					
318	9	Le fournisseur de services de justificatifs **PEUT** offrir la capacité de récupérer automatiquement un justificatif suspendu (p. ex., réactiver automatiquement un justificatif précédemment suspendu en raison d'un trop grand nombre de tentatives de connexion ayant échoué).	O			
319	10	Le fournisseur de services de justificatifs **DOIT** offrir la capacité de récupérer automatiquement un justificatif suspendu (p. ex., réactiver automatiquement un justificatif précédemment suspendu en raison d'un trop grand nombre de tentatives de connexion ayant échoué).		O	O	
320	**CRMA**	**Entretien des justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
321	**INITIÉ PAR UN SUJET**					
322	1	Le fournisseur de services de justificatifs **DEVRAIT** offrir la capacité de mettre à jour les authentificateurs liés au justificatif lorsque c'est possible (p. ex., mise à jour de mot de passe, association avec un nouvel authentificateur, etc.).	O			
323	2	Le fournisseur de services de justificatifs **DEVRAIT** offrir la capacité de modifier les attributs de justificatifs (p. ex., mot de passe, Foire aux questions, codes de récupération).	O			
324	3	Le fournisseur de services de justificatifs **DOIT** offrir la capacité de mettre à jour les authentificateurs associés au justificatif lorsque c'est possible (p. ex., mise à jour de mot de passe, association avec un nouvel authentificateur, etc.).		O	O	
325	4	Le fournisseur de services de justificatifs **DOIT** offrir la capacité de modifier les attributs de justificatifs (p. ex., mot de passe, Foire aux questions, codes de récupération).		O	O	

326	5	Le fournisseur de services de justificatifs **DOIT** exiger l'authentification à un niveau d'assurance équivalent ou supérieur à celui de l'attribut du justificatif modifié (p. ex., un sujet qui a établi une connexion à l'aide d'un mot de passe à un facteur ne devrait pas pouvoir modifier des codes de récupération et les valeurs de mot de passe temporaires).		O	O	
327	**INITIÉ PAR UN ÊTRE HUMAIN**					
328	6	Le fournisseur de services de justificatifs **PEUT** permettre à du personnel autorisé de mettre à jour les authentificateurs liés au justificatif (p. ex., supprimer un authentificateur ou lancer la réinitialisation d'un mot de passe).	O	O	O	
329	7	Le fournisseur de services de justificatifs **PEUT** permettre à du personnel autorisé de mettre à jour les attributs des justificatifs.	O	O	O	
330	8	Le fournisseur de services de justificatifs **DEVRAIT** imposer des contrôles d'accès pour s'assurer que seul le personnel autorisé a accès à ce processus.	O			
331	9	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès pour s'assurer que seul le personnel autorisé a accès à ce processus.		O	O	
332	10	En plus des exigences du niveau LOA2, le fournisseur de services de justificatifs **DOIT** exiger que le personnel autorisé fournisse un justificatif de niveau LOA3 ou supérieur.			O	
333	11	Le fournisseur de services de justificatifs **DEVRAIT** exiger que le sujet accomplisse les activités liées aux justificatifs qui sont initiées par l'administrateur (p. ex., un administrateur ne peut pas changer le mot de passe du sujet, seulement lancer une réinitialisation).	O			
334	12	Le fournisseur de services de justificatifs **DOIT** exiger que le sujet accomplisse les activités liées aux justificatifs qui sont initiées par l'administrateur (p. ex., un administrateur ne peut pas changer le mot de passe du sujet, seulement lancer une réinitialisation).		O	O	
335	**INITIÉ PAR UN SYSTÈME**					

336	13	Le fournisseur de services de justificatifs **DEVRAIT** imposer des exigences relatives à la complexité des authentificateurs et une actualisation périodique des authentificateurs (p. ex., exigences concernant la complexité de la Foire aux questions, mise à jour des mots de passe, mise à jour des mots de passe temporaires).	O			
337	14	Le fournisseur de services de justificatifs **DOIT** imposer des exigences relatives à la complexité des authentificateurs et une actualisation périodique des authentificateurs (p. ex., exigences concernant la complexité de la Foire aux questions, mise à jour des mots de passe, mise à jour des mots de passe temporaires).		O	O	
338	**CRVX**	**Révocation des justificatifs**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
339	**INITIÉE PAR LE SUJET**					
340	1	Le fournisseur de services de justificatifs **DEVRAIT** permettre à un utilisateur de révoquer son propre justificatif.	O			
341	2	Le fournisseur de services de justificatifs **DOIT** permettre à un utilisateur de révoquer son propre justificatif.		O	O	
342	**INITIÉE PAR UN ÊTRE HUMAIN**					
343	3	Le fournisseur de services de justificatifs **PEUT** avoir la capacité de permettre à du personnel autorisé de révoquer un justificatif.	O			
344	4	Le fournisseur de services de justificatifs **DEVRAIT** imposer des contrôles d'accès de sorte que seul le personnel autorisé ait accès à son processus.	O			
345	5	Le fournisseur de services de justificatifs **DOIT** avoir la capacité de permettre à du personnel autorisé de révoquer un justificatif.		O	O	
346	6	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès de sorte que seul le personnel autorisé ait accès à son processus.		O	O	
347	7	En plus des exigences du niveau LOA2, le fournisseur de services de justificatifs **DOIT** exiger que le personnel autorisé fournisse un justificatif de niveau LOA3 ou supérieur.			O	

Tableau 2. Critères de conformité de la connexion vérifiée

Notes de bas de page

[1] Le profil d'assurance de niveau 4 est actuellement en dehors de la portée, mais il sera établi prochainement.