Ébauche de recommandations pour le profil de conformité des Justificatifs (Relations et Attributs) du Cadre de confiance pancanadien V1.0

Cette ébauche de recommandations a été préparée par le Comité d'experts du Cadre de confiance (TFEC) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN). Le TFEC est régi par les politiques du CCIAN en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'entente de contributeur du CCIAN.

Le CCIAN prévoit modifier et améliorer cette ébauche de recommandations 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 CCIAN 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.

Table des matières

1 Introduction aux critères de conformité des Justificatifs (Relations

et Attributs) du Cadre de confiance pancanadien

Ce document spécifie les critères de conformité pour la composante « Justificatifs » (Relations et Attributs) du Cadre de confiance pancanadien (CCP). Les critères de conformité tiennent une place centrale dans le cadre de confiance, car ils spécifient les exigences essentielles convenues par les participants du cadre de confiance afin d'assurer l'intégrité de leurs processus. Cette intégrité est de la plus haute importance, car elle permet à de nombreux participants de multiples organisations, administrations et secteurs de s'y fier.

Les critères de conformité du CCP visent à compléter les lois et règlements en vigueur sur la protection de la vie privée.

Remarque : Les critères de conformité du CCP ne remplacent ou n'annulent pas des règlements existants; on s'attend à ce que les organisations et les personnes se conforment aux lois, politiques et règlements pertinents en vigueur dans leur administration.

2 Conventions de la composante « Justificatifs (Relations et Attributs) »

Chaque composante du CCP inclut des conventions qui assurent une utilisation et une interprétation uniformes des termes et notions apparaissant dans la composante. L'aperçu de la composante « Justificatifs (Relations et Attributs) » du CCP fournit des conventions pour cette composante. Ces conventions incluent des définitions et des 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

Remarques :

- Les conventions peuvent varier selon les composantes du CCP. Les lecteurs sont invités à examiner les conventions de chacune des composantes du CCP qu'ils lisent.
- Pour les besoins de ce profil de conformité, les termes et les définitions contenus dans l'aperçu de la composante « Justificatifs (relations et attributs) » et le glossaire du CCP s'appliquent. Les principaux termes et notions décrits et définis dans cet aperçu et ce glossaire sont écrits avec une majuscule initiale tout au long de ce document.
- Des liens hypertextes peuvent être intégrés dans les versions électroniques de ce document. Ils étaient tous utilisables lors 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 sont écrits en caractères **gras** et en MAJUSCULES dans ce profil de conformité.

3 Relations de confiance

L'authenticité, la validité et la sécurité des Participants qui interviennent dans la création, l'émission, le stockage, la présentation et la vérification des Justificatifs numériques sont essentielles pour évaluer la fiabilité de ces Justificatifs. Cette composante du CCP identifie les principales relations de confiance qui entrent en ligne de compte pour évaluer la fiabilité des Justificatifs numériques. Étant donné cela, les Critères de conformité associés aux relations et aux processus de confiance identifiés dans la présente composante du CCP mettent l'accent sur la transparence et la vérifiabilité, en plus des moyens techniques utilisés pour instaurer la confiance parmi les parties en cause. La figure 1 illustre la façon dont divers rôles sont reliés entre eux et créent le besoin d'avoir ces relations de confiance.

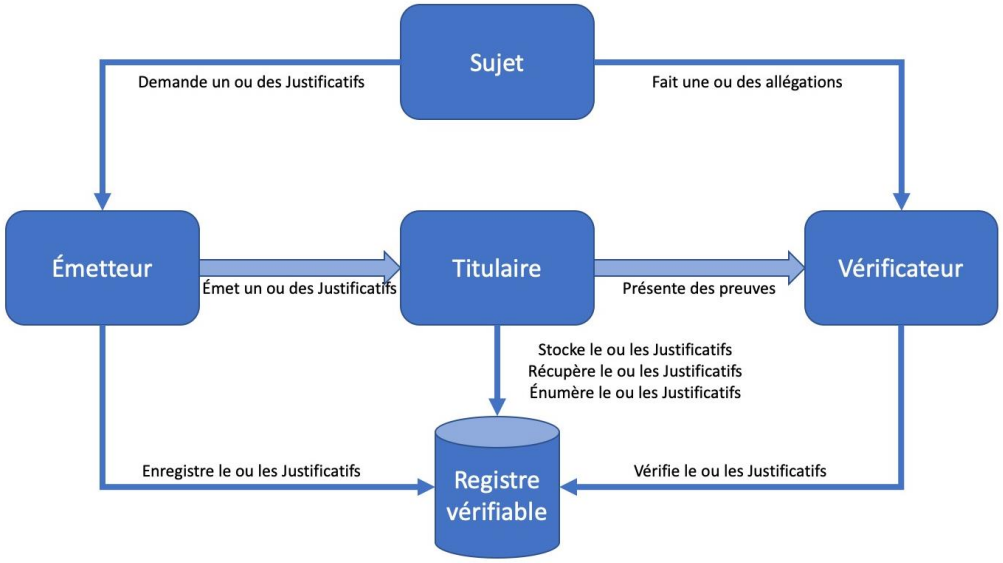

Figure 2. Rôles et relations liés aux Justificatifs (Relations et Attributs) (illustration)

La composante « Justificatifs (Relations et Attributs) du CCP définit cinq facteurs qui sont essentiels pour établir la confiance dans ces relations et qui affectent la fiabilité d'un justificatif :

1. Les Participants doivent se fier à l'autorité et à la fiabilité des émetteurs, et avoir l'assurance que ces émetteurs établissent avec soin l'exactitude des renseignements contenus dans un Justificatif.
2. Les Participants doivent avoir l'assurance que les Émetteurs délivrent des Justificatifs avec le consentement des Sujets ou d'une entité admissible à agir au nom du Sujet.
3. Les Participants doivent avoir l'assurance que les Justificatifs émis contiennent des renseignements exacts, fiables et à jour.
4. Les Participants doivent avoir l'assurance que les Justificatifs compromis ou non valides sont traités d'une manière appropriée et prompte, et qu'ils ne sont rendus inutilisables que dans des circonstances légitimes.
5. Les Participants doivent avoir l'assurance que les renseignements qu'ils partagent avec d'autres Participants ou qui sont entreposés dans des Référentiels ou Registres vérifiables ne sont pas utilisés par le Fournisseur de services ou le Vérificateur, sauf tel que demandé avec le consentement express du Sujet ou d'une entité autorisée à agir en son nom. Par exemple, les Participants ne doivent pas utiliser des justificatifs qui leur ont été confiés pour représenter les Sujets ou s'entendre avec d'autres Participants pour regrouper ou partager des renseignements sans un tel consentement.

4 Niveaux d'assurance

Il est essentiel que les Participants qui créent ou utilisent des Justificatifs comprennent le niveau de confiance qu'ils peuvent leur accorder. La composante « Justificatifs (Relations et Attributs) du Cadre de confiance pancanadien emploie pour cela une approche basée sur des niveaux d'assurance. La figure 3 donne un aperçu des niveaux d'assurance des Justificatifs tels qu'ils sont utilisés dans tout le CCP. L'assurance d'un Justificatif fait intervenir le processus qui

consiste à associer un Justificatif à une personne en particulier. Quand un Justificatif est authentifié, la Partie utilisatrice est grandement assurée que la personne qui présente le Justificatif est la même que celle qui l'a initialement reçu.

	Niveau d'assurance	Description de la qualification
120-b	Niveau 1 (CAL1)	• Un faible niveau de confiance est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis. • Répond aux critères de conformité du niveau 1
120-c	Niveau 2 (CAL2)	• Un certain niveau de confiance est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis. • Répond aux critères de conformité du niveau 2
120-d	Niveau 3 (CAL3)	• Un niveau de confiance élevé est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis; • Répond aux critères de conformité du niveau 3
120-e	Niveau 4 (CAL4) Facultatif	• Un niveau de confiance très élevé est requis pour assurer qu'une personne a conservé le contrôle sur un justificatif qui lui a été émis et que ce justificatif n'a pas été compromis. • Répond aux critères de conformité du niveau 4

Figure 3. Niveaux d'assurance des Justificatifs (Relations et Attributs)

Ces niveaux d'assurance sont reflétés dans le document sur les critères de conformité ci-joint.

C'est important de noter qu'un Justificatif doit, pour atteindre un niveau d'assurance spécifique, doit remplir chaque critère de conformité applicable correspondant au moins à la norme associée à ce niveau. Autrement dit, le niveau d'assurance maximal pouvant être attribué à un Justificatif spécifique sera le niveau le plus bas qu'il atteint pour *n'importe lequel* des critères du Profil de conformité. Par exemple, si un Justificatif a atteint la norme du niveau CAL4 pour neuf critères et celle du niveau CAL1 pour un critère, le niveau établi pour le Justificatif ne peut être supérieur à CAL1.

5 Évaluation des risques

La figure 4 contient une énumération des risques couramment utilisée pour évaluer le niveau d'assurance exigé pour une interaction numérique spécifique. Précisons que ce tableau se veut

illustratif de par sa nature. Il ne vise pas à être exhaustif ni directif. Les Parties utilisatrices doivent évaluer les risques et préjudices potentiels qui les attendent, et évaluer les niveaux de risque qu'elles sont disposées à accepter pour une transaction spécifique dans leur contexte opérationnel. Certains critères illustratifs utilisent donc une terminologie qui est sujette à interprétation (p. ex. « élevé », « moyen », « faible »). Cela permet aux praticiens d'établir un profil de risque correspondant à leur ministère, service ou type d'entreprise. Par exemple, une grande institution financière peut considérer le risque de perdre 100 000 $ comme étant « limité » ou « faible », tandis qu'un risque de cette taille peut être « grave » ou « élevé » pour une petite entreprise ou une entreprise en démarrage.

Comme les niveaux de risque sont fonction des circonstances propres à une Partie utilisatrice et des politiques, lois et/ou règlements applicables, il incombe à la Partie utilisatrice de documenter d'une façon explicite sa tolérance au risque. Cela permettra de s'assurer que les risques font l'objet de contrôles systématiques qui ne sont pas trop permissifs ni trop rigoureux, peu importe les personnes qui les mettent en place, et qu'ils sont évalués d'une façon équitable lors des audits.

La Partie utilisatrice doit aussi tenir compte de la fiabilité des Entités intervenant dans une transaction lorsqu'elle évalue la fiabilité d'une transaction, d'une Relation ou d'un Attribut, tel que documenté dans les composantes « Personne vérifiée », « Organisation vérifiée » et « Authentification » du CCP.

149-a

Catégorie d'impact	**Niveau d'assurance requis**			
	CAL1	**CAL2**	**CAL3**	**CAL4**
Désagrément, détresse, préjudice pour la situation ou la réputation	Au pire, désagrément, détresse, embarras ou préjudice limités à court terme pour la situation ou la réputation d'une partie	Au pire, désagrément, détresse ou préjudice graves à court terme ou limités à long terme pour la situation ou la réputation d'une partie	Désagrément, détresse ou préjudice graves ou sérieux à long terme pour la situation ou la réputation d'une partie (ordinairement réservé aux situations qui ont des effets graves ou qui touchent beaucoup de personnes)	Désagrément, détresse ou préjudice graves et permanents pour a situation ou la réputation d'une partie

149-b

149-c	**Perte financière**	Au pire, perte financière insignifiante ou sans conséquence pour une partie ou encore responsabilité sans conséquence	Au pire, perte financière sérieuse pour une partie ou responsabilité sérieuse	Grave perte financière pour une partie ou grave responsabilité	Perte financière catastrophique pour une partie ou responsabilité catastrophique
149-d	**Préjudice pour un programme ou l'intérêt public**	Au pire, effet négatif limité sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., diminution de la capacité à mener des missions au point et assez longtemps pour que l'organisation accomplisse ses fonctions principales avec une efficacité nettement réduite; préjudice mineur pour les actifs organisationnels ou les intérêts publics)	Au pire, sérieux effet négatif sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., diminution importante de la capacité à mener des missions au point et assez longtemps pour que l'organisation accomplisse ses fonctions principales avec une efficacité nettement réduite; sérieux préjudice pour les actifs organisationnels ou les intérêts publics)	Grave effet négatif sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., grave diminution ou perte de la capacité à mener des missions au point et assez longtemps pour que l'organisation soit incapable d'accomplir une ou plusieurs de ses fonctions principales; important préjudice pour les actifs organisationnels ou les intérêts publics)	Effet catastrophique sur les opérations ou les actifs organisationnels ou une organisation, un programme ou un actif du gouvernement ou l'intérêt public (p. ex., diminution ou perte catastrophique de la capacité à mener des missions au point et assez longtemps pour que l'organisation soit incapable d'accomplir ses fonctions principales; préjudice catastrophique pour les actifs organisationnels ou les intérêts publics)

149-e	**Divulgation non autorisée de renseignements personnels ou commerciaux sensibles**	Au pire, divulgation limitée de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée entraînant une perte de confidentialité ayant un faible impact	Au pire, divulgation limitée de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée ayant un impact modéré	Divulgation limitée de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée ayant un impact sérieux	Divulgation limitée de renseignements personnels ou de renseignements sensibles du point de vue commercial à des parties non autorisées ou violation de la vie privée ayant un impact catastrophique
149-f	**Divulgation non autorisée de renseignements gouvernementaux sensibles** **(gouvernements uniquement)**	Perte de confidentialité ayant peu d'impact	Effet négatif limité sur les opérations et les actifs organisationnels par suite d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées	Effet négatif sérieux sur les opérations et les actifs organisationnels par suite d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées	Effet négatif catastrophique sur les opérations et les actifs organisationnels par suite d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées

149-g	**Infractions civiles ou pénales**	Secteur privé : au pire, risque d'infractions civiles ou pénales d'une nature qui ne serait normalement pas assujettie à des efforts pour faire appliquer la loi Secteur public : tout compromis impliquant une infraction juridique est évalué comme étant au moins de niveau 2	Infraction civile ou pénale qui peut avoir des conséquences mineures et être assujettie à des efforts pour faire appliquer la loi	Infraction civile ou pénale pouvant avoir des conséquences sérieuses qui sont importantes pour les programmes visant à faire appliquer la loi	Infraction pouvant avoir des conséquences exceptionnellement graves qui sont particulièrement importantes pour les programmes visant à faire appliquer la loi
149-h	**Santé et sécurité du personnel**	Secteur privé : au pire, blessure mineure ne nécessitant pas de traitement médical Secteur public : toute atteinte à la santé et la sécurité est évaluée comme étant au moins de niveau 2	Secteur privé : au pire, risque modéré de blessure mineure ou risque limité de blessure nécessitant un traitement médical Secteur public : blessure personnelle mineure ne nécessitant pas de soins médicaux	Secteur privé : au pire, faible risque de blessure grave ou de décès Secteur public : blessure personnelle nécessitant des soins médicaux	Risque de blessure personnelle grave ou de décès
149-i	**Intérêt national** **(gouvernements uniquement)**	(Toute atteinte impliquant l'intérêt national est évaluée comme étant au moins de niveau 2)	Un inconvénient pour l'intérêt national	Une atteinte à l'intérêt national	Une atteinte sérieuse ou exceptionnellement grave à l'intérêt national

161 **Figure 4 : Tableau d'évaluation des risques**

162 5.1 Évaluation du niveau de risque

163 Les risques ci-dessus devraient être évalués comme suit :

152-a	Niveau d'assurance requis	Critère
152-b	**Niveau 1 (CAL1)**	Un ou plusieurs risques sont évalués comme étant de niveau 1 et aucun risque n'est évalué comme dépassant le niveau 1
152-c	**Niveau 2 (CAL2)**	Un ou plusieurs risques sont évalués comme étant de niveau 2 et aucun risque n'est évalué comme dépassant le niveau 2
152-d	**Niveau 3 (CAL3)**	Un ou plusieurs risques sont évalués comme étant de niveau 3 et aucun risque n'est évalué comme dépassant le niveau 3
152-e	**Niveau 4 (CAL4)**	Un ou plusieurs risques sont évalués comme étant de niveau 4

164 **Figure 5 : Évaluation des niveaux de risque**

5.2 Risques pesant sur les Justificatifs

Les Justificatifs fournissent les bases de la confiance dans un écosystème numérique. C'est important que les organisations qui participent à un écosystème de confiance comprennent les risques qui pèsent sur les justificatifs qu'elles créent, possèdent et/ou utilisent, et qu'elles prennent des mesures appropriées pour protéger leur intégrité. La figure 6 contient un tableau qui illustre les risques pensant sur les justificatifs et des exemples de stratégies d'atténuation.

Activité	Menace	Exemple	Exemple de stratégie d'atténuation
Stockage des justificatifs	Divulgation	Les noms d'utilisateur et les mots de passe stockés dans un fichier système sont divulgués.	Recourir à des mécanismes de contrôle assurant une protection contre les divulgations non autorisées des justificatifs stockés. Protéger les noms d'utilisateur/les mots de passe au moyen de fonctions sécurisées de salage et de hachage ou de techniques de chiffrement approuvées, de façon à rendre impossible la récupération des mots de passe pouvant résulter de la fuite d'un fichier de mots de passe.
	Trafiquage	Le fichier qui établit la correspondance entre les noms d'utilisateurs et les mots de passe au sein du FJI est piraté, ce qui entraîne une modification des correspondances et le remplacement des mots de passe légitimes par des mots de passe connus d'un auteur de menaces.	Recourir à des mécanismes de contrôle assurant une protection contre le trafiquage des justificatifs et des jetons.
Services de vérification des justificatifs	Divulgation	Un auteur de menaces parvient à visualiser les demandes et les réponses circulant entre un FJI et un vérificateur.	Recourir à un protocole de communication qui offre des fonctions de protection de la confidentialité.

158-e		Trafiquage	Un auteur de menaces parvient à se faire passer pour un FJI et fournit des réponses erronées aux demandes de vérification de mots de passe d'un vérificateur.	Veiller à ce que les vérificateurs authentifient les FJI avant d'accepter une réponse de vérification de la part desdits FJI. Recours à un protocole de communication qui offre des fonctions de protection de l'intégrité.
158-f		Non-disponibilité	Le fichier de mots de passe ou le FJI ne sont pas disponibles et ne peuvent donc pas fournir les correspondances entre les mots de passe et les noms d'utilisateur.	Veiller à ce que les FJI disposent d'un plan de contingence perfectionné et éprouvé.
158-g			Les vérificateurs ne peuvent obtenir les certificats de clés publiques des requérants parce que les systèmes annuaires sont en panne (par exemple, aux fins de maintenance ou à la suite d'une attaque par déni de service).	
158-h	**Émission ou renouvellement ou réémission des justificatifs**	Divulgation	Le mot de passe d'un abonné est renouvelé par un FJI puis copié par un auteur de menaces pendant que ledit mot de passe est envoyé par le FJI vers l'abonné.	Recourir à un protocole de communication qui soit apte à protéger la confidentialité des données de session.
158-i		Trafiquage	Un nouveau mot de passe créé par un abonné est modifié par un auteur de menaces pendant que ledit mot de passe est acheminé à un FJI pour remplacer un mot de passe expiré.	Recourir à un protocole de communication qui soit apte à authentifier le FJI avant l'enclenchement des mesures de réémission des jetons et à protéger l'intégrité des données transmises.

158-j		Émission non autorisée	Un FJI est victime de compromission à la suite d'un accès logique ou physique non autorisé rendu possible par l'émission de justificatifs frauduleux.	Mettre en place des contrôles d'accès physiques et logiques qui soient aptes à prévenir la compromission du FJI.
158-k		Renouvellement ou réémission non autorisés	Un auteur de menaces incite frauduleusement un FJI à réémettre un justificatif pour un abonné légitime – le nouveau justificatif lie l'identité dudit abonné à un jeton fourni par l'auteur de menaces.	Mettre en œuvre une politique exigeant qu'un abonné prouve qu'il a possession du jeton original avant d'en arriver à engager le processus de réémission. Toute tentative d'engagement du processus de réémission au moyen d'un jeton expiré ou révoqué devrait échouer.
158-l			Un auteur de menaces parvient à tirer avantage d'un faible protocole de renouvellement des justificatifs et à prolonger la période de validité des justificatifs d'un abonné légitime.	
158-m	**Révocation ou destruction des jetons et des justificatifs**	Temporisation de la révocation ou de la destruction de justificatifs	Les listes de certification de révocation qui ne sont pas à jour permettent à des auteurs de menaces d'utiliser des comptes périmés (comptes qui pourtant auraient dû être verrouillés suivant la révocation de leurs justificatifs).	Révoquer ou détruire les justificatifs dès que l'avis de révocation ou de destruction des justificatifs a été signifié.
158-n			Les comptes utilisateur ne sont pas supprimés lorsque des employés quittent une entreprise, ce qui crée le risque que des personnes non autorisées se servent desdits comptes.	
158-o			Un jeton matériel est utilisé après la révocation ou l'expiration des justificatifs correspondants.	Détruire les jetons après la révocation des justificatifs correspondants.

Figure 6 : Risques pesant sur les Justificatifs

5.3 Gestion des Justificatifs

La façon dont les Justificatifs sont gérés aura un impact direct sur leur fiabilité. La figure 7 contient un tableau qui illustre les exigences pour la gestion des Justificatifs et l'impact que cela peut avoir sur leur fiabilité. Tel que mentionné dans la discussion préalable de ce document à propos des risques, les parties utilisatrices doivent évaluer le niveau de risque qu'elles sont disposées à accepter et ajuster en conséquence leurs propres paramètres de risque. Comme cela a aussi été indiqué, il est important que ces niveaux soient délibérément établis et enregistrés afin d'être mis en œuvre et évalués d'une manière uniforme.

Niveau	Exigences				
	Stockage des justificatifs	**Services de vérification des jetons et des justificatifs**	**Renouvellement/réémission des jetons et des justificatifs**	**Révocation et destruction des jetons et des justificatifs**	**Exigences en matière de conservation des documents**
CAL1	Les fichiers de secrets partagés employés par les vérificateurs seront protégés par des contrôles d'accès dans le but de réserver l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. Les fichiers de secrets partagés ne devront pas être enregistrés en texte clair. Le hachage unidirectionnel ou une autre fonction semblable doit être employé avant l'enregistrement desdits fichiers.	Les secrets à long terme des jetons ne devraient pas être partagés avec d'autres parties, sauf en cas de nécessité absolue.	Aucune exigence	Aucune exigence	Aucune exigence

166-d

CAL2	Les fichiers de secrets partagés employés par les vérificateurs devront être protégés par des contrôles d'accès dans le but de réserver l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. De tels fichiers de secrets partagés ne devront contenir aucun mot de passe ni aucun secret en texte clair. Ainsi, deux options peuvent être employées pour protéger les secrets partagés : 1. Les mots de passe peuvent être concaténés à une variable de salage (variable distribuée dans un groupe de mots de passe stockés dans un même espace) puis hachés au moyen d'un algorithme approuvé, faisant ainsi que les calculs informatiques employés pour exécuter une attaque par dictionnaire ou une attaque exhaustive visant un fichier de mots de passe volé deviennent inutiles à l'occasion d'attaques ultérieures sur d'autres fichiers de mots de passe. Les mots de passe hachés sont ensuite enregistrés dans le fichier de mots de passe. Les variables de salage peuvent consister en une fonction de salage global (la même variable pour tous les mots de passe d'un groupe) et en un nom d'utilisateur (un par mot de passe) ou encore en une technique permettant de garantir l'unicité du salage au sein d'un groupe de mots de passe. 2. Les secrets partagés peuvent être chiffrés et enregistrés au moyen de procédures et d'algorithmes approuvés. Les secrets ne doivent être déchiffrés qu'au moment voulu, soit dès lors que l'authentification l'exige. De plus, toute méthode devant servir à la protection des secrets partagés de niveau 3 ou 4 peut également être employée au niveau 2.	S'ils sont utilisés, les secrets partagés à long terme aux fins d'authentification ne devront jamais être révélés à quelque partie que ce soit, sauf aux vérificateurs relevant des FJI. Toutefois, les secrets partagés aux fins de sessions (temporaires) peuvent être fournis aux vérificateurs par les FJI à des vérificateurs indépendants. Des mesures de protection cryptographiques sont requises pour tous les messages échangés entre un FJI et un vérificateur, qui contiennent des justificatifs personnels ou qui confirment la validité des justificatifs faiblement liés ou possiblement révoqués. Les justificatifs personnels ne devraient être acheminés par voie de sessions protégées à une partie obligatoirement authentifiée, de façon à garantir la confidentialité et à contrer le trafiquage.	Les FJI devront mettre en œuvre des politiques adéquates de renouvellement et de réémission des jetons et des justificatifs. La preuve de possession d'un jeton encore valide devra être confirmée par le requérant avant qu'un FJI accorde le renouvellement ou la réémission. Les mots de passe ne devront pas être renouvelés. Ils seront plutôt réémis. Au terme de la période de validité d'un jeton ou d'un délai de grâce, ni la réémission ni le renouvellement ne devront être autorisés. À la réémission, les secrets de jetons ne devront ni revenir à une valeur par défaut ni être réutilisés. Toutes les transactions devraient se faire par voie de session protégée, notamment par SSL ou par TSL.	Les FJI devront révoquer ou détruire les justificatifs et les jetons dans les 72 heures suivant la réception d'un avis indiquant qu'un justificatif n'est plus valide ou qu'un jeton a été compromis, et ce, pour empêcher l'authentification de requérants qui s'aviseraient d'employer les justificatifs ou les jetons en question. Lorsqu'il émet des justificatifs qui expirent automatiquement après 72 heures (p. ex. émission quotidienne de nouveaux certificats valides pour 24 heures) un FJI n'est pas tenu de fournir un mécanisme particulier pour révoquer les justificatifs. Les FJI qui enregistrent des mots de passe devraient veiller à ce que la révocation ou la radiation de ceux-ci s'exécute dans les 72 heures.	L'inscription, l'historique et l'état des jetons et des justificatifs (y compris la révocation) devront être enregistrés et conservés par les FJI ou par leur représentant. La période de conservation des données pour les justificatifs de niveau 2 est de sept ans et six mois suivant l'expiration ou la révocation (l'échéance la plus tardive prévaut) de ces justificatifs.

CAL3	Les fichiers de secrets partagés employés par les vérificateurs devraient être protégés par des contrôles d'accès dans le but de réserver l'accès aux administrateurs ainsi qu'aux applications et au personnel autorisés. Les fichiers contenant des secrets partagés doivent être chiffrés. Voici les exigences minimales concernant le chiffrement : 1. La clé de chiffrement pour le secret partagé est elle-même chiffrée selon une clé conservée dans un module cryptographique matériel FIPS 140-2 de niveau 2 ou supérieur ou encore dans un module cryptographique FIPS 140-2 de niveau 3 ou 4; elle n'est déchiffrée qu'au besoin, lorsqu'elle doit faire partie de mesures d'authentification. 2. Les secrets partagés sont protégés en tant que clés dans un module cryptographique matériel FIPS 140-2 de niveau 2 ou supérieur ou encore dans un module cryptographique FIPS 140-2 de niveau 3 ou 4; ils ne sont jamais exportés en texte clair depuis le module en question.	Les FJI devront fournir un mécanisme sécurisé qui permettra aux vérificateurs et aux PC de vérifier la validité des justificatifs. Ce type de mécanisme peut recourir à des serveurs de validation en ligne ou à des serveurs FJI qui ont accès aux enregistrements de statut pendant les transactions d'authentification. Au nombre des services de vérification offerts par les FJI, des clés temporaires d'authentification de session peuvent être générées par ces FJI à partir de clés de secrets partagés à long terme, puis distribuées à de tiers vérificateurs. Toutefois, les secrets partagés à long terme ne seront, en soi, jamais partagés avec une tierce partie ni même avec les tiers vérificateurs.	Le renouvellement et la réémission ne devraient avoir lieu qu'avant l'expiration des justificatifs concernés. Dans les cas de renouvellement ou de réémission des justificatifs, les requérants devraient être authentifiés auprès des FJI au moyen du jeton et des justificatifs existants. Toutes les transactions devraient se faire par voie de session protégée, notamment par SSL ou par TSL.	Les FJI devraient disposer d'une procédure permettant de révoquer les justificatifs et les jetons dans les 24 heures. Les vérificateurs doivent veiller à ce que les jetons employés soient ou bien fraîchement émis (depuis au plus 24 heures) ou bien encore valides. Les systèmes d'authentification fondés sur les secrets partagés peuvent tout simplement supprimer, dans la base de vérification, les noms d'utilisateurs dont l'accès a été révoqué.	Aucune exigence additionnelle par rapport au niveau 2.

166-f	**CAL4**	Aucune exigence additionnelle par rapport au niveau 3.	Aucune exigence additionnelle par rapport au niveau 3.	Les transferts de données sensibles devront être authentifiés par voie cryptographique, au moyen de clés liées au processus d'authentification. Toutes les clés temporaires ou à court terme qui sont produites pendant l'authentification initiale devront expirer, ce qui nécessitera une nouvelle authentification dans les 24 heures de l'authentification initiale.	Les FJI doivent disposer d'une procédure permettant de révoquer les justificatifs dans les 24 heures suivant l'authentification. Les vérificateurs ou les PC doivent veiller à ce que les justificatifs employés soient ou bien fraîchement émis (depuis au plus 24 heures) ou bien encore valides.	Toutes les stipulations relevant des niveaux 2 et 3 s'appliquent. La période minimale de conservation des données constituant les justificatifs de niveau 4 est de 10 ans et six mois suivant l'expiration ou la révocation de ces justificatifs.

180 **Figure 7 : Gestion des justificatifs**

181 6 Processus de confiance

182 Le CCP favorise la confiance grâce à un ensemble de processus vérifiables.

183 Un processus est une activité commerciale ou technique, ou un ensemble d'activités, qui
184 transforme une condition d'entrée en condition de sortie dont dépendent souvent d'autres
185 processus. Une condition est un état ou une circonstance spécifique qui s'applique à un
186 Processus de confiance. Une condition peut être une entrée, une sortie ou une dépendance
187 relative à un processus de confiance. Les Critères de conformité spécifient ce qui est requis
188 pour transformer une condition d'entrée en condition de sortie. Ils spécifient, par exemple, ce
189 qui est nécessaire pour que le processus Relation vérifiée transforme une condition d'entrée
190 « Relation approuvée » en condition de sortie « Relation vérifiée ».

191 Un processus est désigné comme étant un Processus de confiance lorsqu'il est évalué et
192 certifié conforme aux Critères de conformité définis dans un profil de conformité du CCP.
193 L'intégrité d'un Processus de confiance est fondamentale, car de nombreux participants se fient
194 au résultat du processus, souvent par-delà les frontières territoriales, organisationnelles et
195 sectorielles, et à court et long terme.

La composante « Justificatifs (Relations et Attributs) » du CCP définit cinq processus de confiance rattachés aux Relations :

1. Définir la relation
2. Déclarer la relation
3. Approuver la relation
4. Vérifier la relation
5. Réfuter la relation

La composante « Justificatifs (Relations et Attributs) » du CCP définit quatre processus de confiance rattachés aux Attributs :

1. Définir l'attribut
2. Lier l'attribut
3. Maintenir l'attribut
4. Révoquer l'attribut

7 Critères de conformité des Justificatifs

Les critères de conformité sont catégorisés par élément de confiance. Pour faciliter la référence, on peut se référer à un critère de conformité spécifique par son numéro de catégorie et de référence. Exemple : « RABS1 » fait référence au « critère de conformité de base nº 1 ».

Remarques :

- Les Critères de conformité de base sont également inclus dans ce profil de conformité.
- Les Critères de conformité spécifiés dans d'autres composantes du CCP peuvent aussi s'appliquer à la composante « Justificatifs (Relations et Attributs) » du CCP.

Référence	Critères de conformité	Niveau d'assurance			
RABS	**Ces Critères de base s'appliquent à <u>tous</u> les processus rattachés aux Relations et aux Attributs**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
1	Ces critères de conformité ne remplacent ou n'annulent pas les règlements existants; on s'attend à ce que les organisations et les personnes se conforment aux lois, aux politiques et aux règlements en vigueur dans leur administration.	X	X	X	X
RDEF	**Définir la relation**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
1	L'Émetteur **NE DEVRAIT PAS** inclure des renseignements à propos d'un cas spécifique de la relation type qui est définie.	X	X	X	X

208	2	L'Émetteur **DEVRAIT** inclure des renseignements qui identifient clairement le créateur de la définition de la relation.	X	X		
209	3	L'Émetteur **DOIT** inclure des renseignements qui identifient clairement le créateur de la définition de la relation.			X	X
210	4	L'Émetteur **DEVRAIT** indiquer l'autorité sous laquelle la relation peut être divulguée (p. ex., un certificat de mariage ne peut être divulgué légitimement que par une partie ayant autorité appropriée comme un tribunal ou un organisme d'État; l'appartenance à une association communautaire peut être légitimement réfutée d'une manière volontaire ou être réfutée par la direction de l'association).	X			
2	5	L'Émetteur **DOIT** indiquer l'autorité en vertu de laquelle la relation peut être réfutée (p. ex., un certificat de mariage ne peut être divulgué légitimement que par une partie ayant autorité appropriée comme un tribunal ou un organisme d'État; l'appartenance à une association communautaire peut être légitimement réfutée d'une manière volontaire ou être réfutée par la direction de l'association).		X	X	X
3	6	L'Émetteur **DEVRAIT** déclarer si le type de Relation décrite doit être approuvé pour être considéré fiable (voir les critères énumérés sous REND pour les détails).	X			
4	7	L'Émetteur **DOIT** déclarer si le type de Relation décrite doit être approuvé pour être considéré fiable (voir les critères énumérés sous REND pour les détails).		X	X	X
5	8	Dans la mesure du possible, et si approprié, l'Émetteur **PEUT** utiliser des définitions juridiques pertinentes, des définitions des normes de l'industrie ou des références à des schémas pertinents.	X	X		
6	9	Dans la mesure du possible, et si approprié, l'Émetteur **DEVRAIT** utiliser des définitions juridiques pertinentes, des définitions des normes de l'industrie ou des références à des schémas pertinents.			X	X
7	**RDEC**	**Déclarer la relation**	**CAL1**	**CAL2**	**CAL3**	**CAL4**

8	1	L'Émetteur **PEUT** utiliser une définition de la Relation comme base pour la Relation déclarée et y faire référence dans la Relation déclarée.	X			
9	2	L'Émetteur **DOIT** utiliser une définition de la Relation comme base pour la Relation déclarée et y faire référence dans la Relation déclarée.		X	X	X
10	3	L'émetteur **PEUT** fournir aux participants un résumé de son mandat et son autorité reliés à la Relation qu'il déclare.	X			
11	4	L'émetteur **DOIT** fournir aux participants un résumé de son mandat et son autorité reliés à la Relation qu'il déclare.		X	X	X
12	5	Le cas échéant, l'Émetteur **DEVRAIT** fournir aux Participants la preuve qu'il remplit toutes les exigences juridiques et réglementaires s'appliquant aux types de Relations qu'il déclare.	X			
13	6	Le cas échéant, l'Émetteur **DOIT** fournir aux participants la preuve qu'il remplit toutes les exigences juridiques et réglementaires s'appliquant aux types de Relations qu'il déclare.		X	X	X
14	7	L'Émetteur **PEUT** fournir aux Participants les conditions générales régissant l'utilisation légitime des Relations déclarées qu'il émet (p. ex., il y a des cas où la carte d'assurance maladie provinciale ou le numéro d'assurance sociale devraient être utilisés, et des cas où ils ne devraient pas être utilisés ou leur utilisation est interdite par un règlement, une loi ou une politique).	X			
15	8	L'Émetteur **DEVRAIT** fournir aux Participants les conditions générales régissant l'utilisation légitime des Relations déclarées qu'il émet (p. ex., il y a des cas où la carte d'assurance maladie provinciale ou le numéro d'assurance sociale devraient être utilisés, et des cas où ils ne devraient pas être utilisés ou leur utilisation est interdite par un règlement, une loi ou une politique).		X		
16	9	L'Émetteur **DOIT** fournir aux Participants les conditions générales régissant l'utilisation légitime des Relations déclarées qu'il émet (p. ex., il y a des cas où la carte d'assurance maladie provinciale ou le numéro d'assurance sociale devraient être utilisés, et des cas où ils ne devraient pas être utilisés ou leur utilisation est interdite par un règlement, une loi ou une politique).			X	X

17	10	L'Émetteur **DOIT** fournir aux Participants un point de contact leur permettant d'obtenir de l'information sur ses Attributs et processus connexes.		X	X	X
18	11	Le cas échéant, l'Émetteur **DOIT** permettre au Sujet de spécifier l'endroit (c.-à-d., référentiel de justificatifs local ou hébergé) où la Relation sera fournie, à moins que ce ne soit interdit par un règlement, une politique ou une loi.	X	X	X	X
19	12	L'Émetteur **PEUT** fournir aux Participants des détails concernant la preuve et les processus spécifiques sur lesquels il s'est fié pour vérifier et valider les renseignements sur le Sujet contenus dans une Relation.	X			
20	13	L'Émetteur **DEVRAIT** fournir aux Participants des détails concernant la preuve et les processus spécifiques sur lesquels il s'est fié pour vérifier et valider les renseignements sur le Sujet contenus dans une relation.		X		
21	14	L'Émetteur **DOIT** fournir aux Participants des détails concernant la preuve et les processus spécifiques sur lesquels il s'est fié pour vérifier et valider les renseignements sur le Sujet contenus dans une relation.			X	X
22	15	L'Émetteur **PEUT** fournir des références aux Justificatifs ou Attributs de tierces parties (c.-à-d., des Justificatifs ou Attributs émis par d'autres Entités) dont il s'est servi pour vérifier et valider les renseignements contenus dans une Relation qu'il a déclarée.	X			
23	16	L'Émetteur **DEVRAIT** fournir des références aux Justificatifs ou Attributs de tierces parties (c.-à-d., des Justificatifs ou Attributs émis par d'autres entités) dont il s'est servi pour vérifier et valider les renseignements contenus dans une Relation qu'il a déclarée.		X		
24	17	L'Émetteur **DOIT** fournir des références aux Justificatifs ou Attributs de tierces parties (c.-à-d., des Justificatifs ou Attributs émis par d'autres entités) dont il s'est servi pour vérifier et valider les renseignements contenus dans une relation qu'il a déclarée.			X	X
25	18	Les renseignements contenus dans une Relation **DOIVENT** concorder avec ceux qui sont contenus dans les dossiers de l'Émetteur.	X	X	X	X

26	19	L'Émetteur **DEVRAIT** fournir des renseignements indiquant la confiance qu'il faisait à l'exactitude des renseignements contenus dans la Relation quand celle-ci a été déclarée.		X	X	X
27	20	L'Émetteur **DEVRAIT** fournir des renseignements indiquant la confiance qu'il faisait à l'identité du Sujet ou celle de la personne agissant pour le compte du Sujet quand la Relation déclarée a été émise.	X	X		
28	21	L'Émetteur **DOIT** fournir des renseignements indiquant la confiance qu'il faisait à l'identité du Sujet ou celle de la personne agissant pour le compte du Sujet quand la Relation a été déclarée.			X	X
29	22	L'Émetteur **PEUT** être capable de démontrer qu'une Relation déclarée émanait de l'Émetteur et qu'elle n'a pas été altérée pendant la transmission à un autre Participant (Sujet, Détenteur, Partie utilisatrice, etc.).	X			
30	23	L'Émetteur **DEVRAIT** être capable de démontrer qu'une Relation déclarée émanait de l'Émetteur et qu'elle n'a pas été altérée pendant la transmission à un autre Participant (Sujet, Détenteur, Partie utilisatrice, etc.).		X		
31	24	L'Émetteur **DOIT** être capable de démontrer qu'une Relation déclarée émanait de l'émetteur et qu'elle n'a pas été altérée pendant la transmission à un autre Participant (Sujet, Détenteur, Partie utilisatrice, etc.).			X	X
32	25	Un Justificatif de Relation déclarée **DOIT** inclure des renseignements qui identifient l'Émetteur.		X	X	X
33	26	L'Émetteur **DOIT** inclure la date à laquelle la Relation a été déclarée, et étiquetée comme telle sans ambiguïté.		X	X	X
34	27	L'Émetteur **PEUT** fournir une date d'expiration pour toutes les Relations qu'il déclare ou indiquer que la Relation n'a pas de date d'expiration.	X			
35	28	L'Émetteur **DOIT** fournir une date d'expiration pour toutes les Relations qu'il déclare ou indiquer que la Relation n'a pas de date d'expiration.		X	X	X

36	29	En déclarant une Relation, l'Émetteur **PEUT** indiquer qu'elle est entièrement ou partiellement contestée. En pareil cas, l'Émetteur **DEVRAIT** inclure une référence à d'autres Relations déclarées qui contiennent des renseignements contestés et/ou faisant l'objet d'un examen.	X	X	X	X
37	30	L'Émetteur **DEVRAIT** fournir aux Participants des conditions générales en vertu desquelles les Relations qu'il déclare deviendront inutilisables ou non fiables.	X			
38	31	L'Émetteur **DOIT** fournir aux Participants des conditions générales en vertu desquelles les Relations qu'il déclare deviendront inutilisables ou non fiables.		X	X	X
39	32	L'Émetteur **DOIT** s'assurer que le Référentiel auquel il transmet une Relation déclarée est adéquatement sécurisé, trouvé d'une manière légitime et situé dans une administration tel qu'exigé par la loi, une politique et/ou un règlement.		X	X	X
40	**REND**	**Approuver la relation**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
41	1	Une Partie qui approuve **PEUT** être une Partie ayant autorité qui est une Personne vérifiée ou une Organisation vérifiée.	X			
42	2	Une Partie qui approuve **DEVRAIT** être une Partie ayant autorité qui est une Personne vérifiée ou une Organisation vérifiée.		X		
43	3	Une Partie qui approuve **DOIT** être une Partie ayant autorité qui est une Personne vérifiée ou une Organisation vérifiée.			X	X
44	**RVER**	**Vérifier la relation**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
45	1	Les Vérificateurs **DEVRAIENT** fournir assez de renseignements à la Partie utilisatrice pour lui permettre d'évaluer convenablement le niveau d'assurance qui peut être associé à chaque Relation.	X	X		
46	2	Les Vérificateurs **DOIVENT** fournir assez de renseignements à la Partie utilisatrice pour lui permettre d'évaluer convenablement le niveau d'assurance qui peut être associé à chaque Relation.			X	X

47	3	Les Vérificateurs **PEUVENT** confirmer que la Partie qui approuve ou qui déclare est une Partie ayant autorité et que le ou les Sujets sont des Personnes ou des Organisations vérifiées.	X			
48	4	Les Vérificateurs **DEVRAIENT** confirmer que la Partie qui approuve ou qui déclare est une Partie faisant autorité et que le ou les Sujets sont des Personnes ou des Organisations vérifiées.		X		
49	5	Les Vérificateurs **DOIVENT** confirmer que la Partie qui approuve ou qui déclare est une Partie ayant autorité et que le ou les Sujets sont des Personnes ou des Organisations vérifiées.			X	X
50	6	Les Vérificateurs **DEVRAIENT** informer la Partie utilisatrice si la Partie qui approuve ou qui déclare est une Partie ayant autorité et si le ou les Sujets sont des Personnes ou des Organisations vérifiées.		X		
51	7	Les Vérificateurs **DOIVENT** informer la Partie utilisatrice si la Partie qui approuve ou qui déclare est une Partie ayant autorité et si le ou les Sujets sont des Personnes ou des Organisations vérifiées.			X	X
52	8	La Partie qui approuve ou qui déclare **PEUT** être une Personne ou une Organisation vérifiée.	X			
53	9	La Partie qui approuve ou qui déclare **DEVRAIT** être une Personne ou une organisation vérifiée.		X		
54	10	La Partie qui approuve ou qui déclare **DOIT** être une Personne ou une Organisation vérifiée.			X	X
55	11	Le Vérificateur **DEVRAIT** être une Personne ou une Organisation vérifiée.	X			
56	12	Le Vérificateur **DOIT** être une Personne ou une Organisation vérifiée.		X	X	X
57	13	Le Vérificateur **NE DEVRAIT PAS** garder des copies des Présentations ou des Présentations vérifiées qu'il vérifie, ni des données qu'elles contiennent ni des données dérivées de ces données, à moins qu'un règlement, une politique ou une loi ne l'exige.	X	X	X	X

58	14	Les Vérificateurs **NE DOIVENT PAS** partager les renseignements qui leur sont présentés dans le cadre du processus de vérification avec d'autres Vérificateurs, d'autres participants à l'écosystème numérique ou qui que ce soit d'autre que la ou les Parties utilisatrices sans le consentement express du Sujet, à mois que cela ne soit exigé par un règlement, une politique ou la loi.	X	X	X	X
59	15	Les Relations incluses dans une Présentation ou une Présentation vérifiable qui est soumise à un Vérificateur **DEVRAIENT** être sous la forme d'une Relation déclarée, approuvée ou vérifiable.	X	X	X	X
60	**RDIS**	**Réfutation de la Relation**	**CAL**	**CAL2**	**CAL3**	**CAL4**
61	1	La Partie qui réfute **DOIT** réfuter, ou rendre inutilisable ou non fiable, une Relation si elle décèle des indices d'une Relation compromise ou non valide.	X	X	X	X
62	2	La Partie qui réfute **DOIT** mettre à la disposition des Participants le statut de toutes les Relations autrement inutilisables ou non fiables qu'elle a émises.	X	X	X	X
63	3	La Partie qui réfute **DOIT** saisir les détails suivants à propos des Relations que l'émetteur a rendues inutilisables ou non fiables : date à laquelle la mesure a été prise, raison de la mesure, indication générale de qui a initié la mesure (p. ex., Sujet ou Émetteur).	X	X	X	X
64	4	La Partie qui réfute **DOIT** uniquement réfuter les détails saisis à propos de Relations inutilisables ou non fiables selon UNUS-3 à des Participants connus qui ont un besoin raisonnable d'avoir l'information.	X	X	X	X
65	5	La Partie qui réfute **DOIT** divulguer la raison pour laquelle elle réfute la Relation au ou aux Sujets.	X	X	X	X
66	6	La Partie qui réfute **NE DOIT PAS** réfuter arbitrairement des Relations. Les Relations réfutées devraient être le résultat de politiques, procédures, lois ou règlements pertinents ou encore d'activités malveillantes confirmées ou suspectées, comme de la fraude, qui présenteraient un risque indu si la Relation était acceptée.	X	X	X	X

67	7	La Partie qui approuve **DEVRAIT** fournir aux Sujets la capacité d'amorcer un processus pour réfuter, ou autrement rendre inutilisable ou non fiable, une Relation quand le Sujet décèle des indications d'une Relation compromise ou invalide.	X	X	X	X
68	**ADEF**	**Définir l'attribut**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
69	1	L'Émetteur **NE DEVRAIT PAS** inclure des renseignements à propos d'un cas spécifique de type d'attribut défini.	X	X	X	X
70	2	L'Émetteur **DEVRAIT** inclure des renseignements qui identifient clairement le créateur de la Définition de l'attribut.	X	X		
71	3	L'émetteur **DOIT** inclure des renseignements qui identifient clairement le créateur de la Définition de l'attribut.			X	X
72	4	Dans la mesure du possible, et si approprié, l'Émetteur **PEUT** utiliser des définitions juridiques pertinentes, des définitions standard de l'industrie ou des références à des schémas pertinents.	X	X		
73	5	Dans la mesure du possible, et si approprié, l'Émetteur **DEVRAIT** utiliser des définitions juridiques pertinentes, des définitions standard de l'industrie ou des références aux schémas pertinents.			X	X
74	**ABND**	**Lier d'attribut**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
75	1	L'Émetteur **PEUT** utiliser une Définition de l'Attribut comme base pour l'Attribut lié et y faire référence dans l'Attribut lié.	X			
76	2	L'Émetteur **DOIT** utiliser une définition de l'Attribut comme base pour l'Attribut lié et y faire référence dans l'attribut lié.		X	X	X
77	3	L'Émetteur **PEUT** fournir aux Participants un résumé de son mandat et de son autorité, car ils sont reliés aux Attributs qu'il émet.	X			
78	4	L'Émetteur **DOIT** fournir aux Participants un résumé de son mandat et de son autorité, car ils sont reliés aux Attributs qu'il émet.		X	X	X
79	5	L'Émetteur **DEVRAIT** fournir aux Participants la preuve qu'il répond à toutes les exigences juridiques et réglementaires applicables aux types d'Attributs qu'il émet.	X			

80	6	L'Émetteur **DOIT** fournir aux participants la preuve qu'il répond à toutes les exigences juridiques et réglementaires applicables aux types d'Attributs qu'il émet.		X	X	X
81	7	L'Émetteur **PEUT** fournir aux Participants les conditions générales qui régissent l'émission et l'utilisation des Attributs qu'il émet.	X			
82	8	L'Émetteur **DEVRAIT** fournir aux Participants les conditions générales qui régissent l'émission et l'utilisation des Attributs qu'il émet.		X		
83	9	L'Émetteur **DOIT** fournir aux Participants les conditions spécifiques qui régissent l'émission et l'utilisation d'un Attribut spécifique qu'il a émis.			X	X
84	10	L'Émetteur **DOIT** donner aux Sujets qui demandent l'émission d'un Attribut un avis stipulant que le fait de faire des déclarations ou de fournir des informations fausses ou trompeuses peut entraîner une violation des conditions régissant son émission et son utilisation.		X	X	X
85	11	L'Émetteur **DOIT** confirmer que les Sujets comprennent et acceptent l'avis précisant que toute déclaration fausse ou trompeuse peut entraîner une violation des conditions générales régissant l'émission et l'utilisation des Justificatifs.		X	X	X
86	12	L'Émetteur **DOIT** fournir aux Participants un point de contact pour obtenir des renseignements à propos de ses Justificatifs et processus associés.		X	X	X
87	13	Le cas échéant, l'Émetteur **DOIT** permettre au Sujet de spécifier l'endroit (c.-à-d. un Référentiel de Justificatifs local ou hébergé) où l'attribut sera livré, à moins qu'un règlement, une politique ou la loi ne l'interdise.	X	X	X	X
88	14	L'Émetteur **PEUT** fournir aux Participants les détails des preuves et processus spécifiques auxquels il s'est fié pour vérifier et valider les renseignements sur le Sujet contenus dans un Attribut.	X			
89	15	L'Émetteur **DEVRAIT** fournir aux Participants les détails des preuves et processus spécifiques auxquels il s'est fié pour vérifier et valider les renseignements sur le Sujet contenus dans un Attribut.		X		

299	16	L'Émetteur **DOIT** fournir aux Participants les détails des preuves et processus spécifiques auxquels il s'est fié pour vérifier et valider les renseignements sur le Sujet contenus dans un Attribut.			X	X
90	17	L'Émetteur **PEUT** fournir des références aux Justificatifs ou Attributs de tierces parties (c.-à-d., les Justificatifs ou Attributs émis par d'autres Entités) qu'il a utilisés pour vérifier et valider les renseignements contenus dans un Attribut qu'il a émis.	X			
91	18	L'Émetteur **DEVRAIT** fournir des références aux Justificatifs ou Attributs de tierces parties (c.-à-d., les Justificatifs ou Attributs émis par d'autres Entités) qu'il a utilisés pour vérifier et valider les renseignements contenus dans un Attribut qu'il a émis.		X		
92	19	L'Émetteur **DOIT** fournir des références aux Justificatifs ou Attributs de tierces parties (c.-à-d., les Justificatifs ou Attributs émis par d'autres Entités) qu'il a utilisés pour vérifier et valider les renseignements contenus dans un Attribut qu'il a émis.			X	X
93	20	Les renseignements contenus dans un Justificatif **DOIVENT** correspondre à ceux qui sont contenus dans les dossiers de l'Émetteur.	X	X	X	X
94	21	L'Émetteur **DEVRAIT** fournir des renseignements indiquant qu'il s'est fié à l'exactitude des renseignements contenus dans l'Attribut lorsque celui-ci a été émis.	u	X	X	X
95	22	L'Émetteur **DOIT** émettre un Attribut uniquement à la demande ou avec le consentement du Sujet ou d'une personne admissible à agir pour le compte du Sujet, sauf lorsqu'une politique, un règlement ou une loi le permet.	X	X	X	X
96	23	L'Émetteur **DOIT** prendre des mesures raisonnables pour s'assurer que des attributs liés sont émis à la demande et/ou avec le consentement du Sujet en droit de le faire ou d'une personne autorisée à agir pour le compte du Sujet.	X	X	X	X
97	24	L'Émetteur **DEVRAIT** fournir des renseignements indiquant qu'il s'est fié à l'identité du Sujet ou de la personne agissant pour le compte du Sujet quand l'Attribut lié a été émis.	X	X		

98	25	L'Émetteur **DOIT** fournir des renseignements indiquant qu'il s'est fié à l'identité du Sujet ou de la personne agissant pour le compte du Sujet quand l'Attribut lié a été émis.			X	X
99	26	L'Émetteur **PEUT** démontrer qu'un Attribut provenait de lui et qu'il n'a pas été altéré pendant la transmission à un autre Participant (Sujet, Titulaire, Partie utilisatrice, etc.).	X			
100	27	L'Émetteur **DEVRAIT** pouvoir démontrer qu'un Attribut provenait de lui et qu'il n'a pas été altéré pendant la transmission à un autre Participant (Sujet, Titulaire, Partie utilisatrice, etc.).		X		
101	28	L'Émetteur **DOIT** pouvoir démontrer qu'un Attribut provenait de lui et qu'il n'a pas été altéré pendant la transmission à un autre Participant (Sujet, Titulaire, Partie utilisatrice, etc.).			X	X
102	29	Un Attribut lié **DOIT** inclure des renseignements qui identifient l'Émetteur de cet attribut.		X	X	X
103	30	L'Émetteur **DOIT** inclure la date à laquelle l'Attribut a été émis et étiqueté comme tel d'une façon non ambiguë.		X	X	X
104	31	L'Émetteur **PEUT** fournir une date d'expiration pour tous les Attributs qu'il émet ou indiquer que l'Attribut n'a pas de date d'expiration.	X			
105	32	L'émetteur **DOIT** fournir une date d'expiration pour tous les attributs qu'il émet ou indiquer que l'attribut n'a pas de date d'expiration.		X	X	X
106	33	Lorsqu'il émet un Attribut, l'Émetteur **PEUT** indiquer que cet Attribut est contesté en tout ou en partie. En pareil cas, l'Émetteur **DEVRAIT** inclure une référence à d'autres Attributs qui contiennent des renseignements contestés et/ou en cours d'examen.	X	X	X	X
107	34	L'Émetteur **DEVRAIT** fournir aux Participants les conditions générales en vertu desquelles les Attributs seront rendus inutilisables ou non fiables.	X			
108	35	L'Émetteur **DOIT** fournir aux Participants les conditions générales en vertu desquelles les Attributs seront rendus inutilisables ou non fiables.		X	X	X

109	36	L'Émetteur **DOIT** s'assurer que le Référentiel auquel il envoie un attribut est adéquatement sécurisé, trouvé d'une manière légitime et situé dans une administration comme l'exige la loi, une politique et/ou un règlement.		X	X	X
110	**AMNT**	**Maintenir l'Attribut**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
111	1	L'Émetteur **DEVRAIT** établir, maintenir et faire connaître à d'autres participants un processus pour régler les différends à propos de l'exactitude des renseignements contenus dans les Attributs qu'il a émis.	X	X		
112	2	L'Émetteur **DOIT** établir, maintenir et faire connaître à d'autres Participants un processus pour régler les différends à propos de l'exactitude des renseignements contenus dans les Attributs qu'il a émis.			X	X
113	3	L'Émetteur **DOIT** fournir au Sujet la raison pour laquelle un Attribut est mis à jour.	X	X	X	X
114	4	L'Émetteur **DOIT** informer le ou les Sujets de tout changement apporté à un Attribut.	X	X	X	X
115	5	L'Émetteur **DOIT** révoquer, mettre à jour ou rendre autrement inutilisable ou non fiable un Attribut s'il décèle des indications comme quoi cet Attribut est compromis ou non valide.	X	X	X	X
116	6	L'Émetteur **DOIT** saisir les détails suivants concernant les Attributs qu'il a mis à jour : date de l'intervention, raison de l'intervention, indication générale de qui a initié l'intervention (p. ex., Sujet ou Émetteur).	X	X	X	X
117	7	Les Participants **DOIVENT** divulguer uniquement les détails relevés à propos des Attributs inutilisables ou non fiables d'après UNUS-3 à d'autres Participants connus ayant un besoin raisonnable d'avoir ces renseignements.	X	X	X	X
118	8	L'Émetteur **NE DOIT PAS** changer arbitrairement des Attributs. Les changements devraient être le résultat de politiques, procédures, lois ou règlements pertinents ou d'activités malveillantes confirmées ou suspectées, comme la fraude, qui indiqueraient un risque indu si l'Attribut était accepté.	X	X	X	X

119	9	L'Émetteur **DEVRAIT** fournir au Sujet la capacité d'amorcer un processus pour révoquer, mettre à jour ou autrement rendre inutilisable ou non fiable un Attribut qu'il a émis à ce Sujet lorsque ce dernier décèle des indications comme quoi l'Attribut est compromis ou non valide.	X	X	X	X
120	**AREV**	**Révoquer l'Attribut**	**CAL1**	**CAL2**	**CAL3**	**CAL4**
121	1	L'Autorité qui révoque **DOIT** initier un processus pour révoquer, mettre à jour ou autrement rendre inutilisable ou non fiable un Attribut si elle décèle des indications comme quoi l'Attribut est compromis ou non valide.	X	X	X	X
122	2	L'Autorité qui révoque **DOIT** fournir aux Participants le statut de tous les Attributs révoqués ou autrement inutilisables ou non fiables qu'il a émis (p. ex., si un Attribut est un « Attribut révoqué »).	X	X	X	X
123	3	L'autorité qui révoque **DOIT** saisir les détails suivants à propos des Attributs que l'Émetteur a rendus inutilisables ou non fiables : date de l'intervention, raison de l'intervention, indication générale de qui a amorcé l'intervention (p. ex., Sujet ou Émetteur).	X	X	X	X
124	4	L'Autorité qui révoque **DOIT** divulguer uniquement les détails saisis à propos des Attributs inutilisables ou non fiables selon UNUS-3 à des Participants connus ayant un besoin raisonnable d'avoir l'information.	X	X	X	X
125	5	L'Autorité qui révoque **DOIT** fournir au Sujet la raison de la révocation.	X	X	X	X
126	6	L'Autorité qui révoque **NE DOIT PAS** révoquer arbitrairement des Attributs. La révocation devrait être le résultat de politiques, procédures, lois ou règlements pertinents ou d'activités malveillantes confirmées ou suspectées, comme la fraude, qui indiqueraient un risque indu si l'Attribut était accepté.	X	X	X	X
127	7 8	L'Émetteur **DEVRAIT** fournir au Sujet la capacité d'initier un processus pour révoquer, mettre à jour ou autrement rendre inutilisable ou non fiable un Attribut qu'il a émis à ce Sujet quand le Sujet décèle des indications comme quoi l'Attribut est compromis ou non valide.	X	X	X	X

128	9	L’Autorité qui révoque **DEVRAIT** établir, maintenir et faire connaître aux autres Participants un processus pour résoudre les différends à propos de l’exactitude de l’information contenue dans les Attributs qu’elle a révoqués.	X	X		
129	10	L’Autorité qui révoque **DOIT** établir, maintenir et faire connaître aux autres Participants un processus pour résoudre les différends à propos de l’exactitude de l’information contenue dans les Attributs qu’elle a révoqués.			X	X

340 **Figure 8 : Critères de conformité des Justificatifs (Relations et Attributs)**