« Authentification » du CCP

Statut du document : Recommandation finale V1.2

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

Ce document a été élaboré par le comité d'experts du cadre de confiance du CCIAN avec les commentaires du public recueillis et traités dans le cadre d'un processus ouvert d'examen par les pairs. On s'attend à ce que le contenu de ce document soit examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois, règlements et politiques. Les avis concernant les changements apportés à ce document seront partagés sous la forme de communications électroniques, notamment le courriel et les réseaux sociaux. Les notifications seront également consignées dans le programme de travail du Cadre de confiance pancanadien (CCP).

Table of Contents

1. Introduction à la composante << Authentification >> du CCP

Le contenu ici présent concerne un sujet spécifique au domaine de ce composant du Cadre de confiance pancanadien (CPP). La section d'aperçu fournit des informations nécessaires pour une interprétation cohérente des critères de conformité inclus. Pour une introduction générale au CPP, veuillez consulter l'Aperçu du CPP, qui décrit le contexte, le but, la portée, les principes et les objectifs du cadre.

1.1 Portée

La composante « Authentification » du CCP définit :

1. Un ensemble de processus qui permettent d'accéder à des systèmes numériques.
2. Un ensemble de critères de conformité pour chaque processus qui, lorsqu'un processus s'avère conforme, permettent de lui faire confiance.

Remarque : Les processus de confiance de la composante « Authentification » du CCP définis pour cette composante sont agnostiques en ce qui concerne la façon dont les identités numériques sont attribuées et gérées au niveau technologique. Chaque participant devra déterminer quelles technologies et méthodes conviennent le mieux aux exigences de leurs constituants et de leurs propres résultats opérationnels ciblés.

1.2 Raison d'être et avantages anticipés

La composante « Authentification » du CCP vise à assurer l'intégrité constante des processus de connexion et d'authentification en certifiant, par le biais d'un processus d'évaluation, qu'ils se conforment à des critères de conformité uniformisés. Les critères de conformité pour cette composante peuvent servir à garantir :

- Que les processus de confiance donnent une représentation d'un sujet unique à un niveau d'assurance comme quoi il s'agit du même sujet à chaque connexion réussie auprès d'un fournisseur de services d'authentification.
- La prévisibilité et la continuité des processus de connexion qu'ils offrent ou dont ils dépendent.

Tous les participants bénéficieront :

- De processus de connexion et d'authentification qui sont répétitifs et uniformes (qu'ils offrent ces processus, dépendent d'eux ou les deux).

- De l'assurance que les utilisateurs identifiés peuvent s'engager dans des interactions autorisées avec des systèmes à distance.

Les parties dépendantes bénéficieront de :

- La capacité de tirer parti de l'assurance que les processus de confiance de l'authentification identifient d'une manière unique, à un niveau de risque acceptable, un sujet à l'intérieur de leurs applications ou programmes.

1.3 Biométrie et authentification

D'une façon générale, les normes de l'industrie pertinentes à cette composante du CCP ne recommandent pas d'utiliser la biométrie comme seul facteur d'authentification dans un système donné. Les consignes actuelles suggèrent plutôt qu'une utilisation appropriée de la biométrie est un moyen de débloquer un authentifiant local (qui existe peut-être sur un appareil local) pour faciliter l'authentification à un service à distance :

- La publication **800-63-3 (Digital Identity Guidelines) (révision 3)** du US National Institute of Standards and Technology (NIST) décrit l'utilisation de la biométrie de la façon suivante : « La biométrie n'est pas un secret. Par conséquent, ces consignes permettent uniquement d'utiliser la biométrie pour l'authentification lorsqu'elle est étroitement liée à un authentifiant physique ».
- La publication **Information Technology Security Guidance for the Practitioner 30.031 V3 (User Authentication Guidance for Information Technology Systems)** du Communications Security Establishment décrit l'utilisation de la biométrie de la façon suivante : « Quelque chose qu'un utilisateur est ou fait et qui peut être reproduit. Un auteur malveillant peut obtenir une copie de l'empreinte digitale du propriétaire d'un jeton et la reproduire – en supposant que le ou les systèmes biométriques utilisés ne bloquent pas de telles attaques en employant de robustes techniques de détection d'une vraie personne ». Et « Biométrie : reconnaissance automatisée des personnes basée sur leurs caractéristiques comportementales et biologiques. Dans ce document, la biométrie peut servir à débloquer des jetons d'authentification et à éviter la répudiation de l'inscription. »

Cette version de la composante « Authentification » du CCP s'aligne sur ces lignes directrices et considère l'authentification biométrique comme étant appropriée uniquement en combinaison avec un autre facteur d'authentification. Un exemple consisterait à employer une solution biométrique qui fonctionne sur tous les canaux au moyen de la reconnaissance du visage, des empreintes digitales ou de la voix (ce que vous êtes) en plus d'une autre méthode d'authentification comme le contrôle et la possession d'un appareil mobile (ce que vous avez).

1.4 Relation avec le Cadre de confiance pancanadien

Le Cadre de confiance pancanadien comprend un ensemble de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées indépendamment les unes des autres pour être considérées comme des composantes de confiance. Le CCP, qui se fonde sur une approche pancanadienne, permet aux secteurs public et privé de collaborer pour protéger les identités numériques en uniformisant les processus et pratiques dans tout l'écosystème numérique canadien.

La figure 1 est une illustration des composantes du modèle de Cadre de confiance pancanadien.

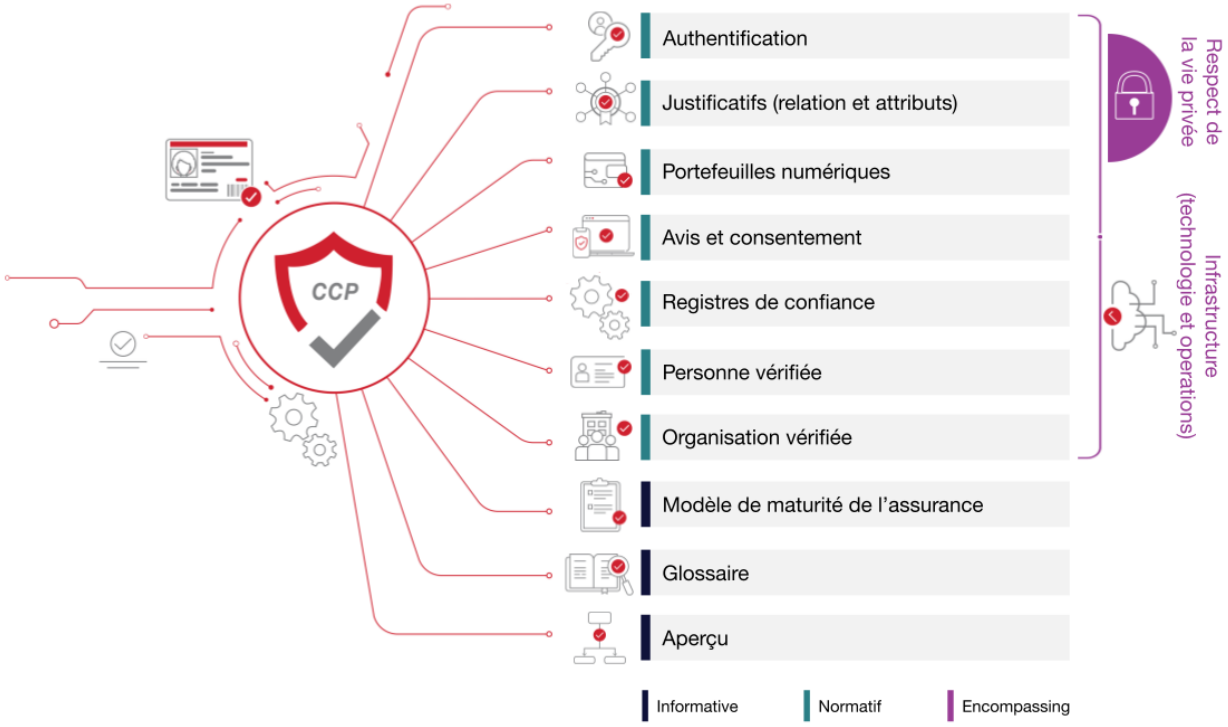

Figure 1. Composantes du Cadre de confiance pancanadien

Les avantages associés à la composante « Authentification » du CCP sont obtenus en partie en élargissant les processus définis dans la composante « Personne vérifiée » du CCP (et, dans une certaine mesure, la composante « Organisation vérifiée » du CCP). À cet égard, le CCP fait la distinction entre les processus de « vérification » et d'« authentification », et reconnaît que les sessions authentifiées restent nécessaires pour assurer la sécurité et la confidentialité en ligne.

2. Conventions d’authentification

Cette section décrit et définit les principaux termes et notions utilisés dans la composante « Authentification » du CCP. Ces renseignements sont fournis pour assurer une utilisation et une interprétation uniformes des termes employés dans cet aperçu et dans le profil de conformité de l’authentification du CCP.

Pour les besoins de la présente composante du CCP :

- Les termes « connexion » et « authentification »" ne supposent pas une méthode d’authentification privilégiée (p. ex., nom d’utilisateur/mot de passe) ou une technologie privilégiée (p. ex., clés cryptographiques plutôt que biométrie).
- Une connexion réussie à un système en particulier ne garantit pas l’intégrité des données détenues par ce système.
- Les processus de confiance définis pour les besoins de cette composante sont agnostiques en ce qui concerne la façon dont les identifiants numériques sont attribués et gérés. Par conséquent, cette composante fournit aussi une orientation pertinente pour les identités numériques attribuées et gérées à l’aide de processus d’attribution d’identité décentralisés ou centralisés.

Remarques :

- Les conventions peuvent varier entre les différentes composantes du CCP. Les lecteurs sont invités à examiner celles de chacune des composantes qu’ils lisent.
- Termes définis – Les principaux termes et concepts décrits et définis dans la présente section, la section sur les processus de confiance et le glossaire du CCP sont indiqués en majuscules dans tout le document.
- Liens hypertextes – Des liens hypertextes peuvent être intégrés dans les versions électroniques de ce document. Tous les liens étaient accessibles au moment de la rédaction.

2.1 Termes et définitions

Pour les besoins de la présente composante du CCP, les termes et les définitions contenus dans le glossaire du CCP et les termes et définitions figurant dans cette section s’appliquent.

Authentifiant

Renseignements ou caractéristiques biométriques qu’une personne contrôle et qui sont un cas spécifique d’un type d’authentifiant, lequel relève du contrôle de la personne.

Un authentifiant peut être fourni par le sujet ou par un fournisseur de services.

Authentification

L'authentification est le processus qui consiste à établir une confiance ou une authenticité pour donner l'assurance qu'un sujet contrôle un justificatif d'authentification délivré et que ce justificatif est actuellement valide.

Authentification du risque adaptatif

Ajustement dynamique des étapes d'authentification spécifiques accomplies en fonction du risque adaptatif.

Données de validation des authentifiants

Données relevant du contrôle d'un fournisseur de services qui servent à valider l'authentifiant (fourni par un sujet pendant une tentative d'authentification). Se reporter à l'annexe A pour voir des exemples.

Facteurs d'authentification

Il y a trois facteurs d'authentification :

1. Chose que le sujet a (p. ex., carte clé, porte-clés)
2. Chose que le sujet connaît (p. ex., mot de passe)
3. Chose que le sujet est ou fait (p. ex., biométrie)

Gestion des services de TI

Ensemble des activités – dirigées par des politiques, organisées et structurées dans des processus et procédures qui les soutiennent – qui sont menées par une organisation pour concevoir, planifier, fournir, exploiter et contrôler les services de technologie de l'information offerts aux clients.

Justificatif

Structure de données qui lie d'une manière unique au moins un authentifiant à au moins une revendication à propos d'au moins un sujet.

Pour les besoins de la présente composante du CCP, un justificatif fait référence à n'importe quelles données liées à un sujet qui sont utilisées dans n'importe lequel des processus de confiance décrits dans cette composante.

Justificatif inaccessible

Justificatif qui n'est pas accessible ou disponible ou qui existe dans un état incomplet. Cela peut arriver à la suite d'un processus incomplet ou le processus de suspension de justificatif.

Liaison d'authentifiants

Association d'une ou de plusieurs revendications à propos d'un sujet avec un ou plusieurs authentifiants dans le cadre du processus d'attribution de justificatifs.

Risque adaptatif

Mesure dynamique du risque associé à l'accès à une transaction ou un service compte tenu du contexte et du comportement.

Session et session authentifiée
Une session est une interaction persistante entre un agent logiciel du sujet (p. ex., navigateur Web, appli mobile) et un service logiciel utilisé par des fournisseurs de services ou parties dépendantes. Une session peut être exigée pour satisfaire les cas d'utilisation fédérée et à connexion unique.

Une session authentifiée est une session (interaction persistante entre un agent logiciel du sujet [p. ex., navigateur Web, appli mobile] et un service logiciel utilisé par des fournisseurs de services ou parties dépendantes) qui est relié d'une manière sûre à l'authentification réussie du sujet.

Sujet

Entité liée à un justificatif. Pour les besoins de cette composante du CCP, le terme « sujet » s'applique uniquement aux entités liées de la sorte. Un sujet peut être une personne naturelle, une organisation, une application ou un appareil.

Type d'authentifiant

Classe d'authentifiant à l'intérieur d'un facteur d'authentification spécifique.

Vérification indépendante

La vérification en question doit être effectuée par un groupe d'audit qui n'a aucun lien avec l'unité d'affaires responsable du processus ou de l'activité faisant l'objet de la vérification, qui en est distinct et qui n'en fait pas partie.

Remarque : On trouvera à l'annexe A un exemple de cas d'utilisation qui illustre la façon dont certains des termes ci-dessus sont utilisés dans la composante « Authentification » du CCP.

2.2 Abréviations

Les abréviations et acronymes suivants apparaissent tout au long de cet aperçu et dans le profil de conformité « Authentification » du CCP :

- DIDs – Identifiant(s) décentralisé(s)
- FIPS – Federal Information Processing Standards
- IETF – Groupe de travail sur l'ingénierie Internet
- IT – Technologie de l'information
- ITSG – Information Technology Security Guidance
- ITSP – IT Security Guidance for Practitioners
- LOA(s) – Niveau(x) d'assurance
- NIST – National Institute of Standards and Technology
- OTP – Niveau(x) d'assurance
- PCTF – Cadre de confiance pancanadien
- Q&A – Foire aux questions
- TLS – Transport Layer Security
- W3C – World Wide Web Consortium

2.3 Rôles

Les rôles aident à isoler les différentes fonctions et responsabilités que les participants peuvent remplir à l'intérieur des processus d'authentification de bout en bout. Les rôles n'impliquent ou ne nécessitent pas de solution, d'architecture, de mise en œuvre ou de modèle de gestion en particulier.

Remarques

- Selon le cas d'utilisation, différentes organisations peuvent assumer un ou plusieurs rôles. Par exemple, l'attribution des justificatifs d'authentification peut incomber à une organisation, tandis que l'authentification sera la responsabilité d'une organisation différente.
- Les définitions des rôles n'impliquent ou n'exigent pas une solution, architecture, mise en œuvre ou modèle de gestion en particulier.

Fournisseur de services d'authentification

Entité qui exploite un service mettant en œuvre les processus de confiance de l'authentification reliés à l'authentification :

1. Authentification
2. Début de la session d'authentification (facultatif)
3. Fin de la session d'authentification (facultatif)

Fournisseur de services de justificatifs

Entité qui exploite un service mettant en œuvre les processus de confiance de l'authentification reliés à la gestion des justificatifs d'authentification :

1. Attribution des justificatifs
2. Suspension des justificatifs (facultatif)
3. Récupération des justificatifs (facultatif)
4. Maintenance des justificatifs
5. Révocation des justificatifs

Partie dépendante

Organisation ou personne qui consomme des renseignements d'identité numérique créés et gérés par des participants pour effectuer des transactions électroniques avec des sujets. Il est à noter que dans le contexte de cette composante du CCP, la partie dépendante consomme des justificatifs ou une session authentifiée à partir des processus de confiance de l'authentification.

2.4 Niveaux d'assurance

Un niveau d'assurance est un indicateur qui doit être appliqué et maintenu pour décrire un niveau de confiance dans les processus de confiance de la composante « Authentification » du CCP. Dans le contexte de la présente composante du CCP, les fournisseurs de services de justificatifs, les parties dépendantes et les utilisateurs se servent de niveaux d'assurance pour déterminer quel niveau de confiance l'accès à un système numérique devrait avoir compte tenu du contexte de l'interaction numérique qui s'ensuit.

Pour les besoins de la présente composante du CCP, les critères de conformité sont profilés en termes de niveau d'assurance; les critères de conformité énumèrent explicitement les exigences pour chaque niveau d'assurance d'un processus. Ils spécifient les exigences et la rigueur relative de celles qui doivent être remplies pour atteindre un certain niveau d'assurance pour un processus.

Il est nécessaire de se conformer à tous les critères de conformité d'un niveau d'assurance donné pour tous les processus afin d'atteindre ce niveau d'assurance. Le niveau d'assurance qui résulte pour n'importe quel système d'authentification est le plus bas associé à n'importe lequel des processus de confiance de l'authentification.

Le tableau 1 énumère les quatre niveaux d'assurance définis pour la composante « Authentification » du CCP.

Niveau d'assurance	Description de la qualification
Niveau 1 (LOA1)	• Peu ou pas de niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 1
Niveau 2 (LOA2)	• Un certain niveau (raisonnable) d'assurance nécessaire • Répond aux critères de conformité du niveau 2
Niveau 3 (LOA3)	• Haut niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 3
Niveau 4 (LOA4)	• Très haut niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 4

Tableau 1. Niveaux d'assurance

Remarques :

- La présente version de la composante « Authentification » du CCP ne définit pas les critères de conformité pour le niveau d'assurance 4. Toutefois, le CCP reconnaît l'existence du niveau d'assurance 4 et l'a inclus en prévision de versions futures.
- Chaque niveau d'assurance peut être précisé davantage avec des exigences de contrôle supplémentaires spécifiques à leur type d'industrie ou de services. Par exemple, une partie dépendante dans le secteur des soins de santé peut spécifier dans un profil du CCP une exigence pour un justificatif ayant un niveau d'assurance 3 avec un critère stipulant que l'authentifiant doit être attribué par un fournisseur de soins de santé. Indépendamment des précisions supplémentaires, des critères supplémentaires ne peuvent jamais supprimer ou réduire l'obligation de remplir les critères spécifiés dans ce profil.
- Le niveau d'assurance qui en résulte est défini par les critères de conformité.

3. Processus de confiance

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

Un processus est une activité commerciale ou technique (ou un ensemble de ces activités) qui transforme une condition d'entrée en condition de sortie – un extrant dont dépendent souvent d'autres processus. Une condition est un état ou une circonstance

en particulier qui sont pertinents à un processus de confiance. Il peut s'agir d'un intrant, d'un extrant ou d'une dépendance en relation à un processus de confiance. Les critères de conformité spécifient ce qui est nécessaire pour transformer une condition d'entrée en condition de sortie. Les critères de conformité spécifient, par exemple, ce qui est nécessaire pour que le processus d'attribution de justificatifs transforme une condition d'entrée « Pas de justificatif » en condition de sortie « Justificatif attribué ».

Dans le contexte du CCP, un processus est qualifié de confiance quand il est vérifié et certifié conforme aux critères de conformité définis dans un profil de conformité du CCP. L'intégrité d'un processus de confiance est essentielle, car de nombreux participants—de divers territoires de compétence, organisations et secteurs, et à court et long terme—dépendent de l'extrant de ce processus.

La composante « Authentification » du CCP définit huit processus de confiance :

1. Attribution des justificatifs
2. Authentification
3. Début de la session authentifiée
4. Fin de la session authentifiée
5. Suspension des justificatifs
6. Récupération des justificatifs
7. Maintenance des justificatifs
8. Révocation des justificatifs

Un processus d'authentification est qualifié de processus de confiance quand il est évalué et certifié selon les critères de conformité stipulés par le profil de conformité de l'authentification du CCP. Les critères de conformité spécifiés dans d'autres composantes du CCP peuvent aussi s'appliquer dans certaines circonstances.

3.1 Aperçu conceptuel

La figure 2 donne un aperçu conceptuel et montre l'organisation logique des processus de confiance de la composante « Authentification » du CCP.

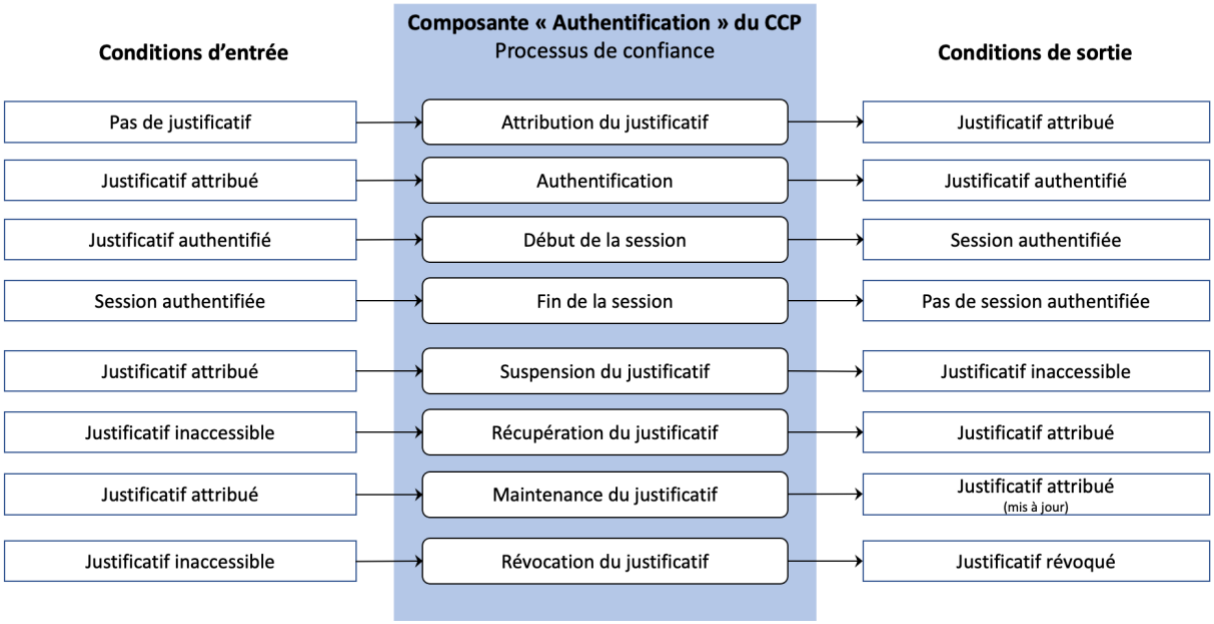

Figure 2. Aperçu de la composante « Authentification »

3.2 Description des processus

Les sections qui suivent définissent les processus de confiance de la composante « Authentification » du CCP. Le profil de conformité de l'authentification du CCP spécifie les critères de conformité permettant d'évaluer la fiabilité de ces processus.

Les processus de confiance de l'authentification sont définis à l'aide des renseignements suivants :

1. Description – Aperçu descriptif du processus (paragraphes d'ouverture)
2. Intrants – Ce qui est entré, ajouté ou utilisé par le processus
3. Extrants – Ce qui est produit par le processus ou en résulte
4. Dépendances – Processus de confiance connexes, principalement ceux qui produisent des extrants dont le processus dépend

Remarques :

- Les intrants et les extrants sont deux types de conditions (les conditions étant des états ou circonstances particuliers qui sont pertinents à un processus de confiance). Dans cette section, les conditions d'entrée et de sortie sont pertinentes à la composante « Authentification » du CCP.
- L'annexe B donne un résumé des conditions d'entrée et de sortie de la composante « Authentification » du CCP.

3.2.1 Attribution des justificatifs

L'attribution des justificatifs est un processus pendant lequel un justificatif décrivant un ou plusieurs sujets est attribué et lié à un ou plusieurs authentifiants appropriés contrôlés par le titulaire. Un justificatif inclut un ou plusieurs identifiants qui peuvent être des pseudonymes et contenir des attributs vérifiés par l'émetteur de justificatifs. Les authentifiants peuvent être attribués pendant ce processus, par le sujet ou par une tierce partie. Les authentifiants liés servent ensuite à prouver, avec le niveau d'assurance spécifié, qu'un justificatif d'authentification se réfère au même sujet initialement lié à ce justificatif.

Remarque : La validation et la vérification de l'identité du sujet peuvent être nécessaires pour s'assurer qu'un justificatif d'authentification est attribué au bon sujet ou à un sujet connu. C'est particulièrement vrai pour des entités qui attribuent et gèrent des justificatifs d'authentification ayant un niveau d'assurance 3 ou supérieur. Se référer à la composante « Personne vérifiée » du CCP pour avoir une description des processus de validation et de vérification de l'identité et des critères de conformité associés.

Intrants	Pas de justificatif – Aucun justificatif n'est attribué au sujet.
Extrants	Justificatif attribué – Un justificatif a été attribué, et lié à un seul sujet et à un ou plusieurs authentifiants appropriés qui sont contrôlés par le sujet.
Dépendances	

3.2.2 Authentification

L'authentification est le processus d'établissement de la vérité ou de l'authenticité en vue de fournir une assurance. En ce qui concerne la présente composante, l'authentification établit, à un niveau d'assurance, qu'un sujet contrôle un justificatif d'authentification attribué et que ce dernier est actuellement valide (c.-à-d. qu'il n'est pas suspendu ou révoqué). Dans l'éventualité où un justificatif d'authentification serait révoqué ou suspendu, l'extrant serait un justificatif d'authentification révoqué ou inaccessible, respectivement, car les processus de révocation ou de suspension des justificatifs d'authentification auraient été appliqués.

Remarque : Dans certains cas, l'authentification peut être bidirectionnelle, chaque partie cherchant aussi à authentifier l'authenticité de l'autre (p. ex., le fait d'ouvrir un compte bancaire en ligne et de fournir des renseignements personnels). Si approprié, les évaluateurs devraient évaluer chaque instruction d'après tous les critères applicables.

Intrants	Justificatif attribué – Un justificatif a été attribué, et lié à un seul sujet et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
Extrants	Justificatif – Le sujet a authentifié avec succès et prouvé qu'il contrôle le justificatif au niveau d'assurance spécifié.
Dépendances	Attribution du justificatif

3.2.3 Début de la session authentifiée

Le début d'une session d'authentification est un processus qui, avec un justificatif authentifié, crée une session sécurisée pour une interaction persistante.

Si le processus d'authentification est conforme au niveau d'assurance 2, la session authentifiée doit alors être considérée comme ayant un niveau d'assurance 2. Si le processus d'authentification est conforme au niveau d'assurance 3, la session authentifiée doit alors être considérée comme ayant un niveau d'assurance 3.

Ce processus est facultatif et peut ne pas être soutenu par tous les fournisseurs de services.

Intrants	Justificatif authentifié – Le sujet a authentifié avec succès et prouvé qu'il contrôle le justificatif au niveau d'assurance spécifié.
Extrants	Session authentifiée – Il y a une interaction continue entre l'agent logiciel d'un sujet (p. ex., navigateur Web, appli mobile) et un service logiciel utilisé par des fournisseurs de services ou des parties dépendantes, qui est relié d'une manière sécuritaire à l'authentification réussie du sujet.
Dépendances	Authentification

3.2.4 Fin de la session authentifiée

La fin de session authentifiée est un processus qui annule une session authentifiée (c.-à-d., rend la session authentifiée inutilisable pour d'autres communications). Les fins de session peuvent être déclenchées au moyen d'événements comme une déconnexion explicite, l'expiration de la session en raison d'une inactivité ou d'une durée maximale ou d'autres moyens.

Ce processus est facultatif et peut ne pas être soutenu par tous les fournisseurs de services.

Intrants	Session authentifiée – Il y a une interaction continue entre l'agent logiciel d'un sujet (p. ex., navigateur Web, appli mobile) et un service logiciel utilisé par des fournisseurs de services ou des parties dépendantes, qui est relié d'une manière sécuritaire à l'authentification réussie du sujet.
Extrants	Pas de session authentifiée
Dépendances	Début de la session authentifiée

3.2.5 Suspension des justificatifs

La suspension des justificatifs est un processus qui transforme un justificatif attribué en justificatif inaccessible, et qui peut être amorcé par l'intervention d'un utilisateur, un administrateur de système ou automatiquement par le système. Un justificatif inaccessible ne devrait pas être utilisé dans le processus d'authentification.

Ce processus est facultatif et peut ne pas être soutenu par tous les fournisseurs de services.

Intrants	Justificatif attribué – Un justificatif a été attribué, et lié à un seul sujet et à un ou plusieurs authentifiants appropriés qui sont contrôlés par le sujet.
Extrants	Justificatif inaccessible – Le sujet est actuellement incapable d'utiliser le justificatif. Cela peut être déclenché par le sujet (p. ex., signalement d'une combinaison nom d'utilisateur – mot de passe compromise) ou le système (p. ex., accès bloqué à la suite de plusieurs tentatives successives d'authentification ratées, d'une inactivité, d'une activité suspecte). Il s'agit d'une condition temporaire qui aboutira à un justificatif attribué ou révoqué.
Dépendances	Attribution du justificatif

3.2.6 Récupération des justificatifs

Le processus de récupération des justificatifs permet de transformer un justificatif inaccessible en justificatif attribué. Il peut être déclenché par un utilisateur, un administrateur de système ou automatiquement par le système.

Ce processus est facultatif et peut ne pas être soutenu par tous les fournisseurs de services.

Intrants	Justificatif inaccessible – Le sujet est actuellement incapable d'utiliser le justificatif. Cela peut être déclenché par le sujet (p. ex., signalement d'une combinaison nom d'utilisateur – mot de passe compromise) ou le système (p. ex., accès bloqué à la suite de plusieurs tentatives successives d'authentification ratées, inactivité, activité suspecte). Il s'agit d'une condition temporaire qui aboutira à un justificatif attribué ou révoqué.
Extrants	Justificatif attribué – Un justificatif a été attribué, et lié à un seul sujet et à un ou plusieurs authentifiants appropriés qui sont contrôlés par le sujet.
Dépendances	Suspension du justificatif

3.2.7 Maintenance des justificatifs

Le processus de maintenance des justificatifs inclut des activités de cycle de vie comme l'association de nouveaux authentifiants, la suppression d'authentifiants et la mise à jour des authentifiants (p. ex., changement de mot de passe, mise à jour des questions et réponses de sécurité) ou encore la mise à jour des attributs des justificatifs. Ce processus est généralement lancé par un utilisateur, mais il peut l'être aussi par un administrateur de système ou automatiquement par le système.

Intrants	Justificatif attribué – Un justificatif a été attribué, et lié à un seul sujet et à un ou plusieurs authentifiants appropriés qui sont contrôlés par le sujet.
Extrants	Justificatif attribué (mis à jour) – Un justificatif a été attribué, et lié à un seul sujet et à un ou plusieurs authentifiants appropriés qui sont contrôlés par le sujet.
Dépendances	Attribution du justificatif, authentification

3.2.8 Révocation des justificatifs

Le processus de révocation des justificatifs assure qu'un justificatif est désactivé ou supprimé d'une façon permanente. Une fois qu'un justificatif est révoqué, il ne peut plus être utilisé. Le système empêchera activement que d'autres processus de confiance soient exécutés relativement à ce justificatif. Le processus peut être lancé par un utilisateur, un administrateur de système ou automatiquement par le système. Précisons qu'un nouveau justificatif peut être attribué pour le même sujet. La réattribution équivaut à révoquer un justificatif et à en attribuer un nouveau pour le même sujet.

Intrants	Justificatif attribué – Le justificatif peut être dans un état autre que révoqué (c.-à-d., inaccessible ou valide).
Extrants	Justificatif révoqué – Le justificatif est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.
Dépendances	Attribution du justificatif, authentification

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

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

4.1 À propos des critères de conformité du CCP

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

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

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

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

5. Conventions d'authentification

Chaque composante du CCP comporte des conventions qui assurent une utilisation et une interprétation uniformes des termes et notions apparaissant dans la composante. Ces conventions incluent des définitions et descriptions des éléments suivants auxquels il est fait référence dans ce profil de conformité :

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

Remarques :

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

5.1 Mots-clés des critères de conformité

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

- **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 bien qu'il existe des raisons valables dans des circonstances particulières pour ignorer l'exigence, toutes les implications doivent être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité ou de choisir une option différente spécifiée 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 en **caractères gras** et en MAJUSCULES tout au long de ce profil de conformit.

5.2 Risques de l'authentification

Type de risque	Catégorie de menace	Scénario de menace / vulnérabilité à la menace	Renseignements supplémentaires	Agent de menace	Impact	Protections proposées (p. ex., commentaires relatifs aux exigences de conformité)
Sécurité de l'information → préjudices pour le titulaire/les parties dépendantes	Risque pour la qualité du produit ou du service	Le produit ou service contient des vulnérabilités logicielles	Intention accidentelle ou malveillante	• Pirate/ agresseur • Conséquences non intentionnelles des failles logicielles	Préjudices pour les participants à l'écosystème : • Confiance dans l'écosystème • Risque pour la réputation de tout l'écosystème Préjudices pour le titulaire : • Vol d'identité • Préjudice financier • Perte de privilèges/d'accès/d'usage • Atteinte à la réputation Préjudices pour les parties dépendantes : • Préjudices financiers • Perte de privilèges/d'accès/d'usage • Atteinte à la réputation • Atteinte à la vie privée	• Le produit est soumis à un processus de certification et, le cas échéant, à un processus de recertification, et il a une marque de confiance prouvant que la personne effectuant la mise en application suit les processus de développement des produits qui sont une pratique courante de l'industrie pendant tout le cycle de vie. • Considérations pour la validation de l'intégrité de la chaîne d'approvisionnement, la sécurité du protocole SDLC, les évaluations de la sécurité des tierces parties, le processus de gestion de la vulnérabilité
Gestion du cycle de vie de la sécurité de l'information → désagréments pour l'utilisateur	Risque pour la qualité du produit ou du service	Le produit ou le service n'est plus soutenu et est désuet	• Failles non corrigées • Manque d'interopérabilité/ d'utilité	• Acteurs malveillants ciblant des logiciels non corrigés	• Le titulaire est incapable d'exécuter les transactions voulues • Justificatifs ou accès compromis	• Le produit et/ou service devrait être mis à jour ou remplacé par un autre plus sécuritaire et un régime de gestion des correctifs devrait être maintenu

				• Logiciels inutilisables (incompatibles)		
Sécurité de l'information → préjudices pour le titulaire	Risque pour l'intégrité du fournisseur de produits ou de service s/la chaîne d'approvisionnement	Des acteurs malicieux fournissent un produit ou service dans l'intention de nuire aux clients	Des acteurs malicieux fournissent un produit ou service qui peut sembler bien connu.	Fournisseur de produits ou services malveillant	• Personnification du titulaire • Atteinte à la vie privée du titulaire • Atteinte à la réputation du titulaire	Le client évalue convenablement les fournisseurs de produits ou services; les clients peuvent se fier aux certifications et/ou marques de confiance
Gestion du cycle de vie de la sécurité de l'information → désagréments pour l'utilisateur	Risque pour la qualité du produit ou du service	Le produit ou le service n'applique pas les normes de l'industrie ou ne s'y conforme pas	Le produit ou service est incapable d'interopérer avec des applications ou d'autres systèmes	Fournisseur de produits ou services	• Déni de service au client • Le titulaire est incapable d'effectuer les transactions requises • L'émetteur est incapable d'attribuer • Le vérificateur est incapable de vérifier	• Le produit ou service applique les normes de l'industrie comme le prouve une marque de confiance ou un programme de certification appropriés • Vérifier l'interopérabilité avec des normes de l'industrie reconnues comme X.509, TOTP, SAML, la famille OIDC, des justificatifs vérifiables du W3C, etc.
Sécurité de l'information → préjudices pour le titulaire	Risque pour la qualité du produit ou du service	Le produit ou le service a des pratiques de gestion ou des contrôles de sécurité techniques inadéquats	La mise en œuvre du produit ou service n'a pas été surveillée d'une manière appropriée	Pirate	Le système est facilement compromis, ce qui pourrait exposer des données ou permettre à un agresseur sophistiqué d'attribuer des justificatifs non autorisés ou de contourner les contrôles d'accs	• Le fournisseur de produits ou services passe par un processus de certification et à une marque de confiance qui prouve sa conformité aux pratiques standards de l'industrie. • Considérations pour la validation de l'intégrité de la chaîne d'approvisionnement, sécurité du SDLC, évaluations de la sécurité des tierces parties, processus de gestion de la vulnérabilité

Sécurité de l'information : gestion des clés → préjudices pour les sujets	Risque d'un accès non autorisé aux données	L'environnement opérationnel ne soutient pas les fonctions de sécurité voulues pour les niveaux d'assurance spécifiques ou ciblés	Les outils et processus de gestion standards des clés de l'industrie ne sont pas utilisés ou pas utilisés efficacement	Acteur malveillant (local ou à distance)	Clés compromises/non-respect de la vie privée/vol d'identité/accès non autorisé aux données	• Le fournisseur de produits ou services soutient explicitement une capacité de gestion des clés adéquate/évaluée **Remarques :** • Cela inclut les fonctions de gestion des clés et les fonctions de sécurité à fort impact gérées sur l'infrastructure du produit ou service et/ou l'équipement de l'utilisateur final • Le protocole « adéquat » (FIPS pour le matériel, NIST pour le logiciel) dépendra du niveau d'assurance
Sécurité de l'information : gestion des clés → préjudices pour les sujets	Risques pour la sauvegarde et la récupération/risques pour la gestion des clés	Le produit ou service a des contrôles de sauvegarde et de récupération inadéquats	Un acteur malveillant vole des clés secrètes en utilisant des mécanismes de sauvegarde/récupération	Acteur malveillant (local ou à distance)	Clés compromises/accès non autorisé aux données/non-respect de la vie privée/vol d'identité	• Les processus de sauvegarde et de récupération seront définis pour le niveau d'assurance correspondant et évalués dans le cadre du processus de certification • Les sauvegardes doivent avoir les mêmes protections du niveau d'assurance que les protections d'origine ou de « service en temps réel »
Sécurité de l'information : gestion des clés → préjudices pour les sujets	Risques de sécurité liés à l'infrastructure, aux logiciels ou aux appareils/risques pour la gestion des clés	Le produit ou service ne soutient pas les fonctions de sécurité requises pour le ou les niveaux d'assurance spécifiques ou ciblés.	• Le logiciel du produit ou service n'a pas de protections adéquates pour la gestion des clés. • Un acteur malveillant vole les clés secrètes (p. ex., il vole la clé de la mémoire, perce le cryptage de la boîte blanche,	Acteur malveillant (local ou à distance)	Clés compromises/accès non autorisé aux données/non-respect de la vie privée/vol d'identité	• Le produit ou service utilise un logiciel et/ou du matériel de gestion des clés qui est adéquat/évalué avec des clés non exportables • **Remarque :** Le protocole « adéquat » (NIST pour le logiciel) dépendra du niveau d'assurance

			l'analyse de la puissance)			
Sécurité de l'information : analyse des données → préjudices pour les sujets	Analyse des données dans le produit ou service	Le produit ou service permet (ou n'interdit pas adéquatement) de partager des renseignements sensibles (p. ex., renseignements sensibles transmis lors de la collecte d'analyse de données)	Non intentionnel ou intentionnel	Acteur malveillant ou effectif insuffisamment formé	• Fuite de données sensibles dans les données d'analyse • Non-respect de la vie privée/vol d'identité	• Si des données sensibles sont nécessaires dans l'analyse, il faut s'assurer qu'elles sont anonymisées ou segmentées en unités et chiffrées avant d'être envoyées, y compris avant d'être enregistrées pour être entreposées localement dans des modes et des sauvegardes hors réseau • La marque de confiance pour assurer l'évaluation des risques pour la vie privée est terminée en ajoutant/modifiant l'analyse des données lorsque l'évaluation inclut le risque d'une utilisation non intentionnelle des données d'analyse • Marque de confiance pour assurer les exigences relatives au contrôle de l'accès aux données d'analyse • Formation de la main-d'œuvre sur les pratiques standard de confidentialité des données
Sécurité de l'information : sécurité de l'environnement → préjudices pour les sujets	Risques pour la sécurité des initiés	Le personnel du fournisseur de produits ou services est compromis	Ingénierie sociale	Accès non autorisé aux données/accès hors sujet	Non-respect de la vie privée/vol d'identité	• Le fournisseur de produits ou services vérifie s'il y a des vulnérabilités connues au lancement, et avise les sujets/clients des vulnérabilités spécifiques et des mesures correctives nécessaires avant l'utilisation du produit ou service • Exigences dictées par le niveau d'assurance
Sécurité de l'information : sécurité de l'environnemen	Risques pour la sécurité des initiés	Le titulaire du justificatif est compromis	Ingénierie sociale	Accès non autorisé aux données/accès hors sujet	Non-respect de la vie privée/vol d'identité	• Le fournisseur de produits ou services vérifie s'il y a des vulnérabilités connues au moment du lancement, avise les sujets/clients

t → préjudices pour le sujet						des vulnérabilités spécifiques et des mesures correctives nécessaires avant d'utiliser le produit ou service • Exigences dictées par le niveau d'assurance
Sécurité de l'information : obligation et authentification → préjudices pour le sujet	Utilisation non autorisée du produit ou service	Authentifiant compromis	Quand les utilisateurs partagent des services, des authentifiants sans contrôles appropriés de l'accès pourraient permettre à d'autres de partager des renseignements du titulaire autorisé sans son consentement	• Pirates • Connaissances • Membres de la famille	Des assertions sont faites de la part de l'utilisateur sans son consentement	• Inclut un langage spécifique dans les conditions générales d'utilisation pour s'assurer que les utilisateurs autorisés comprennent leur responsabilité. • Fournit des expériences en matière d'autorisation qui ne dépendent pas exclusivement de la possession et du contrôle d'un seul appareil. • Applique des techniques supplémentaires d'anti-intrusion et de détection de spontanéité (ISO-30107)
Respect de la vie privée → suivi des utilisateurs	Suivi des utilisateurs	Identification de la corrélation des renseignements sans avis ou consentement	Le produit ou service utilise des identifiants communs à de multiples vérificateurs	Invasion de la vie privée	• Liaison des identifiants de multiples vérificateurs • Suivi des utilisateurs • Agrégation des données	• Le produit ou service utilise des technologies d'identifiants uniques telles que : ○ URI (p. ex., diverses méthodes DID) ○ UUID ○ GUID
Vie privée → partage excessif	Partage excessif	Le produit ou service ne soutient pas la minimisation des données	Le sujet fournit plus de renseignements au vérificateur que c'est approprié	• Vérificateur indésirable ciblant l'utilisateur d'un produit ou service spécifique qui n'offre pas de capacité de minimiser les données	• Le titulaire fournit au vérificateur plus de renseignements que ce qui est approprié • Non-respect de la vie privée/vol d'identité • Non-conformité du vérificateur aux règlements qui régissent la vie privée pour la réception de	Produit ou service pour soutenir les capacités de minimisation des données (p. ex., divulgation sélective, preuve à divulgation nulle de connaissance)

				• Vérificateur non intentionnel qui reçoit plus de renseignements qu'il n'en demande ou en a nécessaire	données dont il n'avait pas besoin pour ses affaires • Incapacité pour un vérificateur gouvernemental de les utiliser car le gouvernement n'a peut-être pas l'autorisation de recevoir des renseignements supplémentaires qu'il n'a pas demandés	
Vie privée → partage excessif	Partage excessif	Le choix du justificatif et/ou des revendications par l'utilisateur final peut entraîner la divulgation de renseignements qui ne sont pas strictement exigés	Avis incomplet, pas clair ou ambigu	• Fournisseur de produit ou service (introduit une menace) – problème de qualité • Vérificateur escroc ciblant l'utilisateur de produits ou services spécifiques qui n'offrent pas de mise en garde appropriée	• Le titulaire fournit au vérificateur plus de renseignements ce qu'il aurait autrement accepté de faire; les décisions prises par le vérificateur concernant ces renseignements pourraient avoir des répercussions négatives pour cet utilisateur • Le titulaire est incapable d'évaluer avec exactitude le risque que pose la divulgation de l'information	• Le produit ou service divulgue efficacement les renseignements à partager avec le titulaire et permet à celui -ci d'exercer un contrôle • Les données qui peuvent ne pas être « compréhensibles » (c.-à-d., données codées) devraient être décrites dans un langage clair
Vie privée → partage excessif	Partage excessif	Le produit ou service recueille plus de revendications que ce qui est strictement nécessaire	Le sujet fournit au vérificateur plus de renseignements que ce qui est approprié. Avis incomplet, pas clair ou ambigu	Le fournisseur de produits ou services fait courir des risques à des renseignements supplémentaires	Le titulaire n'est pas capable d'évaluer avec exactitude le risque de divulgation de l'information	• Le produit ou service limite efficacement les renseignements qu'il recueille • Le produit ou service fournit un avis complet et exhaustif au titulaire.
Conformité → vie privée	Vie privée	Le produit ou service ne se conforme pas à	S.O.	S.O.	Non-respect de la vie privée	Marque de confiance pour assurer la conformité à la composante « Respect de la vie privée » du CCP

		la composante « Respect de la vie privée » du CCP				dans le cadre de la certification du produit ou service
Accessibilité	Expérience utilisateur	Le produit ou service ne se conforme pas aux normes d'accessibilité de l'industrie	S.O.	S.O.	• Le titulaire est incapable d'utiliser le produit ou service en raison de sa situation de handicap; il faut soumettre la population vulnérable à des processus ou outils de rechange qui peuvent comporter des risques différents pour la vie privée • Abandon; risque pour la réputation • Manque de service; partage excessif de données	Le produit ou service instaure des capacités d'accessibilité standards de l'industrie
Utilisabilité	Expérience utilisateur	Les instructions du produit ou service ne sont pas claires	• Les instructions du produit ou service ne sont pas claires pour le titulaire • L'avis est vague ou ambigu • Expérience utilisateur médiocre	S.O.	• Le titulaire utilise le produit ou service d'une manière non prévue qui lui porte préjudice • Divulgation de renseignements personnels à un destinataire non prévu (atteinte accidentelle à la vie privée; hameçonnage)	• Le produit ou service utilise un langage clair, et a un aspect et une convivialité uniformes • Conception robuste du produit ou service : empêche l'accès ou le partage sans valider les entités avec qui les renseignements sont échangés
Sécurité de l'information : sécurité du registre de données → préjudice pour le sujet	Gouvernance	Le produit ou service dépend (fait confiance) d'une autorité en matière de justificatifs qui n'est pas (ou n'est plus) appropriée	Le produit ou service fait confiance à la clé publique de l'acteur malveillant	Acteur malveillant qui établit un registre de données ou une rubrique de registre indésirable	• Les utilisateurs prennent des décisions non intentionnelles ou mal informées sur le partage. • Atteinte à la vie privée/vol d'identité	Le produit ou service authentifie le registre de données comme étant de confiance; l'authentification implique une capacité à assurer qu'elle « est légitime » ou « convient pour les fins définies »

Sécurité de l'information : compromission des canaux → risques pour le sujet	Authentification manquante	• Le canal d'authentification n'est pas sûr ou est compromis (c.-à-d., agresseur au milieu) • Gestion de session non sécuritaire ou piratage de session	S.O.	Tierce partie malveillante	• Accès aux données non autorisé, vie privée • Vol d'identité • Interventions non autorisées	• Le produit ou service met en place des contrôles appropriés pour offrir le niveau d'assurance sélectionné • Le produit ou service a les contrôles qu'il a mis en place, vérifiés et/ou testés activement pour en assurer l'efficacité
Sécurité de l'information : information stockée compromise	Clés compromises	Stockage de justificatifs : le stockage non sécuritaire de justificatifs peut mener à un accès non autorisé si les données stockées sont compromises	• Sauvegarde sécuritaire • Stockage de clés sécuritaire	Tierce partie malveillante	• Atteinte à la vie privée • Vol d'identité • Accès autorisé aux données et/ou à une activité	• Le produit ou service met en place des contrôles appropriés pour offrir le niveau d'assurance sélectionné • Le produit ou service a les contrôles qu'il a mis en place, vérifiés et/ou testés activement pour en assurer l'efficacité

6. Critères de conformité de la composante « Authentification »

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

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

Les critères de conformité sont catégorisés par processus de confiance et profilés selon les niveaux d'assurance. Ils sont groupés par sujet à l'intérieur de chaque catégorie. Pour faciliter la référence, un critère de conformité spécifique peut être mentionné d'après sa catégorie et son numéro de référence. Exemple : « **BASE-1** » fait référence au « critère de conformité de base nº 1 ».

Remarques :

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

Référence	Critères de conformité	Niveau d'assurance			
BASE	**Critères de base**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
CONSIGNATION DES ÉVÉNEMENTS					
1	L'utilisation des justificatifs **PEUT** être consignée et conservée pendant une période prédéfinie en guise de preuve.	X			
2	L'utilisation des justificatifs **DEVRAIT** être consignée et conservée pendant une période prédéfinie en guise de preuve.		X		
3	L'utilisation des justificatifs **DOIT** être consignée et conservée pendant une période prédéfinie en guise de preuve.			X	
4	La gestion et l'utilisation des justificatifs **DOIVENT** être : • Retraçables jusqu'à un justificatif spécifique, et inclure le résultat, la date et l'heure de l'événement consigné; • Protégées par des contrôles pour limiter l'accès uniquement à ceux qui en ont besoin (voir NIST Special Publication 800-92 pour des recommandations concernant la gestion des registres de sécurité).		X	X	
5	Les registres de gestion et d'utilisation des justificatifs **DOIVENT** avoir un mécanisme de détection des tentatives frauduleuses pour déceler les modifications non autorisées.		X	X	
6	Les renseignements personnels et les secrets	X	X	X	

	d'authentification (p. ex., mots de passe, valeurs des mots de passe à usage unique, questions et réponses de sécurité) **NE DOIVENT PAS** être consignés dans le service.				
SÉCURITÉ DE L'INFORMATION					
7	Le fournisseur de services de justificatifs ou d'authentification **PEUT** assurer i) l'intégrité, ii) la confidentialité et iii) la disponibilité des services en suivant une série de consignes et de contrôles de sécurité de l'information (p. ex., CSEC ITSG-33) qui soutiennent ces efforts.	X			
8	Le fournisseur de services de justificatifs ou d'authentification **DOIT** assurer i) l'intégrité, ii) la confidentialité et iii) la disponibilité des services en suivant une série de consignes et de contrôles de sécurité de l'information (p. ex., CSEC ITSG-33) qui soutiennent ces efforts.		X	X	
9	Le fournisseur de services de justificatifs ou d'authentification **DOIT** avoir un rapport de contrôle vérifié d'une manière indépendante pour démontrer la conformité à une série de lignes directrices et de contrôles de sécurité de l'information.			X	
GESTION DES SERVICES TI					
10	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** avoir une pratique de	X			

	gestion des services documentée pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP.				
11	Le fournisseur de services de justificatifs ou d'authentification **DOIT** établir et maintenir une pratique de gestion des services documentée pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP.		X		
12	Le fournisseur de services de justificatifs ou d'authentification **DOIT** : • établir et maintenir une pratique de gestion des services documentée pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP. • avoir une pratique de gestion des services documentée et vérifiée de façon indépendante pour tous les aspects des services qu'il fournit en lien avec les processus de confiance de la composante « Authentification » du CCP.			X	
13	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** se conformer à un cadre de gestion des services	X	X		

	standard de l'industrie (p. ex., ITIL).				
14	Le fournisseur de services de justificatifs ou d'authentification **DOIT** se conformer à un cadre de gestion des services standard de l'industrie (p. ex., ITIL).			X	
SURVEILLANCE					
15	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** avoir des contrôles pour déceler l'utilisation malveillante ou la compromission des justificatifs.	X			
16	Le fournisseur de services de justificatifs ou d'authentification **DOIT** avoir des contrôles pour déceler l'utilisation malveillante ou la compromission des justificatifs.		X	X	
17	Le fournisseur de services de justificatifs **DEVRAIT** amorcer le processus de suspension, de maintenance ou de révocation des justificatifs quand il découvre des indications d'utilisation malveillante ou de compromission des justificatifs donnant lieu à des poursuites.	X			
18	Le fournisseur de services de justificatifs **DOIT** amorcer le processus de suspension, de maintenance ou de révocation des justificatifs quand il découvre des indications d'utilisation malveillante ou de		X	X	

	compromission des justificatifs donnant lieu à des poursuites.				
RESPECT DE LA VIE PRIVÉE					
19	Le fournisseur de services de justificatifs ou d'authentification **DEVRAIT** se conformer aux pratiques de gestion des risques pour la confidentialité de la composante « Respect de la vie privée » du CCP et de tous les profils pertinents du CCP applicables aux services d'identité numérique.	X			
20	Le fournisseur de services de justificatifs ou d'authentification **DOIT** se conformer aux pratiques de gestion des risques pour la confidentialité de la composante « Respect de la vie privée » du CCP et de tous les profils pertinents du CCP applicables aux services d'identité numérique.		X	X	
21	Le fournisseur de services de justificatifs ou d'authentification **DOIT** se conformer aux pratiques de gestion des risques pour le respect de la vie privée qui sont acceptées par et applicables à toutes les parties participant au service d'identité numérique.		X	X	
NOTIFICATIONS					
22	Le fournisseur de services de justificatifs **PEUT** aviser sans délai le sujet (p. ex., notification immédiate par courriel, messagerie texte	X			

	ou comme prescrit par une politique de ce fournisseur) de tout changement aux renseignements sur des justificatifs individuels (p. ex., mise à jour de mot de passe, ajout ou suppression d'authentifiants).				
23	Le fournisseur de services de justificatifs **DOIT** aviser sans délai le sujet (p. ex., notification immédiate par courriel, messagerie texte ou comme prescrit par une politique de ce fournisseur) de tout changement aux renseignements sur des justificatifs individuels (p. ex., mise à jour de mot de passe, ajout ou suppression d'authentifiants).		X	X	
CDIS	**Attribution de justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
LIER UN SUJET					
1	Le fournisseur de services de justificatifs **DEVRAIT** imposer que le justificatif soit uniquement lié à un sujet.	X			
2	Le fournisseur de services de justificatifs **DOIT** imposer que le justificatif soit uniquement lié à un sujet.		X	X	
3	Le fournisseur de services de justificatifs **PEUT** documenter ou avoir un processus documenté pour démontrer le niveau d'assurance de l'identité du sujet quand le justificatif a été attribué.	X			
4	Le fournisseur de services de justificatifs **DOIT** documenter ou avoir un processus documenté pour		X	X	

	démontrer le niveau d'assurance de l'identité du sujet quand le justificatif a été attribué.				
5	Le fournisseur de services de justificatifs **DOIT** mettre à la disposition des fournisseurs de services d'authentification des renseignements sur l'état actuel de tous les justificatifs qu'il a attribués, à moins que les contraintes du respect de la vie privée n'empêchent de partager ces renseignements (p. ex., si un justificatif est « inaccessible » ou « révoqué », le minimum de renseignements nécessaires sur l'état doit être mis à la disposition des fournisseurs de services d'authentification, si permis).	X	X	X	
LIER DES AUTHENTIFIANTS					
6	Le fournisseur de services de justificatifs **PEUT** donner la capacité de lier un authentifiant fourni par le sujet au justificatif.	X	X	X	
7	Le fournisseur de services de justificatifs **DOIT** lier au moins un authentifiant au justificatif (p. ex., mot de passe, Foire aux questions ou mot de passe à usage unique).	X			
8	Le fournisseur de services de justificatifs **DOIT** lier deux authentifiants ou plus au justificatif (p. ex., mot de passe, Foire aux questions ou mot de passe à usage unique).		X	X	

9	Au moins deux authentifiants différents **DEVRAIENT** être liés au justificatif de sorte qu'il soit possible d'en récupérer un (qui a été perdu ou volé) en utilisant un autre authentifiant (p. ex., un compte d'authentifiant pourrait être récupéré avec un code de récupération à usage unique).		X		
10	Au moins deux authentifiants différents **DOIVENT** être liés au justificatif de sorte qu'il soit possible d'en récupérer un (qui a été perdu ou volé) en utilisant un autre authentifiant (p. ex., un compte d'authentifiant pourrait être récupéré avec un code de récupération à usage unique).			X	
11	Les authentifiants supplémentaires, qui pourraient servir à des fins de récupération, **DOIVENT** avoir un niveau d'assurance identique ou supérieur à celui d'un authentifiant à récupérer.		X	X	
12	Le fournisseur de services de justificatifs **PEUT** documenter ou avoir un processus documenté pour démontrer le niveau d'assurance de l'identité du sujet quand le justificatif a été récupéré.	X			
13	Le fournisseur de services de justificatifs **DOIT** documenter ou avoir un processus documenté pour démontrer le niveau		X	X	

	d'assurance de l'identité du sujet quand le justificatif a été récupéré.				
CRÉATION D'UN AUTHENTIFIANT					
14	Quand l'authentifiant est créé (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le créateur **DOIT** avoir un système ou des processus de gestion de la qualité vérifiables.		X		
15	Quand l'authentifiant est créé (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le créateur **DOIT** avoir un système ou des processus de gestion de la qualité vérifiables.			X	
16	Quand l'authentifiant utilise des renseignements intégrés par un fabricant (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le fournisseur de services de justificatifs **DOIT** s'assurer qu'il y a un processus de gestion de la sécurité vérifiable qui empêche les renseignements d'être compromis de la fabrication à la livraison au fournisseur de services de justificatifs.		X		
17	Quand l'authentifiant utilise des renseignements intégrés par un fabricant (p. ex., mot de passe à usage unique pour matériel, dispositif OU logiciel), le fournisseur de services de justificatifs **DOIT** s'assurer qu'il y a un processus de gestion de la sécurité vérifié			X	

	d'une manière indépendante qui empêche les renseignements d'être compromis de la fabrication à la livraison au fournisseur de services de justificatifs.				
ENTREPOSAGE DE JUSTIFICATIFS					
18	Le fournisseur de services de justificatifs ou d'authentification **DOIT** imposer des contrôles pour empêcher l'accès non autorisé aux renseignements sur les justificatifs.	X	X	X	
19	Les secrets liés au justificatif **DOIVENT** être entreposés comme du hash salé ou chiffrés.		X	X	
20	Les attributs des justificatifs qui contiennent des renseignements personnels entreposés dans le service **DOIVENT** être sécurisés (p. ex., chiffrés et/ou hashés).	X	X	X	
21	Les sauvegardes des renseignements liés aux justificatifs **DOIVENT** être chiffrées avant d'être entreposées à long terme et **DOIVENT** rester chiffrées tant qu'elles sont entreposées.		X	X	
22	Les modules cryptographiques **DOIVENT** satisfaire une norme de validation reconnue de l'industrie (p. ex., FIPS 140-3 ou comparable).		X	X	
AUTH	**Authentification**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
AUTHENTIFIANTS					
1	Le fournisseur de services d'authentification **DOIT**	X	X		

	exiger au moins un authentifiant des types suivants : • Chose que le sujet connaît; • Chose que le sujet a; • Chose que le sujet est ou fait.				
2	Si un seul authentifiant est requis, l'authentifiant **DOIT** être du type « chose que le sujet connaît » ou « chose que le sujet a ». Un authentifiant du type « chose que le sujet est ou fait » **NE DOIT ÊTRE** utilisé que comme authentifiant secondaire.		X		
3	Le fournisseur de services d'authentification **DOIT** exiger au moins deux authentifiants différents qui : • fournissent des facteurs d'authentification différents; • ne sont pas susceptibles aux mêmes vecteurs de menaces.			X	
4	Parmi les différents authentifiants exigés par le fournisseur de services d'authentification selon les critères de la section **AUTH** : • un des authentifiants **DOIT** être du type « chose que le sujet a »; • les autres authentifiants **PEUVENT** être du type « chose que le			X	

	sujet connaît » ou « chose que le sujet est ou fait ».				
5	Le fournisseur de services d'authentification **DOIT** consulter les renseignements fournis par le fournisseur de services de justificatifs pour déterminer l'état actuel d'un justificatif.	X	X	X	
6	Une biométrie **NE DEVRAIT PAS** être utilisée, à moins que sa nécessité ne soit démontrée et qu'il s'agisse du meilleur mécanisme pour répondre à un besoin d'authentification spécifique compte tenu de l'éventuelle perte correspondante de confidentialité.	X	X	X	
TYPE D'AUTHENTIFIANT					
7	N'importe quel type d'authentifiant **PEUT** être utilisé.	X			
9	Le fournisseur de services d'authentification **DOIT** utiliser une norme ou une pratique exemplaire de l'industrie pour l'authentification (p. ex., normes développées et approuvées par Kantara, W3C, IETF ou FIDO Alliance).		X	X	
9	Le fournisseur de services d'authentification **DOIT** utiliser des types d'authentifiants qui résistent aux menaces énumérées dans les critères d'**ATTÉNUATION DES MENACES** pour le niveau d'assurance 3.			X	
ATTÉNUATION DES MENACES					

10	Le fournisseur de services d'authentification **DOIT** avoir des processus de contrôle efficaces pour prévenir et déceler au moins les types d'attaques suivants et s'en remettre : • Devinette des secrets des authentifiants; • Rejeu. Cela **PEUT** être inclus dans la portée des lignes directrices décrites dans les critères de la section **BASE**.	X			
11	Le fournisseur de services d'authentification **DOIT** avoir des processus de contrôle efficaces pour prévenir et déceler au moins les types d'attaques suivants et s'en remettre : • Devinette des secrets des authentifiants; • Rejeu; • Écoute illicite; • Piratage de session. Cela **DOIT** être inclus dans la portée des lignes directrices décrites dans les critères de la section **BASE**.		X		
12	Le fournisseur de services d'authentification **DOIT** avoir des processus de contrôle efficaces pour prévenir et déceler au moins les types d'attaques suivants et s'en remettre : • Devinette des secrets des authentifiants; • Rejeu; • Écoute illicite; • Piratage de session;			X	

	• Usurpation d'identité/hameçonnage; • Homme du milieu (p. ex., utilisation d'un TLS mutuellement authentifié). Cela **DOIT** être inclus dans la portée du processus de vérification indépendante exigé dans les critères de la section **BASE**.				
RISQUE D'ADAPTATION					
13	Le fournisseur de services d'authentification **PEUT** offrir la capacité d'authentifier le risque d'adaptation.	X			
14	Le fournisseur de services d'authentification **DEVRAIT** offrir la capacité d'authentifier le risque d'adaptation.		X		
15	Le fournisseur de services d'authentification **DOIT** déceler et atténuer les interactions qui représentent un risque élevé, en se basant sur les renseignements provenant du contexte de l'authentification (comme les transactions provenant d'un endroit ou d'un canal imprévu pour un sujet, ou qui indiquent une configuration matérielle ou logicielle imprévue). -ou- Le fournisseur de services d'authentification **DOIT** traiter chaque interaction comme représentant un risque élevé.			X	

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

	• connue de la partie dépendante.				
INSE	**Lancement de session authentifiée**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
LANCEMENT DE SESSION					
1	Le fournisseur de services d'authentification **DEVRAIT** offrir la capacité de maintenir une session qui lie toutes les parties dépendantes, le lancement de session authentifiée étant un processus soutenu.	X			
2	Le fournisseur de services d'authentification **DOIT** offrir la capacité de maintenir une session qui lie toutes les parties dépendantes, le lancement de session authentifiée étant un processus soutenu.		X	X	
3	Si un sujet est authentifié à un niveau d'assurance donné, la session qui en résulte **DOIT** être considérée comme étant du même niveau d'assurance (p. ex., si le sujet est authentifié au niveau d'assurance 2, la session **DOIT** être considérée comme étant du niveau d'assurance 2), le lancement de session authentifiée étant un processus soutenu.	X	X	X	
RÉAUTHENTIFICATION					
4	Le fournisseur de services d'authentification **DEVRAIT** exiger que le sujet s'authentifie de nouveau après une période ou un événement prédéterminés selon une approche basée sur les risques (p. ex.,	X			

	quand une seule tentative de connexion est effectuée avec une autre partie dépendante dans une fédération).				
5	Le fournisseur de services d'authentification **DOIT** exiger que le sujet s'authentifie de nouveau après une période ou un événement prédéterminés selon une approche basée sur les risques (p. ex., quand une seule tentative de connexion est effectuée avec une autre partie dépendante dans une fédération ou quand une partie dépendante demande une réauthentification).		X	X	
6	Le fournisseur de services d'authentification **PEUT** rallonger les périodes d'inactivité des sessions.	X			
7	Si la réauthentification est au niveau d'assurance 2 ou 3, les périodes d'inactivité des sessions **PEUVENT** être prolongées mais **DOIVENT** correspondre au niveau d'assurance initial et remplir tous les critères d'authentification indiqués plus haut.		X	X	
TESE	**Fin de la session authentifiée**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
SESSION INACTIVE					
1	Le fournisseur de services d'authentification **DEVRAIT** imposer une durée de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la	X			

	durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.				
2	Le fournisseur de services d'authentification **DOIT** imposer une durée de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.		X	X	
3	Le fournisseur de services d'authentification **DEVRAIT** imposer une durée d'inactivité de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.	X			
4	Le fournisseur de services d'authentification **DOIT** imposer une durée d'inactivité de session maximale pour forcer la réauthentification dans un scénario d'ouverture de session unique fédérée après la durée de session prédéfinie, la fin de la session authentifiée étant un processus soutenu.		X	X	
5	Les valeurs de la durée et d'inactivité de session maximales au niveau d'assurance 3 **DEVRAIENT** être plus courtes que celles			X	

	pour le niveau d'assurance 2.				
6	Une session inactive en raison d'un dépassement de la durée ou de la durée d'inactivité de session maximale au niveau d'assurance 3 **PEUT** entraîner une fin de session ou une baisse à une session de niveau d'assurance 2.			X	
7	En cas de passage à une session de niveau inférieur : • Le fournisseur de services d'authentification **DOIT** aviser toutes les parties dépendantes associées à la session de niveau d'assurance 3; • Les sessions inactives en raison d'un dépassement de la durée de session ou de la durée d'inactivité de session maximale **PEUVENT** être prolongées jusqu'aux valeurs du niveau d'assurance 2 (moins le temps déjà passé).			X	
FIN DE SESSION					
8	Le fournisseur de services d'authentification **DEVRAIT** aviser toutes les parties dépendantes que la session est terminée.	X			
9	Le fournisseur de services d'authentification **DOIT** aviser toutes les parties dépendantes que la session est terminée.		X	X	
CRSP	**Suspension de justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
PAR UN SUJET					
1	Le fournisseur de services de justificatifs **DEVRAIT** donner à un sujet la	X	X	X	

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

	la récupération des justificatifs étant un processus soutenu.				
3	Le fournisseur de services de justificatifs **DOIT** donner au sujet la capacité de demander la récupération d'un justificatif suspendu, la récupération des justificatifs étant un processus soutenu.		X	X	
4	Le fournisseur de services de justificatifs **DOIT** exiger que le sujet s'authentifie avec un niveau d'assurance équivalent à celui du justificatif récupéré, la récupération des justificatifs étant un processus soutenu.		X	X	
PAR UN ADMINISTRATEUR					
5	Le fournisseur de services de justificatifs **PEUT** donner au personnel autorisé la capacité d'entreprendre la récupération d'un justificatif pour le sujet.	X	X	X	
6	Le fournisseur de services de justificatifs **DEVRAIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus, la récupération des justificatifs étant un processus soutenu.	X			
7	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus, la récupération des justificatifs étant un processus soutenu.		X	X	
8	Le fournisseur de services de justificatifs **DOIT** obliger le personnel autorisé à fournir un justificatif de			X	

	niveau d'assurance 3 ou supérieur pour récupérer un justificatif, la récupération des justificatifs étant un processus soutenu.				
PAR UN SYSTÈME					
9	Le fournisseur de services de justificatifs **PEUT** offrir la capacité de récupérer automatiquement un justificatif suspendu (p. ex., réactiver automatiquement un justificatif préalablement suspendu à la suite d'un trop grand nombre de tentatives de connexion ratées).	X	X	X	
CRMA	**Maintenance des justificatifs**	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**
PAR UN SUJET					
1	Le fournisseur de services de justificatifs **DEVRAIT** donner la possibilité de mettre à jour les authentifiants liés au justificatif lorsque c'est possible (p. ex., changer de mot de passe, lier un nouvel authentifiant).	X			
2	Le fournisseur de services de justificatifs **DEVRAIT** donner la possibilité de modifier les attributs des justificatifs (p. ex., mot de passe, Foire aux questions, codes de récupération).	X			
3	Le fournisseur de services de justificatifs **DOIT** donner la possibilité de mettre à jour les authentifiants liés au justificatif lorsque c'est possible (p. ex., changer de mot de passe, changer de NIP, rafraîchir la photo du visage en dossier par une		X	X	

	image plus récente ou changer une clé privée).				
4	Le fournisseur de services de justificatifs **DOIT** donner la possibilité de modifier les attributs des justificatifs (p. ex., mot de passe, Foire aux questions, codes de récupération clés cryptographiques, biométrie, alias, DID).		X	X	
5	Le fournisseur de services de justificatifs **DOIT** exiger une authentification à un niveau d'assurance équivalent ou supérieur à celui de l'attribut du justificatif qui est modifié (p. ex., mot de passe, Foire aux questions, codes de récupération clés cryptographiques, biométrie, alias, DID). Par exemple, un sujet connecté à l'aide d'un mot de passe à un seul facteur ne devrait pas pouvoir modifier des codes de récupération et des valeurs de mots de passe à usage unique.		X	X	
PAR UN ADMINISTRATEUR					
6	Le fournisseur de services de justificatifs **PEUT** permettre au personnel autorisé de mettre à jour les authentifiants liés au justificatif (p. ex., supprimer un authentifiant ou entreprendre un changement de mot de passe).	X	X	X	
7	Le fournisseur de services de justificatifs **PEUT** permettre au personnel	X	X	X	

	autorisé de mettre à jour les attributs des justificatifs.				
8	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.	X	X	X	
9	Le fournisseur de services de justificatifs **DOIT** exiger que le personnel autorisé donne un justificatif de niveau 3 ou supérieur pour effectuer la maintenance des justificatifs.			X	
10	Le fournisseur de services de justificatifs **DEVRAIT** exiger que le sujet termine les activités liées aux justificatifs amorcées par un administrateur (p. ex., un administrateur ne peut pas changer le mot de passe d'un sujet, seulement amorcer une réinitialisation).	X			
11	Le fournisseur de services de justificatifs **DOIT** exiger que le sujet termine les activités liées aux justificatifs amorcées par un administrateur (p. ex., un administrateur ne peut pas changer le mot de passe d'un sujet, seulement amorcer une réinitialisation).		X	X	
PAR UN SYSTÈME					
12	Le fournisseur de services de justificatifs **DEVRAIT** imposer des exigences en matière de contrôle et de protection des authentifiants (p. ex., Foire aux questions, exigences en matière de complexité, mises à jour des mots de passe, mises à jour	X			

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

	permettre au personnel autorisé de révoquer un justificatif.				
4	Le fournisseur de services de justificatifs **DOIT** pouvoir permettre au personnel autorisé de révoquer un justificatif.		X	X	
5	Le fournisseur de services de justificatifs **DOIT** imposer des contrôles d'accès afin que seul le personnel autorisé ait accès à ce processus.	X	X	X	
6	Le fournisseur de services de justificatifs **DOIT** obliger le personnel autorisé à fournir un justificatif ayant un niveau d'assurance 3 ou supérieur afin de révoquer un justificatif.			X	

7. Annexe A : Cas d'authentification

Le tableau qui suit présente plusieurs cas d'authentification pour donner un aperçu des diverses mises en œuvre où l'authentification est requise. Ces exemples ont été sélectionnés pour mettre en évidence les différences entre divers types d'authentification, facteurs d'authentification et authentifiants, et ils incluent des considérations qui affectent la détermination du niveau d'assurance.

Exemples (types d'authentifiants)	Facteur d'authentification	Authentifiant	Données de validation de l'authentifiant	Justificatif	Facteurs influençant la détermination des niveaux d'assurance
Nom d'utilisateur et mot de passe	Chose que vous connaissez	Mot de passe actuel du sujet	Hachage du mot de passe actuel du sujet	Données à propos du sujet associé aux données de validation de l'authentifiant (p. ex., prénom du sujet)	• Politique sur la force des mots de passe • Respect rigoureux de la politique Voir les critères de « maintenance des justificatifs » dans le profil de conformité
Justificatifs vérifiables dans un portefeuille numérique mobile	Chose que vous avez	Clé privée	Clé publique et autorité de certification/signature d'émetteur associées	Données à propos du sujet associé aux données de validation de l'authentifiant (p. ex., prénom du sujet)	• Taille de clé • Algorithme de signature • Type d'authentification locale (p. ex., nom d'utilisateur et mot de passe, biométrie) utilisée pour déverrouiller le portefeuille numérique Voir les critères de « maintenance des justificatifs » dans le profil de conformité
Authentifiant biométrique	Chose que vous êtes	Visage	Données géométriques (séquence des mesures de la géométrie faciale comme la distance entre le coin de l'œil et le bout du nez)	Données à propos du sujet associé aux données de validation des authentifiants (p. ex., prénom du sujet)	• Algorithme utilisé • Âge des données • Seuils de confiance Détections de la vivacité

Cas d'utilisation fédérée	Justificatif attribué dans le cadre d'un processus d'authentification concluant	Jeton OAuth/OIDC	Validation de la signature cryptographique associée (p. ex., jeton JWT privé)	Données à propos du sujet associé aux données de validation des authentifiants (p. ex., prénom du sujet)	• Entente de fédération • Évaluations et vérifiabilité des fournisseurs de services en nuage Contexte de l'authentification
Sécurité de la couche de transport mutuelle (mTLS)	Chose que vous avez	Clé privée	Clé publique et autorité de certification/signature d'émetteur associées	Données à propos du sujet associé aux données de validation des authentifiants (p. ex., rubrique de la liste de contrôle d'accès)	• Longueur des clés • Politiques et processus de gestion des clés Versions minimales soutenues

Tableau 2. Cas d'authentification

8. Annexe B : Résumé des conditions des processus de confiance

Le tableau 4 résume les conditions d'entrée et de sortie de la composante « Authentification » du CCP.

Condition	Description
Pas de justificatif	Il n'y a pas de justificatif attribué au sujet.
Justificatif attribué	Un justificatif a été attribué, et lié à un sujet unique et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
Justificatif authentifié	Le sujet a authentifié et prouvé avec succès le contrôle du justificatif au niveau d'assurance spécifié.
Session d'authentification	Il y a une interaction continue entre un sujet et un point ultime.
Justificatif inaccessible	Le sujet est actuellement incapable d'utiliser le justificatif. Cela peut être déclenché par le sujet (p. ex., signalement d'une combinaison nom d'utilisateur-mot de passe compromise) ou le système (p. ex., blocage en raison d'une succession de tentatives d'authentification infructueuses, d'une inactivité ou d'une activité suspecte). Il s'agit d'une situation temporaire qui va déboucher sur l'attribution ou la révocation d'un justificatif.
Justificatif d'authentification révoqué	Le justificatif est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.

Tableau 3. Conditions de la composante « Authentification »

9. Annexe C : Résumé des dépendances des processus de confiance

Les processus de confiance peuvent devoir se fier à une condition qui est le résultat d'un autre processus de confiance. C'est ce qu'on appelle une dépendance. Le tableau 5 résume les intrants, les extrants et les dépendances entre les processus de confiance de la composante « Authentification » du CCP.

Processus de confiance	Condition d'entrée	Dépendance du processus	Condition de sortie
Attribution du justificatif d'authentification	Pas de justificatif	-	Justificatif attribué
Authentification	Justificatif attribué	Attribution du justificatif	Justificatif authentifié
Début de la session authentifiée	Justificatif authentifié	Authentification	Session authentifiée
Fin de la session authentifiée	Session authentifiée	Début de la session authentifiée	Aucune session authentifiée
Suspension du justificatif	Justificatif attribué	Attribution du justificatif	Justificatif inaccessible
Récupération du justificatif	Justificatif inaccessible	Suspension du justificatif	Justificatif attribué
Maintenance du justificatif	Justificatif attribué	Attribution du justificatif, authentification	Justificatif attribué (mis à jour)
Révocation du justificatif	Justificatif inaccessible	Attribution du justificatif, authentification	Justificatif révoqué

Tableau 4. Relations du processus de confiance

10. Références

Cette section énumère toutes les normes et lignes directrices externes et tous les autres documents auxquels il est fait référence dans la présente composante du CCP.

Remarque : Le cas échéant, seul le numéro de version ou publication spécifié dans le présent document s'applique à cette composante du CCP.

Plutôt que de développer des normes entièrement nouvelles, la composante « Authentification » du CCP s'inspire et tire parti de l'expérience et des leçons d'organisations extérieures au CCIAN qui ont élaboré ou sont en train de faire évoluer des processus et normes connexes.

La composante « Authentification » du CCP s'est inspirée des normes et documents d'orientation suivants et est basée en partie sur eux :

1. Gouvernement du Canada. Centre de la sécurité des communications. Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3) - Centre canadien pour la cybersécurité
2. Gouvernement du Royaume-Uni. Cabinet Office and United Kingdom National Technical Authority on Information Assurance. Authentication and Credentials for

use with HMG Online Services (GPG-44). 2014. <https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services >.

3. Gouvernement des États-Unis. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines (NIST Special Publication 800-63-3). 2017. <https://pages.nist.gov/800-63-3/sp800-63-3.html >.
4. Gouvernement des États-Unis. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines: Enrollment and Identity Proofing Requirements (NIST Special Publication 800-63A). 2017. <https://pages.nist.gov/800-63-3/sp800-63b.html >
5. Gouvernement des États-Unis. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B). 2017. <https://pages.nist.gov/800-63-3/sp800-63a.html >
6. Gouvernement des États-Unis. United States Department of Commerce. National Institute of Standards and Technology. Digital Identity Guidelines: Federation and Assertions (NIST Special Publication 800-63C). 2017. <https://pages.nist.gov/800-63-3/sp800-63c.html >

Cette composante du CCP fait référence à ce qui suit à des fins d'exemple, d'information ou d'illustration :

- Gouvernement du Canada. Centre de la sécurité des communications. Conseils en matière de sécurité des technologies de l'information : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33). 2012. La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) - Centre canadien pour la cybersécurité
- Gouvernement des États-Unis. United States Department of Commerce. National Institute of Standards and Technology. Federal Information Processing Standards Publication 140-2 (Security Requirements for Cryptographic Modules). 2001. <https://csrc.nist.gov/publications/detail/fips/140/2/final >
- Gouvernement des États-Unis. United States Department of Commerce. National Institute of Standards and Technology. Guide to Computer Security Log Management (Special Publication 800-92). 2006. <https://www.nist.gov/publications/guide-computer-security-log-management>
- Département du Commerce des États-Unis. National Institute of Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53 (Rev.4). <https://nvd.nist.gov/800-53/Rev4/control/IA-5 https://nvd.nist.gov/800-53/Rev4/control/IA-5>
- AXELOS. ITIL v3 (auparavant l'Information Technology Infrastructure Library). 2011. <https://www.axelos.com/best-practice-solutions/itil >

11. Remarques

- Source : Gouvernement du Canada. Secrétariat du Trésor du Canada.
- Ligne directrice sur la définition des exigences en matière d'authentification. <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26262&section=html> La définition que donne le CCP de l'authentification a été adoptée à partir de la présente publication du gouvernement du Canada.
- Le processus d'authentification est une dépendance quand il est déclenché par un utilisateur (p. ex., sujet ou administrateur).

12. Historique des révisions

Version	Date de publication	Auteur(s)	Description
.05	2018-01-24	TFEC	Ébauche de travail initiale
.06	2019-04-30	Équipe de rédaction du CCP	Modifications au formatage Mise à jour du diagramme de modèle de CCP
.07	2019-10-21	TFEC et équipe de rédaction du CCP	Révision du contenu basée sur les commentaires concernant l'ébauche de discussion
1.0	2019-10-30	TFEC	Approbation comme recommandation préliminaire V1.0
1.1	S.O.	Équipe de rédaction du CCP	Mises à jour apportées en fonction des commentaires reçus pendant la période d'examen de la recommandation préliminaire
1.0	2020-05-11	Équipe de rédaction du CCP	Approbation comme recommandation finale V1.0
1.1	2023-11-15	Équipe de conception de l'authentification du CCP	Mises à jour apportées en fonction de la rétroaction reçue dans le cadre des essais alpha du CCP et de commentaires reportés lors d'itérations antérieures
1.1	2023-12-01	Équipe de conception de l'authentification du CCP	Approbation du TFEC comme recommandation finale V1.1

1.2	2024-05-10	Équipe de conception de l'authentification du CCP	Approbation du TFEC comme recommandation finale V1.2
1.2	2024-07-08	Équipe de conception de l'authentification du CCP	Approuvé en tant que recommandation finale V1.2 par vote du membre de soutien du CCIAN