Aperçu de la composante « Authentification » du CCP

Statut du document : Recommandation finale V1.1

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

Ce document a été préparé par le Comité d'experts du Cadre de confiance pancanadien (TFEC) du CCIAN. 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.

30

31

32

33 # Table des matières

61

1. Introduction à la composante « Authentification » du CCP

Ce document donne un aperçu de la composante « Authentification » du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale sur le CCP, veuillez vous référer au document « Aperçu du modèle de Cadre de confiance pancanadien ». Cet aperçu présente les buts et objectifs du CCP, un aperçu général du modèle de CCP et des renseignements contextuels.

Chaque composante du CCP comporte deux documents :

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

Cet aperçu fournit des renseignements reliés au profil de conformité de la composante « Authentification » du CCP, qui sont nécessaires pour une interprétation uniforme.

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 uniquement en combinaison avec

un autre facteur d'authentification. Un exemple d'un tel scénario est quelqu'un qui utilise Apple TouchID ou FaceID pour débloquer un iPhone; cela dépend du fait que cette personne contrôle et possède le iPhone (ce que vous possédez), et contrôle et possède une biométrie qui concorde (ce que vous êtes).

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.

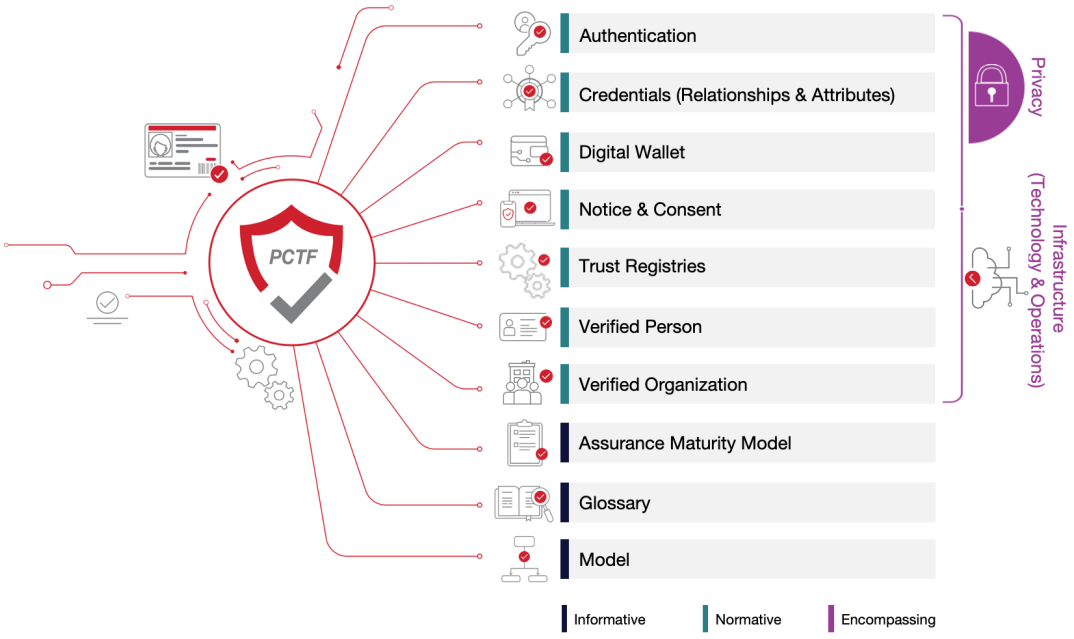

Figure 1. Composantes du Cadre de confiance pancanadien

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

298c	Niveau 2 (LOA2)	• Un certain niveau (raisonnable) d'assurance nécessaire • Répond aux critères de conformité du niveau 2
298d	Niveau 3 (LOA3)	• Haut niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 3
298e	Niveau 4 (LOA4)	• Très haut niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 4

316 **Tableau 1. Niveaux d'assurance**

317 Remarques

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

331 # 3. Processus de confiance

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

334 Un processus est une activité commerciale ou technique (ou un ensemble de ces
335 activités) qui transforme une condition d'entrée en condition de sortie – un extrant dont
336 dépendent souvent d'autres processus. Une condition est un état ou une circonstance
337 en particulier qui sont pertinents à un processus de confiance. Il peut s'agir d'un intrant,
338 d'un extrant ou d'une dépendance en relation à un processus de confiance. Les critères
339 de conformité spécifient ce qui est nécessaire pour transformer une condition d'entrée
340 en condition de sortie. Les critères de conformité spécifient, par exemple, ce qui est
341 nécessaire pour que le processus d'attribution de justificatifs transforme une condition
342 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.

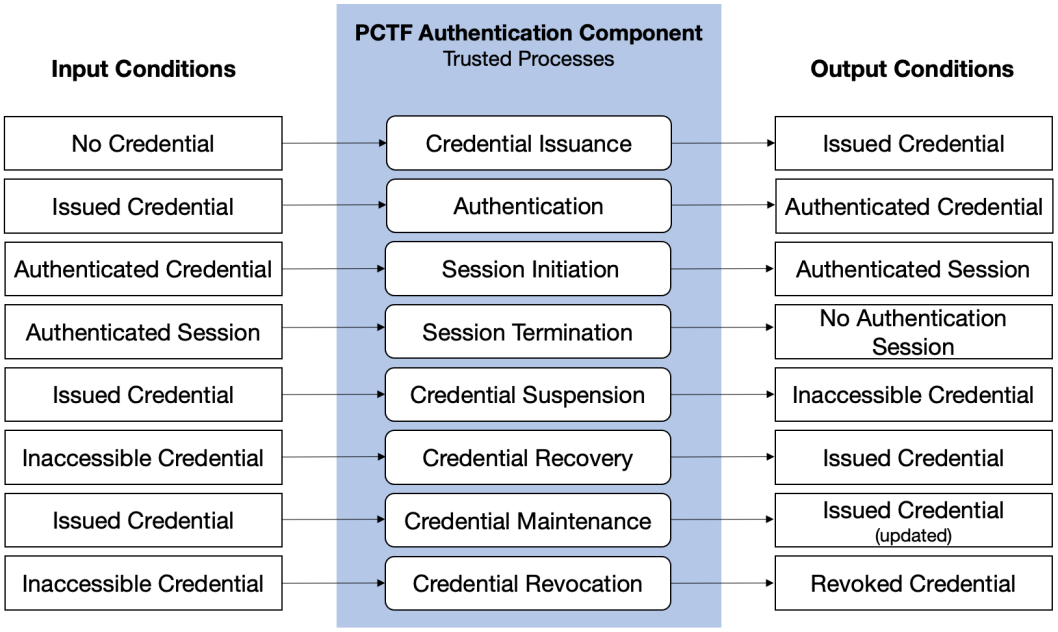

Figure 2. Aperçu de la composante « Authentification »

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

Remarque

- 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.

375a	**Intrants**	Pas de justificatif – Aucun justificatif n'est attribué au sujet.
375b	**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.
375c	**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.

389a	**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.

389b	**Extrants**	Justificatif – Le sujet a authentifié avec succès et prouvé qu'il contrôle le justificatif au niveau d'assurance spécifié.
389c	**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.

397a	**Intrants**	Justificatif authentifié – Le sujet a authentifié avec succès et prouvé qu'il contrôle le justificatif au niveau d'assurance spécifié.
397b	**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.
397c	**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.

405a	**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.
405b	**Extrants**	Pas de session authentifiée
405c	**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.

412a	**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.
412b	**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.
412c	**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.

418a	**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.
418b	**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.
418c	**Dépendances**	Suspension du justificatif

448 3.2.7 Maintenance des justificatifs

449 Le processus de maintenance des justificatifs inclut des activités de cycle de vie comme
450 l'association de nouveaux authentifiants, la suppression d'authentifiants et la mise à
451 jour des authentifiants (p. ex., changement de mot de passe, mise à jour des questions
452 et réponses de sécurité) ou encore la mise à jour des attributs des justificatifs. Ce
453 processus est généralement lancé par un utilisateur, mais il peut l'être aussi par un
454 administrateur de système ou automatiquement par le système.
455

425a	**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.
425b	**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.
425c	**Dépendances**	Attribution du justificatif, authentification

456 3.2.8 Révocation des justificatifs

457 Le processus de révocation des justificatifs assure qu'un justificatif est désactivé ou
458 supprimé d'une façon permanente. Une fois qu'un justificatif est révoqué, il ne peut plus
459 être utilisé. Le système empêchera activement que d'autres processus de confiance
460 soient exécutés relativement à ce justificatif. Le processus peut être lancé par un
461 utilisateur, un administrateur de système ou automatiquement par le système.
462 Précisons qu'un nouveau justificatif peut être attribué pour le même sujet. La
463 réattribution équivaut à révoquer un justificatif et à en attribuer un nouveau pour le
464 même sujet.
465

433a	**Intrants**	Justificatif attribué – Le justificatif peut être dans un état autre que révoqué (c.-à-d., inaccessible ou valide).
433b	**Extrants**	Justificatif révoqué – Le justificatif est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.
433c	**Dépendances**	Attribution du justificatif, authentification

466

4. 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. <Using authenticators to protect an online service >.
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. <NIST Special Publication 800-63-3 >.
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. <NIST Special Publication 800-63B >
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. <NIST Special Publication 800-63A >
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. <NIST Special Publication 800-63C >

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. <Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules >
- 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. <Guide to 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). <Access CPRT - Cybersecurity and Privacy Reference Tool | CSRC | CSRC >
- AXELOS. ITIL v3 (auparavant l'Information Technology Infrastructure Library). 2011. <ITIL | IT Service Management | Axelos >

5. Remarques

- Source : Gouvernement du Canada. Secrétariat du Trésor du Canada.
- Ligne directrice sur la définition des exigences en matière d'authentification. <Ligne directrice sur la définition des exigences en matière d'authentification> 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).

6. 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.

501a

Exemples (types d'authentifiants)	Facteur d'authentification	Authentifiant	Données de validation de l'authentifiant	Justificatif	Facteurs influençant la détermination des niveaux

						d'assurance
501b	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
501c	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
501d	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
501e	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
501f	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	• Longueur des clés • Politiques et processus de gestion des clés • Versions minimales soutenues

				de contrôle d'accès)	

537 **Tableau 2. Cas d'authentification**

538 7. Annexe B : Résumé des conditions des 539 processus de confiance

540 Le tableau 2 résume les conditions d'entrée et de sortie de la composante
541 « Authentification » du CCP.
542

	Condition	Description
507b	Pas de justificatif	Il n'y a pas de justificatif attribué au sujet.
507c	Justificatif attribué	Un justificatif a été attribué, et lié à un sujet unique et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
507d	Justificatif authentifié	Le sujet a authentifié et prouvé avec succès le contrôle du justificatif au niveau d'assurance spécifié.
507e	Session d'authentification	Il y a une interaction continue entre un sujet et un point ultime.
507f	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.
507g	Justificatif d'authentification révoqué	Le justificatif est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.

543
544 **Tableau 3. Conditions de la composante « Authentification »**

8. 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 3 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
516b	Attribution du justificatif d'authentification	Pas de justificatif	-	Justificatif attribué
516c	Authentification	Justificatif attribué	Attribution du justificatif	Justificatif authentifié
516d	Début de la session authentifiée	Justificatif authentifié	Authentification	Session authentifiée
516e	Fin de la session authentifiée	Session authentifiée	Début de la session authentifiée	Aucune session authentifiée
516f	Suspension du justificatif	Justificatif attribué	Attribution du justificatif	Justificatif inaccessible
516g	Récupération du justificatif	Justificatif inaccessible	Suspension du justificatif	Justificatif attribué
516h	Maintenance du justificatif	Justificatif attribué	Attribution du justificatif, authentification	Justificatif attribué (mis à jour)
516i	Révocation du justificatif	Justificatif inaccessible	Attribution du justificatif, authentification	Justificatif révoqué

Tableau 4. Relations du processus de confiance

9. Historique des révisions

	Version	Date de publication	Auteur(s)	Description
518b	.05	2018-01-24	TFEC	Ébauche de travail initiale
518c	.06	2019-04-30	Équipe de rédaction du CCP	Modifications au formatage Mise à jour du diagramme de modèle de CCP
518d	.07	2019-10-21	TFEC et équipe de	Révision du contenu basée sur les commentaires concernant l'ébauche de discussion

			rédaction du CCP	
518e	1.0	2019-10-30	TFEC	Approbation comme recommandation préliminaire V1.0
518f	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
518g	1.0	2020-05-11	Équipe de rédaction du CCP	Approbation comme recommandation finale V1.0
518h	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
518i	1.1	2023-12-01	Équipe de conception de l'authentification du CCP	Approbation du TFEC comme recommandation finale V1.1

554