Aperçu de la composante « Authentification » du CCP

Statut du document : Recommandation finale version 1.0

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

Ce document a été préparé par le Comité d'experts du Cadre de confiance pancanadien du CCIAN avec l'apport du public recueilli et traité par le biais d'un processus d'examen ouvert mené par des pairs. On s'attend à ce que le contenu de ce document soit examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois, règlements et politiques. Les avis concernant les changements apportés à ce document seront partagés au moyen de communications électroniques, notamment le courriel et les réseaux sociaux. Les notifications seront également consignées dans le programme de travail du Cadre de confiance pancanadien (CCP). Les changements apportés à ce document qui pourraient se répercuter sur l'état des certifications et des marques de confiance seront définis dans la composante « Évaluation » du CCP.

Table des matières

1 Introduction à la composante « Authentification » du CCP

Ce document donne un aperçu de la composante « Authentication » du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale sur le cadre de confiance pancanadien, veuillez-vous référer au document « Aperçu du modèle de Cadre de confiance pancanadien ». Cet aperçu présente les buts et objectifs du CCP, un aperçu de haut niveau 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 l'authentification du CCP, qui sont nécessaires pour l'interpréter d'une manière 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.

1.2 Raison d'être et avantages anticipés

Le cadre de confiance pancanadien 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 faciliterl'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 dans le contexte consistant à débloquer l'accès à un autre authentifiant. Un exemple d'un tel scénario est quelqu'un qui utilise Apple TouchID ou FaceID pour débloquer un iPhone et accède ensuite à un mot de passe à usage unique ou un autre authentifiant mobile enregistré et généré localement.

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.

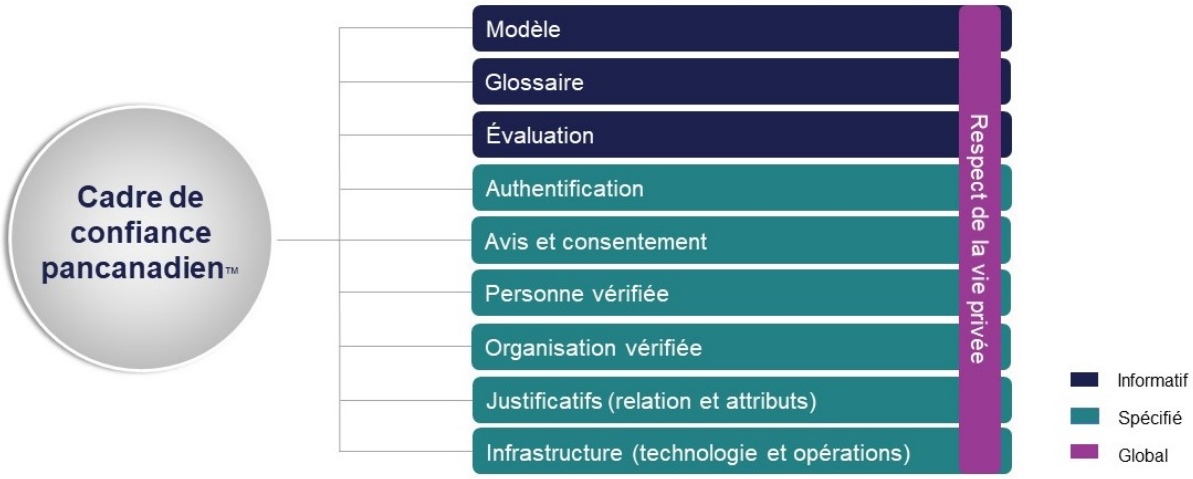

Figure 1. Composantes du cadre de confiance pancanadien

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 :

- Le terme « connexion » ne fait pas exclusivement référence à 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. À ce titre, les identifiants numériques attribués et gérés à l'aide d'une identité

autosouveraine ou des processus d'attribution plus conventionnels peuvent tirer parti de cette composante.

Remarque

- 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 définitions énumérés dans le glossaire du CCP et ceux employés dans la présente section s'appliquent.

Risque adaptatif

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

Authentification du risque adaptatif

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

Facteurs d'authentification

Il y a trois facteurs d'authentification :

1. Chose que le sujet a
2. Chose que le sujet connaît
3. Chose que le sujet est ou fait

Authentifiant

Renseignements ou caractéristiques biométriques qu'une personne contrôle et qui sont un cas particulier d'un type d'authentifiant, lequel relève du contrôle de la personne. Exemples :

1. Clé de signature privée égale à 011011101010101011000101
2. Mot de passe égal à A$n45!R78oR
3. Visage d'une personne (remarque : l'image du visage est saisie et potentiellement soumise à un traitement supplémentaire en vue d'être analysée d'après les données de validation de l'authentifiant)

Type d'authentifiant

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

Exemples :

1. Clés cryptographiques et jeton RSA avec mot de passe à usage unique – chose que vous avez
2. Mots de passe et authentifiant basé sur les connaissances (authentification basée sur les connaissances, p. ex. réponses à des questions de sécurité) – chose que vous connaissez
3. Empreintes digitales, rétines, vitesse de frappe au clavier, démarche – chose qui vous caractérise

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).

Exemples :

1. Clé de validation d'une signature publique (associée à la clé privée du sujet) égale à 00100110101111111010000
2. Hash du mot de passe du sujet A$n45!R78oR ou état actuel d'un générateur de mots de passe à usage unique
3. Image faciale enregistrée par le sujet (ou modèle biométrique de l'image faciale enregistrée par le sujet, selon ce qui est entreposé par le fournisseur de services de justificatifs)

Justificatif d'authentification

Données qui lient d'une façon unique les données de validation de l'authentifiant à celles de l'identité. Pour les besoins de la présente composante du CCP, le « justificatif d'authentification » fait uniquement référence à la structure des données numériques.

Exemples :

1. Le numéro de permis de conduire du sujet (et possiblement d'autres pointeurs de dossiers de données) lie de dossier d'identité du ministère des Transports du sujet à l'image faciale ou au modèle biométrique du sujet dans la base de données biométriques du ministère des Transports.
2. Le numéro de compte bancaire du sujet lie les données d'identité du sujet à la banque avec le hash du mot de passe du compte bancaire du sujet.

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.

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.

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.

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
- TI – 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 – Mot de passe à usage unique
- CCIAN – Cadre de confiance pancanadien
- FAQ – Foire aux questions
- TLS – Transport Layer Security
- W3C – Consortium World Wide Web

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.

Remarque

- 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 d'authentification
2. Suspension des justificatifs d'authentification
3. Récupération des justificatifs d'authentification
4. Maintenance des justificatifs d'authentification
5. Révocation des justificatifs d'authentification

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 d'authentification 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. Les exigences de chaque niveau d'assurance sont cumulatives – des niveaux d'assurance successivement plus grands imposent que les exigences pour les niveaux d'assurance inférieurs aient aussi été remplies.**

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	• Peu ou pas de niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 1
Niveau 2	• Un certain niveau (raisonnable) d'assurance nécessaire • Répond aux critères de conformité du niveau 2
Niveau 3	• Haut niveau d'assurance nécessaire • Répond aux critères de conformité au niveau 3
Niveau 4	• Très haut niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 4

Tableau 1. Niveaux d'assurance

Remarque

- 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 davantage précisé à l'aide d'un qualificateur. 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 qualificateur stipulant que l'authentifiant doit être attribué par un fournisseur de soins de santé.

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

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.

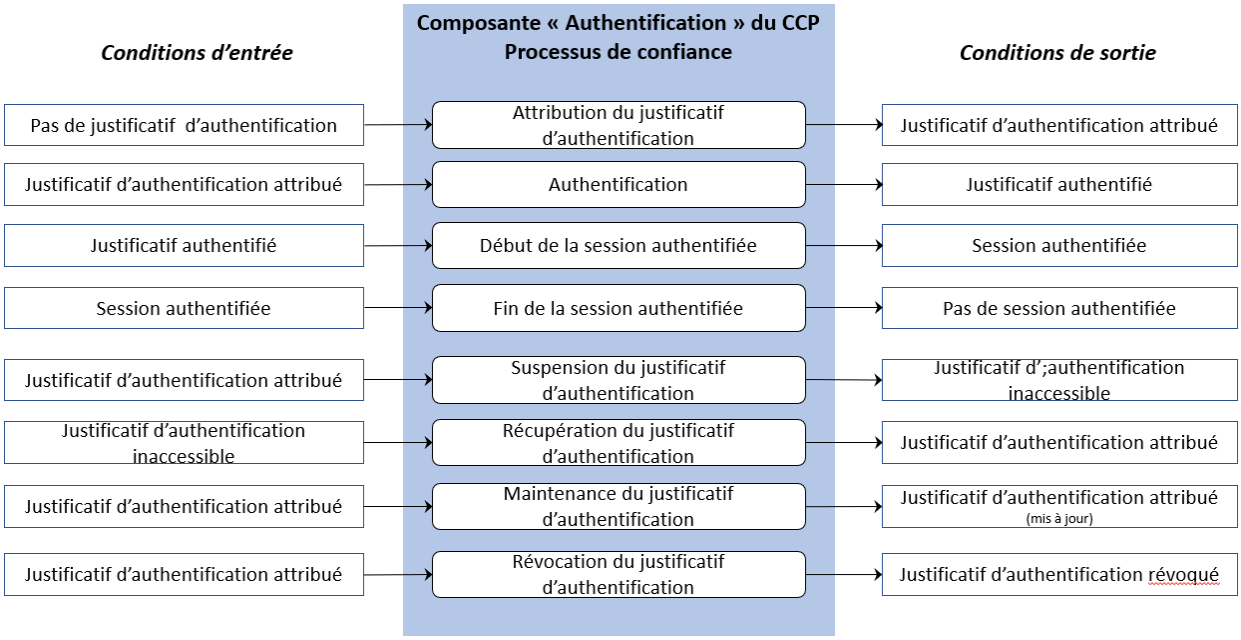

Figure 2. Aperçu conceptuel de la composante « Authentification »

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 d'authentification

L'attribution des justificatifs d'authentification est un processus d'inscription pendant lequel un justificatif d'authentification est attribué, lié à un sujet unique et lié à un ou plusieurs authentifiants appropriés contrôlés par le sujet. Un justificatif d'authentification inclut un ou plusieurs identifiants qui peuvent être des pseudonymes et contenir des attributs vérifiés par l'émetteur de justificatifs d'authentification. 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 au justificatif d'authentification.

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 d'authentification – Aucun justificatif d'authentification n'est attribué au sujet.
Extrants	Justificatif d'authentification attribué – Un justificatif d'authentification 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. [1] 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.

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

3.2.3 Début de la session authentifiée

À un certain moment pendant une session, une sous-session peut être lancée pour authentifier un sujet. La session authentifiée doit être lancée avec un justificatif authentifié. L'extrant du début de la session authentifiée est une session authentifiée

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.

Intrants	Justificatif authentifié – Le sujet a authentifié avec succès et prouvé qu'il contrôle le justificatif d'authentification 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 service 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

Le processus de fin de session authentifiée est nécessaire quand on utilise des sessions authentifiées. Une session authentifiée prend fin à l'aide d'événements comme une déconnexion explicite, une expiration de session en raison d'une inactivité ou d'une durée maximale ou par d'autres moyens.

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 service 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 d'authentification

Ce processus transforme un justificatif d'authentification attribué en justificatif d'authentification inaccessible, et il peut être amorcé par l'intervention d'un utilisateur, un administrateur de système ou automatiquement par le système. Il est interdit d'utiliser un justificatif d'authentification inaccessible à des fins d'authentification.

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

3.2.6 Récupération des justificatifs d'authentification

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

Intrants	Justificatif d'authentification 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 d'authentification attribué – Un justificatif d'authentification 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 d'authentification

3.2.7 Maintenance des justificatifs d'authentification

Le processus de maintenance des justificatifs d'authentification 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 d'authentification. 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 d'authentification attribué – Un justificatif d'authentification a été attribué, et lié à un seul sujet et à un ou plusieurs authentifiants appropriés qui sont contrôlés par le sujet.
Extrants	Justificatif d'authentification attribué (mis à jour) – Un justificatif d'authentification 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 d'authentification, authentification [2]

3.2.8 Révocation des justificatifs d'authentification

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

Intrants	Justificatif d'authentification inaccessible – Le sujet n'est actuellement pas en mesure d'utiliser le justificatif d'authentification.
Extrants	Justificatif d'authentification révoqué – Le justificatif d'authentification est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.
Dépendances	Attribution du justificatif d'authentification, authentification [2]

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. *Conseils en matière de sécurité des technologies de l'information pour les praticiens : Guide sur l'authentification des utilisateurs dans les systèmes de TI (ITSP.30.031 V3)*. 2018. <https://www.cse-cst.gc.ca/fr/publication/itsp.30.031v3
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. Département du Commerce des États-Unis. 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. Département du Commerce des États-Unis. 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. Département du Commerce des États-Unis. National Institute of Standards and Technology. *Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B)*. 2017. <https://pages.nist.gov/800-633/sp800-63a.html>
6. Gouvernement des États-Unis. Département du Commerce des États-Unis. National Institute of Standards and Technology. D*igital 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 :

1. Gouvernement du Canada. Centre de la sécurité des communications. *Conseil 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. <https://cyber.gc.ca/fr/orientation/apercu-itsg-33>

2. Gouvernement du Canada. Secrétariat du Conseil du Trésor. *Orientation sur les mots de passe*. 2020. < https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientation-sur-mots-passe.html>
3. Gouvernement des États-Unis. Département du Commerce des États-Unis. 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>
4. Gouvernement des États-Unis. Département du Commerce des États-Unis. 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-logmanagement>
5. 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>
6. AXELOS. *ITIL v3 (auparavant l'Information Technology Infrastructure Library).* 2011. <https://www.axelos.com/best-practice-solutions/itil>

5 Remarques

1. Source : Gouvernement du Canada. Secrétariat du Conseil 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.
2. 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

Scénario

Authentification bancaire pour accéder à un service gouvernemental à l'aide d'une connexion bancaire (appareil d'authentification inconnu (p. ex., navigateur inconnu)); numéro de carte bancaire, mot de passe, mot de passe à usage unique à une adresse connue (p. ex., numéro de cellulaire, adresse de courriel).

Dans ce scénario...

Les facteurs d'authentification sont :

1. Une chose que vous connaissez
2. Une chose que vous avez

Les types d'authentifiants sont :

1. (chose que vous connaissez) : mot de passe

2. (chose que vous avez) :
    1. Mot de passe à usage unique pour une adresse connue
    2. Appareil d'authentification (p. ex., navigateur) (utilisé dans le processus de validation, mais pas utile dans cet exemple étant donné que le navigateur n'est pas connu)

Les authentifiants sont :

1. Le mot de passe actuel du sujet
2. Le navigateur du sujet – identifié à l'aide de l'empreinte digitale du navigateur
3. L'accès à l'adresse connue du sujet (p. ex., accès à un compte de courriel d'une adresse de courriel connue, accès à un cellulaire d'un numéro de cellulaire connue, accès à une boîte aux lettres physique)
4. Mot de passe à usage unique (en tant que mécanisme pour authentifier la possession d'un cellulaire connu)

Les données de validation de l'authentifiant sont :

1. Les données sur l'empreinte digitale du navigateur (pour le navigateur utilisé précédemment par le sujet)
2. Le hash du mot de passe actuel du sujet
3. L'adresse connue qui a été utilisée pour la distribution du mot de passe à usage unique au sujet
4. Le hash du mot de passe à usage unique généré pendant l'authentification (quand le mot de passe à usage unique a été envoyé au cellulaire)

Le justificatif d'authentification :

1. Numéro de compte bancaire (référence au dossier contenant les renseignements sur le client avec les données d'identité)
2. Référence qui lie le numéro de compte bancaire aux données de validation de l'authentifiant du sujet

7 Annexe B : Résumé des conditions des processus de confiance

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

Condition	Description
Pas de justificatif d'authentification	Il n'y a pas de justificatif d'authentification attribué au sujet.
Justificatif d'authentification attribué	Un justificatif d'authentification 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 d'authentification au niveau d'assurance spécifié.
Session d'authentification	Il y a une interaction continue entre un sujet et un point ultime.
Justificatif d'authentification 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 d'authentification.
Justificatif d'authentification révoqué	Le justificatif d'authentification est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.

Tableau 2. Conditions de la composante « Authentification »

8 Annexe C : Résumé des dépendances du processus de confiance

Les processus de confiance peuvent devoir se fier à une condition qui est le résultat d'autres 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
Attribution des justificatifs d'authentification	Pas de justificatif d'authentification	-	Justificatif d'authentification attribué
Authentification	Justificatif d'authentification attribué	Attribution des justificatifs d'authentification	Justificatif authentifié

Début de la session d'authentification	Justificatif authentifié	Authentification	Session authentifiée
Fin de la session d'authentification	Session d'authentifiée	Lancement de la session authentifiée	Aucune session authentifiée
Suspension des justificatifs d'authentification	Justificatif d'authentification attribué	Attribution des justificatifs d'authentification	Justificatif d'authentification inaccessible
Récupération des justificatifs d'authentification	Justificatif d'authentification inaccessible	Suspension des justificatifs d'authentification	Justificatif d'authentification attribué
Maintenance des justificatifs d'authentification	Justificatif d'authentification attribué	Authentification de l'attribution des justificatifs d'authentification [2]	Justificatif d'authentification attribué (mis à jour)
Révocation des justificatifs d'authentification	Justificatif d'authentification inaccessible	Authentification de l'attribution des justificatifs d'authentification [2]	Justificatif d'authentification révoqué

Tableau 3. Relations du processus de confiance

9 Contrôle des versions du document

Numéro de version	Date de publication	Auteurs	Description
0.05	2018-01-24	TFEC	Ébauche de travail initiale
0.06	2019-04-30	Équipe de rédaction du CCP	Changements de formatage. Mise à jour du diagramme de modèle de CCP
0.07	2019-10-21	TFEC et équipe de rédaction du CCP	Contenu révisé en fonction des commentaires sur l'ébauche de discussion
1.0	2019-10-21	TFEC	Approbation en tant qu'ébauche de recommandations V1.0
1.1	N/A	Équipe de rédaction du CCP	Mise à jour en fonction des commentaires reçus pendant la période d'examen des ébauches de recommandations
1.0	2020-05-11	Équipe de rédaction du CCP	Recommandation finale V1.0