Ébauche de recommandations pour l'aperçu de la composante connexion vérifiée du cadre de confiance pancanadien V1.0

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

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

Les prochaines versions du cadre de confiance pancanadien vont étoffer, clarifier et peaufiner le contenu de ce document..

L'auditoire ciblé pour cette ébauche de recommandations sont les décideurs qui peuvent être ou non des experts dans la technologie des domaines. En examinant cette ébauche, veuillez répondre aux questions ci-dessous et noter que vos réponses ne sont pas contraignantes et visent à améliorer le cadre de confiance pancanadien.

1. Si votre organisation devait s'autoévaluer aujourd'hui, est-ce qu'elle serait conforme?
2. Votre organisation pourrait-elle se conformer?
3. Votre organisation pourrait-elle identifier des obstacles à la conformité (commerciale, juridique ou technique)?
4. Seriez-vous disposé à faire une auto-évaluation non contraignante? Si oui, seriez-vous disposé à partager ces résultats avec le Comité d'experts du cadre de confiance du DIACC?
5. La description des processus de confiance est-elle claire et exacte?
6. Les critères de conformité sont-ils clairs et mesurables ou évaluables?
7. Êtes-vous d'accord avec les termes utilisés pour décrire la connexion vérifiée et l'emploi de la formulation « connexion vérifiée » pour cette composante?
8. Êtes-vous d'accord pour que les renseignements descriptifs soient retirés du document sur le profil de conformité et intégrés dans celui sur l'aperçu?
9. Êtes-vous d'accord pour que le document sur l'aperçu soit restructuré en mettant tous les termes, définitions, rôles et autres renseignements clés dans une seule section?

Table des matières

1. Introduction à la composante connexion vérifiée du cadre de confiance pancanadien
    1.1. Portée
    1.2. Raison d'être et avantages anticipés
    1.3. Biométrie et connexion vérifiée
    1.4. Relation avec le cadre de confiance pancanadien
2. Conventions de la connexion vérifiée
    2.1. Termes et définitions
    2.2. Abréviations
    2.3. Rôles
    2.4. Niveaux d'assurance
3. Processus de confiance
    3.1. Aperçu conceptuel
    3.2. Description des processus
        3.2.1. Attribution de justificatifs
        3.2.2. Authentification
        3.2.3. Début de session authentifiée
        3.2.4. Fin de session authentifiée
        3.2.5. Suspension des justificatifs
        3.2.6. Récupération des justificatifs
        3.2.7. Maintenance des justificatifs
        3.2.8. Révocation des justificatifs
4. Références
5. Remarques

Annexe A : Cas d'utilisation des authentifiants

Annexe B : Résumé des conditions du processus de confiance

Annexe C : Résumé des dépendances du processus de confiance

1 Introduction à la composante connexion vérifiée du cadre de confiance pancanadien

Ce document donne un aperçu de la composante connexion vérifiée du cadre de confiance pancanadien. 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 cadre de confiance pancanadien, un aperçu de haut niveau du modèle de cadre de confiance pancanadien et des renseignements contextuels.

Chaque composante du cadre de confiance pancanadien 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 connexion vérifiée du cadre de confiance pancanadien, qui sont nécessaires pour l'interpréter d'une manière uniforme.

1.1 Portée

La composante connexion vérifiée du cadre de confiance pancanadien définit :

1. Un ensemble de processus qui permettent d'accéder à des systèmes numériques. Les processus couverts par la présente composante comprennent notamment le fait de lier un justificatif à un sujet et des authentifiants à un justificatif, la gestion d'une session et les fonctions de gestion du cycle de vie des justificatifs (p. ex., mises à jour, suspension, récupération et révocation);
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 en appliquant des critères de conformité uniformisés pour l'évaluation et la certification des processus. Les critères de conformité de la présente composante permettent de s'assurer que :

- Les processus de confiance donnent une représentation d'un sujet unique et d'avoir un niveau d'assurance comme quoi il s'agit du même sujet à chaque connexion réussie auprès d'un fournisseur de services d'authentification;

- Les processus de confiance nécessaires pour maintenir l’intégrité et la sécurité des authentifiants utilisés pour accéder à des systèmes à distance sont fiables.

Tous les participants bénéficieront :

- Du caractère répétitif et de la continuité que les processus de connexion offrent ou dont ils dépendent;
- De l'assurance que les utilisateurs identifiés peuvent s'engager dans des interactions autorisées avec des systèmes à distance.

Les parties utilisatrices bénéficieront :

- De la capacité de tirer parti de l'assurance des processus de connexion vérifiée pour identifier d'une manière unique un sujet à l'intérieur de leurs applications ou programmes.

1.3 Biométrie et connexion vérifiée

Étant donné le manque inhérent de révocabilité de la biométrie, les normes de l'industrie pertinentes à cette composante considèrent d'une façon générale la biométrie comme un moyen de débloquer un authentifiant à l'intérieur d'un appareil local pour faciliter l'authentification à distance avec un service. Un exemple d'un tel scénario serait une personne qui utilise Apple TouchID ou FaceID pour débloquer l'accès à un mode de passe mobile à usage unique ou un autre authentifiant mobile entreposé et généré localement.

- **NIST 800-63** décrit l'utilisation de la biométrie de la façon suivante : « La biométrie n'est pas un secret. Par conséquent, ces consignes permettent uniquement d'utilisation de la biométrie pour l'authentification lorsqu'elle est étroitement liée à un authentifiant physique ».
- **ITSP.30.031** 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 « 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. »

Étant donné les indications fournies par NIST et ITSP, cette version de la composante connexion vérifiée du cadre de confiance pancanadien considères l'authentification biométrique uniquement dans le contexte consistant à débloquer l'accès à un autre authentifiant, l'exemple le plus répandu étant le fait de débloquer l'accès par la biométrie à un authentifiant mobile.

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 cadre de confiance pancanadien, 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.

Figure 1 is an illustration of the components of the draft Pan-Canadian Trust Framework.

Figure 1. Composantes du cadre de confiance pancanadien

Les avantages associés à la composante connexion vérifiée du cadre de confiance pancanadien sont obtenus en partie en élargissant les processus définis dans la composante personne vérifiée du cadre de confiance pancanadien (et, dans une certaine mesure, la composante organisation vérifiée du cadre de confiance pancanadien). À cet égard, le cadre de confiance pancanadien 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 de connexion vérifiée

Cette section décrit et définit les principaux termes et concepts utilisés dans la composante connexion vérifiée du cadre de confiance pancanadien. 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 la connexion vérifiée du cadre de confiance pancanadien.

Pour les besoins de la présente composante du cadre de confiance pancanadien :

- 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).
- 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 cadre de confiance pancanadien. 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 cadre de confiance pancanadien 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 cadre de confiance pancanadien, les termes et définitions énumérés dans le glossaire du cadre de confiance pancanadien 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 0010011010111111010000
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

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 cadre de confiance pancanadien, le « justificatif » fait uniquement référence aux structures 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 sur l'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 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.

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 connexion vérifiée du cadre de confiance pancanadien.

2.2 Abréviations

Les abréviations et acronymes suivants apparaissent tout au long de cet aperçu et dans le profil de conformité de la connexion vérifiée du cadre de confiance pancanadien :

- DIDs – Identifiant(s) décentralisé(s)
- IETF – Groupe de travail sur l'ingénierie Internet
- TI – Technologie de l'information
- ITIL – Information Technology Infrastructure Library
- 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
- cadre de confiance pancanadien – Pan-Canadian Trust Framework
- FAQ – Foire aux questions
- TLS – Transport Layer Security
- W3C – Consortium World Wide Web

2.3 Rôles

Les rôles suivants et leurs définitions s'appliquent dans la portée et le contexte de la composante connexion vérifiée du cadre de confiance pancanadien. Ces rôles aideront à isoler les différentes fonctions et responsabilités à l'intérieur des processus de confiance de la connexion vérifiée de bout en bout.

Remarque

- Selon le cas d'utilisation, différentes organisations peuvent assumer un ou plusieurs rôles. Par exemple, l'attribution des justificatifs 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 la connexion vérifiée 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 qui met en œuvre les processus de confiance de la connexion vérifiée reliés à la gestion des justificatifs :

1. Attribution des justificatifs

2. Suspension des justificatifs
3. Récupération des justificatifs
4. Maintenance des justificatifs
5. Révocation des justificatifs

Partie utilisatrice

Entité qui dépend d'une mise en œuvre conforme des processus de confiance de la connexion vérifiée.

Sujet

Un sujet peut être une personne naturelle, une organisation, une application ou un appareil lié à un justificatif.

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 connexion vérifiée du cadre de confiance pancanadien. Dans le contexte de la présente composante du cadre de confiance pancanadien, les fournisseurs de justificatifs, parties utilisatrices et utilisateurs emploient des 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. Un niveau d'assurance indique aussi que les processus de connexion vérifiée ont été évalués et/ou certifiés conformément aux critères de conformité de la connexion vérifiée du cadre de confiance pancanadien.

Pour les besoins de la présente composante du cadre de confiance pancanadien, 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 de connexion vérifiée est le plus bas associé à n'importe lequel des processus de confiance de la connexion vérifiée. 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 connexion vérifiée du cadre de confiance pancanadien.

	Niveau d'assurance	Description de la qualification
280-a	Niveau 1	• Peu ou pas de niveau d'assurance nécessaire • Répond aux critères de conformité du niveau 1
280-b	Niveau 2	• Un certain niveau (raisonnable) d'assurance nécessaire • Répond aux critères de conformité du niveau 2

	Niveau d'assurance	Description de la qualification
280-c	Niveau 3	• Haut niveau d'assurance nécessaire • Répond aux critères de conformité au niveau 3
280-d	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 connexion vérifiée du cadre de confiance pancanadien ne définit pas les critères de conformité pour le niveau d'assurance 4. Toutefois, le cadre de confiance pancanadien 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 utilisatrice dans le secteur des soins de santé peut spécifier dans un profil du cadre de confiance pancanadien 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 cadre de confiance pancanadien 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. 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 cadre de confiance pancanadien, un processus est qualifié de confiance quand il est vérifié et certifié conforme aux critères de conformité définis dans un profil de conformité du cadre de confiance pancanadien. L'intégrité d'un processus 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 connexion vérifié du cadre de confiance pancanadien 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 de connexion vérifiée est qualifié de processus de confiance quand il est vérifié et certifié selon les critères de conformité stipulés par le profil de conformité de la connexion vérifiée du cadre de confiance pancanadien. Les critères de conformité spécifiés dans d'autres composantes du cadre de confiance pancanadien 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 connexion vérifiée du cadre de confiance pancanadien.

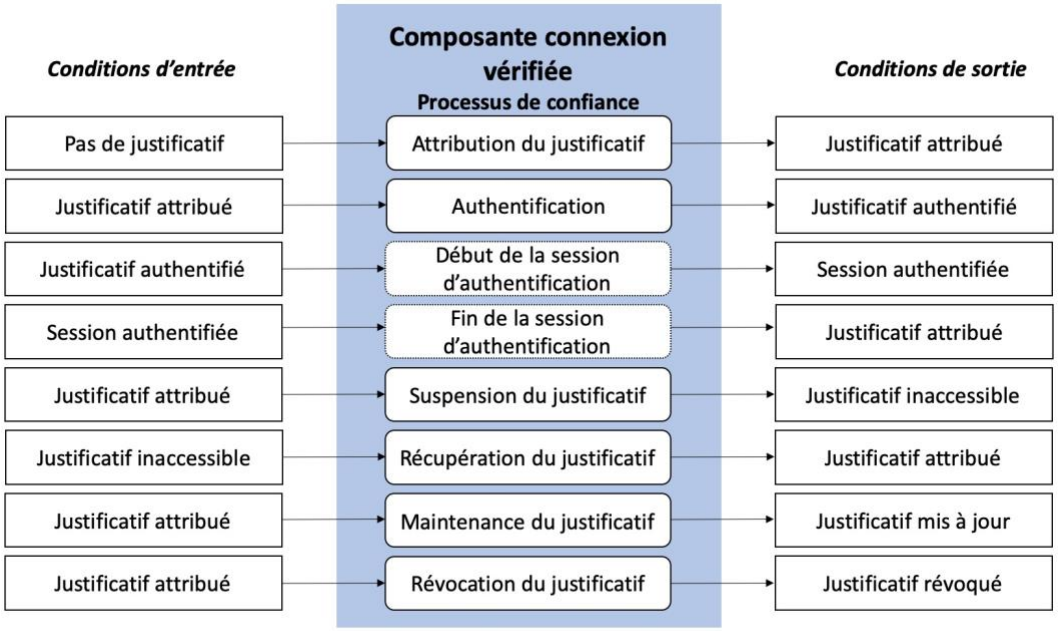

Figure 2. Aperçu conceptuel de la composante connexion vérifiée

3.2 Description des processus

Les sections qui suivent définissent les processus de confiance de la composante connexion vérifiée du cadre de confiance pancanadien. Le profil de conformité de la connexion vérifiée du cadre de confiance pancanadien spécifie les critères de conformité permettant d'évaluer la fiabilité de ces processus.

Les processus de confiance de la connexion vérifiée 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 connexion vérifiée.

3.2.1 Attribution des justificatifs

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

Remarque

- La validation et la vérification de l'identité du sujet ne font pas partie de ce processus. La validation et/ou la vérification de l'identité du sujet sont effectuées, au besoin, dans la composante personne vérifiée du cadre de confiance pancanadien.

Intrants Pas de justificatif – Aucun justificatif n'est attribué au sujet.

Extrants Session authentifiée – Il y a une interaction persistante entre un sujet et un point ultime.
.

Dépendances Authentification

3.2.2 Authentification

L'authentification est définie dans la Ligne directrice sur la définition des exigences en matière d'authentification du gouvernement du Canada (section 1.3) [1] comme étant « le processus d'établissement de la vérité ou de l'authenticité en vue de la génération d'une assurance ». Elle établit la certitude, ou le niveau d'assurance, qu'un sujet contrôle le justificatif qu'il a attribué et que le justificatif est actuellement valide (c.-à-d. qu'il n'est pas suspendu ou révoqué). Dans l'éventualité où un justificatif serait révoqué ou suspendu, l'extrant serait un justificatif révoqué ou inaccessible, respectivement, car les processus de révocation ou de suspension des justificatifs seraient en cause.

Intrants Justificatif attribué – Un justificatif a été attribué, lié à un seul sujet, et lié à un ou plusieurs authentifiants appropriés contrôlés par le sujet.

Extrants Justificatif authentifié – Le sujet a authentifié et prouvé avec succès le contrôle du justificatif au niveau d'assurance spécifié.

Dépendances Attribution du justificatif

3.2.3 Début de la session d'authentification

Une interaction continue est une session entre un sujet et un point ultime, comme un fournisseur de justificatifs ou une partie utilisatrice. Une session peut être nécessaire, par

exemple, pour satisfaire des cas d'utilisation comme une connexion fédérée et unique. Ce processus de confiance est facultatif.

Le début de la session d'authentification doit commencer avec un justificatif authentifié. L'extrant du début de la session authentifiée est une session authentifiée, qui est une interaction continue entre le sujet et un point ultime. 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 et prouvé avec succès le contrôle du justificatif au niveau d'assurance spécifié.
Extrants	Session authentifiée – Il y a une interaction continue entre un sujet et un point ultime.
Dépendances	Authentification

3.2.4 Fin de la session authentifiée

Le processus de fin de session authentifiée est nécessaire quand on utilise des sessions de connexion. 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 un sujet et un point ultime.
Extrants	Justificatif attribué – Un justificatif a été attribué, lié à un sujet unique et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
Dépendances	Début de la session authentifiée

3.2.5 Suspension des justificatifs

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

Intrants	Justificatif attribué – Un justificatif a été attribué, lié à un sujet unique et à un ou plusieurs authentifiants appropriés 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., mot de passe oublié) ou le système (p. ex., verrouillage 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.
Dépendances	Attribution d'un 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.

Intrants	Justificatif inaccessible – Le sujet est actuellement incapable d'utiliser le justificatif. Cela peut être déclenché par le sujet (p. ex., mot de passe oublié) ou le système (p. ex., verrouillage 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.
Extrants	Justificatif attribué – Un justificatif a été attribué, lié à un sujet unique et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
Dépendances	Attribution d'un 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). 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, lié à un sujet unique et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
Extrants	Justificatif attribué (mis à jour) – Un justificatif a été attribué, lié à un sujet unique et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
Dépendances	Authentification de l'attribution du justificatif [2]

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 – Un justificatif a été attribué, lié à un sujet unique et à un ou plusieurs authentifiants appropriés contrôlés par le sujet.
Extrants	Le justificatif est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.
Dépendances	Authentification de l'attribution du justificatif [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 cadre de confiance pancanadien.

Remarque

- Le cas échéant, seul le numéro de version ou publication spécifié dans le présent document s'applique à cette composante du cadre de confiance pancanadien.

Plutôt que de développer des normes entièrement nouvelles, la composante connexion vérifiée du cadre de confiance pancanadien s'inspire et tire parti de l'expérience et des leçons des organisations extérieures au DIACC qui ont élaboré ou sont en train de faire évoluer des processus et normes connexes.

La composante connexion vérifiée du cadre de confiance pancanadien s'est inspirée des normes et documents d'orientation suivants et est basée en partie sur eux :

1. ITSP.30.031 v3 User Authentication Guidance for Information Technology System (ITSP.30.031)
2. NIST 800-63-3 Digital Identity Guidelines (800-63-3, 800-63A, 800-63B et 800-63C)
3. Good Practice Guide No. 44 Authentication and Credentials for use with HMG Online Service (GPG-44)

Cette composante du cadre de confiance pancanadien fait référence aux éléments suivants à titre d'exemple, d'information ou d'illustration :

1. CSEC ITSG-33
2. FIPS 140-2

5 Remarques

1. Source : Gouvernement 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

2. Le processus d'authentification est une dépendance quand le processus est amorcé par un utilisateur.

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 un 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 été envoyé au cellulaire)

Le justificatif :

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

Annexe B : Résumé des conditions des processus de confiance

Le tableau 2 résume les conditions d'entrée et de sortie de la composante connexion vérifiée du cadre de confiance pancanadien.

Condition	Description
Pas de justificatif	Il n'y a pas de justificatif attribué au sujet.
Justificatif attribué	Un justificatif a été attribué, 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., mot de passe oublié) ou le système (p. ex., verrouillage 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 révoqué	Le justificatif est désactivé ou supprimé d'une façon permanente. Il s'agit d'une condition définitive.

Tableau 2. Conditions de la composante connexion vérifiée

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 connexion vérifiée du cadre de confiance pancanadien.

513-a	**Processus de confiance**	**Condition d'entrée**	**Dépendance du processus**	**Condition de sortie**
513-b	**Attribution des justificatifs**	Pas de justificatif	-	Justificatif attribué
513-c	**Authentification**	Justificatif attribué	Attribution des justificatifs	Justificatif authentifié
513-d	**Début de la session d'authentification**	Justificatif authentifié	Authentification	Session d'authentification
513-e	**Fin de la session d'authentification**	Session d'authentification	Lancement de la session d'authentification	Justificatif attribué
513-f	**Suspension des justificatifs**	Justificatif attribué	Attribution des justificatifs	Justificatif inaccessible
513-g	**Récupération des justificatifs**	Justificatif inaccessible	Attribution des justificatifs	Justificatif attribué
513-h	**Maintenance des justificatifs**	Justificatif attribué	Authentification de l'attribution des justificatifs [2]	Justificatif attribué (mis à jour)
513-i	**Révocation des justificatifs**	Justificatif attribué	Authentification de l'attribution des justificatifs [2]	Justificatif révoqué

Tableau 3. Relations du processus de confiance