Document de travail sur l'aperçu du volet connexion vérifiée - version 0.06

Ce document de travail a été préparé 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 ce document de travail 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 inclut des décideurs qui peuvent être ou non des experts dans la technologie des domaines.

Table des matières

1 Aperçu du volet connexion vérifiée

Le volet connexion vérifiée définit un ensemble de processus utilisés pour accéder à des systèmes numériques et un ensemble de critères de conformité pour chaque processus. Ces processus consistent notamment à lier un justificatif à un sujet et des authentificateurs à un justificatif, et comprennent des fonctions de gestion du cycle de vie qui incluent des mises à jour, la récupération et la révocation, et la gestion de sessions. Pour les besoins de la connexion vérifiée, un sujet peut être une personne, une organisation, une application ou un appareil.

Le volet connexion vérifiée a pour objectif d'assurer l'intégrité permanente des processus de connexion en appliquant des critères de conformité uniformisés pour l'évaluation et la certification. La connexion vérifiée est un ensemble de processus visant à donner une certitude et une assurance quant à l'utilisation d'une identité numérique fiable. Un processus certifié est un processus de confiance auquel peuvent se fier les autres participants au cadre de confiance pancanadien.

La figure 1 donne un aperçu conceptuel et montre l'organisation logique du volet connexion vérifiée.

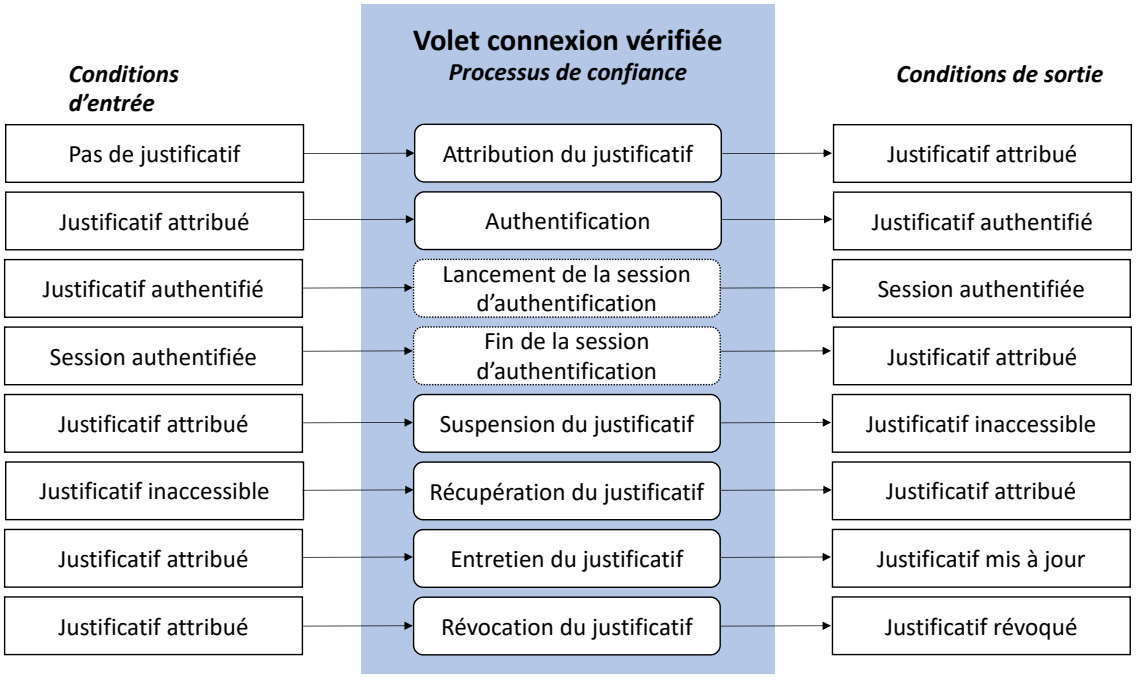

Figure 1. Volet connexion vérifiée

Le volet connexion vérifiée comprend des éléments indiquant ce qui suit :

- **Processus de confiance** – ensemble de processus conformes aux critères (c.-à-d., critères de conformité) spécifiés par le cadre de confiance pancanadien et auxquels les autres peuvent se fier (c.-à-d., faire confiance).
- **Conditions** – états ou circonstances particuliers s'appliquant à la connexion.
- **Intrants** – ce qui est entré dans les processus de confiance, p. ex., un justificatif attribué.
- **Extrants** – résultat des processus de confiance, p. ex., un justificatif authentifié comme ayant un niveau d'assurance spécifique.
- **Dépendances** – relations entre les processus de confiance.
- **Profils** – critères supplémentaires reflétant les exigences ou contraintes qui sont pertinentes à un contexte spécifique (p. ex., industrie, secteur public ou privé). Ils servent à assurer l'uniformité de la mise en œuvre et à faciliter la certification du cadre de confiance pancanadien.

1.1 Relation avec le cadre de confiance pancanadien

Le cadre de confiance pancanadien consiste en une série de composantes modulaires ou fonctionnelles pouvant être évaluées et certifiées indépendamment pour être considérées comme des éléments de confiance. Le cadre de confiance pancanadien, qui mise sur une approche pancanadienne, permet au public et au secteur privé de collaborer pour préserver les identités numériques en uniformisant les processus et les pratiques dans tout l'écosystème numérique canadien.

La figure 2 illustre l'ébauche visuelle du modèle de cadre de confiance pancanadien. Les processus du volet connexion vérifiée sont effectués par les participants dans les catégories « Créer et gérer des identités numériques » et « Utiliser l'identité numérique ».

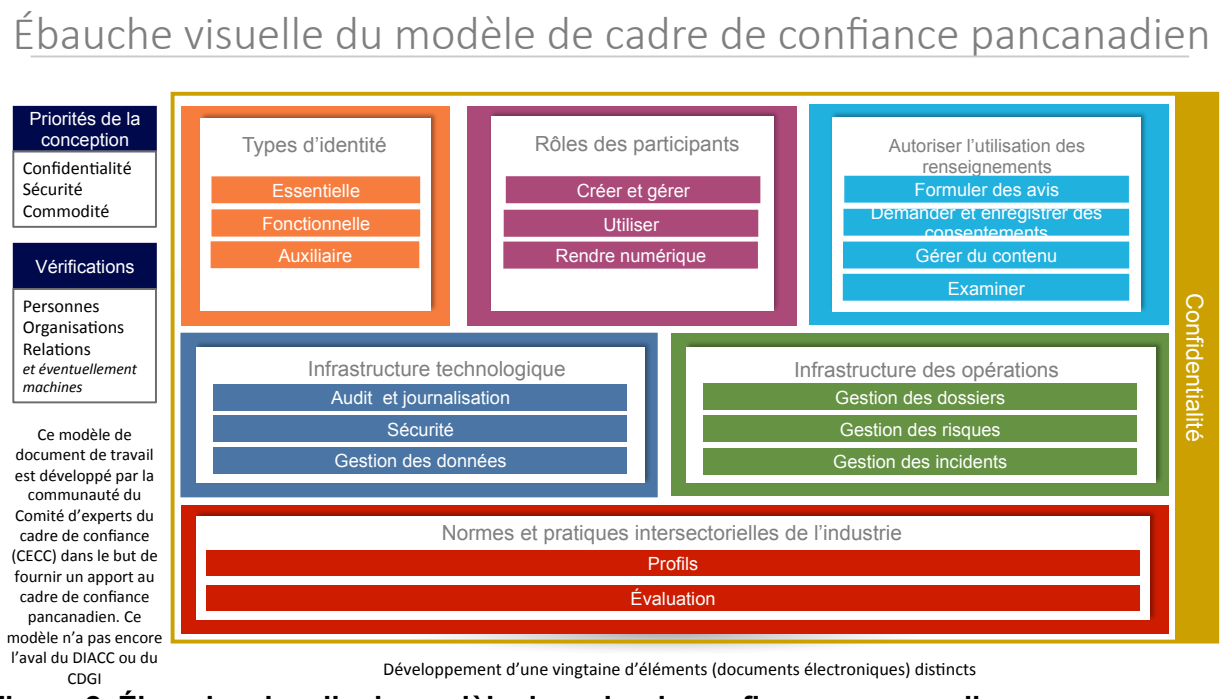

Figure 2. Ébauche visuelle du modèle de cadre de confiance pancanadien

2 Éléments de confiance de la connexion vérifiée

2.1 Processus et conditions de confiance

Un processus de confiance est une activité commerciale ou technique (ou un ensemble de ces activités) qui transforme une condition d'entrée en une condition de sortie. Une condition est un état ou une circonstance en particulier qui est propre à un processus de confiance. Il peut s'agir d'un intrant, d'un extrant et/ou d'une dépendance par rapport à un processus de confiance. Les critères de conformité spécifient ce qui est exigé pour transformer une condition d'entrée en condition de sortie, p. ex., pour qu'un processus d'attribution de justificatifs transforme une condition d'entrée « sans justificatifs » en condition de sortie « avec justificatifs ». Un processus de confiance commercial ou technique de connexion vérifiée est évalué et certifié selon des critères de conformité stipulés par le profil de conformité de la connexion vérifiée et le cadre de confiance pancanadien.

2.2 Processus de confiance de la connexion vérifiée

Le volet connexion vérifiée définit huit processus de confiance :

1. Attribution des justificatifs
2. Authentification
3. Lancement de la session d'authentification
4. Fin de la session d'authentification
5. Suspension des justificatifs
6. Récupération des justificatifs
7. Entretien des justificatifs
8. Révocation des justificatifs

2.2.1 Attribution des justificatifs

L'attribution des justificatifs est un processus d'inscription pendant lequel un justificatif est créé et lié à un ou plusieurs authentificateurs. Les authentificateurs peuvent être attribués pendant ce processus, fournis par le sujet ou par une tierce partie. Les authentificateurs 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.

2.2.2 Authentification

L'authentification est définie dans le modèle d'assurance pancanadien[1] comme étant « le processus consistant à établir la véracité ou l'authenticité pour donner une assurance ». Cela 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).

2.2.3 Lancement de la session d'authentification

Une session permet une interaction continue entre un sujet et un point ultime, par exemple un fournisseur de justificatifs ou une partie dépendante, tout en éliminant le besoin de répéter continuellement le processus d'authentification entre les interactions. Ce processus de confiance est facultatif, mais il peut être nécessaire pour satisfaire certains cas d'utilisation comme une connexion fédérée ou unique. Une session débute quand un justificatif entre dans l'état justificatif authentifié. La session se voit attribuer un niveau d'assurance qui est égal ou inférieur à celui attribué au justificatif correspondant; le niveau d'assurance de la session ne doit pas être supérieur à celui du justificatif.

2.2.4 Fin de la session d'authentification

Le processus de fin de la session d'authentification est nécessaire quand on utilise des sessions de connexion. Une session est terminée avec une déconnexion explicite, une expiration de session en raison d'une inactivité ou d'une durée maximale, ou encore par d'autres moyens.

2.2.5 Suspension des justificatifs

Ce processus transforme un justificatif attribué en justificatif inaccessible, et il peut être amorcé par un utilisateur ultime, un administrateur de système ou automatiquement par le système. Il est interdit de passer un justificatif suspendu à des parties utilisatrices, ce qui assure que le sujet n'y a pas accès.

2.2.6 Récupération des justificatifs

Le processus de récupération des justificatifs permet de rendre utilisable un justificatif inaccessible. Il peut être déclenché par un utilisateur ultime, un administrateur de système ou automatiquement par le système. Exemples :

- Un utilisateur ultime répond correctement aux questions de sécurité pour réinitialiser un mot de passe oublié;
- Un administrateur de système attribue un justificatif qui a été suspendu en raison d'une inactivité;
- Au bout de 24 heures, le système attribue automatiquement un justificatif qui avait été suspendu en raison d'un excès de tentatives d'authentification infructueuse.

2.2.7 Entretien des justificatifs

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

2.2.8 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 ultime, un administrateur de système ou automatiquement par le système.

2.3 Conditions de la connexion vérifiée

2.3.1 Conditions d'entrée et de sortie

Le tableau 1 spécifie les conditions d'entrée et de sortie pour le volet connexion vérifiée.

	Condition	**Description**
154-b	Pas de justificatif	Il n'y a pas de justificatif attribué au sujet.
154-c	Justificatif attribué	Un justificatif a été lié à un seul sujet et les authentificateurs appropriés ont été liés.
154-d	Justificatif authentifié	Le sujet s'est authentifié avec succès et a prouvé qu'il contrôle le justificatif au niveau d'assurance spécifié.
154-e	Session d'authentification	Interaction persistante entre un sujet et un point ultime.
154-f	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'authentifications successives infructueuses, d'une inactivité, d'une activité suspecte, etc.). Il s'agit d'une situation provisoire qui aboutira à l'attribution ou à la révocation du justificatif.
154-g	Justificatif mis à jour	Le justificatif a été mis à jour. Il s'agit d'une situation provisoire qui aboutira à l'attribution ou à la révocation du justificatif.
154-h	Justificatif révoqué	Le justificatif a été désactivé ou supprimé de façon définitive. Il s'agit d'une situation permanente.

Tableau 1. Conditions du volet connexion vérifiée

2.3.2 Dépendances

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 2 spécifie les intrants, extrants et dépendances entre les processus de confiance du volet connexion vérifiée.

	Processus de confiance	Condition d'entrée	Dépendance du processus	Condition de sortie
160-b	**Attribution des justificatifs**	Pas de justificatif	-	Justificatif attribué
160-c	**Authentification**	Justificatif attribué	Attribution des justificatifs	Justificatif authentifié
160-d	**Lancement de la session d'authentification**	Justificatif authentifié	Authentification	Session d'authentification
160-e	**Fin de la session d'authentification**	Session d'authentification	Lancement de la session d'authentification	Justificatif attribué
160-f	**Suspension des justificatifs**	Justificatif attribué	Attribution des justificatifs	Justificatif inaccessible
160-g	**Récupération des justificatifs**	Justificatif inaccessible	Attribution des justificatifs	Justificatif attribué
160-h	**Entretien des justificatifs**	Justificatif attribué	Attribution des justificatifs Authentification[2]	Justificatif mis è jour
160-i	**Révocation des justificatifs**	Justificatif attribué	Attribution des justificatifs Authentification [2]	Justificatif révoqué

Tableau 2. Relations du processus de confiance

3 Niveaux d'assurance

Un niveau d'assurance est une qualification qui doit être appliquée et maintenue pour indiquer un niveau de confiance dans les processus de confiance de la connexion vérifiée. Il est utilisé par les fournisseurs de justificatifs, les parties utilisatrices et les utilisateurs ultimes pour déterminer le degré de confiance qui devrait être attribué à l'accès à un système numérique étant donné le contexte de l'interaction numérique qui en découle.

Le niveau d'assurance indique aussi que les processus du volet connexion vérifiée ont été évalués et/ou certifiés selon les critères de conformité du cadre de confiance. Le tableau 3 montre les quatre niveaux d'assurance définis dans les cadres de confiance existants.

	Niveau d'assurance	Description de la qualification
184-b	Niveau 1 (LOA1)	• Peu ou pas de degré de confiance nécessaire • Conforme aux critères de conformité de niveau 1
184-c	Niveau 2 (LOA2)	• Certain degré (raisonnable) de confiance nécessaire • Conforme aux critères de conformité de niveau 2
184-d	Niveau 3 (LOA3)	• Degré élevé de confiance nécessaire • Conforme aux critères de conformité de niveau 3
184-e	Niveau 4 (LOA4)	• Degré très élevé de confiance nécessaire • Conforme aux critères de conformité de niveau 4

183 **Tableau 3. Niveaux d'assurance**

184 Chaque niveau d'assurance peut être précisé davantage par un qualificateur. Par exemple, une
185 partie dépendante dans le secteur des soins de santé peut spécifier l'exigence pour un
186 justificatif LOA3, et un qualificateur précisera que l'authentificateur doit être attribué par un
187 fournisseur de soins de santé.

188 Le niveau d'assurance qui en résulte pour n'importe quel système de connexion vérifiée est le
189 plus pas associé à un des sept processus de confiance de la connexion vérifié. Ce principe est
190 connu comme le « niveau de basse mer ». Les exigences de chaque niveau d'assurance sont
191 cumulatifs – les niveaux d'assurance successivement plus élevés exigent que les conditions
192 des niveaux d'assurance inférieurs soient aussi remplies.

193 4 Notes et hypothèses

194 **Plus d'une organisation peut être responsable de mener de bout en bout le processus de**
195 **confiance de la connexion vérifiée.**

196 Par exemple, l'attribution des justificatifs peut être la responsabilité d'une organisation, tandis
197 que l'authentification peut incomber à une autre organisation. L'intervention de plusieurs
198 organisations peut compliquer le processus d'évaluation et de certification, mais le cadre de
199 confiance pancanadien n'impose pas d'approches spécifiques en ce qui concerne la mise en
200 œuvre.

201 **Notes de bas de page**

202 [1] Modèle d'assurance pancanadien : https://www.tbs-sct.gc.ca/pol/doc-
203 fra.aspx?id=26262&section=html

204 [2] Le processus d'authentification est une dépendance quand le processus est lancé par un
205 utilisateur ultime.