Ébauche de recommandations sur le modèle de maturité de l'assurance du CCP V1.0

Cette ébauche de recommandations a été préparée par le Comité d'experts du Cadre de confiance (TFEC) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN). Le TFEC est régi par les politiques du CCIAN en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'entente de contributeur du CCIAN.

Le CCIAN 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 CCIAN 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.

Table des matières

1. Conventions documentaires

Dans ce document, les termes *en italiques* (p. ex. *justificatif*) sont définis dans le glossaire du CCP V1.0.

2. Introduction

Il est essentiel que les *participants* à un écosystème numérique aient une façon d'évaluer la robustesse et la fiabilité des transactions effectuées dans cet écosystème. Pour ce faire, les *participants* doivent avoir un vocabulaire commun qui décrit le degré de confiance qu'ils peuvent associer à une *entité* ou transaction, ainsi qu'une façon commune de déterminer ce niveau de confiance.

Dans le Cadre de confiance pancanadien[MC] (CCP), un *niveau d'assurance* (LoA) représente le degré de confiance qu'une *entité* peut avoir dans les processus et autres critères de conformité définis dans une composante du CCP. Les *niveaux d'assurance* sont fondamentaux pour créer des réseaux de confiance. Les modèles de niveaux d'assurance fonctionnent uniquement si tous les *participants* d'un écosystème numérique sont capables de les interpréter d'une manière uniforme. Il est donc essentiel que tous les *participants* d'un écosystème s'entendent sur un ensemble minimum de critères pour chaque *niveau d'assurance*. C'est seulement à ce moment-là qu'une *partie dépendante* de cet écosystème sera capable d'évaluer convenablement les risques inhérents dans une relation ou transaction, et le *niveau d'assurance* qui peut être placé dans les *participants*, les *justificatifs* et ces transactions. Les composantes du CCP décrivent les critères de conformité détaillés qui devraient être utilisés pour évaluer de tels *niveaux d'assurance* dans le contexte d'une composante donnée du CCP. Ce document fournit des conseils sur la façon d'utiliser ces critères afin de classifier convenablement les *niveaux d'assurance*.

2.1 L'approche traditionnelle

Quand le CCP a été introduit, l'approche la plus largement répandue des *niveaux d'assurance* correspondait à la figure 1.

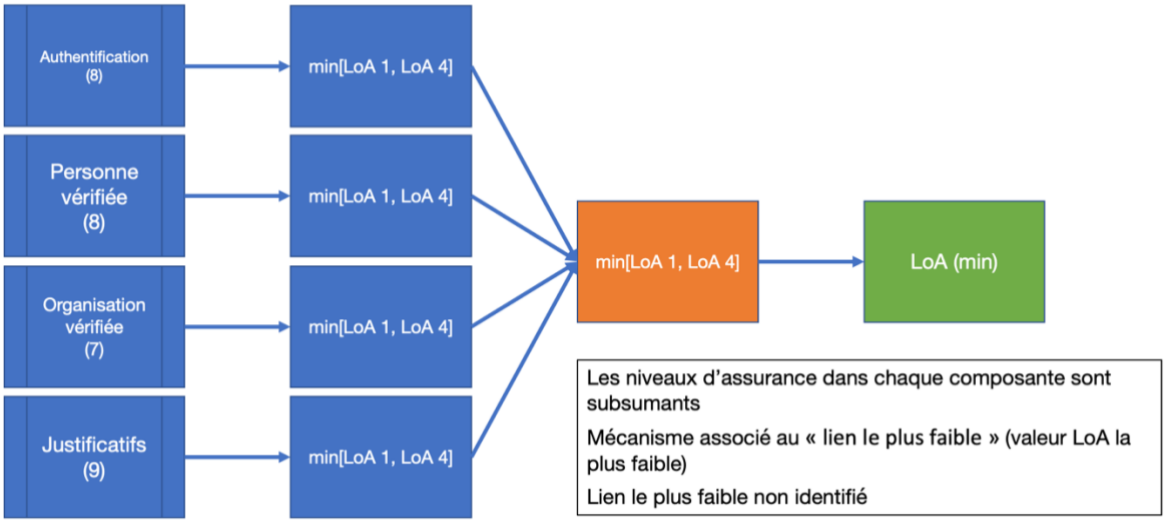

Figure 1 : Modèle de niveaux d'assurance traditionnels

(Remarque : Le chiffre indiqué sous le nom de chaque composante dans la figure 1 correspond au nombre de *processus de confiance* décrits dans cette composante en date de la version 1.0 du CCP.)

Cette approche suit un processus simple en trois étapes pour déterminer le *niveau d'assurance* d'une transaction :

1. Les critères de conformité pertinents de chaque composante sont évalués pour déterminer quel niveau d'assurance a été atteint pour chaque critère.
2. Le *niveau d'assurance* pour une composante spécifique est égal au niveau d'assurance le plus faible établi pour tous les critères pertinents de cette composante du CCP.
3. Le *niveau d'assurance* global est égal au niveau d'assurance le plus faible établi pour l'ensemble des composantes du CCP.

Il s'agit du mécanisme de maillage le plus faible. Autrement dit, le *niveau d'assurance* le plus élevé pouvant être atteint est celui du critère le plus faible.

Prenons, par exemple, un scénario où les critères pertinents sont les suivants :

- Évaluation des critères pour la composante Authentification : critère 1 : LoA 3; critère 2 : LoA 3; critère 3 : LoA 3; critère 4 : LoA 3
- Évaluation des critères pour la composante Personne vérifiée : critère 1 : LoA 3; critère 2 : LoA 3; critère 3 : LoA 2; critère 4 : LoA 3
- Évaluation des critères pour la composante Organisation vérifiée : critère 1 : LoA 3; critère 2 : LoA 3; critère 3 : LoA 3; critère 4 : LoA 3
- Évaluation des critères pour la composante Justificatifs : critère 1 : LoA 3; critère 2 : LoA 3; critère 3 : LoA 1; critère 4 : LoA 3

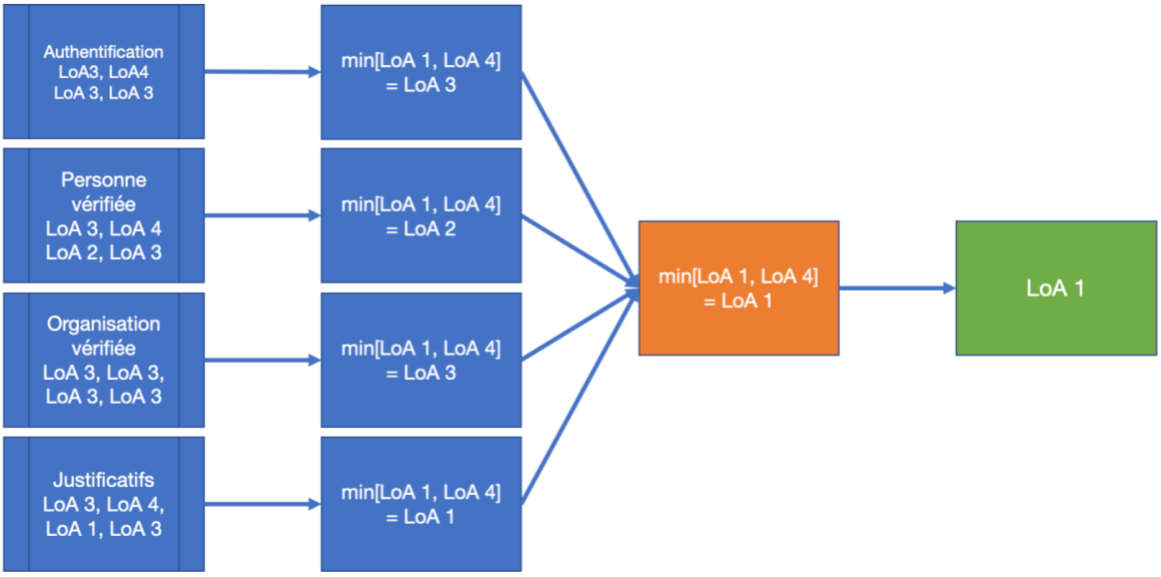

Figure 2 : Exemple d'évaluation utilisant les critères de conformité initiaux du CCP

Comme le montre la figure 2, le *niveau d'assurance* associé au scénario dans ces conditions serait LoA 1, soit le niveau associé aux critères les plus faibles.

Bien qu'il s'agisse du mécanisme de maillage le plus faible, cette approche ne nécessite pas que le ou les liens les plus faibles soient signalés à la *partie dépendante*. Et les liens les plus robustes ne sont pas identifiés. Cela peut poser des défis aux *parties dépendantes* qui essaient d'instaurer une approche de l'assurance basée sur les risques, car elle ne suffit pas lorsqu'il y a de nombreux cas d'utilisation.

2.1.1 Le lanceur d'alerte : Illustration d'un cas d'utilisation

Prenons, par exemple, le cas d'un lanceur d'alerte fictif. Dans notre exemple, quelqu'un a appris qu'un groupe dont il fait partie prend part à une activité illégale, immorale ou qui met même la vie en danger. La personne en question doit signaler cette activité afin de préserver l'intégrité du groupe et de protéger la vie de ceux que cela touche. Elle doit rester anonyme. Le fait de dévoiler son identité peut l'obliger à quitter le groupe, donc l'empêcher de mettre à jour les actes malveillants et, surtout, d'en atténuer les méfaits. De plus, le dévoilement de son identité peut causer des torts irréparables à sa carrière ou à sa capacité de gagner un revenu. Dans des cas extrêmes, cela peut aussi mettre en danger sa vie ou celle de ses amis et de sa famille.

Dans une transaction numérique ordinaire, une question essentielle consiste à se demander « est-ce que je connais cette personne (ou entité) et est-elle celle qu'elle affirme être? ». Toutefois, le *sujet* ne divulguera jamais sa véritable identité. Une fois que cette personne a établi un premier contact et prouvé sa validité en tant qu'initié (p. ex., en fournissant des renseignements vérifiables qui confirment leur provenance),

cette question devient « s'agit-il de la personne avec qui j'ai traité auparavant? ». Une fois que nous lui faisons confiance, nous devons nous assurer entre autres que son compte n'a pas été compromis, que personne n'a usurpé son identité, qu'elle utilise une robuste authentification cryptographique et que l'activité numérique n'est pas vulnérable à une attaque d'un intermédiaire.

Une transaction numérique de cette nature peut comporter les attributs suivants :

- Identité
  - Auto-affirmée, constante à la longue
- Justificatifs
  - Témoins de sessions
  - Appareil connu
  - Secret partagé
  - Clé cryptographique asymétrique
  - Jeton matériel scellé
  - Preuve complète exigée pour chaque émission ou rotation, et révoquée lorsqu'une activité suspecte est décelée
- Présentation de l'assertion
  - Assertion vérifiable signée, passée par un canal d'arrière-plan
  - Assertion cryptée dans la clé de la *partie dépendante*

Même si une transaction ayant ces caractéristiques semble assez robuste pour ce cas de lanceur d'alerte, le fait qu'elle utilise une identité auto-affirmée – que les critères classifient comme une identité de niveau LoA 1 – fera que toute la transaction sera évaluée au niveau LoA 1 dans le cadre de ce mécanisme d'assurance. Par conséquent, elle risquerait d'être évaluée par une *partie dépendante* comme n'étant pas fiable. Étant donné que ce mécanisme donne un seul *niveau d'assurance*, la *partie dépendante* n'aurait aucun moyen de savoir que la transaction est assez robuste pour le cas d'utilisation, ni pourquoi elle a été évaluée comme étant de niveau LoA 1. La partie utilisatrice ne saurait pas que la transaction a été authentifiée au niveau LoA 3 et celle-ci a été globalement évaluée au niveau LoA 1 uniquement en raison du fait que l'identité a été auto-affirmée.

2.1.2 La nécessité d'une approche évolutive

Il y a de nombreux cas d'utilisation où un mécanisme associé au maillon le plus faible comme celui-ci est insuffisant. Mais ce genre de mécanismes ont été largement adoptés et ne peuvent pas être ignorés. Il est donc évident que le CCP exige une approche évolutive qui offre aux *parties dépendantes* une série d'options en matière d'assurance qui leur permet de commencer avec les modèles largement utilisés aujourd'hui et qui évoluent en fonction de leurs propres risques et exigences.

3. Le modèle de maturité de l'assurance du Cadre de confiance pancanadien

Le modèle de maturité de l'assurance du Cadre de confiance pancanadien comprend trois modèles de maturité interopérables :

1. Niveaux d'assurance traditionnels.
2. Niveaux d'assurance discrets.
3. Vecteurs de confiance.

Bien que cela représente un modèle évolutif, précisons que rien n'oblige les praticiens à adopter un de ces modèles. Les praticiens peuvent commencer à n'importe quel stade dans le modèle et passer directement à un autre modèle, et ils n'ont pas besoin d'avoir adopté précédemment un autre modèle.

3.1 Modèle 1 : Niveaux d'assurance traditionnels

Le modèle des niveaux d'assurance traditionnels décrit plus tôt devient la base du modèle de maturité 1. Il s'agit du mécanisme d'assurance le plus largement implanté au moment de la rédaction de ce document et il fournit une rampe d'accès au CCP pour ceux qui ont déjà adopté ce mécanisme.

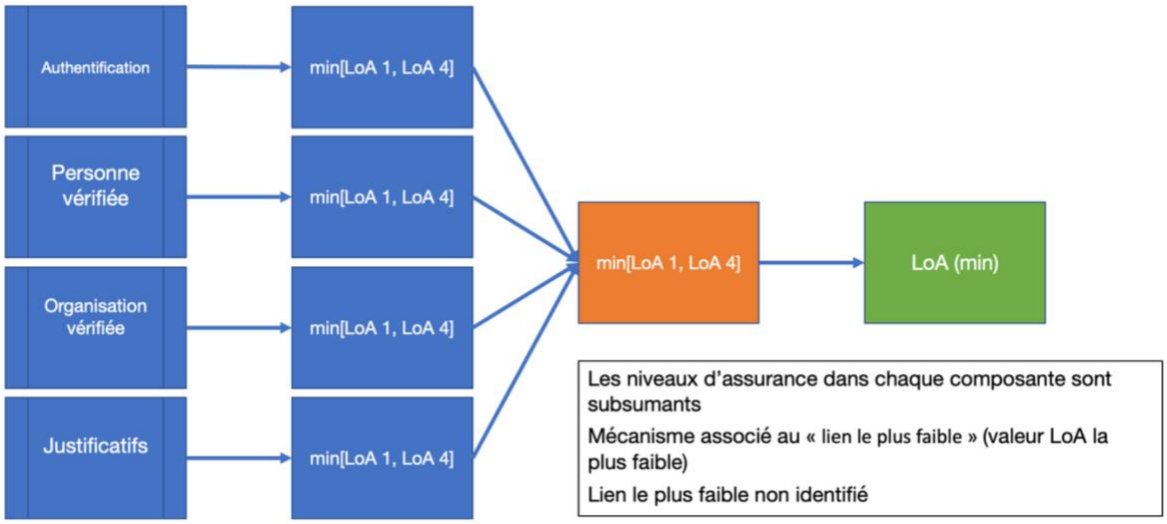

Figure 3 : Niveaux d'assurance traditionnels

Dans ce modèle, les *niveaux d'assurance* varient entre « LoA 1 », le moins fiable, et « LoA 4 », le plus fiable. Le niveau LoA 4 concerne habituellement les cas d'utilisation à très haute sécurité et est principalement utilisé par les praticiens du secteur public. La plupart des profils de conformité de la version 1 du CCP ne définissent pas de critères

de conformité pour le niveau LoA 4. Chaque *niveau d'assurance* est habituellement subsumant et inclut la plupart si ce n'est la totalité des critères pour tous les niveaux qui se trouvent en dessous (c.-à-d., ceux qui ont un plus petit numéro). Dans un mécanisme LoA traditionnel, les niveaux d'assurance sont habituellement caractérisés d'une manière générale, comme le montre la figure 4.

Niveau d'assurance	Description
Niveau 1	• Remplit tous les critères de conformité du niveau 1 pour la composante du CCP appropriée • Peu ou pas de confiance nécessaire • Peu nécessaire d'avoir la certitude qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 2	• Remplit tous les critères de conformité du niveau 2 pour la composante du CCP appropriée • Une certaine confiance nécessaire • Un peu nécessaire d'avoir la certitude qu'une entité a gardé le contrôle d'un justificatif qui lui a été confié et que le justificatif n'a pas été compromis
Niveau 3	• Remplit tous les critères de conformité du niveau 3 pour la composante du CCP appropriée • Haut degré de confiance nécessaire • Particulièrement nécessaire d'avoir la certitude qu'une entité a gardé le contrôle d'un justificatif qui lui a été attribué et que le justificatif n'a pas été compromis
Niveau 4	• Remplit tous les critères de conformité du niveau 3 pour la composante du CCP appropriée • Très haut degré de confiance nécessaire • Hautement nécessaire d'avoir la certitude qu'une entité a gardé le contrôle d'un justificatif qui lui a été attribué et que le justificatif n'a pas été compromis • **Remarque** : La plupart des profils de conformité de la version 1 du CCP ne définissent pas de critères pour le niveau LoA 4.

Figure 4. Niveaux d'assurance (illustration)

(Remarque : Les exemples dans la figure 4 sont fournis à titre illustratif. Veuillez consulter les critères de conformité des composantes du CCP pour avoir de l'information à jour.)

L'évaluation des niveaux d'assurance traditionnels se fait selon un processus en trois étapes :

1. Les critères de conformité pertinents de chaque composante sont évalués afin de déterminer le niveau d'assurance atteint par chaque critère.
2. Le *niveau d'assurance* d'une composante spécifique est égal au niveau d'assurance le plus bas établi pour tous les critères pertinents de cette composante du CCP.
3. Le *niveau d'assurance* global est égal au niveau d'assurance le plus faible établi pour toutes les composantes du CCP.

Il s'agit du mécanisme de maillage le plus faible. Autrement dit, le *niveau d'assurance* le plus élevé pouvant être atteint est celui du critère le plus faible.

3.1.1 Niveaux d'assurance traditionnels et l'exemple du lanceur d'alerte

Si nous poursuivons avec les paramètres discutés dans l'exemple du lanceur d'alerte évoqué plus tôt, le fait que le lanceur d'alerte a présenté une identité auto-affirmée – qui répond aux critères du niveau LoA 1 – fera que la transaction au complet sera évaluée au niveau LoA 1.

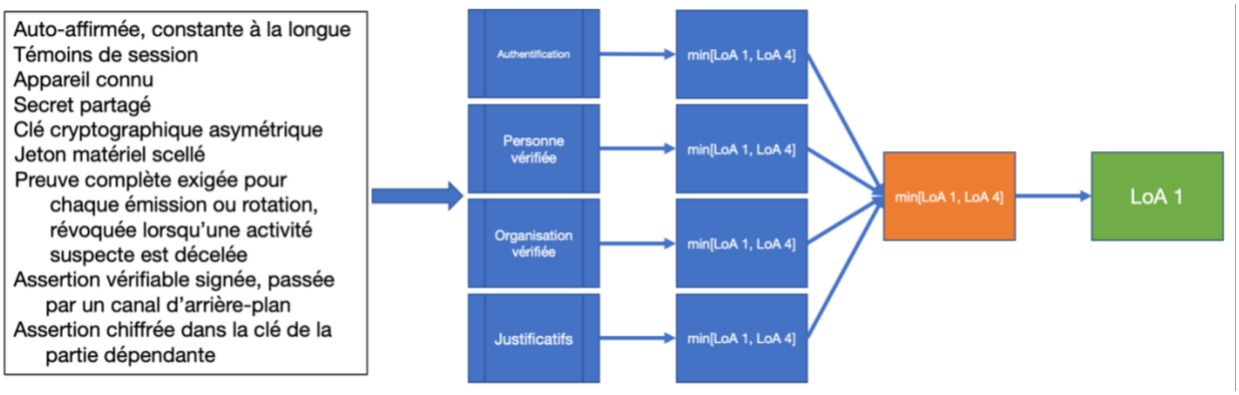

Figure 5 : Exemple du lanceur d'alerte et niveaux d'assurance traditionnels (illustration)

Comme cela a été démontré dans l'application des niveaux d'assurance traditionnels à l'exemple du lanceur d'alerte, le défi d'un mécanisme associé à des niveaux d'assurance traditionnels est qu'il peut être difficile, généralement impossible, pour la *partie dépendante* de déterminer où réside le maillon le plus faible ou encore où se trouvent les forces. Les *parties dépendantes* ont besoin d'une façon d'évaluer d'une

manière indépendante les nombreuses menaces présentes dans un écosystème numérique, notamment :

- Si l'*identité* d'un sujet est constante à la longue.
- S'il est probable qu'un imposteur utilise l'identité.
- Si les *justificatifs* utilisés sont robustes ou vulnérables.
- Si les *justificatifs* utilisés sont bien gérés et des pratiques exemplaires pour l'hygiène des *justificatifs* sont employées.
- Si la transaction a été transmise d'une manière robuste et il est peu probable qu'elle a été assujettie à une mystification ou une divulgation d'information non intentionnelle.

Le deuxième modèle du modèle de maturité de l'assurance du CCP commence à traiter de cela.

3.2 Modèle 2 : Niveaux d'assurance discrets

Le modèle 2 du modèle de maturité introduit des niveaux d'assurance discrets. Un niveau d'assurance discret brise les maillons entre chacune des composantes du mécanisme d'assurance et permet une évaluation indépendante des niveaux d'assurance de l'authentification (AAL), des niveaux d'assurance de l'identité (IAL) et des niveaux d'assurance des justificatifs (CAL). Il met plus d'emphase sur les exigences de la *partie dépendante* en portant davantage attention à l'analyse des menaces et risques. Il aligne aussi les critères de conformité sur les risques identifiés pour la *partie dépendante* et s'assure qu'ils sont évalués d'une manière qui correspond à ces risques.

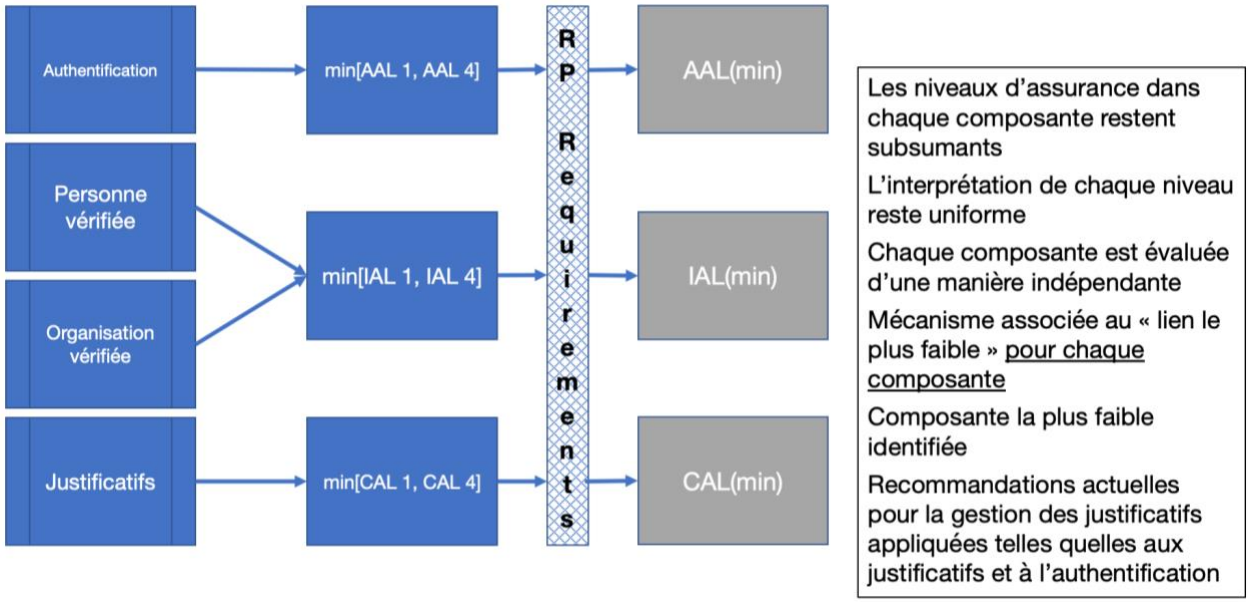

Figure 6 : Niveaux d'assurance discrets

L'évaluation des niveaux d'assurance discrets est la suivante :

1. Les critères de conformité pertinents dans chaque composante sont évalués afin de déterminer le niveau d'assurance atteint pour chaque critère.
2. Le *niveau d'assurance* pour une composante spécifique est égal au niveau d'assurance le plus faible établi pour l'ensemble des critères pertinents de cette composante du CCP.
3. Le *niveau d'assurance* de chaque composante est déclaré d'une manière indépendante.

La caractérisation des niveaux d'assurance discrets demeure conforme aux caractéristiques indiquées dans la figure 4, bien que chaque composante soit caractérisée indépendamment des autres. Même s'il semble dans la figure 6 que l'évaluation d'une personne vérifiée et d'une organisation vérifiée soient combinées dans l'évaluation d'un niveau IAL, une *entité* serait soit une personne vérifiée soit une organisation vérifiée, mais pas les deux. Par conséquent, une seule s'appliquerait à une *entité* et serait prise en considération pendant l'évaluation de son niveau IAL.

Remarque : La plupart des profils de conformité de la version 1 du CCP ne fournissent pas de critères de conformité pour l'assurance au niveau 4.

L'approche selon des niveaux d'assurance discrets est très similaire à celle des niveaux d'assurance traditionnels, bien qu'elle possède quelques avantages importants. Elle élimine l'approche basée sur le maillon le plus faible des *niveaux d'assurance* qu'on retrouve dans l'approche traditionnelle et permet aux *parties dépendantes* de tenir indépendamment compte de la force et de la robustesse de chaque composante d'une transaction numérique. Elle met aussi l'emphase sur l'évaluation des risques dans le contexte de chaque *partie dépendante*. Pour illustrer les différences, revenons l'exemple du lanceur d'alerte.

3.2.1 Niveaux d'assurance discrets et l'exemple du lanceur d'alerte

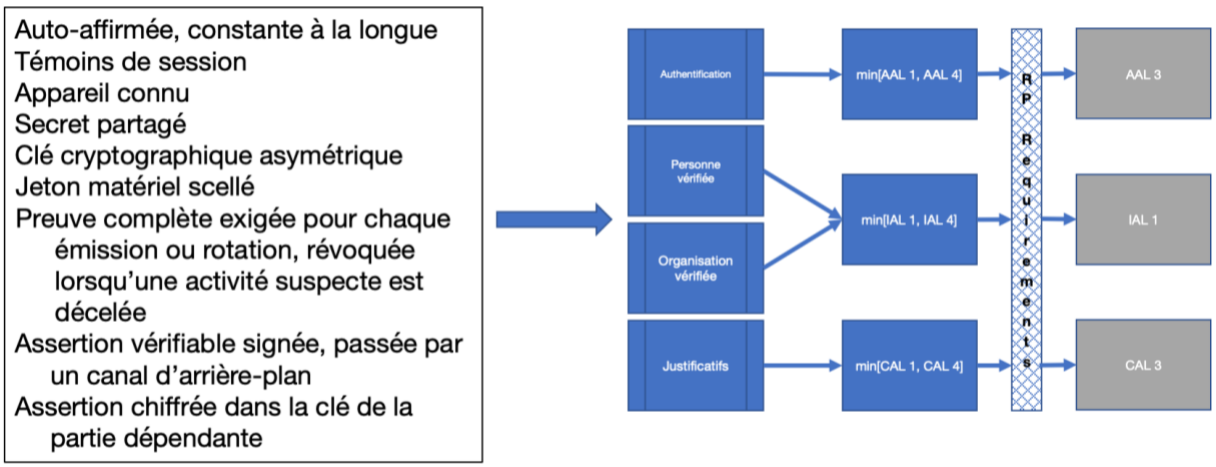

Figure 7 : Exemple du lanceur d'alerte et niveaux d'assurance discrets (illustration)

En utilisant l'approche selon les niveaux d'assurance discrets pour évaluer ces paramètres, la *partie dépendante* est à présent en mesure de comprendre que, même si la preuve d'identité a été évaluée au plus bas *niveau d'assurance* (IAL 1), le lanceur d'alerte utilise un justificatif très robuste (CAL 3) avec une authentification robuste (AAL 3). Cela lui donne de l'information essentielle pour l'aider à répondre à la question posée plus tôt : « S'agit-il de la même personne avec qui j'ai traité? ».

Un avantage essentiel de l'approche selon les niveaux d'assurance discrets c'est qu'elle peut être mise en place en évaluant les critères de conformité existants du CCP. D'une certaine façon, elle donne une meilleure acuité en éliminant une étape de l'approche des niveaux d'assurance traditionnels (c.-à-d., agrégation et réduction des composantes).

3.3 Modèle 3 : Vecteurs de confiance

Bien que l'approche selon les niveaux d'assurance discrets fournit nettement plus d'acuité et de flexibilité qu'une approche selon les niveaux d'assurance traditionnels, il s'agit, tout comme le mécanisme associé aux niveaux d'assurance traditionnels, d'une approche agrégée qui n'identifie pas spécifiquement la raison d'être d'un *niveau d'assurance* attribué, le maillon le plus faible et les forces spécifiques. Par exemple, même si dans l'exemple du lanceur d'alerte, elle fournit une meilleure information du fait que la *partie dépendante* sait que les niveaux AAL et CAL sont robustes, et que l'identité est la composante la plus faible, elle n'indique pas à la *partie dépendante* quel aspect de l'identité est faible. La *partie dépendante* peut ne pas savoir que l'identité est constante à la longue, ce qui est une considération importante dans l'exemple et essentielle pour répondre à la question « s'agit-il de la personne avec laquelle j'ai traité par le passé? ».

Ce n'est qu'un exemple de scénario qui illustre le besoin immédiat de pouvoir évaluer indépendamment différentes menaces. Le modèle de maturité de l'assurance du CCP répond à ce besoin dans son troisième modèle de maturité : les vecteurs de confiance.

L'approche de l'assurance selon les vecteurs de confiance fournit des renseignements détaillés à propos des vecteurs de menaces potentielles d'une transaction. Cela fournit à la *partie dépendante* l'information qui lui permet de mieux évaluer le risque associé à une transaction et qui est nettement plus exploitable.

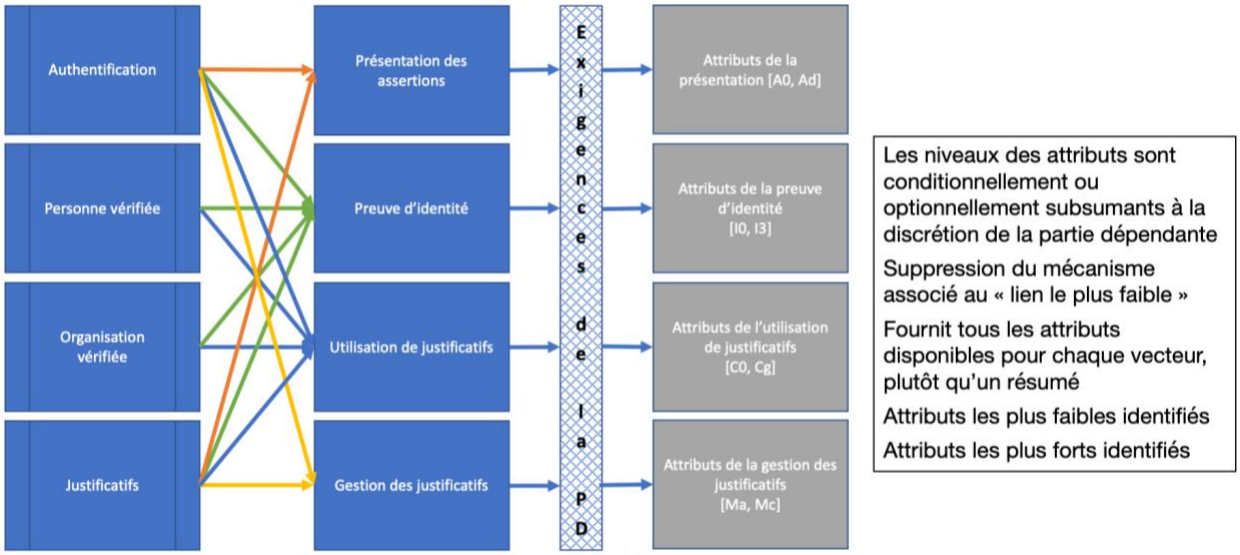

Figure 8 : Modèle d'assurance des vecteurs de confiance

Le mécanisme associé aux vecteurs de confiance du CCP inclut des détails relatifs à quatre nouveaux vecteurs, comme le montre la figure 9.

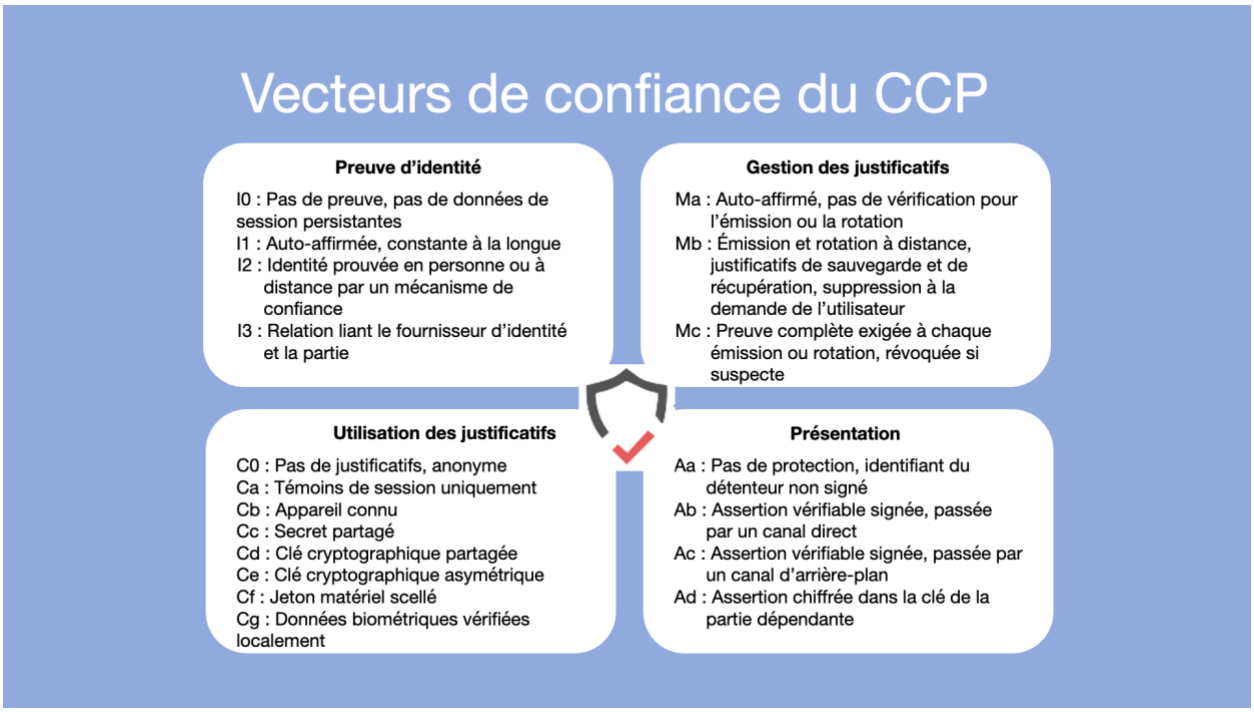

Figure 9 : Vecteurs de confiance du CCP (nouveau)

L'approche de l'assurance selon les vecteurs de confiance :

- Permet à la *partie dépendante* d'évaluer le risque avec plus d'acuité que les mécanismes associés aux niveaux d'assurance traditionnels et discrets.
- Permet aux *parties dépendantes* de décider quelles composantes sont pertinentes à leurs risques ou de demander uniquement les composantes dont elles ont besoin.
- Est flexible à mettre en œuvre.
- Peut être cartographiée selon les mécanismes associés aux niveaux d'assurance traditionnels et discrets pour une question d'interopérabilité.
- N'est pas assujettie à des incohérences dans l'évaluation des niveaux d'assurance ou une dérive des niveaux d'assurance.
- N'a pas besoin de recalibrage pour tenir compte des nouvelles technologies et des pratiques exemplaires.
- Fournit des précisions sur les forces et les faiblesses spécifiques d'une transaction.
- Est extensible à mesure que le CCP se développe.
- Est conçue pour évoluer avec les nouvelles technologies et pratiques exemplaires.

Le CCP fournit un ensemble de vecteurs et d'attributs de base, mais les *parties dépendantes* et les *participants* peuvent négocier des attributs spécifiques qui répondent le mieux à leurs besoins et s'attaquent à leurs risques spécifiques. Cela peut inclure des composantes vectorielles supplémentaires et certaines, la totalité ou aucune des composantes vectorielles de base.

3.3.1 Vecteurs de confiance et l'exemple du lanceur d'alerte

L'approche reliée aux vecteurs de confiance exprime l'assurance d'une façon très différente de celles reliées aux niveaux d'assurance traditionnels et discrets. Au lieu de fournir une seule mesure composite des niveaux d'assurance, comme c'est le cas d'un mécanisme associé à des niveaux d'assurance traditionnels, ou quatre mesures composites des niveaux d'assurance dans le cas d'un mécanisme associé à des niveaux d'assurance discrets, un mécanisme relié à des vecteurs de confiance fournit un seul vecteur qui contient une expression de chaque composante pertinente à la transaction. Pour montrer comment cela fonctionne, revenons à l'exemple du lanceur d'alerte.

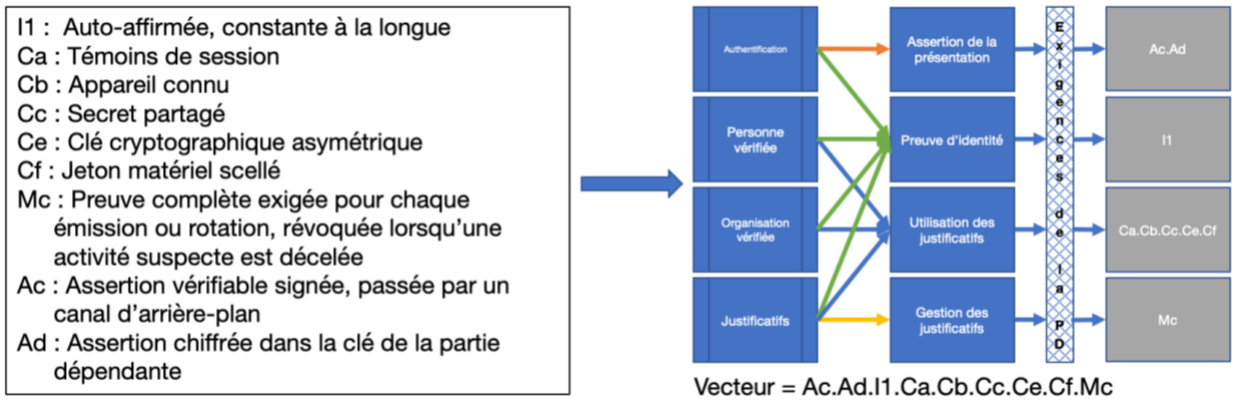

Figure 10 : Exemple du lanceur d'alerte et vecteurs de confiance (illustration)

Selon l'approche associée aux vecteurs de confiance, la *partie dépendante* reçoit le vecteur « Ac.Ad.I1.Ca.Cb.Cc.Ce.Cf.Mc ». Ce vecteur est interprété à l'aide du mécanisme illustré dans la figure 10, comme suit :

- Authentification
  - Ac : Assertion vérifiable signée, passée par un canal d'arrière-plan
  - Ad : Assertion chiffrée dans la clé de la *partie dépendante*
- Identité
  - I1 : Auto-affirmée, constante à la longue
- Utilisation de justificatifs
  - Ca : Témoins de session
  - Cb : Appareil connu
  - Cc : Secret partagé
  - Ce : Clé cryptographique asymétrique
  - Cf : Jeton matériel scellé
- Gestion des justificatifs
  - Mc : Vérification complète requise pour chaque émission ou rotation, révoquée lorsqu'une activité suspecte est décelée

Avec ce niveau de détail, la *partie dépendante* peut déterminer clairement, en fonction de ses propres priorités et tolérances au risque, si elle peut se fier à cette transaction. Elle peut répondre à coup sûr à la question « est-ce probable qu'il s'agisse de la personne avec qui j'ai traité auparavant? ».

3.3.2 Interopérabilité avec la mise en œuvre des modèles 1 et 2 : Vecteurs de confiance des composantes du CCP

Lorsque ce document a été créé, les niveaux d'assurance traditionnels et discrets étaient les mécanismes d'assurance les plus couramment mis en place, le niveau d'assurance traditionnel étant le modèle le plus fréquemment rencontré. Étant donné que ce modèle de maturité a, entre autres, pour objectif de permettre aux *entités* utilisant les trois mécanismes de collaborer, il y a un besoin d'interopérabilité entre ces

modèles et les vecteurs de confiance du CCP. C'est pourquoi le mécanisme associé aux vecteurs de confiance du CCP inclut aussi sept dimensions spécifiques, chacune étant alignée sur une composante du CCP (tableau 1).

Nom de la composante du CCP	Symbole de démarcation	Valeurs définies	Remarques
Authentification	T	0, 1, 2, 3, 4	La valeur numérique correspond au niveau d'assurance atteint avec le modèle 1 ou 2
Personne vérifiée	H	0, 1, 2, 3, 4	La valeur numérique correspond au niveau d'assurance atteint avec le modèle 1 ou 2
Organisation vérifiée	O	0, 1, 2, 3, 4	La valeur numérique correspond au niveau d'assurance atteint avec le modèle 1 ou 2
Justificatifs (relations et attributs)	R	0, 1, 2, 3, 4	La valeur numérique correspond au niveau d'assurance atteint avec le modèle 1 ou 2
Respect de la vie privée	V	0, 1	0 = Non conforme; 1 = Conforme
Avis et consentement	N	0, 1	0 = Non conforme; 1 = Conforme
Infrastructure (technologie et opérations)	S	0, 1	0 = Non conforme; 1 = Conforme

Figure 11 : Dimensions et valeurs définies des vecteurs de confiance des composantes du CCP

L'utilisation des vecteurs de confiance des composantes du CCP permet aux *entités* et aux *parties dépendantes* d'utiliser le modèle 1 ou 2 pour continuer d'évaluer et d'établir le risque sans faire de modification, tout en fournissant un niveau d'acuité supplémentaire à ceux qui utilisent le modèle 3.

3.3.3 Explication des vecteurs de confiance des composantes du CCP

3.3.3.1 Authentification (« T »)

La dimension d'authentification des vecteurs de confiance du CCP devrait exprimer la valeur du niveau d'assurance le plus faible établi selon les critères de conformité de la composante Authentification du CCP. Par exemple, une évaluation de la conformité du niveau LoA 2 d'après les critères de conformité de la composante Authentification serait exprimée comme « T2 ». La valeur « T0 » peut être utilisée pour documenter une évaluation qui n'a pas trouvé de conformité avec aucun des niveaux d'assurance définis par la composante Authentification. Si une évaluation de la conformité d'après la composante Authentification n'a pas été effectuée, une composante « T » ne doit pas être incluse dans un vecteur.

3.3.3.2 Personne vérifiée (« H »)

La dimension Personne vérifiée des vecteurs de confiance du CCP devrait exprimer la valeur du niveau d'assurance le plus faible établie d'après les critères de conformité de la composante Personne vérifiée du CCP. Par exemple, une évaluation de conformité de niveau LOA 2 d'après les critères de conformité de la composante Personne vérifiée serait exprimée comme « H2 ». La valeur « H0 » peut être utilisée pour documenter une évaluation qui n'a pas trouvé de conformité avec aucun niveau d'assurance défini par la composante Personne vérifiée. Si une évaluation de conformité d'après la composante Personne vérifiée n'a pas été effectuée, une composante « H » ne doit pas être incluse dans un vecteur.

3.3.3.3 Organisation vérifiée (« O »)

La dimension Organisation vérifiée des vecteurs de confiance du CCP devrait exprimer la valeur du niveau d'assurance le plus faible établie d'après les critères de conformité de la composante Organisation vérifiée du CCP. Par exemple, une évaluation de la conformité de niveau LOA 2 d'après les critères de conformité de la composante Organisation vérifiée serait exprimée comme « O2 ». La valeur « O0 » peut être utilisée pour documenter une évaluation qui n'a pas trouvé de conformité avec aucun niveau d'assurance défini par la composante Organisation vérifiée. Si une évaluation de la conformité d'après la composante Organisation vérifiée n'a pas été effectuée, une composante « O » ne doit pas être incluse dans un vecteur.

3.3.3.4 Justificatifs (relations et attributs) (« R »)

La dimension Justificatifs (relations et attributs) des vecteurs de confiance du CCP devrait exprimer la valeur du niveau d'assurance le plus faible établie d'après les critères de conformité de la composante Justificatifs (relations et attributs) du CCP. Par exemple, une évaluation de la conformité de niveau CAL 2 d'après les critères de conformité de la composante Justificatifs (relations et attributs) serait exprimée comme « R2 ». La valeur « R0 » peut être utilisée pour documenter une évaluation qui n'a pas trouvé de conformité avec aucun niveau d'assurance défini par la composante Justificatifs (relations et attributs). Si une évaluation de la conformité d'après la composante Justificatifs (relations et attributs) n'a pas été effectuée, une composante « R » ne doit pas être incluse dans un vecteur.

3.3.3.5 Protection de la vie privée (« V »)

La dimension Protection de la vie privée des vecteurs de confiance du CCP devrait exprimer la conformité qui a été établie d'après les critères de la composante Protection de la vie privée du CCP. Par exemple, une évaluation de la « conformité » serait exprimée comme « V1 ». La valeur « V0 » peut être utilisée pour documenter une évaluation « non conforme » à la composante Protection de la vie privée. Si une évaluation de la conformité d'après la composante Protection de la vie privée n'a pas été effectuée, une composante « V » ne doit pas être incluse dans un vecteur.

3.3.3.6 Avis et consentement (« N »)

La dimension Avis et consentement des vecteurs de confiance du CCP devrait exprimer le fait que la conformité a été établir d'après les critères de la composante Avis et consentement du CCP. Par exemple, une évaluation « conforme » serait exprimée comme « N1 ». La valeur « N0 » peut servir à documenter une évaluation « non conforme » à la composante Avis et consentement. Si aucune évaluation de la conformité par rapport à la composante Avis et consentement n'a été effectuée, une composante « N » ne doit pas être incluse dans un vecteur.

3.3.3.7 Infrastructure (technologie et opérations) (« S »)

La dimension Infrastructure (technologie et opérations) des vecteurs de confiance du CCP devrait exprimer le fait que la conformité a été évaluée d'après les critères de la composante Infrastructure (technologie et opérations) du CCP. Par exemple, une évaluation de « conformité » serait exprimée comme « S1 ». La valeur « S0 » peut être utilisée pour documenter une évaluation « non conforme » de la composante Infrastructure (technologie et opérations). Si une évaluation de conformité d'après la composante Protection de la vie privée n'a pas été effectuée, une composante « S » ne doit pas être incluse dans un vecteur.

3.3.4 Vecteurs de confiance des composantes du CCP et l'exemple du lanceur d'alerte

Pour revenir à notre exemple du lanceur d'alerte, les vecteurs de confiance des composantes du CCP seraient évalués comme le montre la figure 12.

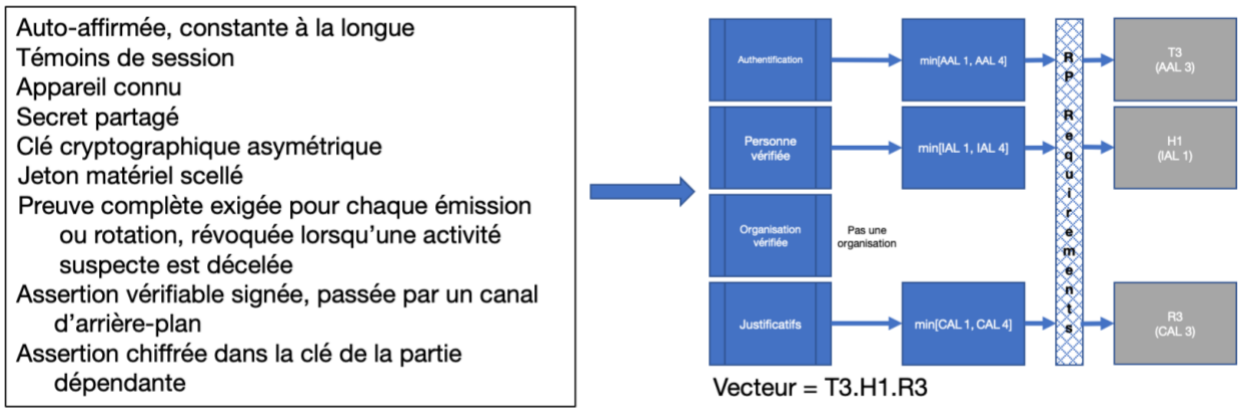

Figure 12 : Exemple du lanceur d'alerte et vecteurs de confiance des composantes (illustration)

En utilisant l'approche des vecteurs de confiance, la *partie dépendante* se voit attribuer le vecteur « T3.H1.R3 ». Ce vecteur est interprété à l'aide du schéma illustré à la figure 12, comme suit :

- Authentification
  - T3 : Établi au niveau LOA 3 ou AAL 3 du CCP – le système a utilisé de robustes processus d'authentification
- Personne vérifiée
  - H1 : Établi au niveau LOA 1 ou IAL 1 du CCP – le système ne connaît pas l'identité de la personne, bien qu'il suppose que c'est la même personne avec laquelle il a traité précédemment
- Organisation vérifiée
  - Étant donné qu'il n'y a pas d'organisation impliquée, la conformité à l'organisation vérifiée n'a pas été évaluée ni incluse
- Justificatifs (relations et attributs)
  - R3 : Établi au niveau LOA 3 ou CAL 3 du CCP – le système a utilisé de robustes processus pour documenter un attribut (p. ex. caractéristique ou qualificatif) de la personne
- Protection de la vie privée
  - La conformité n'a pas été établie
- Avis et consentement
  - La conformité n'a pas été établie
- Infrastructure (technologie et opérations)
  - La conformité n'a pas été établie

Avec ce niveau de détail, la *partie dépendante* peut clairement déterminer, en fonction de ses propres priorités et tolérance au risque, si elle peut faire confiance à cette transaction. Par conséquent, elle peut tout à fait répondre à la question « Est-ce probable qu'il s'agisse de la personne avec qui j'ai déjà traité? ».

4. Soutien concurrent pour tous les modèles de maturité

Notre capacité à utiliser l'exemple du lanceur d'alerte pour les trois modèles de maturité, quoique avec des résultats qui s'améliorent régulièrement, est annonciatrice de celle qu'a le CCP de soutenir simultanément les trois modèles de maturité.

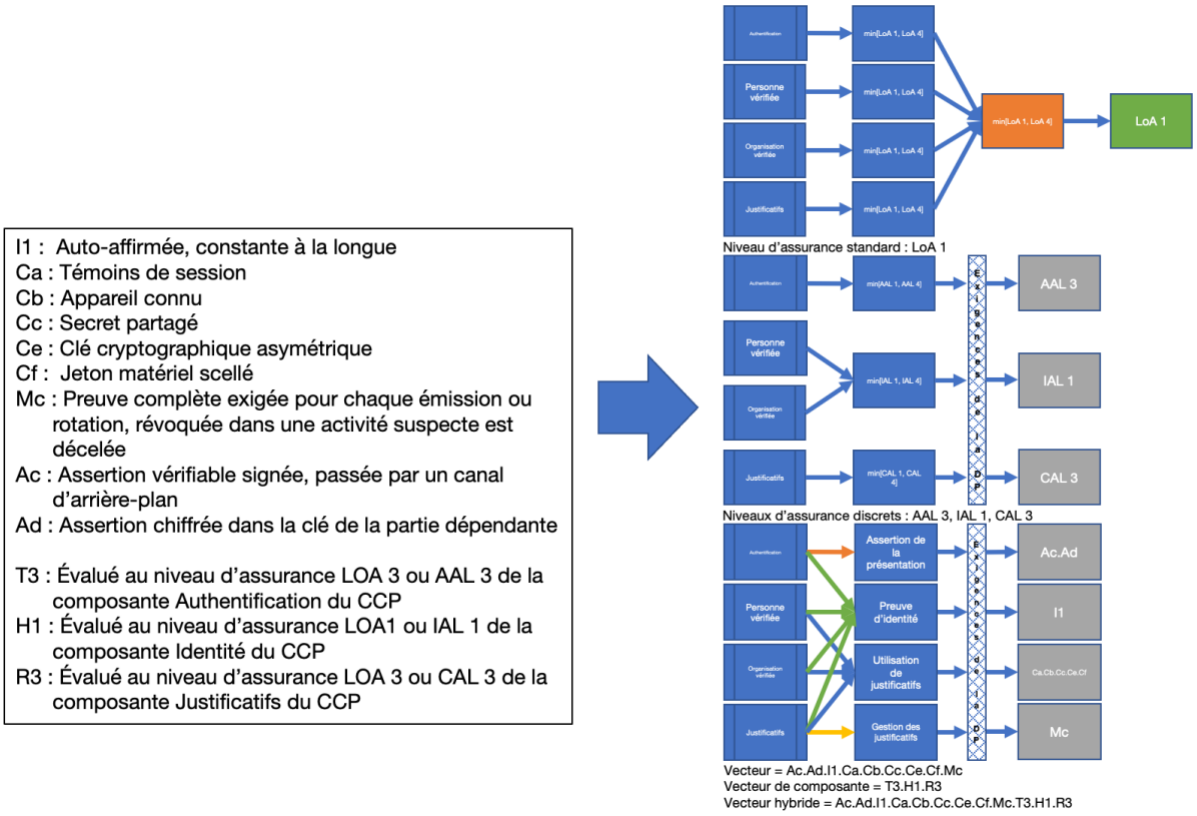

Figure 13 : Les trois modèles du modèle de maturité de l'assurance du CCP et l'exemple du lanceur d'alerte (illustration)

Le mécanisme illustré dans la figure 13 donne aux participants la flexibilité d'utiliser n'importe lequel des trois modèles décrits dans ce document. De plus, les participants à un écosystème peuvent s'entendre pour présenter et/ou recevoir un vecteur hybride qui permettra aux autres participants d'évaluer le niveau d'assurance d'une transaction à l'aide de n'importe lequel des trois modèles. Par exemple, le vecteur hybride présenté à la figure 13 peut être interprété selon les trois façons suivantes :

1. **Niveau d'assurance traditionnel (modèle 1) : LOA 1** = Min[T3 (Authentification LOA 3), H1 (Identité LOA 1), R3 (Justificatif LOA 3)]
2. **Niveau d'assurance discret (modèle 2) : AAL 3; IAL 1; CAL 3** = T3(AAL 3).H1(IAL 1).R3(CAL 3)

3. **Vecteurs de confiance (modèle 3) : Ac.Ad.I1.Ca.Cb.Cc.Ce.Cf.Mc** = Les éléments T, H et R des composantes du CCP ont été ignorés

5. Mappage des trois modèles

Une clarification du mappage des trois modèles de maturité suit. Ce mappage aidera les praticiens à travailler ensemble, mais c'est au final la *partie dépendante* qui évalue son propre niveau de risque et qui décide en dernier lieu si elle peut, ou devrait, faire confiance à une transaction.

Remarque : Ces mappages sont des illustrations et ne visent pas à définir des équivalences rigoureuses. Les résultats d'une évaluation dans le contexte du CCP devraient être documentés conformément à la composante Évaluation du CCP et ils peuvent inclure une expression d'assurance conformément à un ou plusieurs modèles d'assurance présentés ici.

Dans les tableaux qui suivent :

- Le « modèle d'assurance traditionnel » fournit le niveau d'assurance le plus élevé possible qui correspond aux « caractéristiques à prendre en considération ».
- Le « modèle d'assurance discret » fournit le niveau d'assurance le plus élevé possible qui correspond aux « caractéristiques à prendre en considération ».
- La « composante vectorielle » fournit le vecteur des composantes du CCP qui correspond aux « caractéristiques à prendre en considération ».
- Les « caractéristiques à prendre en considération » documentent les caractéristiques importantes du système ou de la transaction qui correspondent aux valeurs suggérées dans les autres colonnes de la même rangée.

Comme dans l'exemple ci-dessus et dans la section décrivant le modèle 1, le niveau d'assurance traditionnel global est calculé en prenant le niveau d'assurance traditionnel le plus bas établi pour toutes les composantes évaluées.

Remarque : Même si toutes les cartes ci-dessous incluent un mappage vers le niveau LoA 4, les composantes du CCP n'incluent pas toutes des critères de conformité du niveau LoA 4. Même si le résultat indique que ce n'est actuellement pas possible d'évaluer un niveau d'assurance traditionnel supérieur à 3 dans ce genre de cas, les mappages de niveau LoA 4 étaient inclus pour tenir compte de l'amélioration future de ces composantes.

5.1 Mappage des composantes du CCP

5.1.1 Mappage de la composante Authentification

Modèle d'assurance traditionnel	Modèle d'assurance discret	Composante vectorielle	Caractéristiques à prendre en considération
Non spécifié	Non spécifié	Non spécifiée	• Aucune évaluation de la conformité aux critères de conformité de la composante Authentification du CCP n'a été faite
Non spécifié	Non spécifié	T0	• Aucune authentification conforme à un niveau d'assurance de la composante Authentification du CCP n'a été faite
LoA 1	AAL 1	T1	• Une authentification conforme aux critères de conformité LoA 1 de la composante Authentification du CCP a été faite
LoA 2	AAL 2	T2	• Une authentification conforme aux critères de conformité LoA 2 de la composante Authentification du CCP a été faite
LoA 3	AAL 3	T3	• Une authentification conforme aux critères de conformité LoA 3 de la composante Authentification du CCP a été faite

LoA 4	AAL 4	T4	• Une authentification conforme aux critères de conformité LoA 4 de la composante Authentification du CCP a été faite • **Remarque** : Le profil de conformité de la composante Authentification du CCP V1.0 ne définit pas les critères de conformité pour le niveau LoA 4.

562 **Figure 14 : Mappage de la composante Authentification**

563 ### 5.1.2 Mappage de la composante Personne vérifiée

Modèle d'assurance traditionnel	Modèle d'assurance discret	Composante vectorielle	Caractéristiques à prendre en considération
Non spécifié	Non spécifié	Non spécifiée	• Aucune évaluation des critères de conformité de la composante Personne vérifiée du CCP n'a été faite
Non spécifié	Non spécifié	H0	• Aucune preuve d'identité n'est conforme aux critères de la composante Personne vérifiée du CCP
LoA 1	IAL 1	H1	• Conforme aux critères de conformité LoA 1 de la composante Personne vérifiée du CCP
LoA 2	IAL 2	H2	• Conforme aux critères de conformité LoA 2 de la composante Personne vérifiée du CCP

LoA 3	IAL 3	H3	• Conforme aux critères de conformité LoA 3 de la composante Personne vérifiée du CCP
LoA 4	IAL 4	H4	• Conforme aux critères de conformité LoA 4 de la composante Personne vérifiée du CCP • **Remarque** : Le profil de conformité de la composante Personne vérifiée du CCP V1.0 ne définit pas les critères de conformité pour le niveau LoA 4.

564 **Figure 15 : Mappage de la composante Personne vérifiée**

565 5.1.3 Mappage de la composante Organisation vérifiée

Modèle d'assurance traditionnel	Modèle d'assurance discret	Composante vectorielle	Caractéristiques à prendre en considération
Non spécifié	Non spécifié	Non spécifiée	• Aucune évaluation des critères de conformité de la composante Organisation vérifiée du CCP n'a été faite
Non spécifié	Non spécifié	O0	• Aucune preuve d'identité n'est conforme aux critères de conformité de la composante Organisation vérifiée du CCP
LoA 1	IAL1	O1	• Conforme aux critères de conformité LoA 1 de la composante Organisation vérifiée du CCP

LoA 2	IAL2	O2	• Conforme aux critères de conformité LoA 2 de la composante Organisation vérifiée du CCP
LoA 3	IAL3	O3	• Conforme aux critères de conformité LoA 3 de la composante Organisation vérifiée du CCP
LoA 4	IAL4	O4	• Conforme aux critères de conformité LoA 4 de la composante Organisation vérifiée du CCP • **Remarque** : Le profil de conformité de la composante Organisation vérifiée du CCP V1.0 ne définit pas les critères de conformité pour le niveau LoA 4.

566 **Figure 16 : Mappage de la composante Organisation vérifiée**

567

568

569

570 ### 5.1.4 Mappage de la composante Justificatifs (relations et attributs)

Modèle d'assurance traditionnel	Modèle d'assurance discret	Composante vectorielle	Caractéristiques à prendre en considération
Non spécifié	Non spécifié	Non spécifiée	• Aucune évaluation des critères de conformité de la composante Justificatifs (relations et attributs) du CCP n'a été faite

Non spécifié	Non spécifié	R0	• Aucun des processus de confiance ne se conforme aux critères de conformité CAL de la composante Justificatifs (relations et attributs) du CCP
LoA 1	CAL1	R1	• Aucun des processus de confiance ne se conforme aux critères de conformité CAL 1 de la composante Justificatifs (relations et attributs) du CCP
LoA 2	CAL2	R2	• Aucun des processus de confiance ne se conforme aux critères de conformité CAL 2 de la composante Justificatifs (relations et attributs) du CCP
LoA 3	CAL3	R3	• Aucun des processus de confiance ne se conforme aux critères de conformité CAL 3 de la composante Justificatifs (relations et attributs) du CCP
LoA 4	CAL4	R4	• Aucun des processus de confiance ne se conforme aux critères de conformité CAL 4 de la composante Justificatifs (relations et attributs) du CCP

571 **Figure 17 : Mappage de la composante Justificatifs (relations et attributs)**

572

573 ### 5.1.5 Mappage de la composante Protection de la vie privée

Modèle d'assurance traditionnel	Modèle d'assurance discret	Composante vectorielle	Caractéristiques à prendre en considération
Non spécifié	Non spécifié	Non spécifiée	• Aucune évaluation des critères de conformité de la composante Protection de la vie privée du CCP n'a été faite
Non spécifié	Non spécifié	V0	• Le système ne se conforme pas aux critères de conformité de la composante Protection de la vie privée du CCP
LoA3	AAL3, IAL3, CAL4	V1	• Le système se conforme aux critères de conformité de la composante Protection de la vie privée du CCP

574 **Figure 18 : Mappage de la composante Protection de la vie privée**

575 **Remarque :** La composante Protection de la vie privée du CCP ne définit pas les
576 niveaux d'assurance. Lorsque la protection de la vie privée est prise en compte dans
577 une évaluation, un système non conforme ne peut pas documenter un niveau
578 d'assurance conforme à l'aide du modèle d'assurance traditionnel ou discret.

579 ### 5.1.6 Mappage de la composante Avis et consentement

Modèle d'assurance traditionnel	Modèle d'assurance discret	Composante vectorielle	Caractéristiques à prendre en considération
Non spécifié	Non spécifié	Non spécifiée	• Aucune évaluation des critères de conformité de la composante Avis et consentement du CCP n'a été faite

Non spécifié	Non spécifié	N0	• Le système ne se conforme pas aux critères de conformité de la composante Avis et consentement du CCP
LoA3	AAL3, IAL3, CAL4	N1	• Le système se conforme aux critères de conformité de la composante Avis et consentement du CCP

Figure 19 : Mappage de la composante Avis et consentement

Remarque : La composante Avis et consentement du CCP ne définit pas les niveaux d'assurance. Lorsque l'avis et le consentement sont pris en compte dans une évaluation, un système non conforme ne peut pas documenter un niveau d'assurance conforme à l'aide du modèle d'assurance traditionnel ou discret.

5.1.7 Mappage de la composante Infrastructure (technologie et opérations)

Modèle d'assurance traditionnel	Modèle d'assurance discret	Composante vectorielle	Caractéristiques à prendre en considération
Non spécifié	Non spécifié	Non spécifiée	• Aucune évaluation des critères de conformité de la composante Infrastructure (technologie et opérations) du CCP n'a été faite
Non spécifié	Non spécifié	S0	• Le système ne se conforme pas aux critères de conformité de l'infrastructure (technologie et opérations) du CCP

LoA3	AAL3, IAL3, CAL4	S1	• Le système ne se conforme pas aux critères de conformité de la composante Infrastructure (technologie et opérations) du CCP

Figure 20 : Mappage de la composante Infrastructure (technologie et opérations)

Remarque : La composante Infrastructure (technologie et opérations) du CCP ne définit pas les niveaux d'assurance. Lorsque l'infrastructure (technologie et opérations) est prise en compte dans une évaluation, un système non conforme ne peut pas documenter un niveau d'assurance conforme à l'aide du modèle d'assurance traditionnel ou discret.

5.2 Mappage des nouveaux vecteurs de confiance

Remarque : Si les niveaux d'assurance traditionnels et discrets sont subsumants (c.-à-d. que des niveaux plus élevés sont intrinsèquement plus robustes que des niveaux inférieurs et se conforment à tous les critères des niveaux inférieurs), les vecteurs de confiance ne sont pas intrinsèquement subsumants. Par conséquent, des codes numériques plus élevés ou des codes alphabétiques dont les lettres se suivent ne devraient pas être interprétés séparément comme étant une indication de la robustesse de l'élément.

5.2.1 Assurance de l'identité

La composante Assurance de l'identité principale de cette définition vectorielle représente les résultats de l'évaluation faite d'après la composante Personne vérifiée ou Organisation vérifiée ou selon le niveau d'assurance le plus faible de l'évaluation de ces deux composantes. Une seule valeur distincte provenant de cette catégorie peut être utilisée dans une seule transaction. Cette composante vise à s'aligner sur les définitions des valeurs des composantes par défaut des vecteurs de confiance spécifiées dans l'annexe A, section A.1 de la demande de commentaires 8485. Cette composante pourrait ne pas être incluse dans un vecteur si aucune évaluation n'a été faite avec la composante Personne vérifiée ou Organisation vérifiée du CCP ou encore si une telle évaluation a établi qu'aucun *niveau d'assurance* défini n'a été atteint (une condition qui devrait être documentée comme « I0 »).

5.2.2 Mappage de la composante Assurance de l'identité

Niveau d'assurance traditionnel	Niveau d'assurance discret	ID vectorielle	Caractéristiques communes	Caractéristiques définissant l'ID vectorielle
S. O.	S. O.	I0		Aucune preuve; aucune donnée de session persistante
LoA 1	IAL 1	I1	Remplit tous les critères de conformité du niveau 1 de la composante Personne vérifiée ou Organisation vérifiée, ou – si les deux sont évaluées – de ces deux composantes. •Peu ou pas d'assurance nécessaire Les attributs sont auto-affirmés mais constants à la longue Éventuel pseudonyme	Auto-affirmé, constant à la longue
LoA 2	IAL 2	I2	Remplit tous les critères de conformité du niveau 2 de la composante Personne vérifiée ou Organisation vérifiée, ou – si les deux sont évaluées – de ces deux composantes. •Une certaine assurance nécessaire L'identité a été prouvée en personne ou à distance à l'aide de mécanismes de confiance	Identité prouvée en personne ou à distance à partir d'un mécanisme de confiance

LoA 3	IAL 3	I3	Remplit tous les critères de conformité du niveau 3 de la composante Personne vérifiée ou Organisation vérifiée, ou – si les deux sont évaluées – de ces deux composantes. •Grande assurance nécessaire Il existe une relation qui lie le fournisseur d'identité et la partie identifiée	Relation qui lie le fournisseur d'identité et la partie

615 **Figure 21 : Mappage de la composante Assurance de l'identité**

616 ### 5.2.3 Utilisation des justificatifs principaux

617 La composante Utilisation des justificatifs principaux de cette définition vectorielle
618 représente des catégories distinctes de justificatifs principaux pouvant être utilisées
619 ensemble dans une seule transaction. Lorsque c'est approprié, plusieurs valeurs
620 distinctes provenant de cette catégorie peuvent être utilisées dans une seule
621 transaction. Cette composante vise à s'aligner sur les définitions de la valeur par défaut
622 des vecteurs de confiance spécifiées dans l'annexe A, section A.2 de la demande de
623 commentaires 8485. Il se peut que cette composante ne soit pas incluse dans un
624 vecteur si aucune évaluation n'a été faite avec la composante Authentification du CCP
625 ou si une telle évaluation a montré qu'aucun niveau d'assurance défini n'a été atteint
626 (une condition qui devrait être documentée comme « T0 »).

627 ### 5.2.4 Mappage de la composante Utilisation des justificatifs principaux

Niveau d'assurance traditionnel	Niveau d'assurance discret	ID vectorielle correspondante	Caractéristiques communes	Caractéristiques définissant l'ID vectorielle
S. O.	S. O.	C0		Aucun justificatif utilisé; service public anonyme

LoA 1	AAL 1	Ca	Remplit tous les critères de conformité du niveau 1 de la composante Authentification Faible certitude nécessaire qu'une *Entité* a gardé le contrôle des données de validation de l'authentificateur qui lui ont été confiées et que les données n'ont pas été compromises	Simples témoins http de session (avec rien d'autre)
LoA 1	AAL 1	Cb		Appareil connu, comme ceux indiqués à partir de systèmes de posture ou de gestion d'appareils
LoA 2	AAL 2	Cc	•Remplit tous les critères de conformité du niveau 2 de la composante Authentification • Certaine certitude nécessaire qu'une *Entité* a gardé le contrôle des données de validation de l'authentificateur qui lui ont été confiées et que les données n'ont pas été compromises	Secret partagé, comme une combinaison nom d'utilisateur et mot de passe
LoA 2	AAL 2	Cd		Preuve cryptographique de la possession de la clé à l'aide d'une clé partagée

LoA 3	AAL 3	Ce	• Remplit tous les critères de conformité du niveau 3 de la composante Authentification • Grande certitude nécessaire qu'une *Entité* a gardé le contrôle des données de validation de l'authentificateur qui lui ont été confiées et que les données n'ont pas été compromises	Preuve cryptographique de la possession de la clé à l'aide d'une clé asymétrique
LoA 4	AAL 4	Cf	• Remplit tous les critères de conformité du niveau 4 de la composante Authentification • Très grande certitude nécessaire qu'une *Entité* a gardé le contrôle des données de validation de l'authentificateur qui lui ont été confiées et que les données n'ont pas été compromises	Jetons matériels scellés ou clés entreposés dans un module de plateforme de confiance
LoA 4	AAL 4	Cg		Données biométriques vérifiées localement

628 **Figure 22 : Mappage de la composante Assurance des justificatifs**

629 ## 5.2.5 Gestion des justificatifs principaux

630 La composante Gestion des justificatifs principaux de cette définition vectorielle
631 représente des catégories distinctes de gestion qui peuvent être prises en considération
632 séparément ou ensemble dans une seule transaction. Lorsque c'est approprié,

plusieurs valeurs distinctes provenant de cette catégorie peuvent être utilisées dans une seule transaction. Cette composante vise à s'aligner sur les définitions de la valeur des composantes par défaut des vecteurs de confiance spécifiées dans l'annexe A, section A.3 de la demande de commentaires 8485. Il se peut que cette composante ne soit pas incluse dans un vecteur si aucune évaluation n'a été faite avec la composante Authentification du CCP ou si une telle évaluation a montré qu'aucun *niveau d'assurance* défini n'a été atteint (une condition qui devrait être documentée comme « T0 »). Le *niveau d'assurance* résultant de l'évaluation de la composante Authentification devrait être exprimé dans le même vecteur avec une composante « T ».

5.2.6 Mappage de la composante Gestion des justificatifs

Niveau d'assurance traditionnel	Niveau d'assurance discret	ID vectorielle correspondante	Caractéristiques communes	Caractéristiques définissant l'ID vectorielle
LoA 1	CAL 1	Ma	Remplit tous les critères de conformité du niveau 1 de la composante Authentification ou Justificatifs (Relations et attributs) Faible certitude nécessaire qu'une *Entité* a gardé le contrôle des données de validation de l'authentificateur qui lui ont été confiées et que le justificatif n'a pas été compromis	*Authentificateur* principal auto-déclaré (l'utilisateur choisit ses propres justificatifs et doit en faire un roulement ou les révoquer manuellement); pas de vérification supplémentaire pour l'émission ou le roulement des justificatifs

LoA 2	CAL 2	Mb	Remplit tous les critères de conformité du niveau 2 de la composante Authentification ou Justificatifs (relations et attributs) Certaine certitude nécessaire qu'une *Entité* a gardé le contrôle des données de validation de l'authentificateur qui lui ont été confiées et que le justificatif n'a pas été compromis	Émission et rotation à distance; utilisation de justificatifs pour récupérer la sauvegarde (p. ex., vérification du courriel); suppression d'une demande d'utilisateur
LoA 3	CAL 3	Mc	Remplit tous les critères de conformité du niveau 3 de la composante Authentification ou Justificatifs (relations et attributs) Grande certitude nécessaire qu'une *Entité* a gardé le contrôle des données de validation de l'authentificateur qui lui ont été confiées et que le justificatif n'a pas été compromis	Preuve complète requise pour chaque émission et rotation; révocation lorsqu'une activité suspecte est décelée

643 **Figure 23 : Mappage de la composante Utilisation des justificatifs**

5.2.7 Présentation des assertions

La composante Présentation des assertions de cette définition vectorielle représente des catégories distinctes d'assertions qu'il est recommandé d'utiliser d'une manière subsumante, mais qui peuvent être employées ensemble. Lorsque c'est approprié, plusieurs valeurs distinctes provenant de cette catégorie peuvent être utilisées dans une seule transaction. Cette composante vise à s'aligner sur les définitions de la valeur des composantes par défaut des vecteurs de confiance spécifiées dans l'annexe A, section A.3 de la demande de commentaires 8485. Il se peut que cette composante ne soit pas incluse dans un vecteur si aucune évaluation n'a été faite avec la composante Authentification du CCP ou si une telle évaluation a montré qu'aucun *niveau d'assurance* défini n'a été atteint (une condition qui devrait être documentée comme « T0 »). Le *niveau d'assurance* résultant de l'évaluation de la composante Authentification devrait être exprimé dans le même vecteur avec une composante « T ».

Remarque : Le CCP ne fournit pas actuellement de critères de conformité pour guider la sélection des valeurs appropriées afin d'inclure le composante Présentation des assertions. Une personne qui fait une évaluation peut se fier à l'ensemble des lignes directrices et contrôles reliés à la sécurité de l'information qui ont identifiés pour la conformité avec les références BASE 6 et/ou BASE 7 dans le profil de conformité de la composante Authentification.

5.2.8 Mappage de l'assurance de la présentation

Niveau d'assurance traditionnel	Niveau d'assurance discret	ID vectorielle correspondante	Caractéristiques communes	Caractéristiques définissant l'ID vectorielle
LoA 1	PAL 1 FAL 1 (NIST)	Aa	Remplit les critères de conformité BASE 6 de la composante Authentification	Pas de protection; identifiant du titulaire non signé (p. ex., témoin de session HTTP dans un navigateur web)
LoA 2	PAL 2 FAL 2 (NIST)	Ab	Remplit les critères de conformité BASE 7 de la composante Authentification	Assertion signée et vérifiable, passée par l'agent utilisateur (navigateur web)

LoA 2	PAL 2 FAL 2 (NIST	Ac	Remplit les critères de conformité BASE 7 de la composante Authentification	Assertion signée et vérifiable, passée par un canal d'arrière-plan
LoA 2	PAL 2 FAL 2 (NIST)	Ad	Remplit les critères de conformité BASE 7 de la composante Authentification	Assertion chiffrée sur la clé de la *partie dépendante*

664 **Figure 24 : Mappage de l'assurance de la présentation**

665 # 6. Évaluation des risques

666 La figure 25 contient une énumération des risques couramment utilisés pour évaluer le
667 *niveau d'assurance* requis pour une interaction numérique spécifique. Il est à noter que
668 ce tableau est de nature illustrative. Il n'est pas destiné à être exhaustif et ne se veut
669 pas directif. Par conséquent, il ne présente pas de critères de conformité
670 supplémentaires et n'a pas besoin d'être utilisé dans le cadre d'une évaluation. Les
671 *parties dépendantes* doivent évaluer les risques et torts potentiels qu'ils pourraient
672 rencontrer, et évaluer les niveaux de risque qu'elles sont disposées à accepter pour une
673 transaction spécifique dans leur contexte opérationnel. Étant donné cela, certains des
674 critères illustratifs utilisent une terminologie qui est sujette à interprétation (p. ex.,
675 « élevé », « moyen », « faible »). Cela permet aux praticiens d'établir un profil de risque
676 qui correspond à leur ministère, service ou type d'entreprise. Par exemple, une grande
677 institution financière peut considérer le risque de perdre 100 000 $ comme étant
678 « limité » ou « faible » tandis qu'un risque de cette taille peut être « grave » ou « élevé »
679 pour une petite entreprise, une entreprise en démarrage ou une personne.

680 Étant donné que les niveaux de risque sont fonction des circonstances propres à une
681 partie dépendante et à toute politique, toute loi et/ou tout règlement auxquels ils sont
682 assujettis, il incombe à la *partie dépendante* de documenter explicitement sa tolérance
683 au risque. Cela assurera que les contrôles des risques sont mis en place d'une manière
684 uniforme et qu'ils ne sont ni trop laxistes ni trop rigoureux, peu importe les personnes
685 qui les ont établis. Cela garantira aussi que les contrôles sont évalués d'une manière
686 équitable lorsqu'ils sont audités. Ces risques devraient aussi être documentés de façon
687 à être évidents et clairement compréhensibles pour les *entités* avec qui ils interagissent.

688 La figure 25 est un tableau illustratif des risques qui vise à aider les *parties*
689 *dépendantes* à comprendre comment elles peuvent évaluer leurs propres risques et
690 déterminer le niveau d'assurance qu'il leur faut.

Catégorie d'impact	Niveau d'assurance nécessaire			
	LoA 1 ou équivalent	**LoA 2 ou équivalent**	**LoA 3 ou équivalent**	**LoA 4 ou équivalent**
Désagréments, détresse, torts pour l'image ou la réputation	Au pire, désagréments, détresse, embarras ou torts pour l'image ou la réputation d'une partie, qui sont limités et à court terme	Au pire, désagréments, détresse ou torts pour l'image ou la réputation d'une partie, qui sont sérieux à court terme ou limités à long terme	Désagréments, détresse ou torts pour l'image ou la réputation d'une partie, qui sont graves ou sérieux à long terme (ordinairement réservé à des situations avec des effets graves ou qui touchent de nombreuses personnes)	Désagréments, détresse ou torts pour l'image ou la réputation d'une partie, qui sont graves et permanents
Perte financière	Au pire, perte financière an insignifiante ou sans conséquences pour n'importe quelle partie ou, au pire, responsabilité sans conséquences	Au pire, perte financière sérieuse pour n'importe quelle partie ou responsabilité sérieuse	Grave perte financière pour n'importe quelle partie ou responsabilité grave	Perte financière catastrophique pour n'importe quelle partie ou responsabilité catastrophique

Torts à un programme ou un intérêt public	Au pire, un effet négatif sur les opérations ou les actifs organisationnels, sur une organisation, un programme ou un actif du gouvernement, ou encore sur l'intérêt public (p. ex., dégradation des capacités d'une mission dont l'ampleur et la durée sont telles que l'organisation est capable d'accomplir ses fonctions principales avec une efficacité nettement réduite; torts mineurs pour les actifs organisationnels ou l'intérêt public)	Au pire, un sérieux effet négatif sur les opérations ou les actifs organisationnels, sur une organisation, un programme ou un actif du gouvernement, ou encore sur l'intérêt public (p. ex., nette dégradation des capacités d'une mission dont l'ampleur et la durée sont telles que l'organisation est capable d'accomplir ses fonctions principales avec une efficacité significativement réduite; torts considérables pour les actifs organisationnels ou l'intérêt public)	Un grave effet négatif sur les opérations ou les actifs organisationnels, sur une organisation, un programme ou un actif du gouvernement, ou encore sur l'intérêt public (p. ex., grave dégradation des capacités d'une mission dont l'ampleur et la durée sont telles que l'organisation est incapable d'accomplir une ou plusieurs de ses fonctions principales; torts importants pour les actifs organisationnels ou l'intérêt public)	Effet négatif catastrophique sur les opérations ou les actifs organisationnels, sur une organisation, un programme ou un actif du gouvernement, ou sur l'intérêt public (p. ex., dégradation ou perte catastrophique d'une mission ou dont l'ampleur et la durée sont telles que l'organisation est incapable d'accomplir ses fonctions principales; torts catastrophiques pour les actifs organisationnels ou l'intérêt public)

Divulgation non autorisée de renseignements personnels ou commerciaux sensibles	Au pire, divulgation limitée de renseignements personnels ou d'information commercialement sensible à des parties non autorisées, ou encore violation de la confidentialité entraînant une perte de confidentialité de faible impact	Au pire, divulgation de renseignements personnels ou d'information commercialement sensible à des parties non autorisées, ou encore violation de la confidentialité ayant un impact modéré	Divulgation de renseignements personnels ou d'information commercialement sensible à des parties non autorisées, ou encore violation de la confidentialité ayant un impact sérieux	Divulgation de renseignements personnels ou d'information commercialement sensible à des parties non autorisées, ou encore violation de la confidentialité ayant un impact catastrophique
Divulgation non autorisée de renseignements gouvernementaux sensibles	Perte de confidentialité avec peu d'impact	Effet négatif limité sur les opérations et actifs organisationnels en raison d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées	Effet négatif sérieux sur les opérations et actifs organisationnels en raison d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées	Effet catastrophique sur les opérations et actifs organisationnels en raison d'une perte de confidentialité résultant de la divulgation de renseignements gouvernementaux sensibles à des parties non autorisées

Infractions civiles ou pénales	Secteur privé : Au pire, risque d'infractions civiles ou pénales d'une nature qui ne serait normalement pas assujettie à mesures pour faire respecter la loi Secteur public : Tout compromis impliquant une infraction de la loi est évaluée au moins au niveau 2	Infraction civile ou pénale qui peut avoir des conséquences mineures et peut être assujettie à des mesures pour faire respecter la loi	Infraction civile ou pénale qui peut avoir des conséquences sérieuses qui sont importantes pour les programmes d'application de la loi	Infraction pouvant avoir des conséquences exceptionnellement graves qui revêtent une importance spéciale pour les programmes d'application de la loi
Santé et sécurité des personnes	Secteur privé : Au pire, blessure mineure n'exigeant pas de traitement médical Secteur public : Toute atteinte à la santé et la sécurité est évaluée au moins au niveau 2	Secteur privé : Au pire, risque modéré de blessures mineures ou de blessures nécessitant un traitement médical Secteur public : Blessures personnelles mineures ne nécessitant pas d'attention médicale	Secteur privé : Au pire, faible risque de blessures graves ou de décès Secteur public : Blessure personnelle nécessitant une attention médicale	Risque qu'une personne se blesse grièvement ou décède

Intérêt national	(tout compromis impliquant l'intérêt national est évalué au minimum à un niveau 2)	Désavantage pour l'intérêt national	Atteinte à l'intérêt national	Atteinte sérieuse ou grave à l'intérêt national

Figure 25 : Évaluation des risques (illustration)

7. Références

Cette section fournit la liste des principales normes extérieures et lignes directrices et autres documents ayant servi de référence pour la création de ce module du CCP.

Remarque

- Le cas échéant, seul le numéro de version ou de mise à jour spécifié dans ce document s'applique.

Cette composante du CCP tire parti des compétences, de l'expérience et des leçons apprises d'autres organisations qui cherchent à améliorer ce domaine, et elle a tenu compte du matériel provenant des sources suivantes :

- Internet Engineering Task Force (IETF): Demande de commentaires 8485, Vecteurs de confiance <https://www.rfc-editor.org/info/rfc8485>
- U.S. Department of Commerce, National Institute of Standards and Technology: NIST Special Publication 800-63-3 Digital Identity Guidelines <https://pages.nist.gov/800-63-3/sp800-63-3.html>
- Gouvernement du Canada, Secrétariat du Conseil du trésor du Canada : Profil du secteur public du Cadre de confiance pancanadien version 1.1 <https://canada-ca.github.io/PCTF-CCP/>
- Ligne directrice sur l'assurance de l'identité
- World Wide Web Consortium (W3C): Verifiable Credentials Data Model 1.0 <https://www.w3.org/TR/vc-data-model/>

8. Spécification de la norme de vecteurs de confiance du CCP

8.1 URL de la marque de confiance

L'URL pour les vecteurs de la marque de confiance du CCP du CCIAN est <à déterminer >. La valeur du champ vtm sera <la même valeur à déterminer >.

8.2 Registre des composantes des vecteurs de confiance

Cette spécification ajoute les valeurs suivantes au registre « Composantes des vecteurs de confiance » établi par [RFC8485] pour utilisation avec la marque de confiance des vecteurs de confiance du CCP du CCIAN.

- Symbole de démarcation : I
- Description : Preuve d'identité
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Modèle de maturité de l'assurance du CCP]
- Symbole de démarcation : C
- Description : Utilisation des justificatifs
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Modèle de maturité de l'assurance du CCP]
- Symbole de démarcation : M
- Description : Gestion des justificatifs
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Modèle de maturité de l'assurance du CCP]
- Symbole de démarcation : A
- Description : Présentation
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Modèle de maturité de l'assurance du CCP]
- Symbole de démarcation : T
- Description : Authentification
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Aperçu de la composante Authentification] et [Profil de conformité de l'authentification]

- Symbole de démarcation : P
- Description : Personne vérifiée
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Aperçu de la composante Personne vérifiée] et [Profil de conformité de la personne vérifiée]

- Symbole de démarcation : O
- Description : Organisation vérifiée
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Aperçu de la composante Organisation vérifiée] et [Profil de conformité de l'organisation vérifiée]

- Symbole de démarcation : R

- Description : Justificatifs (relations et attributs)
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Aperçu de la composante Justificatifs (relations et attributs)] et [Profil de conformité des justificatifs (relations et attributs)]

- Symbole de démarcation : V
- Description : Protection de la vie privée
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Aperçu de la composante Protection de la vie privée] et [Profil de conformité de la protection de la vie privée]

- Symbole de démarcation : N
- Description : Avis et consentement
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Aperçu de la composante Avis et consentement] et [Profil de conformité de l'avis et du consentement]

- Symbole de démarcation : S
- Description : Infrastructure (technologie et opérations)
- Contrôleur des changements : CCIAN
- Document(s) sur les spécifications : [Aperçu de la composante Infrastructure (technologie et opérations)] et [Profil de conformité de l'infrastructure (technologie et opérations]

9. Historique des révisions

Version	Date	Auteur	Commentaires
0.01	2020-09-29	Équipe d'édition du CCP	Ébauche initiale
0.02	2021-01-29	Équipe de conception	Tenir compte des commentaires reçus à la suite de l'examen initial du TFEC
0.03	2021-05-17	Équipe de conception	Aligner la section Vecteurs de confiance sur les composantes actuelles du CCP et les mises à jour supplémentaires découlant de l'examen de l'équipe de conception
1.0	2021-06-09	Équipe de conception	Approuvé par le TFEC en tant qu'ébauche de recommandations V1.0