Note de la rédaction : Composante « Connexion vérifiée »

Cadre de confiance pancanadien

5 juillet 2019
Version 0.2

1 À propos de ce document

Ce document fournit un résumé des commentaires reçus pendant la période d'examen ouvert de la composante connexion vérifiée du cadre de confiance pancanadien. **Cet examen a porté sur les documents de travail « Aperçu de la connexion vérifiée » (V0.06) et « Profil de conformité de la connexion vérifiée » (V0.03)**. Le DIACC a mené cet examen du 15 mai au 17 juin 2019.

Sur les 225 commentaires soumis pendant la période d'examen :

- 81 étaient reliés à l'aperçu et 140 au profil de conformité;
- l'équipe de rédaction a examiné chaque commentaire et déterminé que 105 étaient de nature rédactionnelle. Toutefois, celles-ci sont autoévaluées par des examinateurs dans la plupart des cas. Bon nombre des points signalés comme étant des changements « rédactionnels » sont en fait de nature « substantielle » et ont été transmis à l'équipe de conception afin d'être résolus;
- l'équipe de rédaction a transmis 117 commentaires à celle de la conception pour qu'elle les règle.

2 Principaux thèmes

L'équipe de révision a noté que les thèmes ci-dessous, qui revenaient dans tous les commentaires, étaient importants.

Étant donné que cette note est basée sur des réponses provisoires aux commentaires, les détails concernant la résolution de ces thèmes ne sont pas encore fournis.

Approches de l'authentification	
Comme la plupart des examinateurs acceptent, du moins implicitement, que les noms d'utilisateurs-mots de passe et l'authentification à deux facteurs qui est associée continuent d'être utilisés à court et moyen terme, de nombreux commentaires suggèrent que cette	Comme nous l'avons vu avec les autres composantes, il y a une pression légère mais distincte pour que le Comité d'experts du cadre de confiance se penche sur les technologies et les enjeux émergents.

composante devrait considérer, pour reprendre les mots d'un examinateur, « le ou les successeurs légitimes des sceaux, autographes et mots de passe en texte traditionnels ». Les modèles d'identité auto-souveraine ont été spécifiquement exclus de cette version du document. La biométrie (et son traitement dans la version actuelle) intéresse aussi les examinateurs.	
Exemples et références externes	
Cette composante comporte de multiples références à des normes externes – avant tout comme des exemples de normes de l'industrie que les organisations devraient ou doivent respecter dans le cadre de la conformité à un critère de conformité donné (p. ex., BASE-5, BASE-11, CRAU-15). Dans certains cas, les examinateurs ont demandé quel était le raisonnement derrière l'utilisation ou la mention de normes spécifiques. D'autres demandent que des éléments supplémentaires soient ajoutés aux critères de conformité. Dans un cas, les examinateurs ont recommandé de supprimer complètement la référence à NIST 800-63 en invoquant le fait que cette norme est basée sur de « vieilles impressions » et « ne tient pas compte des technologies émergentes ».	L'ensemble des commentaires suggère que les documents donnant un aperçu de la composante pourraient comporter une note sur la raison pour laquelle on a inclus (ou, dans certains cas, exclus) d'autres normes qui sont incorporées dans les critères de conformité en guise de référence.
Critères de conformité pour les niveaux d'assurance spécifiques	
Les critères de conformité de cette composante sont structurés autour de quatre niveaux d'assurance. Les rédacteurs ont noté que :	Afin d'éviter des commentaires similaires de la part d'un auditoire plus vaste, les rédacteurs recommandent d'inclure une note disant que les exigences du niveau

• Un certain nombre de commentaires portent sur les détails ou les changements concernant les exigences spécifiées pour un niveau d'assurance donné ou des différences dans les exigences des niveaux d'assurance. Par exemple, un examinateur peut demander pourquoi un critère donné est identifié comme étant une possibilité (PEUT) plutôt qu'une obligation (DOIT) pour le niveau d'assurance 1 et suggère qu'un changement soit apporté. • Plusieurs examinateurs ont fait remarquer qu'il n'y a pas de critères de conformité définis pour le niveau d'assurance 4.	d'assurance 4 ne sont pas spécifiées dans la version actuelle -ou- de supprimer complètement ce niveau d'assurance.
Descriptions des processus de confiance	
Les examinateurs relèvent ce qu'ils considèrent comme des lacunes, inconsistances et descriptions non claires pour les descriptions des processus de confiance de la connexion vérifiée et celles des « intrants » et « extrants » qui y sont associés. Plusieurs commentaires suggèrent des ajouts ou des clarifications ou demandent des clarifications pour améliorer les descriptions.	Les clarifications apportées à la terminologie et au texte vont répondre à bon nombre des commentaires. Toutefois, il est nécessaire d'examiner de plus près les ajouts, car ces définitions des processus sont justifiées étant donné que cela peut se répercuter sur de nombreux critères de conformité.
Révisions apportées au contenu et à la rédaction de l'aperçu	
Les examinateurs ont soumis un grand nombre de commentaires de nature « rédactionnelle. Voici ceux qui sont revenus le plus souvent :	Ces commentaires rappellent le besoin de revoir le contenu de l'aperçu et des critères de conformité – possiblement pour toutes les composantes. Il s'agit

▪ Chevauchements, inconsistances ou questions sur le contenu fourni par les documents sur l'aperçu et le profil de conformité. ▪ Demandes d'emplois et de clarifications terminologiques. ▪ Utilisation uniforme de la terminologie ou d'un terme privilégié. ▪ Demandes d'exemples lorsqu'il est fait référence à des termes, processus ou événements. À ce propos, au moins un commentateur a recommandé de choisir un terme pour définir la priorité des exigences (p. ex., DOIT et DEVRA ont été utilisés dans les documents révisés).	d'une tâche planifiée pour l'équipe de rédaction. En ce qui concerne les demandes répétées de clarification terminologique, les commentaires reçus jusqu'à présent suggèrent que les équipes de conception devraient identifier des termes clés dans leur contenu et les signaler pour être inclus soit dans un glossaire local soit dans celui du cadre de confiance pancanadien. En outre, elles soulèvent des questions à propos de ce que le Comité d'experts du cadre de confiance considère être un niveau de sensibilisation raisonnable parmi l'auditoire de ces documents.
Critères de conformité pour des niveaux d'assurance spécifiques	
Les critères de conformité de cette composante sont structurés autour de quatre niveaux d'assurance. Les rédacteurs font remarquer qu'un certain nombre de commentaires portent sur des détails ou des changements concernant les exigences spécifiées pour un niveau d'assurance donné ou des différences entre les niveaux d'assurances en ce qui concerne les exigences. Les examinateurs ont aussi indiqué qu'il n'y a pas de critères de conformité définis pour le niveau d'assurance 4.	Afin d'éviter des commentaires similaires de la part d'un auditoire plus vaste, les rédacteurs recommandent d'inclure une note disant que les exigences du niveau d'assurance 4 ne sont pas spécifiées dans la version actuelle -ou- de supprimer complètement ce niveau d'assurance.
Sessions	

Les examinateurs relèvent plusieurs problèmes en ce qui concerne la terminologie et les critères de conformité reliés aux « sessions », notamment : • Difficulté de faire la distinction entre les sessions « authentifiées » et « d'authentification »; • Apparence de coordination étroite entre les participants; • Niveau d'authentification d'une session.	Les clarifications apportées à la terminologie et au texte vont répondre à bon nombre des commentaires. Dans certains cas, il est nécessaire d'examiner de plus près les exigences spécifiées pour certains critères de conformité.

3 Autres éléments

L'équipe de rédaction a aussi noté ce qui suit :

1. **Facteurs d'authentification** – Les notions de « chose que vous connaissez », « chose que vous avez » et « chose que vous êtes » sont essentielles pour ce domaine et convenablement incluses dans cette composante du cadre de confiance pancanadien. Toutefois, une brève description de ces notions dans le document d'aperçu pourrait rendre la composante plus accessible à un auditoire plus large.
2. **Confidentialité** – Un nombre limité d'examinateurs se demandent si certains critères de conformité sont contraires à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) (principe 7 – protections). Sans être une préoccupation générale, le sujet est mis en évidence ici étant donné l'engagement que le DIACC a pris à l'égard de la confidentialité pour l'ensemble de son travail.
3. **Hypothèses stylistiques** – La plupart des commentaires portent sur des points très spécifiques dans les documents de la composante. Pris ensemble, toutefois, il ressort que les examinateurs formulent des hypothèses stylistiques générales à propos de ces documents – avant tout en tant que documents sur des normes. Les hypothèses stylistiques peuvent inclure la mise en majuscules de certains termes (selon l'utilisation), l'introduction de nouveaux termes, la façon dont les références extérieures sont notées, quand utiliser des notes dans les lignes, etc.