Le Programme Solutions innovatrices Canada

Défi EN578-170003/35: Système de préparation de poudres de céramique hybrides

Pièce jointe n° 1
Questions et réponses n° 1 à n° 7

Le présent document comprend des questions et des réponses liées au défi.

Question nº 1

Dans la section « Résultats essentiels (obligatoires) », vous énoncez le besoin suivant :

3. incorporer les spécifications d'interopérabilité émergentes et/ou matures suivantes, qui ont été financées, mises à l'essai et/ou défendues par le Département de la sécurité intérieure des États-Unis d'Amérique :
   - justificatifs d'identité vérifiables : le projet Blockcerts et/ou le projet Indy de Hyperledger;
   - identificateurs décentralisés (organismes d'élaboration de normes : Consortium World Wide Web [W3C] ou Decentralized Identity Foundation);
   - justificatifs d'identité vérifiables (organisme d'élaboration de normes – W3C);
   - notation des objets du langage Java pour les données liées/JSON-LD (organisme d'élaboration de normes – W3C).

À la première puce, j'aimerais savoir s'il s'agit d'exemples de justificatifs d'identité vérifiables ou s'il faut réellement utiliser l'une de ces deux bibliothèques?

Réponse nº 1

Le Verifiable Credentials Data Model 1.0 du W3C est passé à l'étape de la recommandation proposée (en anglais seulement - https://www.w3.org/TR/vc-data-model/). À notre connaissance, les principales applications et bibliothèques qui reposent sur ces normes proposées sont **Blockcerts** et **Indy de Hyperledger (Aries)**. C'est pourquoi nous les avons citées dans ce défi. Nous sommes toutefois ouverts à l'utilisation d'autres applications et bibliothèques, pourvu qu'elles respectent les recommandations du W3C précisées dans les puces qui suivent, y compris la **recommandation proposée par le W3C sur les identificateurs décentralisés** (en anglais seulement - https://www.w3.org/2019/08/did-20190828/).

La section « Résultats souhaités et éléments à considérer » a été modifiée de façon à refléter la réponse à cette question.

Question nº 2

Dans la section « Résultats essentiels (obligatoires) », vous énoncez le besoin suivant :

2. protéger la vie privée et l'identité de l'utilisateur en tout temps.

Contre quelles menaces ou parties non autorisées le système doit-il protéger l'utilisateur (pour assurer sa sécurité en tout temps)? Par exemple, peut-on se fier aux protections intégrées des agents

utilisateurs dans lesquels sont stockés les justificatifs d'identité vérifiables non chiffrés, ou doit-on concevoir des protections qui seront évaluées à la fin du projet?

Réponse nº 2

En ce qui concerne la vie privée et l'identité de l'utilisateur, le soumissionnaire doit montrer, dans la proposition, qu'il maîtrise et applique les contrôles pertinents, conformément aux directives applicables, notamment le document ITSP.30.31 du CST, accessible à l'adresse https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsp.30.031v3-fra_0.pdf

Le soumissionnaire doit également, dans la proposition, faire preuve d'une connaissance suffisante pour énumérer les agents de menace possibles et les approches d'atténuation connexes.

La section « Résultats souhaités et éléments à considérer » a été modifiée de façon à refléter la réponse à cette question.

Question nº 3

Le gouvernement fédéral envisage-t-il d'utiliser une méthode d'identification décentralisée donnée ou encore sa propre méthode pour la mise en œuvre? Quelles sont les exigences à l'égard du résolveur d'identificateurs décentralisés?

Réponse nº 3

Aucune méthode d'identification décentralisée n'a été précisée. On s'attend à ce que la solution soit compatible et interopérable avec de multiples méthodes d'identification décentralisée. Quant au résolveur d'identificateurs décentralisés, reportez-vous au contrat octroyé le 26 septembre 2019 par le Département de la sécurité intérieure des États-Unis pour un vérificateur et résolveur universel.

Question nº 4

Blockcerts et Indy ne sont pas (nécessairement) conformes au Verifiable Credentials Data Model 1.0 du W3C. Le gouvernement fédéral s'attend-il à une mise en œuvre normalisée reposant sur les normes du W3C? Peut-on présumer qu'une solution compatible avec les justificatifs d'identité vérifiables du W3C est suffisante?

Réponse nº 4

Une solution compatible avec les justificatifs d'identité vérifiables du W3C est suffisante.

Question nº 5

La solution doit-elle prendre en charge les « trois saveurs » du Verifiable Credential Model 1.0 du W3C, soit INDY ZKP, JSON-LD et JWS Detached (utilisées par UPort et Microsoft)? La cryptographie du système doit-elle être conforme aux normes du gouvernement fédéral (ZKP n'entre pas dans cette catégorie)?

Réponse nº 5

La solution doit au moins respecter les critères établis dans la norme sur les justificatifs d'identité vérifiables du W3C. La méthode JSON-LD est donc obligatoire, et les autres extensions (ou « saveurs ») peuvent être envisagées (JWT, ZKP, etc.).

Il est aussi fortement souhaitable que la solution s'adapte aux normes du gouvernement fédéral, en supposant que les normes du W3C sont compatibles avec différentes suites cryptographiques.

Question nº 6

Dans la section « Résultats souhaités supplémentaires », il y a une directive générale concernant l'interopérabilité et la transférabilité libres (indépendantes de la technologie), qu'on ne retrouve pas actuellement dans le domaine (les identificateurs décentralisés sont liés aux registres des responsables de la mise en œuvre, les justificatifs d'identité vérifiables font l'objet d'une mise en œuvre sur trois, etc.). Pouvez-vous définir le niveau ou les attentes de base par rapport à la transférabilité?

Réponse nº 6

L'objectif est d'obtenir une interopérabilité complète entre les identificateurs décentralisés, les méthodes connexes, ainsi que les registres et les réseaux sous-jacents (p. ex., réseau de jetons), le cas échéant. Dans le cadre du projet, on s'attend à ce que les justificatifs d'identité vérifiables ne soient pas limités à la mise en œuvre d'un portefeuille ou d'un agent donné et, si nécessaire, à ce qu'ils ne dépendent pas non plus des registres ou des réseaux. En présence de contraintes ou de limites, il faudrait envisager une solution pour permettre l'interopérabilité du portefeuille, de l'agent et du réseau.

Question nº 7

Je souhaite obtenir des précisions sur les exigences sur les justificatifs numériques vérifiables axés sur les utilisateurs relatifs à la transmission et à la sauvegarde de données. Je comprends bien que les données doivent être sauvegardées au Canada, mais j'aimerais savoir quelles sont les modalités autorisées pour transmettre les données aux fins de leur authentification. Les données peuvent-elles être acheminées à un serveur situé dans un autre pays, où elles seront traitées aux fins d'authentifications avant d'être retournées au Canada?

Réponse nº 7

Les données en transit doivent être correctement chiffrées, et ne peuvent être déchiffrées pendant le transit. Si c'est le cas, la transmission n'est pas assujettie aux exigences en matière de résidence des données. Toutefois, le traitement constitue un état transitoire qui donne lieu à un risque de fuite et, selon la conception proposée, pourrait ne pas être conforme aux exigences en matière de résidence des données.