Innovative Solutions Canada Program

Challenge EN578-170003/35: User-Centric Verifiable Digital Credentials

Attachment 1
Questions and Answers #1 to #7

This document contains questions and answers related to this challenge.

Question #1:

Within the Essential (Mandatory) Outcomes you reference the need to:

3. Incorporate the following emerging and/or mature specifications for interoperability that have been funded, tested and/or championed by the United States of America Department of Homeland Security:
   - o Verifiable Credentials: Blockcerts and/or Hyperledger Project Indy,
   - o Decentralized Identifiers (Standards Development Organizations: World Wide Web Consortium (W3C) or Decentralized Identity Foundation),
   - o Verifiable Credentials (Standards Development Organization — W3C); and
   - o JavaScript Object Notation for Linked Data / JSON-LD (Standards Development Organization — W3C).

With regards to the first bullet, I'm wondering if those are examples of verifiable credentials, or you actually expect one of those two libraries?

Response #1:

The Verifiable Credentials Data Model 1.0 is now a W3 Proposed Recommendation (https://www.w3.org/TR/vc-data-model/). To our knowledge, the leading implementations and libraries using these proposed standards are **Blockcerts** and **Hyperledger Indy (Aries)** and thus have been referenced in this challenge. However, we are open to other libraries and implementations with the condition that they adhere to the W3 recommendations specified in the following bullets. This also includes the **W3 Proposed Recommendation for decentralized identifiers (DIDS)** found at: https://www.w3.org/2019/08/did-20190828/

The Desired Outcomes and Consideration section has been amended to reflect modifications in response to this question.

Question #2:

With respect to: Essential (Mandatory) Outcomes:
2. Protect the privacy and identity of the user at all times

What threats or unauthorized actors is the system meant to protect against (to keep the user's safe at all times)? For example, is storing an unencrypted Verifiable credential in user agent storage and relying on device level protections sufficient, or are these protections left to the design and subject to evaluation at the completion of the project?

Response #2:

In relation to protecting privacy and identity of the user, the bidder is expected to demonstrate, in the proposal, knowledge and application of relevant controls as outlined in applicable guidance, including but not limited to CSE ITSP.30.31 published at https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v3-eng_0.pdf

It is also expected that the bidder demonstrate, in the proposal, sufficient knowledge to enumerate relevant threat agents and mitigation approaches.

The Desired Outcomes and Consideration section has been amended to reflect modifications in response to this question.

Question #3:

Are any specific DID methods considered for the implementation, does Federal Government think of its own method? And, what are the requirements on the DID resolver?

Response #3:

No specific DID methods are specified. It is expected the solution will support and interoperate with multiple DID methods. As for the DID resolver please see the DHS Award for Universal Verifier and Resolver dated, September 26, 2019

Question #4:

Blockcert and Indy are not (necessarily) W3C Verifiable Credentials 1.0 compliant; does the Federal Government want a standard implementation based on W3C standards? Can we assume that a solution supporting W3C Verifiable Credentials is sufficient?

Response #4:

A solution supporting the W3C Verifiable Credentials standards is sufficient.

Questions #5

Is there a requirement to support "the 3 flavours" of W3C Verifiable Credential 1.0? INDY ZKP, JSON-LD, and detached JWS (used by UPort and Microsoft)? And, is there a requirement for cryptography of the system to be compliant with Canadian Federal standards (e.g. ZKP is not in that category)?

Response #5

The solution must support, at a minimum, what is specified as part of the W3C Verifiable Credentials Standard. JSON-LD is required, the remaining extensions ('flavours') may be considered (JWT, ZKP, etc)

It is also highly desirable that the solution be flexible to support Canadian Federal Standards with the assumption that the W3C standards can support different cryptographic suites.

Question #6

Within the Additional Outcomes section there is a general direction toward free (technology agnostic) interoperability and transferability – which is not present in the Art today (e.g. DIDs are bound to implementer's ledgers, VCs are subject to 1-of-3 implementations, etc…) Is there a definition of what a minimum level / expectation of portability would be?

Response #6

The goal is toward full interoperability between DIDs, their methods, supporting ledgers (if a ledger is required), and supporting networks (e.g. a tokenization network, if required). An expectation of the project is that the verifiable credentials are not constrained to a specific implementation of a wallet or agent and if necessary, can be independent of ledger or network. If there are constraints or limitations, consideration should be given to an eventual path toward wallet/agent/network interoperability.

Question #7

I am looking for requirements clarification for User-Centric Verifiable Digital Credentials regarding the transmission and storage of data. I understand storage of data has to be within Canada but I am curious how the transmission of data for authentication can be handled? Can data be sent to server in another country to be processed for authentication and then returned to Canada?

Response #7

Data in transit must be encrypted appropriately and not decrypted in transit. If this is the case, the transmission is not subject to the data residency requirement. Processing, however, is an intermediate state that creates the risk of data leakage, and depending on the proposed design may not be compliant with the residency requirement.