User-Centric Verifiable Digital Credential Challenge

Canada

Proposed Agenda

1. Welcome and Roll Call – All (10 mins)
2. UCVDCC Challenge Re-Cap – TBS (10mins)
3. Vendor Proposal Briefs (60 mins / 10 mins each)
4. Discussion on Topics (30 mins)
5. Open Discussion (time remaining)
6. Conclusion (time remaining)

Summary Overview

Innovation Solutions Canada Program

- Supports the development of early-stage innovations by small businesses
- Provides innovative solutions to federal department or agency challenges

User-Centric Verifiable Digital Credentials Challenge

- Focus on emerging digital ecosystem for digital credentials.
- Design a portable secure digital credential solution to be held by individuals

Project Details:

- **Internal** (SOWs, Contract details, etc.):
- **Public:** https://canada-ca.github.io/ucvdcc/

Problem Statement

This challenge is seeking a **portable secure digital credentials** (self-sovereign identity) solution held by individuals that can be **independently, cryptographically and rapidly verified** using emerging distributed ledger standards and an approach that may give rise to a **global digital verification platform**.

For many contexts, ranging from applying for a job to transiting checkpoints for aviation security, paper documents remain the predominant way to prove key attributes about an individual, such as their name, date of birth, academic/professional qualifications, or security clearance. While these attributes might be presented in digital form, there are no widely adopted or standardized methods to issue and rapidly verify digital credentials across many different contexts.

There exists no current capability to digitally verify without dependencies on centralized or low-latency network platforms (or both).

Note: The operational solution will be required to store all personal information within Canada

Essential (Mandatory) Outcomes

Proposed solutions must:

1. **Create User-centric Verifiable Digital Credentials** able to operate on a national or global interoperable verification platform;
2. **Protect the privacy and identity** of the user at all times* (see note);
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:
   - Decentralized Identifiers (Standards Development Organizations: World Wide Web Consortium (W3C) or Decentralized Identity Foundation),
   - Verifiable Credentials (Standards Development Organization - W3C); and
   - JavaScript Object Notation for Linked Data / JSON-LD (Standards Development Organization - W3C);
4. **Demonstrate the feasibility of the specifications** described above in support of creating, transmitting and storing verifiable digital credentials using wallet or agent reference implementations. These reference implementations may include but not are limited to: Blockcerts, Hyperledger Indy Aries
5. **Adhere to applicable policy instruments**, guidelines and frameworks, including but not limited to:
   - Requirements specified in the Treasury Board Directive on Identity Management; and
   - Conformance Criteria specified in the Public Sector Profile of the Pan-Canadian Trust Framework.

Additional Outcomes

Proposed solutions should:

1. **Give issuers and recipients ownership** of their official records that can be cryptographically signed and presented anywhere to verify credential provenance and ownership.
2. **Give issuers and recipients autonomy** over how they use their records and verify digital credentials. For example, if issuers decide to switch vendors later on, they retain full access and use of their digital certificates.
3. **Give relying trusted third parties the ability to verify any record independently,** in independent fashion, for free and independent of any software vendor or issuing institution. Relying parties can easily verify any digital credential through widely available technology such as a web browser or a mobile phone. Verification is based on open and interoperable approaches.
4. **Provide leading-edge digital credential security** to enable the global trust economy that are cryptographically signed thus enabling third parties to verify their provenance and ownership.
5. **Demonstrate the components of self-sovereign identity**:
   - decentralized and portable;
   - demonstrated control of attributes; and independence from a centralized registry, identity provider, or certificate authority.
6. **Demonstrate multiple partnerships and interoperability** with other companies within verifiable credential ecosystem.

Vendors	Use Cases
Bluink	Append a Security Clearance to a Government Worker Digital Identity
Aviary Tech	Issuance and Verification of Credentials for Cannabis-Related Interactions
SecureKey	Open a Bank Account for Individuals and Businesses
TerraHub	Verify Individual’s Ability to Work a Job or Enter a Site without 3rd Party Verification
TrustScience	Use of a Decentralized Record of Employment System for Employment Verification
2Keys	Create Foundational Identities that Enable Enrolment into Programs and Services

Challenge Details

- **Challenge Background**
  - **Late 2018** TBS was requested to develop an innovation challenge
  - **Nov 2019** User-Centric Verifiable Digital Credential Challenge was issued
    - 42 respondents, 21 met mandatories, 6 finalist were selected
  - **Jul 2020** - Challenge awarded
  - **Aug 2020** -est. Contract award.

- **Challenge Highlights**
  - Test the feasibility of a verification platform that can be used to independently verify digital credentials
  - Prove that a decentralized, interoperable digital verification ecosystem can be built that can be used by many independent issuers, operators, and users
  - Design portable secure digital credentials, held by individuals, that can be independently, cryptographically and rapidly verified

Common Work plan and Deliverables

1. Develop a Detailed Project Plan
2. Prepare a draft of a Standards-Based Approach Deliverable
3. Participate in a Technical Review Workshop
4. Finalize a Standards-Based Approach Deliverable
5. Participate in a Technical Interoperability Demonstration Workshop
6. Deliver a Final Proof of Concept Report

Milestones Achieved

- **August 2019:** Challenge Issued
  - Published on ISED site.
- **November 2019:** Challenge Closed
  - 42 respondents in total
  - 20 respondents met mandatory requirements
- **June 2020: Evaluation Finalized**
  - 6 respondents selected based on rated criteria
- **September 2020 (est):** Contract Award
  - Project Estimated Start: Sept 15, 2020
  - Project Estimated Completion: March 15, 2021

Conclusion

User-Centric Verifiable Digital Credentials Challenge:

- Design portable secure digital credentials
- Demonstrate interoperability with existing technologies
- Phase 1
  - 6 vendors
  - 6 unique use cases
  - Deliverable is a Proof of concept

Full details can be found at:
https://canada-ca.github.io/ucvdcc