Digital Identity
L A B O R A T O R Y

EXECUTIVE SUMMARY

Trust Registry
Canadian Internet Registry Authority (CIRA)

ABSTRACT
Contains the summary of results of an engagement with CIRA on the subject of decentralized identity trust registries.

DATE
May, 2022

Scope

The Canadian Internet Registration Authority (CIRA) has engaged the Digital Identity laboratory of Canada (IDLab - see appendix A for more details) to **explore the emergence of trust registry services as a means to accelerate the adoption of decentralized digital identity**.

This report (1) defines the concepts for trust registry services, (2) shares key observations and (3) recommends approaches for CIRA to contribute toward digital identity advancement.

Trust Registry Defined

We examined trust registries in the context of decentralized digital identity deployment. In a classic deployment model, verifiable credentials are issued to credential holders for downstream claim(s) presentation to verifying parties for the purposes of accessing services.

The current state of the art ensures the integrity of the credential itself, providing mechanisms that engender trust without the need to consult issuers to ensure (1) they issued the credential and (2) it has not been tampered with.

While the integrity of the issued credential is assured using cryptography, the typical deployment, with its associated protocols and processes, does not provide the means to assure the authority and/or legitimacy of the issuer.

Trust registries, as we will define them herein, **provide a service to deliver attestations as to the real-world identities for credential issuers.**

"A fundamental challenge with issuing digitally signed credentials is confirming that the public key used to sign a credential does in fact belong to the claimed institution."[1]

---

[1] https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

Trust registries, in a decentralized digital identity deployment model, can be depicted as follow:
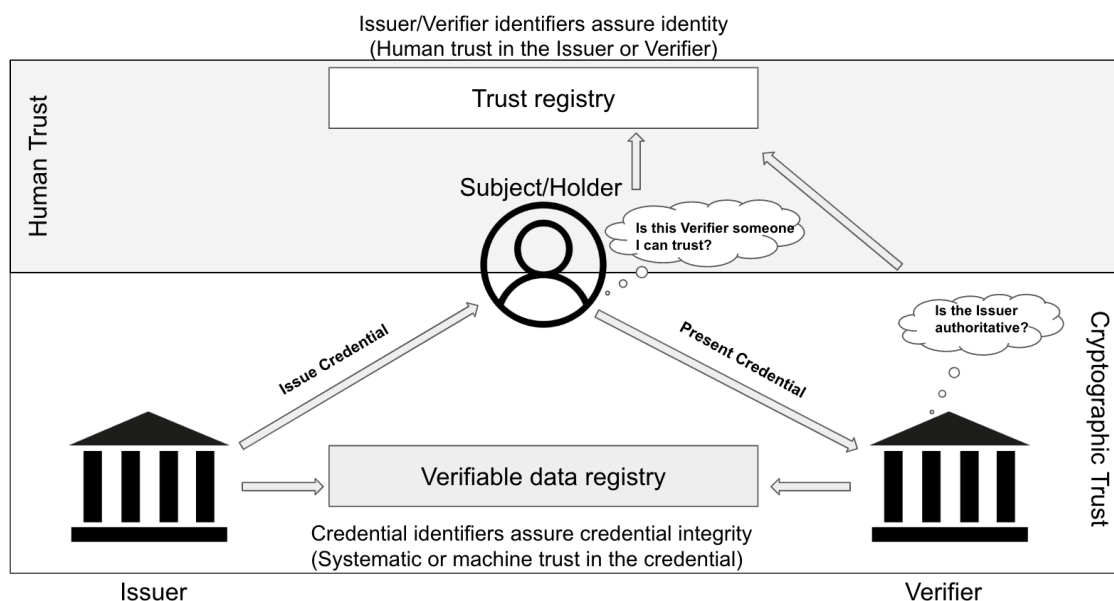
In addition to verifying the fidelity of the credential itself (cryptographic trust layer - authentic, valid and signed document), the diagram above depicts a service to enable any entity to confirm the authority under which the credential issuer is operating - the human trust layer. This serves to elevate the level of assurance for the presented claim.

Observations

The need for trust registry services in the short to medium term is increasingly validated in the marketplace by virtue of activity in standards and frameworks organizations such as the Trust over IP Foundation, Hyperledger Foundation, vertical industry initiatives such as MemberPass, and the Digital ID and Authentication Council of Canada. In addition, technology development work, primarily in the public sector, is underway in several Canadian jurisdictions.

Many parallels can be drawn between trust registry services and CIRA's expertise. To that end, CIRA is in a position to contribute its experience and know-how toward defining the missing trust anchors required to activate large scale deployment of the emerging decentralized identity ecosystem.

Next Steps

Consensus on addressing the "human trust" in decentralized digital identity is immature. This represents both a challenge and an opportunity for Canada. CIRA's position as a trust anchor delivering reliable and safe internet for Canadians would seem to place it in an advantageous position to help address this gap.

To that end, in a spirit of **collaboration and community support**, we recommend CIRA to:

1. rally the market to advance a solution to human trust,
2. contribute in the development and implementation of a proof of concept, and
3. organise discussions towards crystallizing roles and responsibilities in the governance of digital identity ecosystems.

Appendix A - The Digital Identity Laboratory of Canada

The Digital Identity Laboratory of Canada (IDLab) is an independent Canadian non-profit entity dedicated to advancing digital trust by breaking down barriers to digital ID adoption.

The IDLab promotes conformity and interoperability of user-centric digital identity solutions. The IDLab is not an incubator and does not develop or sell digital identity solutions. Our mission is to accelerate the adoption, development and knowledge of compliant and interoperable digital ID solutions.

We accomplish this mission by delivering education, assessment, advisory and sandbox services. When delivering those services, IDLab preserves its neutrality and independence by complying with its Policy on the Limitations of Commercial Activities.