Final Report

Pan-Canadian Trust Registry Community of Practice

V1.0 Outcomes and Recommendations

ABSTRACT

A report outlining the purpose, approach, key findings and recommended next steps in exploring a pan-Canadian Trust Registry.

Convened by the Digital Identity Laboratory of Canada (IDLab)
Contributions from the Community of Practice (CoP)
Sponsored by the Canadian Internet Registration Authority (CIRA)

Edited by:
Cosanna Preston-Idedia
Hadrien Seymour-Provencher

October 2023

Digital Identity LABORATORY

Table of Contents

Copyright Notice & License

Executive Summary

Securing the internet for Canadians is paramount. Verifying the authenticity of individuals or entities, and the information they are presenting, in a digital transaction pose a significant challenge to this effort. Digital credentials[1] offer a promising solution. They enable a participant in the transaction to have a high level of assurance that the information being presented is legitimate and has not been tampered with. However, on their own, they do not speak to the legitimacy of the issuer of the credential. To determine issuer legitimacy we need trust registries. Trust registries "are where you...check if a credential issuer is genuine."[2]

The anticipated emergence of multiple trust registries, each with distinct scopes and governing authority, presents a new challenge. Navigating this landscape requires mechanisms for the discovery of the appropriate trust registry to confirm the legitimacy of the credential issuer, including across international boundaries.

Canada's Internet Registration Authority (CIRA) envisioned a solution - a pan-Canadian registry of trust registries leveraging the DNS to enable a seamless trust registry and issuer discovery process. CIRA engaged the Digital Identity Laboratory of Canada (IDLab) to investigate the feasibility of this concept, employing an approach that involved problem articulation, vision formulation, expert community engagement, feedback collection, iterative refinement, use case definition, and high-level program framework considerations.

This report represents an initial exploration into an additional layer of trust for the internet. The hope is that it fosters further discussion to enhance Canadians' internet safety, encourage global collaboration, drive innovation, and promote interoperability. Empowering individuals, verifiers, and ecosystem players to better authenticate digital credentials creates a more trusted digital ecosystem.

The report elaborates upon this journey: the establishment of a pan-Canadian registry of trust registries Community of Practice (CoP), phases that were undertaken, key findings and recommendations, along with two proposed paths forward to continue progress on the initial vision beyond the scope of the CoP. The findings from the COP provide initial confidence that a registry of registries could be feasible. The proposed next steps will enable participants to drive out greater certainty.

---

[1] A digital credential represents information found in its physical counterpart, such as a passport, or a credential that has no physical equivalent, which is cryptographically signed and verifiable.

[2] Tobin, Andrew. 2023. "EU Wallet In Depth #1: Trusted Lists". https://www.linkedin.com/pulse/eu-wallet-depth-1-trusted-lists-andrew-tobin/?trackingId=NJWU3iKhIW3Gm6L2rorxkw%3D%3D

Introduction

As more transactions move online, we are increasingly scrambling to keep the internet safe for Canadians. A key problem is confirming that the actors in any given transaction are who they say they are and that the information they are presenting is valid. For example, how does an employer in Europe know that the diploma that a Canadian prospective employee is presenting from a small polytechnic institute (polytechnic A) in Canada can be trusted?

Our current ways of solving this problem - sending copies of driver's licences or university diplomas by email - are rife with fraud and privacy risks. Digital credentials[3] are increasingly being proposed as the solution for this problem because the technology that underpins these credentials can confirm for the verifier (the European employer in our example) that the credential they are receiving (e.g. the diploma) is valid (e.g. not expired or rescinded) and is not fraudulent.

However, an employer doing their due diligence would not only want to know that the diploma is legitimate but that the institution issuing the diploma is also legitimate. This is the role of a trust registry. Put simply, trust registries "are where you go to check if a credential issuer is genuine."[4]

The concept of a trust registry has far reaching implications for combating fraud, increasing the adoption of digital credentials, and increasing Canadians' overall trust in the internet. By providing reliable mechanisms for users to be able to confirm that entities issuing credentials are legitimate, trust registries will make it much more difficult for fraudulent actors to represent themselves as an authoritative entity. This acts as a risk mitigation to deter malicious actors from pursuing criminal acts, such as identity theft and scams.

However, a problem arises when we start to think about the emergence of multiple trust registries. We can anticipate multiple trust registries emerging with different scopes and areas of governing authority across Canada and internationally. Some examples are already on the horizon, such as the possibility of a trust registry for all post-secondary education credential issuers or a registry of all sanctioned auditors in the Canadian mining industry (see Appendix B). A

[3] A digital credential represents information found in its physical counterpart, such as a passport, or a credential that has no physical equivalent, which is cryptographically signed and verifiable.
[4] Tobin, Andrew. 2023. "EU Wallet In Depth #1: Trusted Lists". https://www.linkedin.com/pulse/eu-wallet-depth-1-trusted-lists-andrew-tobin/?trackingId=NJWU3iKhlW3Gm6L2rorxkw%3D%3D

non-exhaustive list of the multitude of other kinds of trust registries we could envision might include a provincial government registry of all government ministries, departments and agencies within that province that can issue credentials; a registry of all corporate registries that can issue business registration credentials; a registry of all bar associations in Canada that can issue lawyer credentials, and the list goes on.

Coming back to our example of a Canadian prospective employee (a credential holder) presenting their diploma (the credential) to a European employer (a verifier), this presents a series of questions:

1. How does the European employer know which trust registry to check to confirm appropriate legitimacy and authority of Polytechnic A?
2. If the trust registry is not known, how can it be found?
3. How is this done efficiently to minimize friction?
4. What happens when trust registries exist beyond local, regional or international boundaries?

Providing a solution that would answer these questions would unlock the next layer of trust on the digital stage. Organizations working on these registries are at the forefront of the innovation necessary to better protect Canadians, and contribute to positioning Canada as a key digital partner on the global stage.

To this end, Canada's Internet Registration Authority (CIRA) hypothesized an answer to these questions - that a pan-Canadian registry of trust registries could help international actors to find a desired trust registry within a country, and that DNS could be leveraged to connect registries to one another. CIRA enlisted IDLab to help explore the viability of these hypotheses.

IDLab deployed an approach that included:

- articulating a high-level problem;
- formulating a vision to address the problem founded on the two main hypotheses;
- establishing a community of practice of experts from the digital credentials community to explore the hypotheses and further explore the vision;
- Collecting feedback to garner expertise and continually refine a perspective on the problem statement;
- Defining use cases and a program framework for a prospective pan-Canadian registry of registries; and

- Working iteratively and conducting workshops to get a better picture of possible solutions and refine observations, conclusions, and findings.

A next layer of trust to improve the safety of the internet for Canadians is within reach and this report is an early step in that exploration.

Community of Practice (CoP): Pan-Canadian Trust Registry Exploration

IDLab proposed that through a community of practice we could explore the viability of the following hypotheses:

Hypothesis #1

An efficient structure for a network of trust registries that links Canadian trust registries to one another and the world, while still allowing trust registries within the network to maintain autonomy, includes a pan-Canadian registry of registries with a multi-party governance body that can delegate authority to other trust registries (much like .ca operates today).

Hypothesis #2

DNS is a viable organizing principle for a network of pan-Canadian trust registries needing to link with one another and international trust registries.

IDLab and CIRA put forward these hypotheses in a Vision Document that outlined the vision, approach, and rationale for exploring a pan-Canadian registry of trust registries.[5] The Vision Document was a first point of consideration for the Community of Practice (CoP).

The registry of registries was inspired by directories from the likes of the American Association of Motor Vehicle Administrators, as well as ICAO's Public Key Directory and even the internet itself with top level domains. All of which (regardless of precise technology or centralization executions) point to the need for single points of resolution for a trusted list of lists.

We put forward the organizing principle of DNS for consideration because DNS:

1. Enables a globally interoperable and unique identifier ecosystem.
2. Derisks the execution of a trust registry and increases speed to market.
3. Enables an emerging technology-governance concept (the trust registry) which remains laden with unknowns, through known technology - DNS.

[5] Note in the Vision Document this is referred to as an Apex Pan-Canadian Trust Registry. This terminology shifted on advice of the Community of Practice to a pan-Canadian registry of registries. The rationale for this shift is explained in the Alignment on terminology portion of the Key Findings and Recommendations section.

4. Can be subdivided due to the uniqueness of the identifier, and each subdivision can be managed independently.

This is not to suggest that the entire trust registry would be built in the DNS, but that it could leverage unique DNS identifiers to support the function of the trust registry. These points give the community room to focus on truly unique aspects of trust registry execution, such as supporting interoperability and readability across registries. In conducting this exploration, there were no attempts to make a decision on the organization of trust registries in Canada. Rather this report, resulting from the efforts and input of the CoP, is put forward to inform future discussion, options analysis, decision making, etc. For more information on the CoP, review the Terms of Reference.

Approach, Phases and Key Observations

Vision Document and Community of Practice Kickoff Meeting

The Community of Practice (CoP) Kickoff Meetings were held on March 7 and 9, 2023, following the circulation of the Vision Document. The CoP was set up to inform a proof-of-concept and explore the viability, desirability and feasibility of a pan-Canadian registry of trust registries (i.e. a trust registry responsible for directing traffic from both within and outside Canada to many other trust registries within and outside Canada). The feedback and discussion from the kick-off meetings served as first points of input. Following the kick-off meeting, registration to the CoP was opened and several 1-on-1 discussions with various members were conducted to bring forth key elements, interest, and concerns surrounding the initiative.

The following were the key take-aways from the kick-off meetings. These are further elaborated in Appendix C, which was added to the Vision Document following the kick-off meeting:

- There was interest in a pan-Canadian registry of registries leveraging the DNS;
- There was a desire to:
    - Step back from the hypotheses and properly identify the problem/opportunity statement;
    - identify use cases; and
    - evaluate frameworks and governance models.

Steps were then initiated to integrate the input received into the CoP's approach, including the Use Case Identification and Modelling Discussion Workshops described below.

Use Case Identification Workshop

A Use Case Identification Workshop was held on April 24th, 2023, which aimed to review and evaluate potential use cases for a pan-Canadian trust registry model. During the workshop, CoP participants reviewed and discussed use cases that had previously been submitted. Various considerations were analysed, with an emphasis on international reach and the possibility of leveraging elements of the

DNS and organizing the governance in a pan-Canadian registry of trust registries configuration where a pan-Canadian trust registry could act as a registry of registry to support actors in finding primary trust registries[6] spread across the country.

Key points raised during the discussions included:

- The desire to include a non-credential based use case that requires a trust registry as there are many trust tasks outside of credential exchange scenarios that require authoritative sources.
- A desire for greater clarification on the proposed issuers, verifiers, and the role of the trust registry in each use case.
- The role of DNS in lookup and trust decision: leveraging DNS for trust lookup could be an efficient method to validate trust information.
- The need for international collaboration:
    - global standards and cooperation are vital to foster interoperability between countries and facilitate cross-border interactions;
    - Identifying an international partner(s) to co-create any prospective proof of concept from this COP would be valuable to this exploration.
- The need to select credential use cases that are in test or production environments (as opposed to conceptual) and have existing governance structures. This would ensure the efforts would remain focused on the trust registry rather than bringing the use case to life.
- The desire to better define the specific trust problem before developing a trust solution.

The CoP developed a method to refine and prioritize use cases based on the above feedback, and three were selected by the CoP using a voting tool. The three use cases selected were:

1. Education Credentials: Academic institutions issue credentials such as diplomas, transcripts, proof of enrollment, etc. A pan-Canadian registry of trust registries could help a verifier, for instance from another country, identify the (hypothetical) Canadian post-secondary institution trust registry, in order for the verifier to determine that the issuing academic institution is legitimate.

[6] We use the term *primary trust registry* to refer to all trust registries we anticipate will be established in Canada with responsibility for primary lists (e.g. list of education institution issuers) as opposed to directory type trust registries (e.g. the proposed pan-Canadian registry of trust registries) that would act as a list of lists.

2. Mining Association of Canada, Towards Sustainable Mining (TSM) credential: An auditing organization issues the Towards Sustainable Mining (TSM) credential, accredited by the Mining Association of Canada (MAC), to a mining company so that it can demonstrate environmental, social and governance (ESG) aspects and compliance. A pan-Canadian registry of trust registries could help a verifier (e.g. investment funds, supply chain, buyers, etc.) identify the (hypothetical) Canadian trust registry that registers issuers of auditing conformance credentials, in order for the verifier to determine that the issuing auditing organization is legitimate.
3. Know Your Customer (KYC), Opening a Financial Account: Governments (or other trusted sources) issue identification to individuals. A pan-Canadian registry of trust registries could help a verifying financial institution in another country identify the (hypothetical) provincial trust registries that registered government credential issuers, such as driver's licence issuers, in order for the verifying financial institution to determine that the ID presented as proof of identity to open a bank account is from a legitimate issuer.

See Appendix B - Refined Use Cases for more details on each use case.

Modelling Discussion Workshop

A Modelling Discussion workshop was conducted on June 23, 2023, which gathered input on what a model could look like for a pan-Canadian trust registry, based on attributes from existing trust registry models. The CoP was invited to submit existing reference models for trust registries or trust registry adjacent structures to guide the conversation. A list of models and attributes were circulated beforehand. Attributes discussed included the importance of open standards versus proprietary solutions, the need to leverage existing processes and governance, and the consideration of centralization versus decentralization.

Throughout the June 23 discussion, CoP participants shared their expertise as the group explored trust registry and credential models. Key inputs resulting from this discussion were:

- A trusted path to discover a correct primary trust registry is desirable;
- Established governance and processes must be maintained and respected;
- The DNS system should be used as a means of lookup and referral to trust registries, rather than being a "source of truth" itself;

- There is a strong sense that many primary trust registries will want to retain their own autonomy/authority over their list;
- A pan-Canadian registry of trust registries should have onboarding requirements that confer some level of trust on primary trust registries.

The result of the meeting was a greater consensus on the problem that a pan-Canadian registry of trust registries is trying to solve: how does an actor trust the discovery process of disparate trust registries?

While additional clarity was gained and some progress was made in better understanding the problem statement, subsequent community feedback made it clear that this issue wasn't entirely resolved. This is in part what informed the recommendation for Next Step #2 - Co-created IDLab Project Submission with Design Thinking Framework in the request from COP members to further interrogate the problem that a registry of registries is trying to solve would be more deeply explored, framed in a design thinking mindset.

Program Framework and Governance Model:

Following the distribution of the Vision Document, conducting CoP workshops, and an Interim Report, a program framework and governance model for a pan-Canadian registry of trust registries was circulated to community members (see Appendix D). This framework aimed to concretely define what a pan-Canadian trust registry – a registry of registries – grounded in the DNS could look like. The purpose was still to further explore the central question: how does an actor trust the discovery process of disparate primary trust registries? The outline for potential principles, user stories and data schemas added a layer of consideration for the CoP to ponder and question. The purpose of this pan-Canadian trust registry would still be to facilitate secure and reliable interactions within a digital identity ecosystem.

The document was well received by the CoP, and provided a medium of discussion for some of the details that had either been assumed or mentioned in passing during conversations. This exercise also revealed points that had not been entirely resolved, did not have unanimous consensus or alignment across the community, or additional questions that would need to be explored in greater depth.

For example, principles such as transparency and accountability had previously been taken for granted, and their inclusion in the framework reinforced the CoP's

alignment. However, other points, such as the registration model for a pan-Canadian trust registry, and the impact that the onboarding criteria of a registry of registries may have on an onboarding trust registry's ability to govern itself, were not resolved. The extent to which a pan-Canadian trust registry could be used to inform a verifier's decision to trust an issuer versus directly conferring trust on the issuer was put to question. Previous consensus on how a trusted path to discovery could be desirable was also called into question.

This exercise complemented previous activities and improved the community's understanding, providing valuable feedback and stimulating discussion. IDLab, CoP participants and key stakeholders were able to more directly engage on key points, but not reach full resolution on some of these details.

These important disagreements lead us to favour action over additional hypothetical discussion to further our explorations. Accordingly, the following section elaborates on the important findings that will require further refinement and provides recommendations on how to reach a more complete picture of what is feasible, desirable and viable for a registry of registries that will help a verifier answer the question: is this issuer trustworthy?

Key findings and recommendations

Based on feedback from the distribution of the Community of Practice Interim Report and program framework and governance model outline (Appendix D), many insights came to light as to what a pan-Canadian trust registry could look like. Though there was alignment on some requirements for specific use cases, and the idea of a registry of trust registries was more clearly defined, the CoP did not find resolution on all points. Below are key findings from the CoP initiative with recommendations on how to move forward.

The observations and related recommendations cover a range of considerations for a pan-Canadian registry of trust registries. As such, the common theme of engaging with use-case ecosystem participants, and working closely with would-be verifiers and would-be primary trust registry governance bodies emerges as an overarching recommendation. This applies with respect to determining the appropriate registration model, engaging in prototyping, determining scope and scale, and all other activities in which user and stakeholder feedback will be crucial.

1. **Alignment on terminology**
   One sticking point since the inception of the CoP was concerns over the use of the word “apex” to describe the envisioned pan-Canadian trust registry, as seen in some founding documents, such as the Terms of Reference & Vision Document for the Pan-Canadian Trust Registry CoP. The concern was that the emphasis on *apex* inferred to hierarchy and singularity. Through discussion the CoP gained consensus that there are likely to be multiple registries of registries serving various industry, trade and international relations purposes. There was also consensus that trust registries were not subordinate to a registry of registries. Therefore *apex* was not an appropriate term.

   We have since seen greater alignment in describing these terms, but no consensus has been reached in identifying the best labels to articulate the specific relationships of the entities involved. For now we are using the following working definitions:

- **Primary Trust Registry** refers to the individual registries maintaining a list of entities that can issue digital verifiable credentials within a set ecosystem.

- **Registry of Trust Registries** refers to a registry of primary trust registries, and will replace the term apex trust registry going forward.

Recommendation – Refine terminology: While these definitions are reflected in Appendix A - Key Terms / Glossary, these terms, labels and definitions have continued to cause confusion and conflicting interpretation, due in part to their association to other concepts related to the field of information technology. As this misinterpretation and conflation persists, subsequent terms and definitions that more widely resonate with audiences at all levels of comprehension on the subject should be sought to replace them.

2. **The role of a registry of registries**
   There was consensus that a registry of registries would provide information about primary registries known to it. The presence of a primary trust registry within a pan-Canadian registry of registries is intended as an input to trust decision about whether or not to trust the issuer of the credential in question. It is not meant to be a decision in itself.

   Furthermore, there was discussion about how a registry of registries could provide a trusted path to discovery, meant to facilitate the findability of relevant primary trust registries. Not all CoP participants agreed that a trusted path to discovery of primary trust registries would be favourable, as this may impose inappropriate restrictions on how the primary trust registry would have to conduct and govern itself in order to be included within the registry of registries. A trusted path to discovery implies other paths to discovery with varying degrees of implicit trust, and evokes questions such as:

   a. Who or what governs the list of primary trust registries, including their status within the registry of registries?

   b. What is the criteria for being recognized and accepted, or perhaps more importantly, rejected from being included in the registry of registries?

   c. Is the governing body of the registry of trust registries capable of determining the credibility of one primary trust registry or the other, and does that place these trust registries on some sort of equal footing beyond the authority of represented issuers to issue their respective credentials?

Recommendation – Further refinement: While clear onboarding criteria, transparency and accountability were identified as important aspects of a pan-Canadian registry of primary trust registries, as outlined in the principles section of the program framework and governance model (see Appendix D), further refinement is still necessary. It will be important to continue to engage in material use-cases – working with end-users and governance bodies that may envision operating a primary trust registry (e.g. a corporate registry, a professional association etc.) – to appropriately answer the questions and concerns raised in this finding. These activities will be crucial in producing an end-state that provides benefit to stakeholders without impeding on the rights and authority of existing bodies to operate and govern themselves.

3. **Registration model**
   While the program framework and governance model refers to an opt-in registration model within its principles, this was for the sake of example to elicit discussion. In reviewing the program framework and governance model, CoP members did not reach consensus on if this would be the optimal model for primary trust registries to register with a registry of registries. Two models were explored in the Showcase Findings Presentation: a voluntary opt-in (push) model and public information collection dissemination (pull) registration model (see table below) and there was consensus that the optimal model could change based on the registry of registries' governance, industry, jurisdiction, ecosystem and other contextual considerations.

Collection / Registration Model

Voluntary Opt-in Registration (Push)	**Public Information Collection / Dissemination (Pull)**
A primary registry opts in to be listed (either they initiate process, or are approached as a prospect to begin the process): • Criteria for inclusion are well-defined and communicated • Only trustworthy registries that volunteer are listed	The registry of registries proactively includes trust registries that are meant to be public: • Contain public information (non-PII) • Make decisions by itself about what is registered • Transparent about reasons and criteria for inclusion
Slower growth towards critical mass for	Grow faster and be more immediately useful

usefulness	
Reputation protection is built-in to onboarding process and initial collaboration with trust registries ensure accuracy of their information	Will require more ongoing work to maintain, garner and protect its reputation

Recommendation – Proof-of-concept: More work is required to explore the optimal information collection and entity registration model, and it may not be the case that one model fits all use-cases or environments. It is recommended that a proof-of-concept and prototyping phase be engaged to further explore which model may be appropriate. The model will depend on the prototyping approach, contributors and stakeholder involved.

4. **User stories**
   Generic issuer onboarding and verifier user stories still need to capture use case specific requirements, such as:

   a. Some use cases requires high automation to accommodate scale;

   b. Industry-specific established standards shape direction as dominant standards adopted by key industry stakeholders typically determine the direction for the rest of the industry, which follows suite;

   c. Steps in use case protocols may differ and do not necessarily reflect familiar steps used for physical credential use. For example, in the Aries protocols, which issuers are accepted by a verifier must be known ahead of the point of credential presentation and configured into the proof request; and

   d. Primary trust registries require the independence to register with multiple registries and determine their own governance.

Recommendation – Engage verifiers and primary trust registries:
Engaging with use-case ecosystem participants and working with would-be verifiers and primary trust registry governance bodies will ensure that the correct elements are captured in the user stories to provide the benefits and insights sought from a pan-Canadian registry of trust registries.

5. **Consideration for digital credential holders**
   The holder should also be represented in user stories, as they could benefit from being able to authenticate a verifier before presenting their credentials.

Recommendation – Further explore the inclusion of verifiers in primary trust registries: While the initial conception of a pan-Canadian registry of trust registries focused on primary trust registries that collected and made available authoritative issuer information for holder credentials, additional considerations should be made towards primary trust registry that contain issuers of verifier credentials, so that holders can also determine if they want to trust the entity requesting their credential.

Whether or not trust registries should encompass issuers of verifier credentials depends on the standard or framework reviewed, as does whether or not trust registries should comment on whether or not a verifier is authorized to request a specific credential.[7] It would then follow that user stories encompassing the credential holder could also be included, as they would benefit from being able to authenticate a verifier, and potentially the verifier's authority to request a credential, before presenting their credentials.

It is recommended that these considerations be further explored through a subsequent proof-of-concept and prototyping phase.

6. **Scope and scale**
   A pan-Canadian registry of trust registries should carefully consider the appropriate scope and scale of its registration. Primary trust registries referenced that are either so niche or so obscure (e.g. a "Registry of Best Banjo Players" pushed by the actor Steve Martin), that they aren't useful and could detract from the value provided by a pan-Canadian registry of trust registries.

Recommendation – Feasibility and viability analysis: It is recommended that more defined requirements related to the scoping and scale of a pan-Canadian registry of trust registries be further explored during the feasibility and viability stages of a subsequent proof-of-concept and prototyping phase. This will allow for the determination of the appropriate fit of the prototype, and expose insights specific to the appropriate scope and scale of a production.

7. **Non-credential use cases**
   User stories and data schemas should allow flexibility for non-credential use cases as there are many ecosystems or digital interactions that don't necessarily involve credentials. Examples could include engineering

[7] The Trust Over IP (ToIP) Trust Registry Task Force definition includes verifiers while the Digital Identity and Authentication Council of Canada Trust Registries Component Overview leaves it open to the decision of a particular trust registry.

drawings and documents that require a signature by a professional engineer (an action that a P.Eng. is authorized to do by virtue of being licensed). While the license may be proven through a credential, the signature itself does not constitute a credential, but helping verify its legitimacy could be a function executed by a pan-Canadian Registry of Trust Registries. . Including this kind of non-credential use case for consideration in its scope could lead to greater flexibility and scaling of the applications for a pan-Canadian registry of trust registries.

Recommendation – Desirability analysis: While we can envision benefits from including non-credential considerations in the operation of a pan-Canadian registry of trust registries, scoping and scale of a production has not been fully defined. As described in the previous point, the range of requirements, either for a prototype or end-state production, remain to be determined. It is recommended that the inclusion of non-credential use cases in a pan-Canadian registry of trust registries be further explored during the desirability stage of a subsequent proof-of-concept and prototyping phase. This will allow for the determination of the appropriate fit of the prototype, and expose insights specific to the appropriate requirements for production.

8. **Multiple registries of trust registries in Canada**
   There will likely not only be one registry of trust registries in Canada, and primary registries may be registered with none, one, or more than one registry of trust registries.

Recommendation – Stakeholder analysis: While no pan-Canadian registry of trust registries currently exists, or any specific analogue with which to compare, it will be important to gauge the evolution of the landscape. Furthermore, as with some of the unresolved points and findings listed such as whether to employ a voluntary opt-in (push) or public information collection (pull) model, registries of trust registries may end up taking different shapes, and have different and unique applications. As such, it may be beneficial for primary trust registries to be registered in multiple registries based on their needs. It is recommended that knowledge and best practices sharing be widely adopted by those designing trust registries, interested parties and related communities, to better shape the ecosystem to stakeholder requirements, promote alignment and enable standardization.

9. **Data schemas and protocols**

a. If the DNS is to be leveraged in the design of a registry of primary trust registries it should make elements of the DNS (web domain, URL) as much as possible, as the case allows, aligned with the initial hypothesis of this CoP;

    i. DNS can be used to ensure issuers have unique identifiers based on domain names, and this enables lookup mechanisms, and has the potential to facilitate global interoperability by using DNS as a discovery protocol;

b. Leave the identification method broad enough (e.g. use the term "verifiable identifier" instead of prescribing specifically decentralized identifiers);

c. Include accepted credential formats (E.g. W3C, AnonCreds, etc.) and protocols;

d. Include timestamps for when a primary trust registry record was created/updated, including governance versioning;

e. Include protocol configurations for query resolution TTL (time to live) and return failure (not found); and

f. Have the scope of primary trust registries well defined in the data schema represented in a registry of trust registries, aligned with the primary trust registry's governance. This would include primary trust registry status, onboarding and revocation information.

Recommendation – Prototype scoping: It is recommended that more defined requirements related to the scoping and scale of a pan-Canadian registry of trust registries be further explored during the feasibility, viability and desirability stages of a subsequent proof-of-concept and prototyping phase. This will allow for the determination of the appropriate fit of the prototype, and expose insights specific to the appropriate scope and scale of a production.

10. **Registries of trust registries vs. primary trust registries**
    The exercise of exploring what a pan-Canadian registry of trust registry could look like was informed by an Inventory of trust registries and frameworks for the Pan-Canadian Trust Registry CoP, the Pan-Canadian Trust Framework™ for Trust Registries (Trust Registries Component Overview Draft Recommendation & Conformance Profile Draft Recommendation V1.0) created by the Digital ID and Authentication

Council of Canada (DIACC) , and work done by the Trust Over IP (ToIP) Trust Registry Task Force.

The guidelines, specifications, and existing experimentations are generally intended for primary trust registries. In most cases registries of trust registries and their slightly different considerations and requirements were in scope.

To illustrate this point we highlight below a few diverging points where the Conformance Profile Draft Recommendation V1.0 works for a primary trust registry (the scope of the component) but may need additional consideration if the scope were to broaden to registries of registries. Take the following four points:

- **Ref 106r; row 14:** "An Ecosystem MUST document and publish the policy and process for verification of the legal authority of Registrants to issue credentials or accept credential presentations."

  Ref 106be; row 8: "An Ecosystem MUST require that Registrants conform to a recognized trust framework such as the PCTF."

- **Ref 106ao; row 13:** "A Registry MUST provide information about Registrants and their status in industry standard formats and protocols."

- **Ref 106v; row 18:** "An Ecosystem MUST conform to a recognized Trust Framework such as the PCTF or equivalent."

While a primary trust registry is within its purview to dictate the terms of registration for issuers, or the framework under which it operates, or the status of their registrants, use case representatives have expressed reservations at the idea of a registry of registries dictating these same requirements, as it could infringe on the governance authority of the primary registry.

Recommendation – Registries of registries refinement: For greater resolution and consensus surrounding the principles and standards related to a pan-Canadian registry of trust registries (and registries of registries in general), it is recommended that stakeholder engagement and collaboration continue. It will be important to maintain varied perspectives for future efforts by encouraging active participation from a wide range of stakeholders, including government agencies, private sector entities, non-profit organizations, and most importantly, end-users.

Additional recommendations for CoP participants and stakeholders

While the CoP in its current form has concluded with the circulation of this final report, participants and stakeholders may still wish to further explore a pan-Canadian registry of trust registries, or ideas and concepts related to it in another form. With this in mind, here are some recommendations on what next steps and ongoing activities should consider:

- **Continued stakeholder engagement and collaboration:** Maintain varied perspectives for future efforts. Encourage active participation from a wide range of stakeholders, including government agencies, private sector entities, and non-profit organizations, to ensure diverse perspectives and expertise are represented. Prioritize the involvement of end-users.
- **Knowledge sharing and best practices:** Facilitate regular knowledge-sharing sessions where community members can showcase successful use cases, discuss challenges, and share best practices. This will promote alignment and standardization.
- **Training and capacity building:** Develop and offer training material, workshops, and resources on trust registry work so far, to engage individuals that are new to the discussion, and enhance the capabilities, skills and understanding of existing participants and external stakeholders.
- **Use case documentation:** Encourage continued use case documentation that highlights challenges, ongoing and evolving requirements, and solutions when contemplating or implementing trust registry initiatives. This documentation can serve as a valuable resource for those looking to advance trust registries.
- **Technology evaluation and adoption:** Stay updated on emerging technologies, protocoles, data schemas, credential formats, and solutions related to primary trust registries and registry of trust registries. Evaluate their suitability for specific use cases, share these ideas and maintain open discussions. This will promote common understanding on relevant topics and accelerate discussion and progress.
- **Policy and standards refinement:** Collaborate with other relevant organizations, such as the Digital ID and Authentication Council of Canada (DIACC) and the Trust Over IP (ToIP) Trust Registry Task Force to develop and refine existing frameworks to also encompass registries of primary trust registries.

- **Advocacy and outreach:** Promote the value and potential benefits of registries of primary trust registries within the broader community. Advocate for increased awareness and support from relevant stakeholders, including government agencies, industry associations and international partnerships.

Next steps - two paths forward

The CoP has been able to engage in productive discussion, involving key stakeholders and integrating the insights from a wide range of perspectives and expertise. It is recommended that subsequent activities be undertaken by CIRA and the community that go beyond the scope of the CoP. These next steps are outlined below. They will be important steps towards resolving some of the outlying findings included herein, while further engaging key contributors and producing more material outcomes.

The recommendation is that a proof-of-concept / prototyping exercise be undertaken in one or both of the following methods:

Next Step #1 - Prototype / Assessment:

It is recommended that CIRA pursue the creation of a prototype(s) to continue to investigate the viability of a pan-Canadian registry of registries grounded in DNS. To effectively evaluate the prototype with respect to its ability to address the desirability, feasibility, and viability, an assessment should be performed based on a set of criteria grounded in the findings of the COP. We recommend that:

- CIRA and IDLab define the scope of desired findings from the prototype(s).
- CIRA establishes a prototype team to design and build a prototype(s).
- CIRA pairs that with an IDLab assessment team who performs an independent assessment of the prototype(s).
- The IDLab assessment team creates, based on relevant industry frameworks and findings from the Trust Registry CoP, an evaluation framework aligned with the scope of desired findings.
- The two teams, along with relevant stakeholders, work collaboratively and iteratively to define prototype requirements that are designed to address specific evaluation criteria.
- Each iteration takes a user-centric approach and allows for continuous integration of feedback.
- Findings are then published when the scope of desired findings is achieved through the prototype and assessment activities.

Next Step #2 - Co-created IDLab Project Submission with Design Thinking Framework:

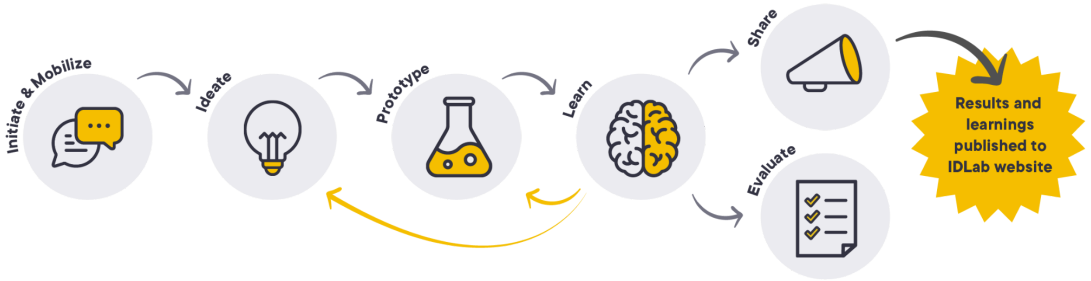
In response to COP member request to further interrogate the problem that a registry of registries is trying to solve, IDLab will leverage its co-created project program, which is grounded in design thinking approach to deepen the exploration of the problem. The proposed focus of this exploration is:

How might we *support international verifiers to find unknown trust registries in Canada so that those verifiers are able to determine if the issuer is legitimate?*

While **Next Step #1** takes the work of the COP and prioritizes convergence and will offer significant technology learnings, the method for **Next Step #2** prioritizes divergence to gather further end-user insights and offer an array of potential prototyping avenues, which in turn may benefit from future convergence and assessment.

The first step to becoming an IDLab Co-created Project is to pass through IDLab's intake process, which includes community outreach and feedback, as well as approval and prioritization by IDLab's independent Steering Committee.

Assuming this proposed project makes it through intake, it would then move on to IDLab's delivery process, which is grounded in Design Thinking.[8] Here we establish a team, gather inspiration from users, brainstorm possible solutions, prototype them, learn through testing and then evaluate and share our learnings publicly.



Our design thinking process is iterative by nature, and the three phases – Ideate, Prototype, Learn – may be repeated to test new ideas (the number of iterations will vary depending on the nature and complexity of the project).

You can learn more about our Project Intake and Delivery process on our website.

[8] IDLab leverages IDEO U's design thinking process: https://www.ideou.com/pages/design-thinking

Conclusion & Closing Remarks

As the shift towards digital transactions and the use of credentials accelerates, ensuring the safety of Canadians becomes paramount. Verifiable credentials have emerged as a real-world solution and they are likely to be a widely adopted tool in establishing the identity of individuals, entities, and otherwise. However, a persistent challenge lies in verifying the legitimacy of actors involved in transactions, especially the legitimacy of issuers.

Trust registries, and a trusted list of these lists, could be a powerful solution to bridge this trust gap. Implementing such registries holds immense potential in protecting Canadians by combating fraud and bolstering the adoption of digital credentials. However, a registry of registries only works if it can be found.

Empowering individuals, verifiers and ecosystem actors to confirm the authenticity of their credentials, and enabling them to exert greater control over their digital identity, is a crucial step in the evolution of a trusted digital ecosystem. Standardizing credential verification through trust registries instills confidence that actors in digital interactions are who they say they are. This not only fortifies the digital landscape by improving cybersecurity, but also empowers individuals with the knowledge and tools they need to foster the trust in these systems that is necessary to promote adoption.

The recommended next steps represent strategic and thorough approaches towards advancing the development of a pan-Canadian registry of trust registries leveraging elements of the DNS. The culmination of productive discussions and initiatives within the CoP paved the way for these additional phases, but much work remains to be done. The two proposed paths forward exemplify harnessing innovation from a community towards positioning Canada as a global leader in digital trust.

Acknowledgements

We extend our sincere gratitude to all the dedicated members of our Community of Practice whose invaluable insights and contributions have been instrumental in shaping this report (and any individuals and organizations not specifically mentioned below including those who have chosen to remain anonymous). Their collective expertise and unwavering commitment to our shared goals have been truly commendable:

- [Name/Organization]
- [Name/Organization]
- [Name/Organization]
- [Name/Organization]
- [Name/Organization]
- [Name/Organization]

We are pleased to acknowledge the contributions of individuals and organizations whose input and support have enriched the content and depth of this report.

We also extend our sincere gratitude to the Canadian Internet Registration Authority (CIRA), the sponsor of this report.

Appendix A - Key Terms / Glossary

Apex pan-Canadian Trust Registry: A trust registry that supports Canadian governments and industries, and acts as a single point of resolution for trust registry routing and verification within the ecosystem network, where needed by ecosystem actors. This term was first employed in the Vision Document for this CoP and has since been replaced by the term: registry of registries.

Digital credentials: A digital credential represents information found in its physical counterpart, such as a passport, or a credential that has no physical equivalent, which is digitally signed and verifiable.

DNSSEC: The DNS Security Extensions (DNSSEC) fortifies the DNS resolution process and strengthens authentication using digital signatures based on public key cryptography so that the DNS data itself is signed by the owner of the data.[9]

Global interoperability: The ability for systems to communicate, interface, translate, interpret, exchange information and ultimately interoperate with each other, internationally and on a global scale, in accordance with established standards and protocols.

Pan-Canadian: Relating to Canada as a whole in reference to collaborative action with partners and stakeholders at all levels and across the public and private sector.

Primary Trust Registry: refers to the individual registries maintaining a list of entities that can issue digital verifiable credentials within a set ecosystem.

Registry of Trust Registries: refers to a registry of primary trust registries, and will replace the term apex trust registry going forward.

Trust Registry:

> ***Layman's definitions:*** Trust registries "are where you go to check if a credential issuer is genuine, or where you check to see if the wallet app you are using is certified, or how you determine if a verifier is the real organisation you think it is or if they are an imposter asking for your data."[10]

[9] ICANN, 2019, 'DNSSEC – What Is It and Why Is It Important?', https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en#
[10] Tobin, Andrew. 2023. "EU Wallet In Depth #1: Trusted Lists". https://www.linkedin.com/pulse/eu-wallet-depth-1-trusted-lists-andrew-tobin/?trackingId=NJWU3iKhlW3Gm6L2rorxkw%3D%3D

Trust over IP's Trust Registry Task Force's definition: a trust registry is "a network service. [It] enables a governing authority for an ecosystem governance framework (EGF) to specify what governed parties are authorized to perform what actions under the EGF."

In doing so a trust registry would support asking the following questions:

1. "Is this Issuer Authoritative to issue a particular credential type under a governance framework?
2. Is a Verifier Authorized to request a presentation under a governance framework?
3. Does the answering Trust Registry acknowledge another Trust Registry under a governance framework?"[11]

Pan-Canadian Trust Framework definition
A digital service operated by a Digital Identity Network that provides information about Registrants. The information can be human readable and/or machine readable such that people and technology services can make informed decisions about the trustworthiness of a Registrant's services (e.g., assurance level as per a Trust Framework). The Trust Registry may include a Verifiable Data Registry component.[12]

Unique identifier: alphanumeric string associated to a single entity within a given system.[13]

Verifiable Data Registry: A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as digital credential schemas, revocation registries, issuer public keys, and so on, which might be required to use digital credentials. Some configurations might require correlatable identifiers for subjects. Some registries, such as ones for UUIDs and public keys, might just act as namespaces for identifiers.[14]

---

[11] Trust over IP. 2023. "ToIP Trust Registry Protocol Specification". https://wiki.trustoverip.org/display/HOME/ToIP+Trust+Registry+Protocol+Specification
[12] Digital Identity and Authentication Council of Canada. 2023. "PCTF Trust Registries Component Overview". https://diacc.ca/wp-content/uploads/2023/03/PCTF-Trust-Registries-Component-Overview_Draft-Recomendation-V1.0r.pdf
[13] Wigmore, 2019, 'What is a unique identifier (UID)', TechTarget, https://www.techtarget.com/iotagenda/definition/unique-identifier-UID#:~:text=A%20unique%20identifier%20(UID)%20is,be%20accessed%20and%20interacted%20with
[14] Sporny et al., 2022, 'Verifiable Credentials Data Model v1.1', W3C, https://www.w3.org/TR/vc-data-model/

Appendix B - Refined Use Cases

#1 - Education Credential

- Academic institutions issue diplomas, transcripts, proof of enrollment, etc. to students and graduates so that they can demonstrate accomplishment of prerequisites to other academic programs or prospective employers for enrollment or proof of qualification.

Status: Organizations currently operating in this space with robust governance in place.

Participation: In conversation representatives to gain input from the education sector.

Trust Registries	1. The primary trust registry is the hypothetical Canadian post-secondary trust registry responsible for maintaining the list of post-secondary credential issuers and responsible to register with the pan-Canadian registry of trust registries. 2. The pan-Canadian registry of trust registries - responsible for maintaining a list of trusted trust registries to direct queries.
Issuers	Academic institutions issue credentials such as transcripts, degree certificates, student cards, employee credentials etc. Use of trust registries: The academic institutions are listed in a Canadian post-secondary trust registry. Onboarding to that trust registry is managed by a designated post-secondary governing authority.
Holders	Students, academic staff and non-academic staff of the universities, alumni. Use of trust registry: They could (if needed) check the trust registry (through their wallet) to confirm that their credential is truly coming from a valid issuer. Their wallet may or may not have a direct connection to the Canadian post-secondary trust registry and may rely on the pan-Canadian registry of trust registries for direction.

Verifiers	A broad group including but not limited to other academic institutions, prospective employers and professional associations both nationally and internationally. Use of trust registries: They would check the trust registry to confirm that the academic institution issuing the credential is legitimate. If they are from outside of Canada or not robustly connected to trust ecosystems within Canada, they may not know how to check/find the Canadian post-secondary trust registry directly and may need the support of a directory (e.g. the pan-Canadian registry of trust registries) to complete this confirmation check.

#2 - Mining Association of Canada, Towards Sustainable Mining (TSM) credential

- An auditing organization issues the Towards Sustainable Mining (TSM) credential, accredited by the Mining Association of Canada (MAC), to a mining company so that it can demonstrate environmental, social and governance (ESG) aspects and compliance to verifiers (investment funds, supply chain, buyers, etc.)

Status: Ongoing pilot project robust governance and close ties to Government of BC.

Participation: Commitment from the Government of BC to participate and high likelihood of MAC participation.

Trust Registries	1. The primary trust registry is the hypothetical Mining Association of Canada trust registry responsible for maintaining the list of auditing firms that are permitted to issue TSM credentials and responsible to connect to the pan-Canadian registry of trust registries (and potentially other national/international industry related trust registries). 2. The pan-Canadian registry of trust registries - responsible for maintaining a list of trusted trust registries, which includes the Mining Association of Canada trust registry, to direct queries.

Issuers	An auditing organization, authorized by the Mining Association of Canada, issues the TSM credential. Use of trust registries: The auditing organization is listed in a Mining Association of Canada trust registry. Onboarding to that trust registry is managed by the Mining Association of Canada or its delegate.
Holders	Mining companies Use of trust registry: Given the relationship with the auditing firm, it is unlikely they would need the trust registry.
Verifiers	A broad group including but not limited to investors, stakeholders, and compliance monitors both nationally and internationally. Use of trust registries: They would check the trust registry to confirm that the auditing organization issuing the credential is legitimate. If the verifier is from outside of Canada or not robustly connected to trust ecosystems within Canada, they may not know how to check/find the Mining Association of Canada trust registry directly and may need the support of a directory (e.g. the pan-Canadian registry of trust registries) to complete this confirmation check.

#3 - Know Your Customer (KYC), Opening a Financial Account

- Government (or other trusted source) issues identification to an individual so that they can present the ID to a financial institution in another country as proof of identity and open a bank account.

Status: Generic use case with no explicit access to collaborating organizations for testing.

Participation: While KYC has been widely developed and adopted, no specific participants have been identified.

Trust Registries	1. The primary trust registries are the hypothetical provincial registries responsible for maintaining the list of entities that can issue government ID. 2. The pan-Canadian registry of trust registries - responsible for maintaining a list of trusted trust registries, which includes these provincial registries.
Issuers	Government issues identification to an individual confirming that they are who they say they are. Use of trust registries: The government entity is listed in a provincial registry of government issuing authorities. Onboarding to that trust registry is managed by the province.
Holders	Individual residents of the province Use of trust registry: Given the relationship with the issuing authority, it is unlikely they would need the trust registry but could use it in the case of a questionable or ambiguous credential.
Verifiers	Financial institutions potentially nationally and internationally. Use of trust registries: They would check the trust registry to confirm that the auditing organization issuing the credential is legitimate. If the verifier is from outside of Canada or not robustly connected to trust ecosystems within Canada, they may not know how to check/find the Canadian provincial trust registry directly and may need the support of a directory (e.g. the pan-Canadian registry of trust registries) to complete this confirmation check.

Appendix C - Feedback on Vision Document from Community of Practice and Next Steps

Feedback on the vision document was collected from those that registered to the Community of Practice. These inputs were captured: during the pan-Canadian Trust Registry kick-off meetings the week of March 6, 2023; as comments captured within the documents; and during 1-on-1 discussions to have a deeper dive about the document's content, up to and including March 22nd, 2023. This feedback, and next steps, have been captured below.

A total of 24 individuals from 13 organizations and 3 Canadian jurisdictions and 1 international jurisdiction have registered for the Pan-Canadian Trust Registry Community of Practice as of Tuesday March 28, 2023.

Interest in an apex pan-Canadian Trust Registry leveraging the DNS

The community as a whole has shown support and appreciation for the need for a functional and accessible mechanism to confirm the legitimacy of actors within the digital credentials ecosystem, such as issuers and verifiers. An apex pan-Canadian trust registry responsible for directing traffic from both within and outside Canada was well received. Many in the community recognized that DNS has the potential to serve as a robust foundation for building a network of trust registries as an organizing principle, and are interested in exploring this concept in greater depth.

Problem/opportunity statement and identification of need being addressed

Multiple stakeholders observed that before proposing a solution, a more elaborated description and understanding of the problem and/or opportunity being solved is required. This desire emanates from a desire to lead with user needs vs technology and is made tangible through two actions further recommended by contributors: identification of use cases and identification of existing trust registry models.

Identification of use cases

It was recommended that concrete use cases be identified and explored. Commentators highlighted a desire to ground the exploration in real-world problems founded in existing and emerging needs and suggested that a use-case approach could result in a more applicable outcome. Where possible, it was also recommended that stakeholders representing these use cases be invited to join the COP.

Evaluation of other frameworks and governance models

There is also a desire to better understand (and capture in the vision document) what models are being used or considered globally in the trust registry space to first contextualize the Apex and DNS proposals. To this end, commentators requested that additional frameworks and governance models be reviewed to better understand the issues and challenges being overcome, and to create greater awareness of other initiatives, the problems they are targeting and their lessons learned.

An important aspect highlighted by commentators was the need to evaluate the level of centralization or federation, the pros and cons across this spectrum, and how to achieve interoperability across disparate system networks.

Next steps to integrating what was heard

To integrate the feedback detailed above, a Community of Practice workshop will be conducted in the last week of April or first week of May. A doodle poll will be circulated to this effect.

During this workshop, use cases and alternative models will be suggested and explored, and discussions will be held regarding their incorporation into the document.

Criteria for both use cases and model identification will be circulated in advance of the workshop. Participants will be invited to submit suggested use cases and models based on this criteria for consideration by the group.

Appendix D - Program Framework and Governance Model

A Pan-Canadian Trust Registry program framework and governance model in the context of defined user stories, with the applicable data schemas, could be designed with the following considerations. The elements outlined herein were informed by the Pan-Canadian Trust Framework™ for Trust Registries (Trust Registries Component Overview Draft Recommendation & Conformance Profile Draft Recommendation V1.0) created by the Digital ID and Authentication Council of Canada (DIACC) on , and work done by the Trust Over IP (ToIP) Trust Registry Task Force:

Principles for Consideration for a Pan-Canadian Trust Registry

- **Transparency and Accountability:** A pan-Canadian trust registry will operate with utmost transparency, clearly defining and publishing its governance model, decision-making processes, and criteria for including a trust registry. A pan-Canadian Trust Registry maintainer must be able to provide justification for decisions regarding inclusion of a trust registry.
- **Opt-in Model with Clear Criteria:** A pan-Canadian trust registry will follow an opt-in model, where another registry voluntarily chooses to be listed. The criteria for inclusion will be well-defined and communicated, ensuring that only trustworthy registries are listed.
- **Authority and Governance:** A pan-Canadian trust registry will register the governance of individual trust registries, ensuring that each entity has its own authority over the way it adheres to relevant governance rules and schemas.
- **Registrant Vetting:** The onboarding process will consist of both registration and verification during which the suitability of a trust registry to act as a trust registry will need to be confirmed.
- **Openness and Reusability:** All data within a pan-Canadian trust registry should be freely available for use or reference, fostering interoperability with other trust frameworks and digital identity systems.
- **Preservation of Information:** A pan-Canadian trust registry must comply with legislation to preserve information, ensuring that records and data are stored securely and accessible for the required duration. It should maintain the legibility, reliability, and integrity of information.

- **Facilitating Findability:** A pan-Canadian trust registry is meant to facilitate the findability of relevant trust registry information, and not as an end-point for inputs to trust decisions.
- **Trust input**: Information provided by a pan-Canadian trust registry and related registries is meant to be used as an input to trust decisions, and not as a decision in itself.
- **Technology and Specification Agnostic:** A pan-Canadian trust registry encourages seamless data exchange and collaboration among various stakeholders, while remaining neutral towards specific technologies or specifications.
- **Wide Use:** A pan-Canadian trust registry will be focused on ecosystems that are broadly usable and recognized as authoritative.

User Stories

Verifiers, who need to verify digital credentials, and Issuers, who issue these credentials, each have distinct requirements that a pan-Canadian trust registry could address. The following outlines two essential user stories: the verifier's need for locating the authoritative origin of an unknown issuer within a trust registry, and the trust registry onboarding process to register with a pan-Canadian trust registry.

Verifier:

1. Requests a credential presentation
2. Seeks to verify the credential
3. Notices that the credential issuer is unknown to them
4. Doesn’t know how to find the primary trust registry associated with the issuer
5. Verifier is aware of the pan-Canadian trust registry, a registry of trust registries, and believes it could help locate the issuer’s trust registry
6. Verifier accesses the pan-Canadian trust registry
7. Pan-Canadian trust registry routes verifier to appropriate primary trust registry or returns a failure (not found).

Primary Trust Registry Onboarding:

1. Primary trust registry wants to be registered with a pan-Canadian trust registry
2. Primary trust registry initiates registration process
3. Primary trust registry demonstrates its ability to be a suitable trust registry

4. Primary trust registry meets onboarding criteria and adheres to onboarding process
5. Primary trust registry is onboarded and can be located using a pan-Canadian trust registry

Data Schemas for Consideration / Inclusion in a Pan-Canadian Trust Registry

Information for organization maintaining a trust registry:

- Name of the organization
- Industry information, scope, jurisdictions (province, territory, etc.)
- Address, contact Information
- Unique Identifier (DID, registration number, etc.)

Supported Credentials:

- List of credentials types, names and descriptions supported by the registrant (e.g., academic degrees, certifications, licenses)

Registry Status:

- Active, Inactive, Dissolved, etc.

Interoperability Standards:

- Information on supported standards or protocols

Governance

- Link to governance framework for the registrant

Authorization and Security Information:

- Date and reference information
- Digital signatures or authentication tokens (if applicable)
- Security measures in place to protect the integrity and privacy of the data
- Compliance with relevant privacy and data protection regulations

Data Sharing Agreements:

- Details of any data sharing agreements between a pan-Canadian Trust Registry and other stakeholders
- API Access Information

API Access Information:

- If applicable, details of the API access to the Credential Registry for integration with other systems

History of Changes / Versioning / Audit and Compliance Records

- Any changes to the trust registries or related governance and processes, as applicable.
- History of audits and compliance checks conducted trust registries