2020-11-23

The material in this document was generated in response to a confidential request for information that was issued by the Government of Ontario. While the information here is not confidential, the request was made in confidence. It should be noted that the Trust Over IP Foundation intends to re-use much of the content as similar queries from various government and non-government sources are received regularly. However, we will remove anything that identifies Ontario as the source of questions and queries.

The work here is the product of over 20 members of Trust Over IP Foundation and as such reflects multiple writing styles and approaches. The foundation is happy to provide a direct discussion with the leaders in the Ontario government if requested.

Please direct any questions or concerns to the undersigned.

Sincerely,

Darrell & RJ

Darrell O'Donnell, P.Eng. Founding Steering Member Trust Over IP Foundation CEO - Continuum Loop Inc. Ottawa, Ontario, CANADA darrell.odonnell@continuumloop.com	**RJ Reiser** Member Trust Over IP Foundation Chief Business Development Officer - KABN Houston, Texas, USA rj.reiser@kabn.network

1. Briefly describe your organization's experience with digital identity in Canada and/or globally. What role do you see your organization playing in a digital identity ecosystem? (i.e. IDP, RP, Identity Network, infrastructure provider, technology provider, other)

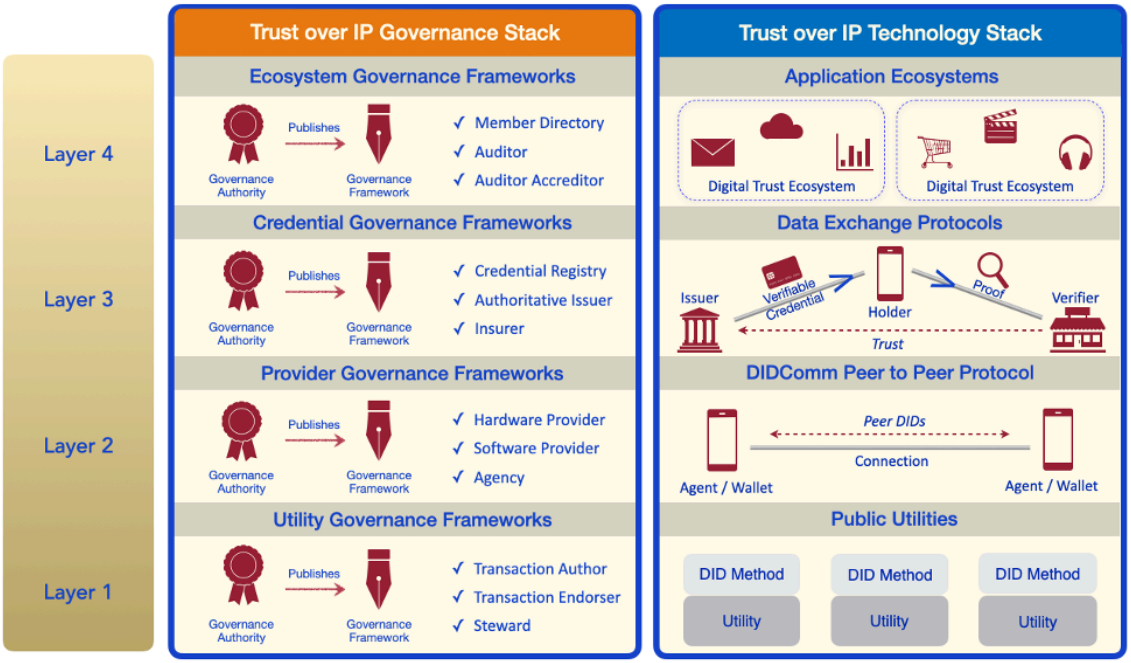
The Trust over IP (ToIP) Foundation was launched in May 2020 as an independent project hosted by the Linux Foundation. As such, ToIP itself is a relatively new contributor in the area of verifiable credentials and decentralized identifiers.

Nevertheless, ToIP members include over 170 leading companies, organizations and individual contributors sharing expertise and defining standards / specifications to advance a secure trust layer for the digital world. In this sense, ToIP brings vast and long-established experience and expertise to its effort to define a complete architecture for Internet-scale digital trust combining cryptographic trust at the machine layer with human trust at the business, legal, and social layers.

In order to enable trusted transactions and relationships online, credentials need to be founded on governance frameworks that spell out the business, legal, and technical rules under which they operate. This is how ToIP proposes to move beyond mere technology "proofing" and foster the emergence of solutions that interoperate at scale: by putting governance first.

Applications that foster digital trust begin with a clear understanding of business requirements, then move to regulatory and policy requirements that are transparently communicated in complete governance frameworks. Only at this stage, when the parameters for creating real human trust are fully articulated, are technology components selected to implement a solution.

This is the insight reflected in ToIP's dual stack model:



ToIP aims to break from the thousands of siloed solutions for digital identity and credential issuance that do not work with each other. This lack of interoperability costs billions of dollars per year in complicated and time-consuming integration and hinders adoption by the very customers they purport to serve.

Our goal is to drive adoption of a new model for digital trust that is every bit as interoperable as the physical wallets and paper or plastic credentials that we use every day—to do everything from getting on a plane to entering a hospital to signing a mortgage. As these new tools emerge, they will become as essential to our digital lives as browsers and email clients have become to the Web today. Interoperable solutions are paramount for a vibrant digital marketplace where consumers are free to choose the vendors and use the digital credentials they prefer.

ToIP aims to define a complete architecture for Internet-scale digital trust that combines cryptographic trust at the machine layer with human trust at the business, legal, and social layers. The Foundation's mission is not to develop all of the standards or components included in the ToIP stack. It is to specify how these elements can be combined to fulfill the requirements of all four layers, bringing both governance and technology together.

ToIP Foundation works closely with other standards development organizations (SDOs), industry foundations, and consortia to combine their open standards, architectures, and protocols into a complete and coherent stack for Internet-scale digital trust.

For a more complete outline of the ToIP Foundation and its mission, please refer to our founding whitepaper.

Finally, though ToIP is a global organization both in its mandate and membership, many of its leaders and key contributors are Canadians and Ontarians.

This includes the Foundation's Executive Director, Mr. John Jordan, who is Head of Digital Services for the Province of British Columbia. It also includes Steering Member, Mr. Darrell O'Donnell (Continuum Loop) and Contributing Members such as Mr. Kevin Dean (Dolphin Data Development), Ms. Victoria Lemieux (University of British Columbia), Ms. Karen Hand (Canada Digital AgriFood), Ms. Carly Huitema (University of Waterloo) and others.

ToIP is proud to have this opportunity to participate in the Government of Ontario's market consultation.

Ecosystem & Offering

2. How could partnership between the public and private sector be arranged to support the development of the DI ecosystem in Ontario? Government-led? Private sector-led? Consortium? Federated alliance of institutions? As a utility?

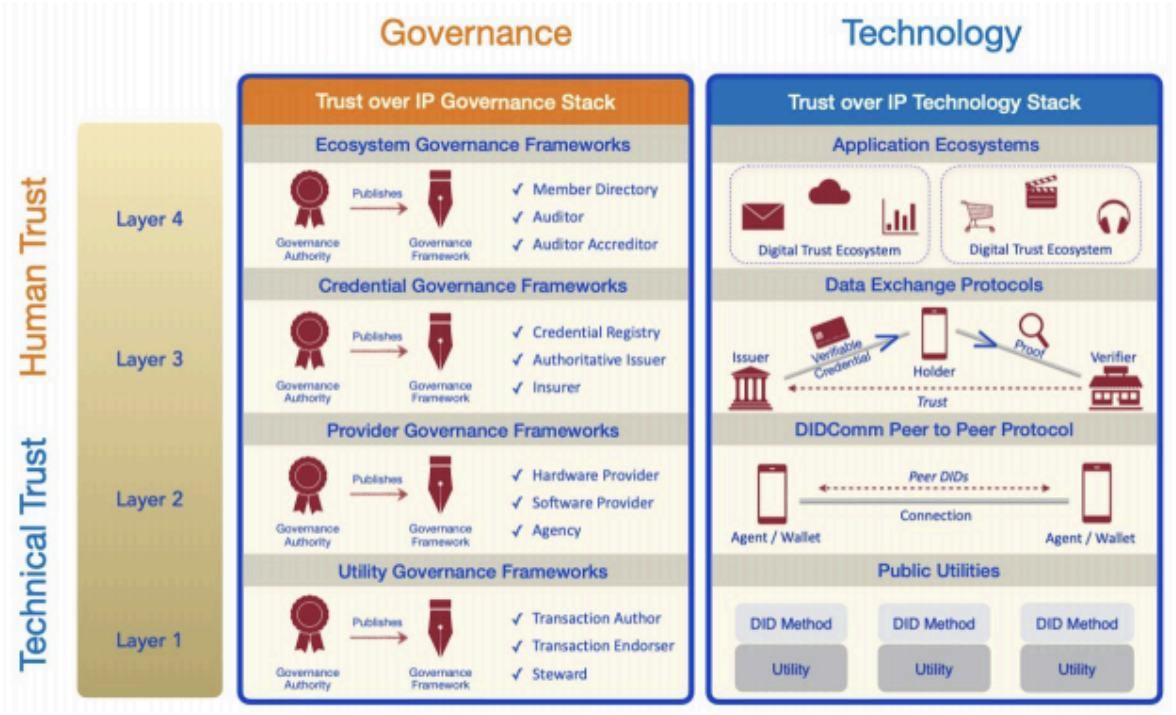
We'd like to break our input into a few sections here:

- General Market Need - describing the Trust Over IP Foundation views about roles at the highest levels.
- ToIP Layers - consideration of the Governance Stack and Technology Stack at various layers of the Trust Over IP Foundation 4-Layer Stack.

General Market Need

Different regions, countries, states and jurisdictions will present varying ways of combining government oversight, regulation and direct delivery with private sector services and solutions to support decentralized credentials. Together, in varying combinations, these actors will constitute a network of peers with some members playing key roles in governance and oversight.

The Trust Over IP model helps clarify where government play an appropriate role by defining the business rules, regulations and policies required to support a digital trust ecosystem before technology decisions are made and implemented.



DI ecosystems that exist entirely in the private sector, without the key Issuers from the Public Sector (F/P/T, municipalities, public utilities, etc.), will be limited in value and scope. The identity anchors that the public sector provides and the trusted exchange that it requires to be more effective and efficient are crucial to driving demand and innovation in the DI ecosystem.

Similarly, a lack of private sector involvement would create an ecosystem that struggles to respond to changes and innovations driven by the market and, as a result, will be very limited as well.

Depending on where we are focused in the ToIP stack, our recommendations change as far as the roles and interplay between the public and private sectors.

Utilities (Layer 1)

The primary purpose of Layer 1 in a DI ecosystem is to provide an “anchor” for key information (DID, DID Documents, key definitions/schema, etc.). The broad availability of

Layer 1 is the key to an ecosystem. Adding complexity at Layer 1 is not recommended as any complexity multiplies at higher layers in the ecosystem.

Layer 1 approximates a pure “utility play” meaning it will, in time, become routine, predictable, and should be available for all citizens and organizations. Layer 1 is used to anchor key data from organizations (note: ToIP Layer 1 utilities should not be used for personal data/PII) and it provides a “source of truth” functions. ToIP Foundation recommends that organizations work in concert as peers when possible. Where there are very discrete needs to be “public sector only” or “private sector only” Layer 1 utilities should be very clear why this separation is a “must”.

For early efforts, a public ledger may suffice or a ledger could be established with a partnership of public and private sectors. Once the deep governance requirements are understood, discrete ledgers could be established based on business needs, though discussions between experts in the Trust Over IP Foundation have rarely found use cases for deeply separated Layer 1 utilities.

Peer-to-Peer (Layer 2)

For the purposes of the ecosystem discussion, we will skip Layer 2 as it relates to communications and storage that don’t require ecosystem focus at the current time.

Information Exchange (Layer 3)

The governance of various parts of the DI ecosystem may require separation of key public sector and private sector roles on a Governance basis but should align on a Technology basis. We will use an example to explain:

> Consider the interplay between two portions of a notional DI ecosystem:
>
> - High-Assurance Digital Identity - Consider a “digital identity card” that provides driver licencing, OHIP, and perhaps other government-issued information. The Governance of this system should (must?) be led by the government - though it may benefit from a partnership with other public sector players. Knowing the definitive list of Issuers is crucial. Otherwise, the system would be ripe for fraud. Establishing the schemas that will be supported should be controlled by the public sector - but parties throughout the DI ecosystem should be consulted when creating these schemas.
> - Digital Insurance Ecosystem - Consider an insurance industry ecosystem that links people and organizations as part of the DI ecosystem. Given a public sector foundational identity capability can be linked to, the likely lead organizations for the Governance of insurance industry ecosystem are private

sector organizations. Public sector organizations certainly play an important role in this ecosystem but they are more likely to be consumers (Verifiers) than the drivers of the ecosystem needs.

Both of the above examples will benefit from a coordinated Technology Stack that supports both parts of the DI ecosystem. Otherwise neither system can leverage the other - creating new siloes.

Information exchange in a DI ecosystem rarely provides a bright line delineating between public OR private sector lead roles. A cons

On the Technology Stack side, the Trust Over IP Foundation is currently developing a Technology Interoperability Profile (TIP) that will, in time, be suitable for use in sharing with the community. This TIP is intended to provide clear guidance and proof of interoperability across Layers 1 through 3 of the ToIP stack.

Layer 4 - Application Ecosystems

Layer 4 provides the meat of an ecosystem - the user-facing applications and tools that can be used. As such it is a logical partnership area for public and private sectors to collaborate. However, key areas need to be considered such as standards, protocols, auditing, and compliance.

For an explanation, we'll use the same High-Assurance Digital Identity and Digital Insurance ecosystems, which we discussed in the prior section.

The High-Assurance Digital Identity Ecosystem would establish the requirements for the full ecosystem. Issuers, in particular, would be held to a standard for each level of assurance that they provide. This approach aligns very well with the Pan-Canadian Trust Framework. While the ecosystem may allow non-government credentials to be issued, they would most likely not be as high-assurance as some government-issued credentials. The key processes that happen before a citizen or organization (Holder) is given a credential by the government (Issuer) are simply more robust and secure.

The Digital Insurance Ecosystem would have its own rules for operating that are somewhat unique to the insurance ecosystem's requirements.

The key that helps is that both of these components of the DI ecosystem would be crucial for both groups. Two simple examples that tie things together will help here:

- Governments require an efficient and effective way of requesting "proof of insurance" from people and organizations. They may also want to limit the use of the credentials that they issue:

    - A digital identity credential may be presented differently depending on who the Verifier is:
        - An “age of majority” (or any age threshold) may present a semi-anonymous proof that a person is over a certain age. The government may set the thresholds (e.g. over 18 for voting; over 19 for alcohol and cannabis) that are allowed by applications that are allowed to operate in the ecosystem.
        - A full sharing of a high-assurance digital identity credential may be limited to known agents - such as law enforcement and government officials.
- Organizations in the insurance industry required high-assurance that an individual or organization is who they say they are to smooth out processes and reduce fraud. Similarly, the people and organizations in the insurance ecosystem want consistency and simplicity.

3. What is the minimal role or involvement by government to establish a stable ecosystem environment, while promoting inclusivity, innovation and private sector involvement? What parts (if any) of the DI ecosystem do you feel must be lead, managed, owned by government in the interest of the public good?

There are many roles a government can and should play within an ecosystem intended to serve its citizens. The roles, responsibility and level of commitment will evolve throughout the lifecycle of the ecosystem, so it is reasonable to think about each role not just in terms of what, but also in terms of when and how much.

Government as ecosystem champion: The desire to implement the conceived ecosystem originates with the government and therefore it is natural that this role is core to everything that will transpire. 'Championing' the ecosystem will look different throughout the lifecycle phases. Early on being a more all-encompassing role, later taking on a more targeted approach.

Government as ecosystem user: In the early growth days, the government should play the role of lighthouse user in order to educate potential participants by example, demonstrate the value that can be realized through participation and educate the ecosystem community by way of real-world pressure testing. As the ecosystem begins to mature, the government in the role of a large user, can both provide a level of stability to the community and potentially act as a significant customer to vendors and service providers. These actions are in addition to the direct benefits realized from the use cases employed by the government at-large to drive specific social goals.

Government as ecosystem patron: As a patron, the government is in a position to invest various amounts and types of resources to build momentum across the ecosystem. They

can also use patronage during later phases to jumpstart innovation initiatives and support important activities when faced with unforeseen challenges.

The response to question 12 describes a number of areas where the government would be a prime candidate to take ownership of with the intent of promoting early growth and maturing the ecosystem. Specifically, the Layer 1 utility and personal wallet. This would entail patronage along with ownership, both of which would be reduced over time.

Government as governance authority: As the top level of trusted entities within a jurisdiction, the government, willingly or unwillingly must take ownership in defining certain rules of engagement. Public companies, trade associations, international groups, etc. will also establish rules of engagement within their own domains, but there are several key issues related to the ecosystem that the government should give strong consideration to proactively taking ownership of:

- Liability rules associated with the issuance, processing and transmission of credentials
- Authority and authorization to demand presentation of certain credentials
- Trust assurance standards for: public identity, public licenses, public health, etc.
- Rules pertaining to vertically integrated use cases (use cases that require controls, or a chain of authorization from issuance through verification) involving public health, inclusion, diversity and commerce
- Rules pertaining to discovery and access by law enforcement

Government as Authoritative Issuer/Trust Authority: Ideally, the government won't be the exclusive source for trusted identity, but initially they are the gold standard for the population at large and have significant infrastructure in place to keep identity current. The government should continue to provide free basic identity credentials to everyone in their jurisdiction. The government however should not attempt to be the definitive source for all use cases. The concept of identity is becoming increasingly rich and is the compilation of a lifetime of recorded interactions and authoritative claims. By this definition of identity, the data principle, not any third party, should always retain control of their information.

For credentials other than identity, the government must continue to act as a trusted authority when appropriate. Licensing is a good example. A business license is meaningful only if issued by the government or by an authorized agent of the government. The license is also meaningful only so long as the government remains a trusted authority.

Government as bootstrapper: The response to question 12 explores this in greater detail, but the government is in a unique and highly leveraged position to seed the ecosystem with identity, create an operable (issuer, holder, verifier) ecosystem, then open it up to private and government organizations to innovate on top of. This, along with vision and purpose, is a rare combination event that will enable this ecosystem which derives value from scale to be bootstrapped at scale very early in its existence.

4. What benefits could be realized through public and private sector collaboration? What models of public-private collaboration have you observed in other jurisdictions that Ontario could adopt as a model? Are there specific partnership models that should be avoided and why?

There are many different models available for collaboration in establishing a digital identity initiative. Given the nature of the government being a crucial Authoritative Issuer for foundational identity for both people and corporations the government needs to be an active player. Many private sector networks feel that the complete digital identity can reside solely in a private sector context - but this is to be avoided. Leaders at the Trust Over IP Foundation disagree - government plays a crucial role in establishing a digital identity ecosystem. The role of government is at least as a peer participant. In some areas government must lead - though that role will likely fall under regulatory and policy cover, and not require all costs to be borne by government.

Given the crucial need for government to be an Authoritative Issuer for key identity credentials, permits, and licenses the Trust Over IP Foundation recommends that Ontario be a full member of any network - thus a public/private partnership of some kind is likely to be the best fit.

As far as structure, a network that is used by Ontario and/or Canada could use the same approach as the Sovrin Network and/or Bedrock. In both of these organizations Stewards run nodes and are selected from various industries and jurisdictions to provide global coverage. The Sovrin Network, run by the Sovrin Foundation, aims to have nodes run in many industries (big business, tech, universities, NGOS, etc.) and locales (all major continents covered). Bedrock is aimed at big business and has Stewards that reflect that. In the case of a government supported network government could run nodes alongside key providers (banking, telecom, universities, NGOs, etc.) that reflect the needs of Canada.

Meaningful and effective public/private sector collaborations, in any economic or industrial sector, require entities with very different bottom lines to agree on how to share risks, ownership, accountability and cost over time. This will continue to be true in the area of decentralized identifiers.

As a standards setting body the Trust Over IP Foundation would also recommend strong involvement of the government in the development and use of standards.

This area is one of the least visible ecosystem activities. Nevertheless, this is an area where the incentives for private entities to define common technical standards often reflect public sector requirements and regulations.

Trust over IP is an example of this: an organization whose mandate is to define an architecture for Internet-scale digital trust, doing so in a way that is open and extensible and that allows for multiple, often competing, participants to work together towards a common goal. Similar organizations exist for defining and managing standards for the Internet (World Wide Web Consortium, Internet Engineering Task Force), industry (Canadian Standards Association), food (Codex Alimentarius), supply chain (GS1), and many more.

Many of the standards that these associations develop are done at the behest of their members, but they also do so in response to legal and regulatory requirements. For example, in the United States, the Drug Supply Chain Security Act (DSCSA) "outlines steps to build an electronic, interoperable system to identify and trace certain prescription drugs as they are distributed in the United States".

In response to this, industry has come together, under the umbrella of GS1 US, to figure out how best to apply existing supply chain identification and traceability standards to the Act[1].

Similarly, Canadian industry worked with GS1 Canada to develop identification and traceability standards for food traceability, resulting in the Canadian Food Traceability Data Standard[2].

Better collaboration in the area of regulation and standards development, therefore, is worth exploring.

Further, a directed outcome approach, where government publishes regulations, backed by formal requirements and performance goals, is a significant enabler of standards development. This methodology merits close consideration as well.

A collaborative model in which industry experts, backed by government funding and supported by government representatives with appropriate project management expertise, can work to meet well-defined requirements put forward by the government, stands the best chance of success by bringing in the appropriate industry knowledge while ensuring that the project is on track and aligned with the government's goals.

Moreover, very important elements related to (among many others) how achieve broad interoperability between digital trust ecosystems, and what design features need to be introduced to support people in navigating the use of these credentials, have yet to be discovered. It is important for the public sector to avoid vendor-lock and the constraints that come along with investing to much, too soon in systems/solutions that are not fully evolved.

[1] https://www.gs1us.org/industries/healthcare/standards-in-use/pharmaceutical
[2] https://gs1ca.org/can-trace/

Where the public sector maintains a clear focus on creating value for citizens and setting the rules of the game, through policy and regulation, the private sector will be able to drive innovation and respond to market dynamics as they emerge.

Inasmuch as this balance can be achieved and sustained, opportunities to pursue public/private collaboration will take many forms.

5. What attributes/features should a digital identities for individuals or businesses include (apart from basic authentication of name, date of birth, registration date, biometric, address). In other words, what other attributes or offerings should be included and why? (i.e. digital signature)

Short answer: It depends.

More detailed response
One needs to make a distinction between key management, claims and mechanisms required to authenticate (i.e data entry [*Inputs domain*]) and attributes, purpose and consent required for information exchange (i.e. data capture [*Semantic domain*]) between government, business or individuals. From a governmental perspective this distinction is required to ensure that flexibility is governed and available to all stakeholders. Without this flexibility, inclusiveness of a government digital identity system will be difficult to implement (e.g. impossibility to sustain the variety of attributes/features for all economical actors).

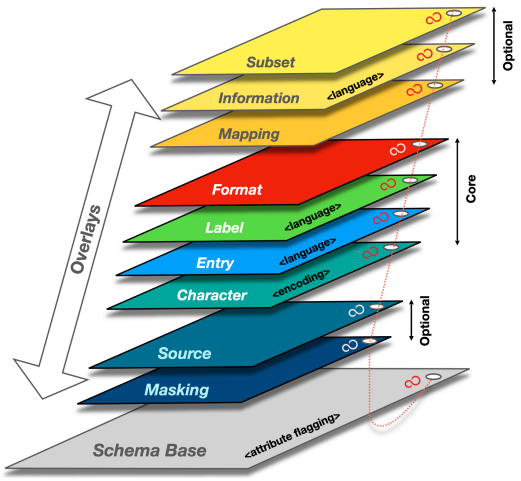
The components/features of a digital system require solid interplay between both domains (*Inputs* & *Semantic*).

Digital identities clearly sit in the authentication space but their real life usage requires the information exchange piece. The Trust over IP Foundation *Semantic Domain Working Group* was established to deal with the data capture side of things (i.e. information exchange) but, since the interplay is so closely bound, that WG will likely be evolving to deal with both authentication and information exchange. The revised WG name will likely be the *Inputs and Semantics Working Group*.

Authentication (*Inputs domain*)
Let's first look at the authentication space. Identity key management refers to the requirements by a stakeholder to ensure that it is interacting with an assured *counterparty* in a secure and authenticable manner. It is thus highly ecosystem dependent and application specific. As opposed to having one *super* ID credential consisting of a large number of form attributes with multiple features, we need to focus on *strong* ID credentials. In certain circumstances, even basic form attributes like names are not necessary for authentication.

As an example, we can use a scenario inspired by the current COVID-19 pandemic where large scale testing is of importance. In this case, for public health reasons a comprehensive coverage of the population is necessary and, for some applications, only a proof of having been tested is necessary, not citizenship or any other PII.
For authentication purposes, Verifiable Credential claims should remain as simple as possible. A government will have to foster a graded authentication system for sake of user acceptance and complexities (cost) of implementation. Here again, the level of authentication will not only be ecosystem and application dependent but also contextual. With respect to a driver's licence, authentication requirements will be different if you have been arrested by a police officer for drunk driving or if you are using this credential only as a proof of age.
Thus design of VC forms, when used as digital identities, should carefully weigh the intended usage with the payload content. Proper segmentation and reference to other VCs where appropriate is a good design to limit data overloading of VC. For example, a driver's licence includes a date of birth. However, that information is present in a birth certificate, so rather than duplicating the data, the driver's licence VC should reference that claim in the driver's birth certificate VC if available. In addition to avoid duplication, this approach is more secure as it ensures that the linked VC is still valid.

Information exchange (*Semantic domain*)
If the Authentication section can be summarised as "knowing who is your counterparty", the Information exchange section should be "knowing what you are talking about". In many scenarios, digital identity can stop at the authentication level (e.g. holder is allowed to enter premises) but in many more scenarios it is the data payload attached to the identifier that is relevant for electronic transactions (e.g. diploma, electronic health record,...). Thus a decentralized authentication system must be accompanied with a decentralized semantic solution allowing each side of the electronic transaction to ensure transparency in the actual information exchange.



At this stage, the ability to recompose the data in ways that preserve privacy is a must. For example, buying at the LCBO currently requires a presentation of ID that includes date of birth. However, ultimate privacy protection should require only a picture (to match to the individual) and an assertion that the person is over 19. For a single claim, this could be cryptographically solved with a VC and zero-knowledge proof (ZKP). However, when the data payload is large enough to warrant a dedicated container or data store to hold data with a VC providing a transitive trust component for authorized access, a ZKP-compliant VC is not sufficient. In this case, a data capture architecture

that can support rich contextual definitions through semantic object interoperability is needed for real world complexities.

Overlays Capture Architecture (OCA) is an architecture that presents a schema as an object consisting of a schema base and overlays. Overlays are task-oriented linked data objects that provide additional extensions, coloration, and functionality to the schema base. This degree of object separation enables issuers to make custom edits to the overlays rather than to the schema base itself. In other words, multiple parties can interact with and contribute to the schema structure without having to change the schema base definition. With schema base definitions remaining stable and in their purest form, a common immutable base object is maintained throughout the capture process which facilitates data standardisation and data language unification.

In conclusion, the list of requirements to be included in a digital offering must distinguish the authentication and the information exchange solutions to ensure the required flexibility of a deployed provincial- (nation-) wide digital identity system.

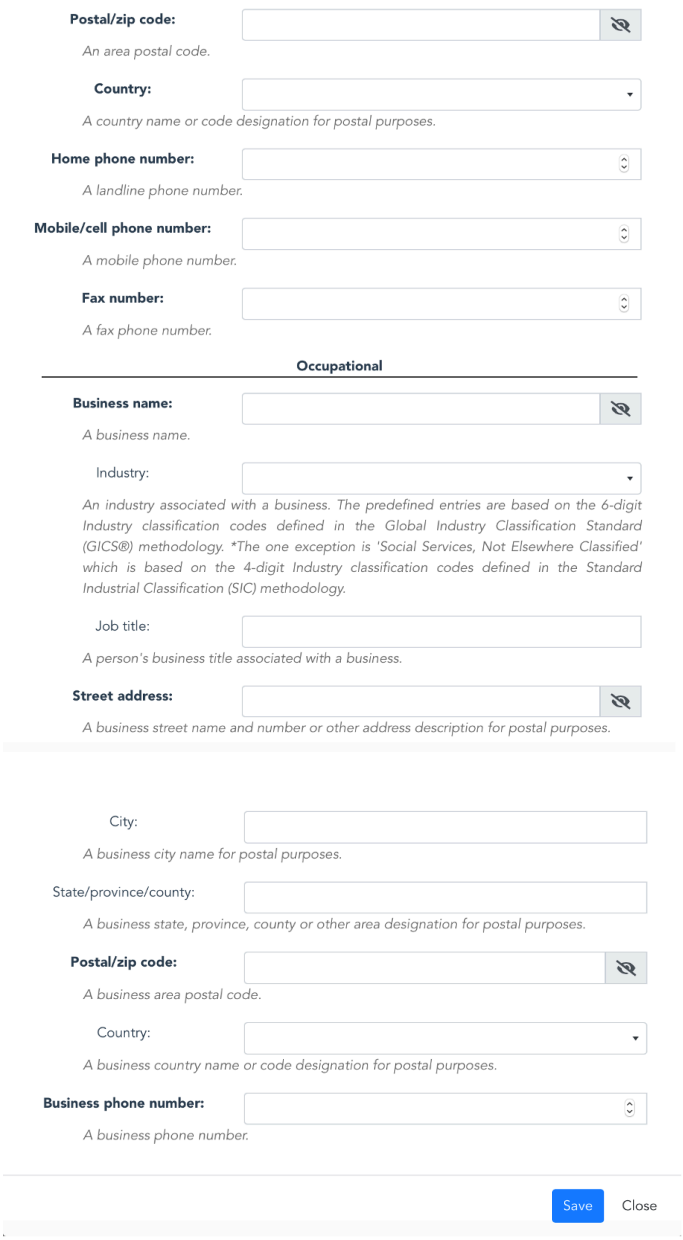
***Core data schema* development**
Spearheaded by contributing members from MyData Global and Trust over IP, a *core data schema* is currently being defined for capturing personal identification and demographic data for active governing entities. https://protocol.jlinc.org/core-data-schema/

The schema requirements document is being developed by contributing members of the MyData Operators WG at MyData Global.
https://docs.google.com/document/d/1-smCcC_Tab7KSuWdaMJCk7mY7zCBoNBk7wSYoHmZPiw/edit

The schema technical specification[3] is being developed by contributing members of the Semantic Domain WG at the Trust over IP Foundation.

Here is a visual representation of the *core data schema* in OCA format:

[3] https://docs.google.com/spreadsheets/d/1tCW0uuY7x1odACK7-adcaaJa6PMVuTHB/edit#gid=773664223



Blinding Identity Taxonomy

The Blinding Identity Taxonomy (BIT) is a defensive tool created for the purpose of reducing the risk of identifying governing entities within blinded datasets. BIT contains a list of elements to be referred to by schema issuers for flagging attributes which may contain identifying information about governing entities. Once attributes have been flagged, any marked data can be removed or encrypted during the data lifecycle.

OCA contains a blinding block in the schema base object that enables issuers to flag any attributes that could potentially unblind the identity of a governing entity. The BIT is the suggested reference for those schema issuers.

The BIT Report is an official Kantara Initiative report

- BIT in PDF format: https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.pdf
- BIT in HTML format: https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.html

6. The long-term vision of the government is to issue verifiable credentials to digital wallets that comply with recognized frameworks and standards such as PCTF and W3C verifiable credentials. Recognizing this and other related standards are still under development, how can government progress towards the verifiable credentials model while delivering on its commitment to launch a digital wallet to the public by the end of 2021?

The concept of a digital wallet is still rapidly evolving and emerging. This particular question implies to the Trust Over IP Foundation that the Ontario government is well aware that this early-stage technology will continue to churn and morph over the next few years.

There are a number of areas where the impact of this rapid evolution can be mitigated and even harnessed. The Trust Over IP Foundation recommends the following:

- Focus on single-use applications initially while using verifiable credentials for exchange - issuing a verifiable credential to a single-purpose application (wallet); requesting a proof of a verifiable credential (e.g. “please present your government identity card”) in simple manners.
- Prepare to adjust to the changing user experiences that will come. While the data constructs for verifiable credentials, DIDs, etc. are becoming more stable the ways that we interact are just beginning to evolve. The protocols for using a verifiable credential are not standardized, though DIDComm and Hyperledger Aries are beginning to create standard communication rituals for:
    - Establishing a secure connection.
    - Offering a Credential across the secure connection.
    - Requesting a credential from an Issuer across the secure connection.
    - Request a privacy-respecting proof from a particular Holder.
    - Sending arbitrary messages across the secure connection.
- While some API-based approaches have been proposed they tend to be simplistic and rely on web-based technologies, making other communication approaches (e.g.

NFC or Bluetooth for touchless communication) difficult. The key learning at this early stage of the wallet space should be focused on the key interactions that are needed to exchange information appropriately.

- Use overlays and semantics to avoid complexity.
- Hide the complexity of the system from the person:
    - Don't ask the user to pick attributes from multiple credentials when a single, much simpler question will help them - or help their wallet/application automatically respond with the correct type of information.
    - A predefined set of mappings for common use cases (e.g. driver's licence to simpler presentation of proof of age for alcohol purchase, without revealing date of birth or address information) would also help users appreciate the value.
- Focus on the use of W3C Verifiable Credentials for …
- Focus on the atomic processes outlined in the PCTF - they provide leverage as they are reusable and are not dependent heavily on the underlying wallet technologies.
- Focus any digital wallet applications on a limited set of interactions and credential types. Arbitrary credentials are difficult to understand for any person - even deeply technical people. While the new pattern for using verifiable credentials are learned, more business use cases and credential types can be added. In time, a set of generic interaction patterns are likely to evolve.
- Focus on the most common interactions, in environments where the government has the most control or influence.
    - Presentation of health card at registration at hospitals.
    - Presentation of driver's licence or other ID at Service Ontario locations.
    - Presentation of proof-of-age at LCBO.
- With clear public communication about the government's commitment to open standards, pick a single wallet implementation for the early phases, while ensuring that representatives for other implementations remain engaged in the process and understand that the end goal is an open market based on finalized standards.
- If a COVID-19 set of use cases are to be explored the COVID-19 Credentials Initiative (https://www.covidcreds.com/) provides numerous guidance points.

Suggested Reading: The Current and Future State of Digital Wallets (disclosure: written by one of the authors).

7. What is the best approach in this timeframe to ensure we deliver on this commitment? What role can your organization play in helping us deliver?

ToIP is set up, with formal Working Groups and focused ad-hoc Task Forces addressing key questions and requirements as they arise, to be nimble and responsive.

Work underway at the Foundation includes technical interoperability testing of components that go into a complete version of the stack, defining key concepts in common glossaries that can be used across Working Groups, establishing Governance models that can be used to define requirements across varied use cases, and designing the human experience of establishing digital trust - among many other activities. Our Foundation can help the Government of Ontario by sustaining an open communication that allows us to share important outcomes of our work while allowing Ontario to communicate priority challenges/questions that our members can help solve directly.

The best way for us to help is to establish an open dialogue that integrates the challenges you face into the on-going work of our community.

We suggest that Ontario consider joining the Trust Over IP Foundation. There is precedent for provincial government involvement. The Government of British Columbia is a founding Steering Member of the foundation.

8. What should be done to drive active user participation, engagement and adoption of digital identity in Ontario?

The Ontario Government should implement a comprehensive and inclusive public engagement strategy involving both open communication and consultation. Key areas to address are:

- Inclusivity as a primary outcome, with all Ontarians able to participate in a frictionless manner;
- Project goals and outcomes will be developed in a shared manner with the people of Ontario –public input and feedback will be a critical to the success of the initiative;
- The services delivered will simplify life for all people of Ontario and enable business to operate more competitively in the global digital world;
- Promote shared ownership of benefits and incentivize behavioural change; and
- Facilitate channels for clear and transparent communications regarding governance, policies, and procedures

Effective public engagement will not only ensure successful user participation, early engagement will mitigate the risk of misconceptions and misinformation; specifically, those associated with privacy protection. Early risk mitigation concerning protection of personal information can result in significant challenges as exemplified by the failure to launch Toronto's Quayside smart city project with Sidewalk Labs and at times, hesitant adoption of COVID Alert, Canada's COVID exposure notification app by risk sensitive individuals.

Public engagement can be achieved through utilization of organizations such as the International Association for Public Participation (IAP2, https://www.iap2.org/page/about) and engagement of IAP2 Canada Public Participation Professional certification (IAP2 Canada professional certification program). IAP2 have developed three pillars for effective public participation (P2) processes that include core values to define expectations and aspirations of the public participation process, code of ethics for IAP2 practitioners and the IAP2 Spectrum to help the public's role and level of participation.

The Trust over IP community has expertise in guiding private public discourse related to the governance, business use case, standards, and technological implementation of user centric ecosystems; together with organizations such as IAP2, the Government of Ontario will have the ability to leverage and engage the Ontario citizens and businesses. Through a consistent and active communication channel with ToIP, the Government of Ontario will have access to the most up-to-date developments in digital identity governance and technologies, critical to ensure inclusivity given the nascent and various maturation stages concerning components of the digital identity governance and technology stack.

9. What are the highest priority use cases for your organization and/or industry/sector that would benefit from the use of digital identities?

The Trust Over IP Foundation does not have a direct set of priority use cases. Due to its global mission of establishing digital trust the members of the foundation are widely dispersed amongst very different industries (finance, health, education, government, etc.).

The Trust over IP Foundation is supported through voluntary efforts of the membership who encompass a broad range of expertise. In their professional lives, ToIP members have extensive business expertise related to decentralized identities and verifiable credential ecosystem enablement in the areas of;

- Public health and safety
- Education
- Financial services
- Supply chains
- Agri-food
- Travel
- Social transformation

ToIP community members operate in front line business applications and are able to provide insight to the Ontario government to realize tangible public private benefits through insightful scoping, governance, and technology applications.

In addition to their expertise, members of ToIP have connections to a variety of industries throughout Ontario, Canada, and the world. They have the ability to bring partners to the table who might otherwise not be aware of this initiative, but who nevertheless would have an interest in it. In such an environment, the highest priority use case is likely to be business identification for business-to-business interaction. The digital identity for a business can include basic registration information (company name and address), corporate officer identification (i.e. those that can bind a company in a contract), and regulatory approvals for the business (e.g., authorization to sell cannabis). All of these can be used to increase trust in business-to-business interactions, especially in the present environment where face-to-face interaction is difficult or prohibited.

10. How can unintended consequences of having digital IDs (e.g. social exclusion, tracing, furthering inequality, profiling) be prevented?

While it is true that any digital ID system may result in unintended consequences, the private/public consortium establishing the digital id ecosystem can take actions that clarify their intent to the marketplace and establish transparent standards to convey its position as providing the system for ethical, lawful and social equality purposes:

- The ecosystem should include in its Governance Framework a set of operating principles that overtly address its intended purpose
- Ensure that the ecosystem consortium has diverse representation which can help identify unintended consequences that may not be obvious to the most dominant members
- Include representatives of user rights groups in the governance and testing phases so the ecosystem has buy-in from the start.
- In its Risk Assessment, the Governance Framework should identify unintended consequences as a specific risk which would be mitigated with detailed requirements for stakeholders to address the risk such as:
    - Disclosing clear language/visuals at point-of-use for how information shared will be used, retained
    - Agreements in place by all parties on the use of identity information
    - Restrictions on the ability to use of sell identity information without consent
    - Alternative access mediums for ID holders to use their ID information for services
    - Privacy enhancing zero knowledge proof schemes when possible
    - Easy to read and use instructions for participants
    - Limit/monitor information sharing / coordination across entities so they can’t build a full picture of someone from the outside-in

    - Ensure that the practice of a citizen not sharing certain information does not unfairly penalize nor exclude them.
    - Ensure that refusal to participate in digital ecosystem (and sticking with physical) does not unfairly penalize or exclude people
- Acknowledge the imbalances in the market and the role that regulation has to play; For example, small disadvantages to many users compared to a large benefit to a single player in the market.
-

Bianca Wylie in her article **Using Government IT to Teach and Build Public Infrastructure**, says it best:

This (technology) evolution would also include addressing how technology teams work together within and across government(s). Big organizational shifts to make, no doubt, but we're also at the breaking point for the limitations old organizational structures are imposing on the people working in tech in government. We the public shouldn't accept this status quo any longer because we are the ones ultimately harmed by it. With differently organized internal technology capacity, there can be new public sector roles to address the digital divide — to make sure that beyond accessible internet for all there is also widespread public ability to use it — socially, politically, employment-wise, artistically — however one may choose.

11. How could the digital identity ecosystem be structured to protect data and privacy, build trust and reduce identity fraud? How can privacy concerns associated with the handling of sensitive user data be mitigated?

See answer to question 10, plus additional material below.

From the ToIP website:

> The ToIP stack has incorporated Privacy by Design from the ground up. This means that it can be used to implement solutions compliant with all major global data protection regulations, including the EU General Data Protection Regulation (GDPR), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), or the California Consumer Privacy Act (CCPA). It can also be used to meet strict privacy and security protection regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA).

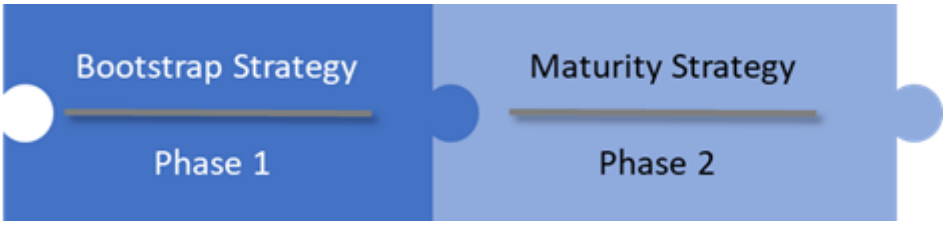
Privacy by Design[4] is a framework, developed under the leadership of former Information and Privacy Commissioner of Ontario Ann Cavoukian, that proposes seven foundational principles:

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full Functionality – **Positive-Sum**, not Zero-Sum
5. End-to-End Security – **Full Lifecycle Protection**
6. **Visibility** and **Transparency** – Keep it **Open**
7. **Respect** for User Privacy – Keep it **User-Centric**

The Trust over IP Foundation has many privacy experts, including a former Senior Advisor in the Office of the Information and Privacy Commissioner of Ontario, participating in the development of its standards. These experts also participate in or monitor the development of privacy frameworks around the world, including MyData Global[5], whose focus is "to make sure individuals are in a position to know and control their personal data, but also to gain personal knowledge from them and to claim their share of their benefits".

12. Once the ecosystem is launched, how could it be matured across public and private sector? What can the government create the conditions for inclusion, competition, innovation, private sector investment and participation in the creation of a financially viable digital identity ecosystem?

The ideal approach requires two distinct phases: 1) Creating the conditions that drive rapid, early adoption; and 2) creating the conditions that ensure innovative growth and operational sustainability. The two phases are tightly interlocked and each is critical for achieving sustainability, viability and long-term value generation for participants of the ecosystem.



A viable digital identity ecosystem requires the ability to sustain critical mass of participation among issuers, holders and verifiers. These participants, in turn, rely on the existence of a

[4] https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
[5] https://mydata.org/

healthy supporting ecosystem of vendors, service providers, standards bodies, legislators and others.

Network effects dominate digital identity ecosystems in that the value realized by participants tracks closely to the number of participants and the amount of participation. There are many examples of this effect in our daily lives to look to for guidance: telecommunications, social media, transportation, web browsers, email and the power grid to name a few. Four aspects that are key to the success of each include the ability to:

1. Keep the cost of core infrastructure and operations low for the majority of participants
2. Keep barriers to adoption low for the majority of participants
3. Maintain a critical mass of participants and participation
4. Ensure the incremental costs for transacting across the infrastructure is low compared to alternatives

In this respect the Ontario government can be a very powerful lever, biased for broad social benefit, to assist in achieving the first three conditions which in turn will drive early adoption and help achieve critical mass of participation. The differentiating value the government can offer over that of the private sector is the ability to facilitate growth and adoption that enables a diverse set of private goals and agendas. The fourth aspect; transaction costs, will be driven by market forces.

Phase 1: Bootstrap Strategy

Keep the cost of core infrastructure components low: The core of an identity ecosystem is built on top of internet infrastructure and is by design decentralized. The advantage being that large amounts of infrastructure rollout is not necessary. Maintaining a set of interoperable distributed ledger(s) – the so-called layer-1 ‘utility’ layer however is one such infrastructure requirement. The government is well suited to take a direct role in establishing this as a public benefit and ensuring its long-term stability.

Direct investment, tax incentives, subsidized access to (network) resources and issuance of public/private contracts are tools that can be leveraged for developing, deploying and maintaining the level 1 utility.

Keep barriers to adoption low: Issuers, holders and verifiers all need to be activated for the ecosystem to function and each will require different levels of time and financial commitment. The most decentralized role by far in the ecosystem is that of the holder. As such it will always be hard for the average citizen to assign a monetary value to the use of the system.

Until business models develop that can hide the cost of user agents (wallets) from the holders, the government should take a direct role in subsidizing the cost and enabling wide scale distribution of these for free or very low cost to the end consumer.

There should be light subsidies or incentives available to encourage development of verification technology, and integration of verification technology into commercial businesses.

Issuers will initially represent the smallest group of participants and will feel pull and market incentives from holders, verifiers, industry groups, etc. to supply the ecosystem with credentials. The ecosystem will permit issuers to effectively monetize their good reputations by applying their name to the issuance of a credential. For these reasons, the government should monitor uptake but not plan on facilitating pro-active incentives.

Maintain a critical mass of participants: Governments are in a unique position in that they are already in the business of identifying and proofing a great number of people and institutions within their jurisdiction. It is also the case that they generally represent the 'gold standard' for basic identity and that basic identity is the foundation for literally everything that can transact across the ecosystem. Being the issuer of record for basic identity credentials, the Ontario government could seed the entire province almost overnight. Once individuals and corporations take possession of their credential by downloading it to their agent (wallet), the trust triangle of issuer:holder:verifier is completed and the ecosystem can function at scale. It is hard to emphasize enough the value that can be realized by seeding the ecosystem like this.

Create an innovation vacuum welcoming to all: Following the previous three strategies, the resulting ecosystem would be operational at large network scale, could function at low cost to participants and would exhibit high identity trust but low utility – creating a vacuum for innovators to fill. This creates fertile ground and a level playing field for enterprising individuals and organizations to innovate on top of.

Obtaining network scale is hard work. Building from scratch tends to motivate successful participants to consolidate control which can restrict broad based innovation. By bootstrapping identity at scale and providing targeted support to infrastructure components, the Ontario government can both significantly reduce the time it takes to reach critical mass and spread the opportunities derived from having critical mass across a wide range of constituents.

Phase 2: Maturity Strategy

Mature ecosystem: Ecosystem Maturity can mean many things, and it would be hard to imagine all the future possibilities. However, one relatively safe definition of this milestone would include the abilities of the ecosystem to:

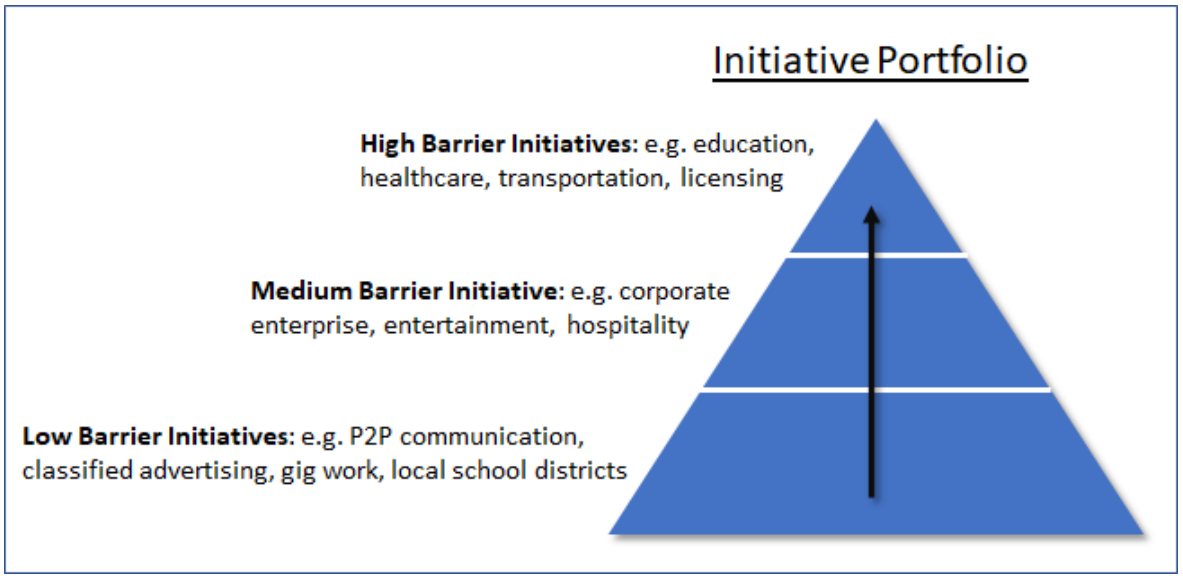
1. Operate stably and fairly

2. Provide wide ranging value to participants
3. Evolve through ongoing innovation
4. Be paid for primarily by the activity of the free market

Attaining this state of maturity would permit the government to transition their resource commitments from subsidizing core ecosystem components to targeted investments and incentives that drive specific innovations, efficiencies and public policy goals.

Getting to this milestone will involve monitoring and continuation of bootstrap policies adjusted to a level that ensures stability and confidence, but the main focus should be on outreach, external investment and growing the number of participants and level of participation, specifically of issuers and verifiers.

A portfolio approach that targets groups of high barrier initiatives, medium barrier initiatives and low barrier initiatives will attract a vibrant mix of participants and use cases. Each group will require a different approach and level of involvement from the Ontario government.



Regional workshops co-sponsored by software vendors might be a great outreach program to encourage low barrier initiatives to flourish. At the other end of the spectrum, the government might need legislative change to enable licensing use cases, privacy protections or assumptions of liability.

Encouraging a healthy vendor and services industry as well as interoperability standards should also be high on the agenda. Working closely with industry to define or adopt interoperability standards, either formal or de-facto is very important in maturing the ecosystem and encouraging broad participation from large and small organizations alike.

Governance & Authority

13. How should responsibilities for different parts of the Digital ID ecosystem must be delineated? What do you envision the role of Public Sector and Private Sector to be in the overall governance model? Do you see benefit in having the Province provide oversight for the ecosystem?

The answer to Question #2 describes the ToIPs layered governance and technology stack that we feel best addresses the many interdependencies in which an identity ecosystem operates within itself and with other ecosystems that may share data and rely on it. The Governance Stack relies on an authoritative body, a Governance Authority, to oversee the ecosystem and establish requirements to all stakeholders. The efficacy of that authority is dependent on each ecosystem. Some may be best driven by public entities alone, some by private interest. Generally, citizens and companies do not want government oversight into their data or even the perception that the government may be viewing their data.
We recommend that a governance authority be composed of a consortium of public sector and private interests composing a variety of stakeholder positions that can be considered to maximize public acceptance. We suggest government endorsement to the consortium and reinforcement to the principles and standards in operation; then letting qualified commercial service providers run the systems.

The Ontario government will need to work to provide expertise and models for ecosystem intellectual property to address Data IP (relating to contribution of data and information from a variety of sources and from which a variety of insights and applications can be developed) and Inventive IP (relating to the tolls, software and inventions, patentable or not, that may arise from projects undertaken as part of a verifiable credential ecosystem and which may make use of Data IP) as well as processes to support collaboration with ecosystem participants/partners, experts in the field and the Canadian Intellectual Property Office. The Ontario government can look for guidance from Canada's Innovation Superclusters as well as practices used in large projects such as the Canadian genome projects.

14. What legal, policy or regulatory changes should be considered to support effective governance and growth of the digital identity ecosystem?

- Global Privacy laws are evolving. Keep close to those sources.

- Reference results of recent Ontario government consultation
- Think global, not just Ontario, so your framework could be a model for other jurisdictions. Important to understand where global jurisdictions may conflict.
- Look to other jurisdictions for what they have done as a model, learn their lessons rather than recreating from scratch

15. What could the core guiding principles of the governance framework be?

As the ToIP Governance Metamodel suggests, the Government of Ontario as a governance authority can define the principles you wish to incorporate into your ecosystem governance framework. Several other ecosystems have formed Task Forces under the ToIP Ecosystem Foundry Working Group to collaborate on similar work. Here are examples of the types of principles that these Task Forces have been evaluating:

- The Laws of Identity (Kim Cameron)
- Self-Sovereign Identity Principles (Christopher Allen & Rebooting the Web of Trust)
- Sovrin Governance Framework (Sovrin Foundation)
- Design Principles for SSI (Jasmin Huber and Johannes Sedlmeir)
- The Windhover Principles for Digital Identity, Trust, and Data (Institute for Data Driven Design)
- Presidio Principles: Foundational Values for a Decentralized Future (World Economic Forum)
- MyData Declaration and MyData Guiding Principles (MyData Global)
- CARE Principles for Indegenious Data Governance
- Universal Declaration of Digital Identity (Tech for Justice)
- Canadian Charter of Rights and Freedoms
- Charter of Fundamental Rights of the European Union (English) (EU Commission)
- Australian Privacy Principles

Of special note is the work of the Sovrin Ecosystem Governance Framework Task Force to develop a third generation of the Sovrin Governance Framework. In this work, the current second-generation Sovrin Governance Framework is being separated into the Sovrin Utility Governance Framework (SUGF) for ToIP Layer 1 and the Sovrin Ecosystem Governance Framework (SEGF) for ToIP Layer 4. The goal is for the SEGF to define a set of universal principles for any ecosystem that wishes to embody the core values of self-sovereign identity. This work is still underway, however the SEGF Task Force expects to complete the Principles of SSI in early December. The current draft is here.

16. What could the key operating standards of the ecosystem be?

This question goes to the very mission of the ToIP Foundation, which is to standardize digital trust infrastructure using a dual stack of governance and technology. So our answer is that the “operating standards” for the Ontario digital trust ecosystem should be based on the ToIP stack. Specifically, the Government of Ontario as the governance authority (in conjunction with all the public and private stakeholders) should develop and publish:

1. **The Ontario Digital Trust Ecosystem Governance Framework** specifying the purpose, principles, and policies for the ecosystem. This ecosystem governance framework should follow the ToIP governance metamodel as well as be compatible and interoperable with the Pan-Canadian Trust Framework. Its Controlled Documents should include a base level of risk assessment, a trust assurance framework, and a certification program.
2. The Ontario Digital Trust Ecosystem Governance Framework should specify technical interoperability using a ToIP Interoperability Profile (TIP) that includes the relevant standards and interoperability profiles at all four layers of the ToIP stack. The technical components of the certification program should operate against this TIP.

17. How would liability be shared among ecosystem participants?

The Trust Over IP Foundation is not a legal advisory group. While many members of the foundation are very savvy about risk, liability, and approaches to deal with both, the foundation is not an authority here.

Technology & Operations

18. What are the necessary foundational pieces of the ecosystem that can be stood up / enabled now while standards continue to mature and evolve?

The Trust over IP model itself, founded on the dual governance and technology stack, and driven by the insight that the business rules and policies that apply to a trust ecosystem must be made explicit before technologies are assembled to produce credentials, reflects the foundational pieces that need to be in place.

First and foremost, it is necessary to completely understand the problem that needs to be solved, the benefit that adopting verifiable credentials can offer and the real-world

constraints and parameters that apply to the business or government-service context. Technology and standards cannot be a substitute for this intelligence.

Borrowing from analyses recently published by Timothy Ruff (https://medium.com/@rufftimo/how-verifiable-credentials-bridge-trust-domains-97155d0f3c17), most organizations today operate “in separate, unconnected trust domains, unable to directly exchange trusted data and reliant on manual processes, often through third-party data brokers acting as intermediaries.” Overcoming these siloes is made especially difficult by the overlapping sets of barriers that, together, block the ability to achieve “transitive trust with rapid verifiability.” These barriers include:

- Having many usernames and passwords
- Cumbersome forms and onboarding processes
- Verbally authenticating when calling a service center, and re-authenticating when being transferred
- Waiting for agreements to be signed or consent to be given
- Waiting for any kind of application to be approved
- Slow verifications of any kind of documents, records
- Many slow and/or tedious processes that rely on verifications

Understanding which kinds of barriers exist in an organization, and targeting those which can be eliminated to support the use and benefits of verifiable credentials in a given context, is critical no matter how the standards develop. The technologies, DID methods and interoperability requirements for decentralized credentials will continually evolve. Being the sort of organization that knows itself, and deeply understands the problem it is trying to solve, is foundational to supporting the emergence of digital trust ecosystems that work.

19. How would you address difficulties in accessing digital identity services for marginalized Ontarians, who may not have immediate access to a digital device or infrastructure (e.g. high-speed internet)?

There are many different ways in which people and communities may come to be excluded from digital trust ecosystems and their benefits.

Some may be excluded due to social biases and economic disadvantages while others will face different kinds of obstacles based on a disability or the location of the community where they live.

Facing this significant challenge, and creating ecosystems that serve diverse communities that fully benefit from their adoption and success, requires that frameworks and services be conceived with these questions in mind from the start.

ToIP, for example, has recent approved the establishment of a Human Experience Working Group that will not only explore the design of applications whose use fosters trust among and between persons. It will also seek to bring the diverse voices and perspectives of people who may not currently have the means to participate in ToIP into our work.

Along with established measures (e.g. all ecosystems which use Hyperledger Indy and Aries components have a design to be used offline and asynchronously), the following other factors need to be considered in ecosystem design:

- Societal exclusion of people and communities where income inequalities, forms of educational/knowledge, among other factors, may make it difficult to adopt advanced digital applications
- Physical or cognitive impairment (e.g. due to disability or mental health condition) including age related conditions such as poor manual dexterity and dementia.
- Geographic exclusion, due to limited access to mobile or fixed line data services
- Language and literacy, (e.g. populations with low or poor literacy in local languages or those for whom French or English are not their native language).

Access to digital services should be addressed in three pillars to develop a fully usable service, and enable the identity holders to have as much self-sovereignty as possible:

1) Use of a special kind of delegation and designation called ‘Guardianship’ which allows for individuals to choose (or have chosen for them depending on the context), a person who manages their ID for them. Guardian examples include children, those who are digitally excluded, and adults living with dementia or with a learning difficulty. This model enables provision of a ‘digital assist’ model of service delivery with intermediaries (for example through networks of banks, post offices, or community groups). For a detailed discussion of digital guardianship, see the Sovrin Foundation Guardianship white paper.
2) Access using low-tech connectors, for example QR Codes and SMS or voice channels allowing access in low/no connectivity areas.
3) Offline connectors that bind the individual to the digital ID (e.g. biometrics, secure tokens or authoritative identity evidence)

The following issues further extend the impact to marginalized Otarians beyond identity:

- Financial exclusion for those without access to a bank account or with a ‘thin’ credit file
- Social or political exclusion, for people and communities faced with persistent bias such as women, cultural minorities, indiginous peoples, and newly arrived migrants.

Including those potentially marginalized populations requires other techniques to design a service that is fit for its purpose.

1) Inclusive and respectful design models which engage early on with representatives from marginalized communities and enable them to co-create the user experiences and define from the outset their requirements
2) Designing all citizen services to be accessible at very low levels of assurance, modularizing them and promoting access to services above identification of the participant
3) Innovation in methods and evidence required for identity vetting allowing alternatives to state-issued documents, financial services and household bills.
4) Understanding of the socio-political factors at play in all of the communities served so that every effort is made to de-politicise and reduce the risk to individual's privacy and personal safety when 'signing up' for, or using a digital ID. This means that the language, design and approach for user interface and service design need to be flexible and adaptable to consider the preferences of marginalized populations.

20. What is your perspective on how to mitigate other technology and operations related risks such as resource gaps, implementation delays, cost-overruns, technology changes over time, technology failure, misuse, device/IP/identity spoofing, bots?

The Trust Over IP Foundation is not an operations focused group. While many members of the foundation support some of the largest systems in the world, the foundation is not an authority here.

Funding Model & Ownership

21. How should a digital identity ecosystem be funded? Who should be responsible for capital and operating costs? Any insights from financing a multi-entity ecosystem in the past, that may also have included public and private sector stakeholders? Should any parts of the DI ecosystem be owned and managed by the government, in the public interest/good?

Funding for an underlying network/ledger should be shared amongst the key stakeholders in an ecosystem. While the government plays a crucial role in this ecosystem as an

Authoritative Issuer it does not need to lead the operations of such a network. It can act as an equal partner of the other stakeholders. If there is a leadership role where the government is uniquely positioned it would be at the governance level where government can set the rules and regulations as it does in many industries.

The Ontario government will need to work to provide expertise and models for ecosystem intellectual property to address Data IP (relating to contribution of data and information from a variety of sources and from which a variety of insights and applications can be developed) and Inventive IP (relating to the tolls, software and inventions, patentable or not, that may arise from projects undertaken as part of a verifiable credential ecosystem and which may make use of Data IP) as well as processes to support collaboration with ecosystem participants/partners, experts in the field and the Canadian Intellectual Property Office. The Ontario government can look for guidance from Canada's Innovation Superclusters as well as practices used in large projects such as the Canadian genome projects.

22. What are the risks associated with your recommendation? How those could be mitigated?

The Trust Over IP Foundation strives to promote open and generally accepted global standards and practices for the betterment of the commercial, private and public sector use of the Internet. Our recommendations are subject to a fluid and changing technological landscape. As such, addressing risks requires an approach that is just as nimble as flexible as this ever-changing environment.

The Governance Authority ("***GA***"), or Credential Issuer ("***Issuer***"), which adheres to the established Governance Framework ("**GF**") must make efforts to assess and proactively manage potential risks associated with the issuance, holding and verification of credentials. The level of effort applied to risk assessment and management must be determined exclusively by the GA or Issuer along with potential advisors, and should be based on whatever risk mitigation such entity considers to be reasonable for the associated stakeholder group. The following guidelines for a GA or Issuer are recommended for risk assessment and management efforts. As such, any GA or Issuer:

1. SHOULD identify key risks that MAY negatively affect the achievement of the GF's purpose within its scope,
2. SHOULD include a Risk Assessment process output that provides an assessment of each key risk that the GF is designed to address and mitigate,
3. SHOULD assess which Roles and Processes are vulnerable to each risk and how they are affected,
4. SHOULD include a Risk Treatment Plan (RTP) for how identified risks are treated (e.g. mitigated, avoided, accepted or transferred),

   [Reference: ToIP Governance Metamodel]

If a GA or Issuer is unfamiliar or not comfortable completing a risk assessment process, along with an appropriate risk management plan, it is recommended that capable advisory support be engaged. However, any decision on how to proceed with this process is at the total discretion of the GA or Issuer. Ultimately, the results of any risk assessment and management effort should be published as one or more supporting documents that are readily available for any credential Issuer, Holder and/or Verifier to review in full.

ToIP offers the following list of potential risk categories for assessment in Table 1. This list is not comprehensive, and other categories may be required for specific situations. Similarly, any number of the risk categories in Table 1 may be determined to be unnecessary. The ultimate range of risk categories considered by any GA or Issuer can only be decided by such GA or Issuer, potentially with input from qualified advisors and stakeholders.

Table 1: Sample Risk Items

[For a more comprehensive list or potential risk items, see: ToIP Risk Assessment List]

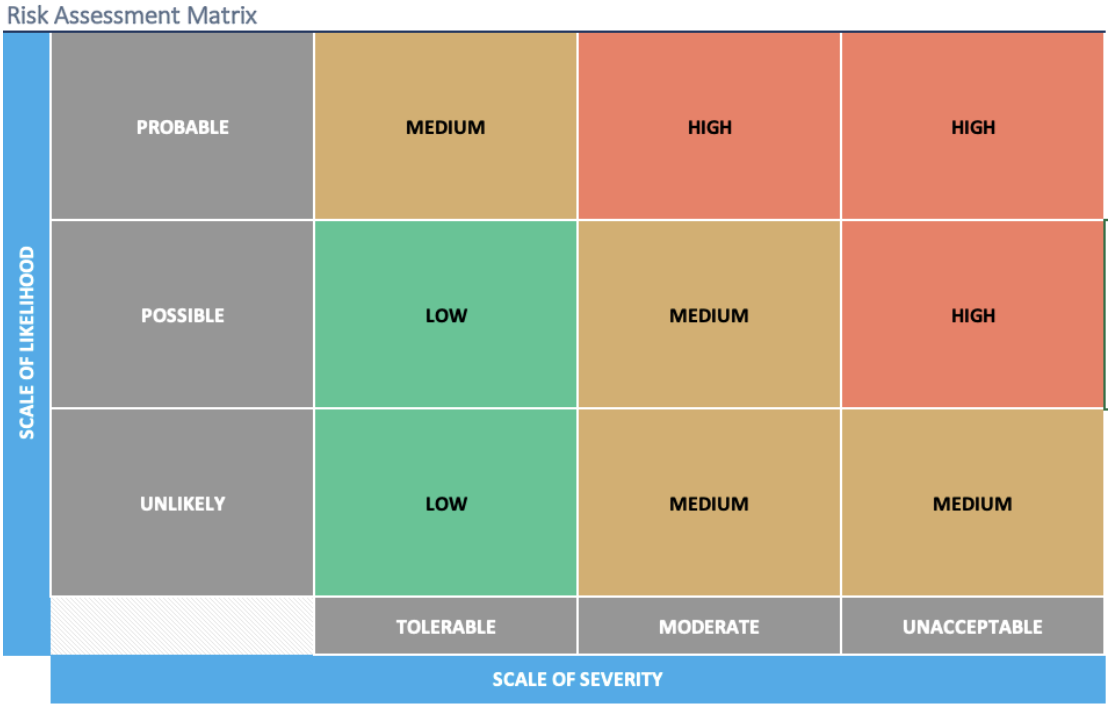
Governance Authority Risks
1. Lack of competence to perform role
2. Lack of appropriate authority
3. Ecosystem Lacks Jurisdictional Acceptance
4. Ecosystem Lacks Industry Acceptance
5. Ecosystem Allowing Inappropriate Actors to Participate in Network
Issuer Risks
6. Credential Issued without sufficient basis
7. Credential Issued before appropriate proofing of basis
8. Credential Issued in the wrong format or structure
9. Credential issued to impostors
10. Issuer Practices Not Accepted by Ecosystem
Verifier Risks
11. Lack of consistent verification practices
12. Evidence of verification incomplete or in incorrect format
13. Verifier Practices Not Accepted by Ecosystem
14. Suspended Credential Being Accepted
15. Revoked Credential Being Accepted
Credential Registry (Ledger) Risks
16. Lack of competence to perform role
17. Unavailable registry
18. Inappropriate access writes to registry
19. Breach of registry

20. Exploited Use of Stolen Credentials
21. Credential Registry Not Accepted by Ecosystem
Credential Holder Risks
22. Counterfeit Credentials Being Created
23. Credential Holder Given Inappropriate Access Rights
24. Imposter Using Valid Credential
25. Credential Wallet Private Key is Compromised
26. Credential Holder's Private Data is Compromised
27. Social Engineering Attacks Successfully Gather Credentials by Perpetrators
Utility Operation Risks
28. Stewards Not Abiding by Governance Practices
29. Inadequate Infrastructure Supporting Steward Operations
30. Inadequate Network Throughput Supporting Steward Operations
31. Inadequate Network Availability Supporting Steward Operations

Deeper analysis of risks items and their potential impacts is beyond the scope of the GF, because it is necessary for this work to be done by GAs and Issuers. However, a simple approach to risk assessment can be calculated using the approach below, which follows guidance from the ToIP Governance Metamodel previously referenced. The potential impact ("***I***") of any risk item is the product of the likelihood ("***L***") of a risk incident occurring multiplied by the outcome severity ("***S***") that would be incurred due to such incident. Quantitative values for *likelihood* and *severity* should be assigned by the risk assessment team, and resulting values can be partitioned into numerically scaled groupings of LOW, MEDIUM and HIGH *impact*.

$$L \times S = I$$

The above approach for estimation of risk impact can then be used to show a distribution of risk items by plotting the risks items in a two dimensional table, such as the sample table shown below. This visualization enables the risk assessment team to have a consolidated view of all risk items, and start to develop a risk management plan for the set of risk items that are considered to be critical for inclusion in such a plan.



We recommend that the Governance Authority create a Risk Treatment Plan for HIGH risks but should also consider a plan for MEDIUM risks.

Generally accepted risk assessment methodologies advocate that some risks may be avoided, transferred or just accepted. The risks that can be mitigated should be attached as control requirements by the Governance Authority to other stakeholders whose accountability could be monitored as part of a Trust Assurance scheme.

Benefits & Monetization

23. What are the opportunities for monetization in the ecosystem for various participants to support its overall longer-term sustainability (e.g., business to business, business to government or vice versa, end user fees, data-related services)?

The support for the Issuer, Holder, and Verifier model allows for multiple areas where monetization can be enabled. The PCTF adds a potential fourth party - a Witness - where there is a requirement for interaction or observation. Payment could go to one or more of the

parties in the credential exchange triad. However, early monetization efforts may focus on direct cost savings to participants.

There are several discrete points that can be considered related to monetization:

- Starting with monetization approaches (e.g. Holder pays extra for a digital identity card) may inhibit adoption and innovation. Proving the value (cost savings or new revenue) before fees are charged will be crucial.
- More broadly – consider the UN SDGs – currently most models are unrealizable and will not be adopted by those who need to implement actionable outcomes. The use of verifiable credentials in various
    - Proof of ethical labour – important for investment community
    - Proof of sustainable on-farm practices – emission markets
- ID issuance is a basic necessity for a jurisdiction and should be issued with as little cost to the ID holder as possible. Monetization of Commercial uses of IDs and ID information should be aligned with the utility that credential information provides.
- B2B examples would include cost saving for many manual processes:
    - Compliance - on major job sites compliance checks (e.g. confirming all personnel are fully trained and certified for particular tasks; permitting) drive costs up. Many compliance checks could be fully automated. The Government of British Columbia has examined opportunities for this kind of automation.

Wrap-Up

24. Have you observed any case studies in other jurisdictions that have made significant progress in implementing a digital ID ecosystem? What has worked well and what are some of the key lessons learned?

While many digital identity solutions are in place at government scale (e.g. India and Estonia for national ID; BC and Alberta for digital linkage to federal services) there are no direct ecosystem examples that the foundation can point to at the moment. Each of the examples “in the wild” are generally centralized and using older generations of technology (PKI, smartcards) or very limited in scope (e.g. government service login).

One of the main drivers behind establishing the Trust Over IP Foundation was the recognition that there are broad differences between jurisdictions globally and that standards

that support the technical and governance needs is crucial. The discrete successes in some areas may require different approaches in other areas.

25. We have identified some potential risks associated with a digital identity enabled ecosystem – based on the list provided, are there additional risk categories or key risks that have not been addressed? Please share your perspective on mitigating the risks that haven't been discussed so far.

Please see the answer to question #22.

26. Is there anything else you would like to share about the approach to developing a digital identity ecosystem?

At the moment no. However, the Trust Over IP Foundation would be happy to offer a short virtual workshop where the Government of Ontario and foundation members could explore concepts and ideas further.

Success in this area of activity is highly dependent on delivery execution. Having the right people in place, and adopting approaches that are proven to be effective, are as critical as tracking the evolution of DID methods and technical standards.