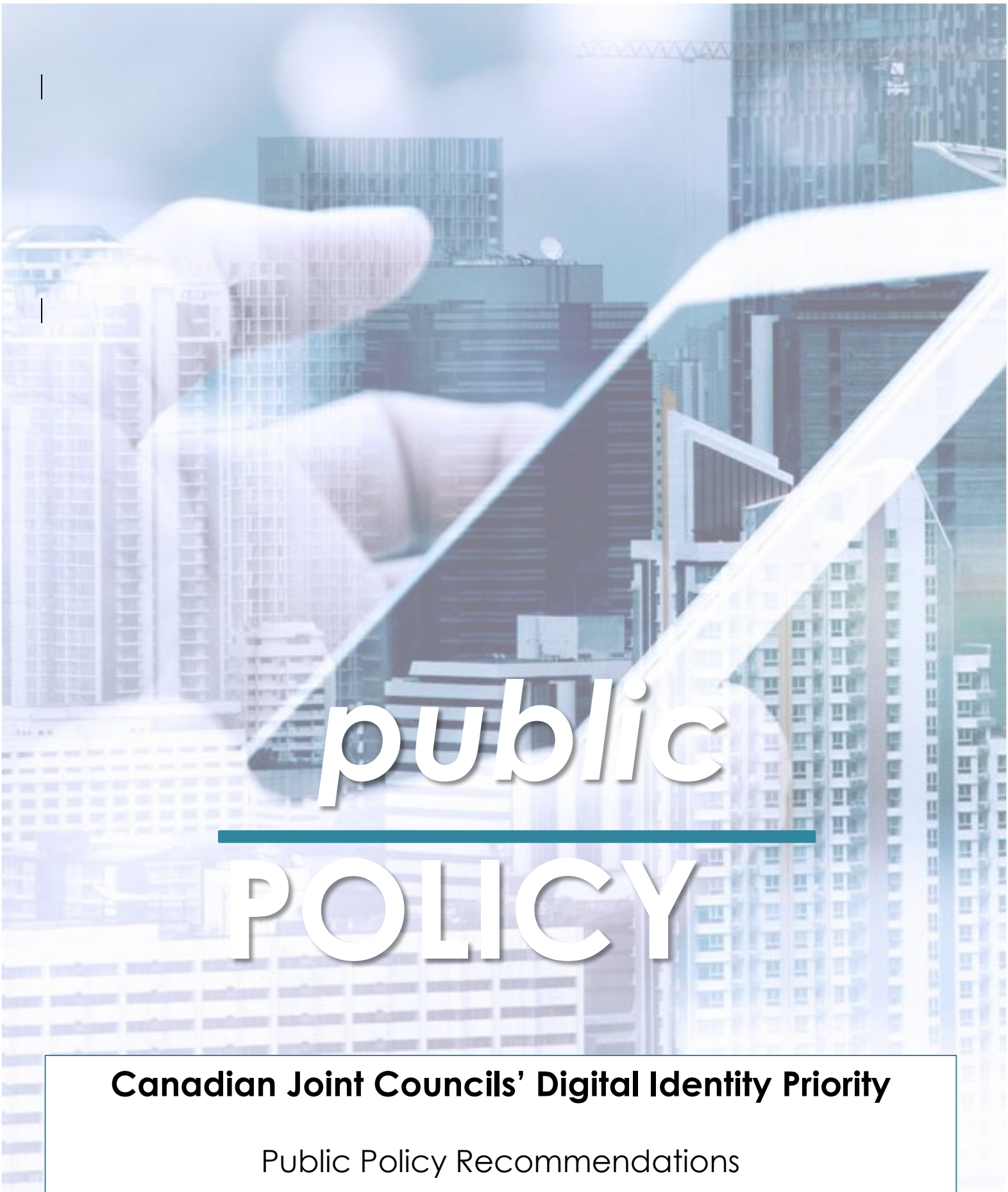


Canadian Joint Councils' Digital Identity Priority

Public Policy Recommendations

Prepared by Public Policy Working Group, February 2019

Table of Contents

To the members of the Canadian Joint Councils

As the co-leads for the Digital Identity priority stream, we are pleased to present the following recommendations for a Pan-Canadian policy position on the question of the roles and responsibilities of public and private sector in digital identity. We believe this moves us closer to transforming government services, enabling government across jurisdictional boundaries, and enabling Canadians to participate confidently and securely in the growing digital society.

Following Joint Councils' approval to establish a Public Policy Working Group, we issued a call for participants to all Identity Management Sub-Committee IMSC/Joint Councils members. The group was established in May 2018 and brought together seventeen representatives at the municipal, provincial and federal levels. This group met over the summer 2018 and this report is the result of their deliberations.

Leveraging existing work by the Pan Canadian Trust Framework (PCTF) group and IMSC, the Working Group identified three guiding principles:

- an individual's' right to an identity cannot be compromised;
- privacy and security are critical in allowing Canadians to participate confidently in the digital society;
- convenience and choice are key drivers for citizens.

Based on these principles, three general themes of accountability are recommended:

- privacy and security: the public sector must retain accountability for setting legal requirements and monitoring compliance;
- establishment and use of digital identities: to meet the demands of convenience and choice, both the public and private sectors have roles to play in the provision, management and use of digital identities;
- foundational evidence of identity (birth and arrival in country records): accountability for the issuance must continue to lie with the public sector.

Within this context, the detailed recommendations recognize the significant value that the private sector will add. We are excited to see what future growth and collaboration in this space will mean for Canadians.

We offer sincere thanks to the working group for their dedication and willingness to tackle this very important question of the appropriate roles of the public and private sector in digital identity.

Jackie Stankey
Director, Enterprise Strategy & Planning
Office of the Corporate Chief Information Officer,
Service Alberta

Sophia Howse
Executive Director, Province of BC,
Provincial Identity Information Management Program

1. Context and Objectives

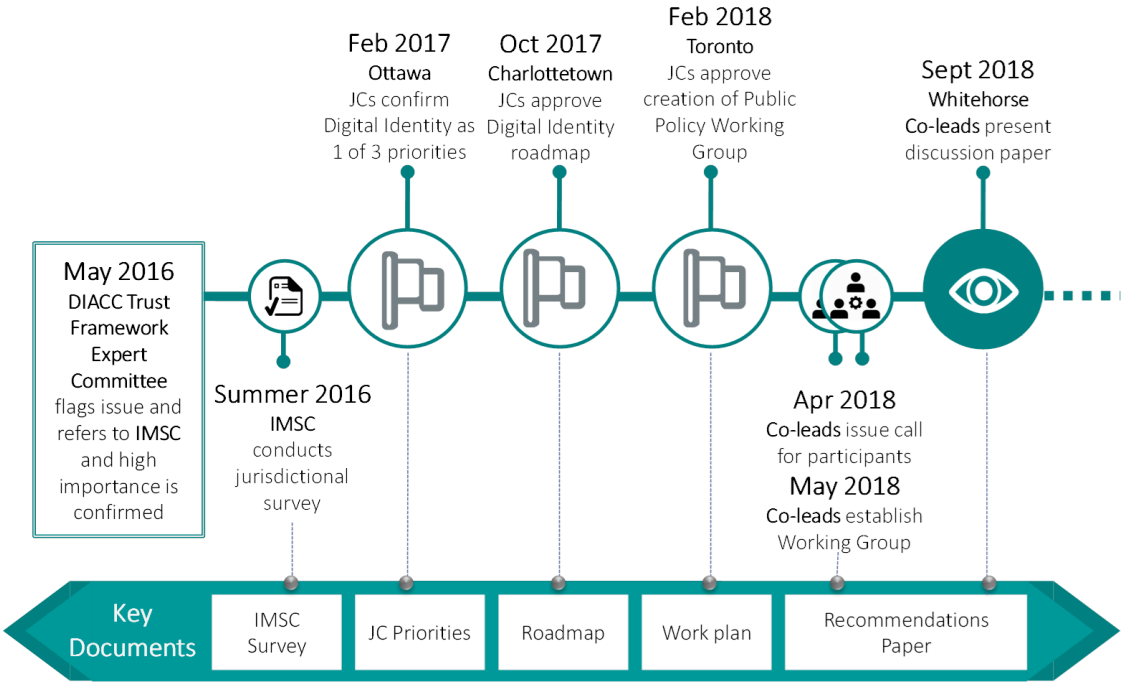
The digital identity space is a rapidly changing environment and as identity increasingly moves from a paper to the digital world, the lines between the public and the private sectors are blurring:

- disruptive technologies are changing the landscape of identity and who acts in the identity space;
- governments act to correct market failures and gaps by providing goods where there is little incentive for the private sector to provide them; and
- new technologies often result in new goods and services.

The Public Policy Working Group (PPWG) was established at the request of the Joint Councils with the objectives of:

- assessing and developing recommendations on the appropriate roles and responsibilities of the public and private sectors in digital identity management for individuals and not businesses; and
- providing policy input into how to move the Pan-Canadian Trust Framework forward.

2. Background



In May 2016, the question of the appropriate roles of the public and private sector in identity management was raised at the DIACC Trust Framework Expert Committee (TFEC). The issue was referred to the Identity Management Sub-Committee (IMSC) and the subsequent discussions confirmed that this was an important area that required further research.

In summer of 2016, prior to the establishment of the PPWG, the IMSC conducted a cross-jurisdictional review to clarify its position on the roles and responsibilities of the public and private sectors and describe the rationale for the decisions. The results were presented in the IMSC's "Discussion Paper: Roles and Responsibilities of the Public and Private Sectors".

In February 2017, the Joint Councils endorsed three priority areas to be actively pursued, one of which was Digital Identity. Two co-leads, Alberta and BC, were identified to plan and coordinate work in this area. In October 2017, the co-leads presented a digital identity roadmap and gained approval from the Joint Councils to proceed with the work. One of the work streams on the roadmap was "Policy and Governance" and at the February 2018 Joint Councils meeting the co-leads gained approval to initiate the work in this area and established the PPWG. The vision was that this Working Group would conduct research, facilitate discussions and develop recommendations for a Pan-Canadian policy approach on the question of the roles of public and private sector in digital identity. In April 2018, a call for participants for the PPWG was issued via e-mail to all IMSC/Joint Councils members and the group was established in May 2018.

This report is the result of the deliberations of the PPWG and is presented to the Joint Councils in September 2018 for consideration, with the intent to seek endorsement following the submission of comments.

3. Key Definitions

Identity management and digital identities are complex and still evolving subjects. There are a number of new terms that have entered our lexicon from these areas; some of these have widely accepted definitions, while others are less standardized. For the purposes of this document, the definitions adopted by IMSC in April 2016 have been used in this document. The key terms are shown in the table below.

Assurance	A measure of certainty that a statement or fact is true.
Authentication	The process of establishing truth or genuineness to generate an assurance.
Credential	A unique physical or electronic object (or identifier) issued to, or associated with, a person, organization or device (e.g. key, token, document, program identifier).
Credential Assurance	The assurance that a person, organization or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).

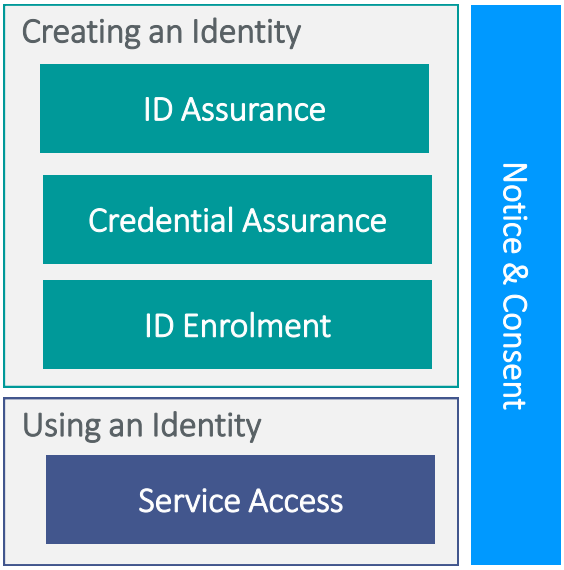
Foundational Evidence of Identity	Issued by a government institution relating to the registration of a vital or major life event, foundational evidence of identity is used to establish core identity information such as given name(s), surname, date of birth and place of birth. Examples of foundational evidence of identity include, but are not limited to: birth certificates, permanent resident cards, and certificates of citizenship.
Identity	A reference or designation used to distinguish a unique and particular person, organization or device.
Identity Assurance	A measure of certainty that a person, organization or device is who or what it claims to be.
Identity Enrolment	Connecting an identity to a credential, therefore linking the real you to the credential
Identity Establishment	The creation of an authoritative record of identity that is relied on by others for subsequent government activities, programs, and services.
Identity Issuance	The creation of evidence of identity that is issued to an individual and can be relied on by others for subsequent government activities, programs, and services.
Identity Verification	The confirmation that the identity information being presented relates to the person who is making the claim.
Trusted Digital Identity	An electronic representation of a person, used exclusively by that person, to receive valued services and to carry out transactions with trust and confidence. A person can be a 'natural person' (e.g., an individual) or it can be a 'legal person', which includes corporations and other organizations.
Verified Person	Knowing (or having a degree of certainty) that an individual is real, identifiable, and has truthfully claimed who he or she is.

4. Working Group Context

Scope

The PPWG was charged with assessing the appropriate roles and responsibilities with respect to trusted digital identities. Referencing the definition above, this is the electronic representation of a person, used exclusively by that same person to receive valued services and to carry out important transactions with trust and confidence.

The PPWG identified five components of a trusted digital identity for individuals and used these for the policy analysis:



- **Creating an Identity**
  - *Identity (ID) assurance*: verification that a person is who they claim to be for the purposes of establishing a digital identity.
  - *Credential assurance*: rules and standards associated with a credential, ensuring that it is secure and can be trusted in future authentication events.
  - *Identity (ID) enrolment*: the binding of an identity with a credential.
- **Using an Identity**
  - *Service Access*: authentication of a person at the point of service, ensuring that the person is who they say they are and can be allowed access.
- **Notice and Consent**
  - *Notice & Consent*: triggered at multiple points when an identity is created or used, notifying an individual of the authorities under which personal information is being collected, how and what personal information will be shared and seeking appropriate consent to proceed.

Working Group Membership

The Working Group had seventeen participants including municipal, provincial and federal representation:

- 2 BC team leads
- 1 representative from a municipality in Ontario
- 5 representatives from the following 3 provinces; Alberta, New Brunswick, and Nova Scotia
- 9 federal representatives from the following departments; Employment and Social Development Canada, Immigration, Refugee and Citizenship Canada and Treasury Board of Canada Secretariat.

Participation in the Working Group was voluntary and carried out over the course of summer 2018.

Key Documents

The PPWG leveraged the IMSC Discussion Paper and the Pan-Canadian Trust Framework to identify the key components of identity management where clarity on roles and responsibilities was required. (See Appendix I for mapping).

Approach

The PPWG leveraged the IMSC Discussion Paper to highlight key points that warranted further exploration. The discussions used the economic public vs. private goods matrix, based on Paul A. Samuelson's theory of public goods and developed by V. Ostrom and E. Ostrom, as a means of assessing where the five components of digital identity lie and what the appropriate roles of the public and private sectors should be. (See Appendix II for further explanation of the Public v. Private Goods matrix.)

Guiding Principles

During the discussions, the PPWG identified three key principles that were applied in defining appropriate roles of the public and private sectors:

- international human rights stipulate that an individual's' right to an identity cannot be compromised;
- meeting citizens' expectations and complying with legislated privacy and security requirements is critical in allowing Canadians to interact confidently with government and participate in a digital society;
- convenience and choice in service access are key drivers for citizens and delivery models must meet these demands.

5. General Themes of Accountability

Based on the guiding principles, the PPWG developed three general themes of accountability that apply across all identified components of a trusted digital identity. These are summarized below and repeated within the more detailed discussion of each component.

Privacy and Security Requirements

Given the criticality of ensuring a high level of confidence in privacy and security protocols, and the significant risks of breaches, the PPWG deemed that **the public sector must retain accountability for setting legal requirements and monitoring compliance**.

All digital identity services, whether they are delivered by the public or private sector, will be expected to comply with these requirements.

Establishment and Use of Digital Identities

Satisfying the twin drivers of "convenience and choice for citizens" demands that both the public and private sectors have major roles in service delivery. These services must comply with the regulatory framework described above.

It is important that the public sector continues to play a role in establishing digital identities to ensure that they are widely available. However, where there is no legal right to service, the private sector can add significant value in the provision and management of digital identities.

Foundational Evidence of Identity

During the discussions, it became apparent that foundational evidence of identity (birth and arrival in country records) has a distinct and special role in creating an identity and merited a unique treatment.

Articles 6 and 16 of the Universal Declaration of Human Rights state that 'everyone has the right to recognition everywhere as a person before the law'. Thus, every individual is entitled to an identity and the establishment of that identity must be considered a public good. **Keeping accountability for foundational documents (e.g., birth, immigration, and citizenship) in the public domain ensures that all individuals are able to obtain a foundational credential.**

Further, the consequences of a data breach associated with foundational documents pose a significant threat and may cause a loss of public trust in government stewardship of personal information. This, again, argues for the public sector to retain the legal and fiduciary accountability and responsibility for establishing and securing these foundational credentials.

Keeping foundational documents in the public domain helps to ensure that there is one registry and that access is not restricted to certain groups or customers. Having a single registry in each jurisdiction helps to uphold the integrity of that registry and limits opportunity for fraud or misuse. Further, should fictitious identities be discovered, there are fewer authoritative sources that have to be reconciled.

The PPWG concluded that accountability for the issuance of foundational evidence of identity must continue to lie with the public sector and cannot be delegated to the private sector. However, it was recognized the private sector may add value in this area by providing services that manage these foundational credentials at the request, and on behalf of the citizen. Further discussion on foundational documents is excluded from the five components below.

6. Identity (ID) Assurance

Identity (ID) Assurance is the measure of certainty that a person, organization or device is who or what it claims to be. Verifying that a person is who they say they are is an essential first step in establishing a digital identity.

Identity assurance includes determining the rules for verifying an individual is who they say they are and establishing an identity; e.g., what types of documents are required, whether a counter visit is required. The rigour required varies with the target level of assurance; e.g., at lower levels of assurance self-attestation may be sufficient, while at higher levels of assurance original foundational evidence and an in-person verification check may be required.

As a result of the verification step, the person is now recognized and a digital identity can be created with a clear level of assurance.

Discussion

The establishment of a digital identity based on identity evidence may be the responsibility of the public or the private sector; e.g., banks establishing a digital identity for a client, or schools establishing a student identity. The relevant organization would be responsible for setting the standards for the verification event and complying with legal requirements for privacy, data protection and notice and consent.

Recommended Roles and Responsibilities

Public Sector	● Accountable for establishing legislation, standards and policies for credentials. ● Accountable for ensuring the compliance of all parties with legislation, standards and policies. ● May provide verification services. ● Accountable for managing the verification process standards for their own credentials. ● Responsible for ensuring that identity assurance services comply with legislation, regulations, policy and standards.
Private Sector	● May provide verification services at the request of and on behalf of the public sector for identity assurance (excluding foundational identity assurance). ● Accountable for managing the verification process standards for their own credentials. ● Responsible for ensuring that identity assurance services comply with legislation, regulations, policy and standards.

7. Credential Assurance

Credential Assurance is the confidence that a person, organization or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).

The goal of credential assurance is to ensure that future authentication events are safe, secure and not easily recreated. This confidence is enabled through setting the minimum standards that govern the strength of the credential (e.g., security features for a physical credential, password standards).

Discussion

Today, both the public and private sectors issue credentials and set standards for credential assurance. Indeed, the private sector is a more significant player in this area. Generally, the issuing organization sets the assurance standards and ensures that they are met. However, credential issuance does not occur in a vacuum and the public sector must retain accountability for maintaining the regulatory framework that will protect the citizen's identity data. For example, it is recommended that the public sector establishes the rules and regulations for what can be done with credential information (i.e., what can and cannot be shared) and all issuing organizations acknowledge and comply with these rules. This will provide a high degree of confidence among citizens.

Within that regulatory context, credential assurance is likely to remain an area where both public and private sectors operate. Indeed, the ecosystem needs to allow for a range of credentials to provide choice and security for the citizen.

Recommended Roles and Responsibilities

Public Sector	● Accountable for establishing legislation, standards and policies for credentials that safeguard security and privacy. ● Accountable for ensuring compliance of all parties with legislation, standards and policies. ● Accountable for setting credential assurance standards for government-issued credentials. ● Responsible for complying with legislative, standards and policies requirements for government-issued credentials.
Private Sector	● May provide credential assurance services at the request of and on behalf and at the request of public sector. ● Accountable for developing credential assurance standards for any credentials issued on behalf of their own organization. ● Responsible for complying with legislative, standards and policies requirements for credentials.

8. Identity (ID) Enrolment

Identity-credential binding associates your identity to a credential used by you, therefore linking the real you to your trusted digital identity. This process can either result in the binding of new identity with an existing credential that you have, or a new credential issued to you. For example, when accessing Government of Canada services, you may wish to use your existing banking credential or a new one issued by the Government of Canada. In British Columbia, your identity is bound to your British Columbia Services Card. In Alberta, your identity is bound to a username and password that you choose to access the MyAlberta Digital ID Program.

Discussion

Within an established framework already discussed as part of credential assurance, both public and private sector organizations may establish a digital identity and proceed with identity enrolment. That organization will be responsible for:

- determining if an existing credential meets established requirements and can be leveraged or a new credential will be issued;
- ensuring that new credentials meet established requirements;
- the subsequent binding of the identity with the credential as a precursor to authentication and service access.

The digital identity ecosystem also opens up opportunities for public/private partnerships. For example, the Government of Canada, uses a mixed public- and private-sector delivery model. Clients are offered the option to sign-in with CRA Login (for CRA services), GCKey, the government-branded credential services, or SecureKey Concierge, a service offered by a private company that enables clients to use their existing bank-issued credentials. When using anonymous credentials (GCKey or SecureKey), federal departments must first determine the identity of the anonymous credential holder, ensure that it is right person using this credential, and finally associate this person to the file associated with them. To complete these processes, the user is asked for selected personal information (e.g., Social Insurance Number, date of birth, postal code, and an amount from recent tax return). Once this information is validated, a security code is mailed out to complete the process binding the client's identity to their preferred credential. By offering a choice of login credentials, the Government of Canada is enabling choice, and making online services more convenient for its clients to access. Many individuals regularly use their online credentials for banking or paying bills, so being able to use the same credential to access government services online means one less username and password for clients to remember.

However, the working group identified that there are specific areas where they felt the public sector should retain accountability:

- sensitive and public services (e.g., health, education and social services);
- where the credential may be used to change tombstone data and the ripple effects could be significant.

Regardless of whether the identity is being established by the public or private sector, responsibility for binding the identity with a credential and, optionally, issuing a new credential may be delegated to a third party, with the understanding that regulatory requirements continue to be met.

Recommended Roles and Responsibilities

Public Sector	● Accountable for establishing legislation, standards and policies for identity enrolment that safeguard security and privacy. ● Accountable for ensuring that identity enrolment regulatory requirements are met. ● Accountable for managing and ensuring the integrity of the binding and issuance processes for public sector-issued credentials. ● Responsible for ensuring that identity enrolment regulatory requirements are complied with.
Private Sector	● Responsible for ensuring that identity enrolment regulatory requirements are complied with. ● Accountable for managing the binding and issuance processes for private sector-issued credentials.

9. Service Access

Service access is where an individual presents a credential with the objective of gaining access to a service. When the service provider (or relying party) receives the credential information it determines if it can be trusted as authentication that the person requesting the service is who they say they are. This determination will be based on the known level of assurance of the identity and the credential and the risk tolerance of the service provider. If the identity is authenticated successfully, the service provider goes on to confirm access is authorized.

Service access may either be a one- time event, or trigger a more persistent service enrolment.

Discussion

In this instance, the service provider owns both the service and the rules over what credentials are to be trusted. The determination of what credentials are to be accepted will be based on the service owner's assessment of the level of assurance required for the particular service. For example, allowing access to medical records would likely require a very high level of assurance, while registering for an electronic newsletter may not.

Service providers may be in both the public and private sector and there is no difference in the roles; **each relying party is responsible for setting standards for access and ensuring that those are met by the credentials presented by the individual**.

Recommended Roles and Responsibilities

Public Sector	● Accountable for determining levels of required assurance for government services and ensuring that service enrolment requirements are in compliance. ● Accountable for ensuring the right digital identity is mapped or linked to the right service recipient for government services.
Private Sector	● Accountable for determining levels of required assurance for their services and ensuring that service enrolment requirements are in compliance. ● Accountable for ensuring the right digital identity is mapped to or linked with the right service recipient.

10. Notice and Consent

Notice and Consent refers to how individuals are made aware and provided choice about how their information is collected, used and disclosed. In notice, personal information controllers should provide clear and easily accessible statements about their practices and policies. Public Sector is concerned with notice (although the public sector also requires consent) and private sector concerns with consent. In order for consent to be meaningful, the user must understand what information is being used and for what purpose. In other words, they must understand what they are consenting to. Under federal legislation, private sector organizations are required to obtain individuals' consent to lawfully collect, use and disclose personal information in the course of commercial activity in accordance with PIPEDA federally and PIPA in BC and AB to name a few. Without consent, the circumstances under which organizations are allowed to process personal information are limited. Notification and consent may be required at multiple points in the digital identity process: verification, authentication and enrolment.

Discussion

The responsibility to provide adequate notice and consent processes lies with the organization collecting, storing and sharing the data. This is governed by a legal framework today. While the public sector could provide more advice on meaningful consent and consequences, ultimately if a citizen is aware of the risks, understands the impacts, and accepts them that is the citizen's right to do so.

It is important to note that there are regulations that limit the third party usage of identity information among other items. There are examples from other industries where the private sector adheres to legal frameworks with requirements for how identity information is handled such as *Proceeds of Crime* (Money Laundering) and *Terrorist Financing Act* overseen by FINTRAC.

There has also been growing public concern about security breaches. The organization collecting the information has the responsibility to notify the sources and the owner of the information. Currently under Bill S-4 the *Digital Privacy Act under Section 10* there are

regulations created for organizations to follow concerning content of notification and disclosure without consent.

Recommended Roles and Responsibilities

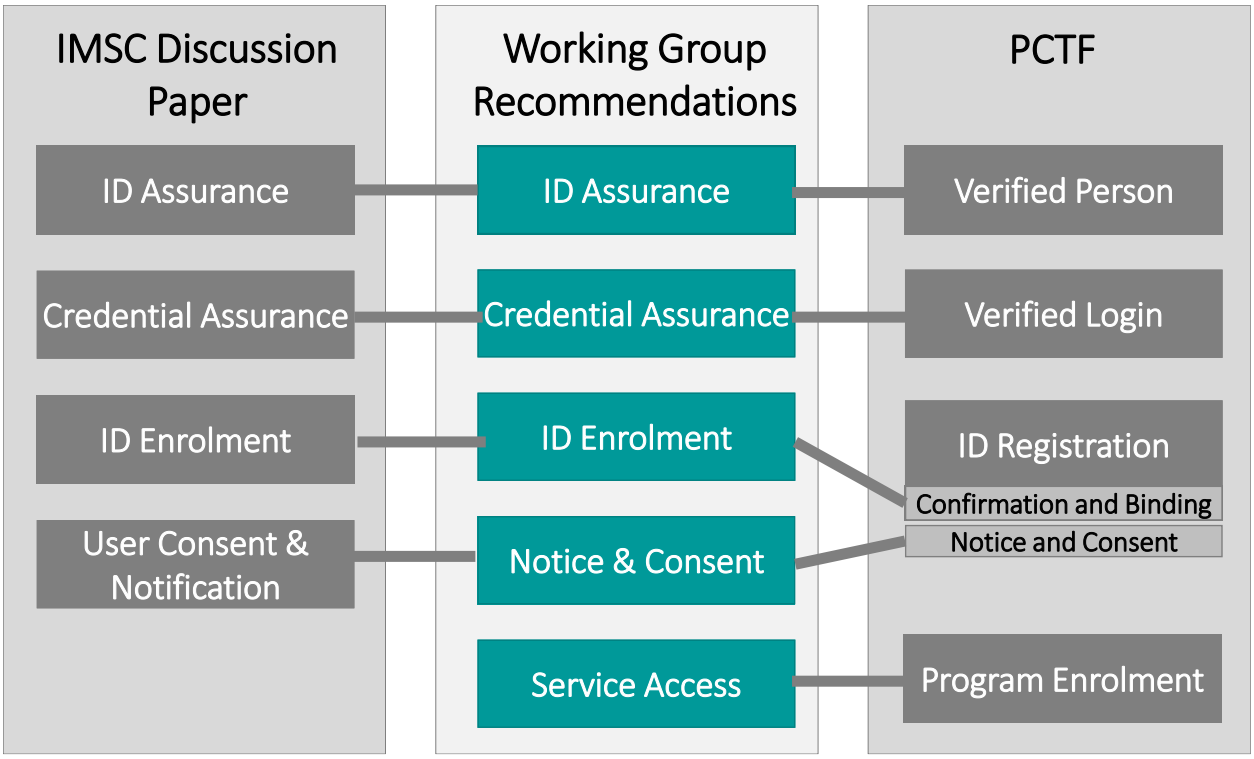
Uniquely, the roles and responsibilities for Notice and Consent fall within the privacy sphere are already well defined and stem from legislation. The current *Digital Privacy Act, Privacy Act and PIPEDA* (at the federal level) and *FOIPPA/PIPA* (at various equivalents across the provincial level) apply.

Public Sector	● Accountable for setting the regulatory framework for notice and consent. ● Accountable for enforcing compliance with regulations. ● Accountable for providing forum for citizen concerns. ● Accountable for ensuring notification and consent processing are in compliance with regulations.
Private Sector	● Responsible to operate in alignment with relevant legislation.

11. Conclusion

It is a human right to be recognized by your country before the law and hold an identity in that nation. Therefore, **Digital Identity is fundamentally a public good**. In Canada by establishing your identity you are automatically enrolled into digital programs and services that the government provides. There are also additional digital services such as education, and banking that are not a right but a privilege and therefore they can leave the realm of public goods and enter private. Throughout the discussion one theme continues to appear; accountability, holding the service provider accountable if there is a breach in trust or privacy. The concept of accountability requires government to implement procedures that protect the citizen's personal information, establish procedures to follow when developing digital identity initiatives or questions, train staff and be transparent about all procedures and practices. This is a recommendations paper, and the recommendation is to develop an accountability model in the public sector so that private sector can develop one that is similar. Of course, there is risk associated using accountability models in the ability to resolve misuse follows non-compliance and proof of non-compliance for affected individuals. This paper articulates the need for the creation of new regulatory instruments to supplement existing policy for this emergent area involving interactions within and between personal, public and private interests. Privacy laws and regulations should be leveraged. Meeting the citizen demands and expectations for service access and participation in the digital society requires an established standard for digital identity for the service providers to follow. Trust and inclusion must be established by the public sector as a standard for all organizations who establish, manage or use digital identities in Canada.

Appendix I - Mapping to IMSC Discussion Paper and Pan-Canadian Trust Framework



The mapping process identified a gap in the components identified in the IMSC Discussion Paper: service access or program enrolment. Although the IMSC paper included "ID Enrolment", it was felt that there was a significant enough difference between the binding of an identity to a credential and the subsequent use of the credential to access services that the two components should be separated. (Person X has an Ontario birth certificate, and therefore can create a driver's license) and service access allows that verified person to access a service (Person X now has a driver's license and is over the age of 19 they can now be served alcohol or able to drive a car).

"Service access" was selected for clarification, and to differentiate it from the preliminary identity establishment components.

Appendix II - Public/Private Goods Matrix

A private good is a product that must be purchased to be consumed, and consumption by one individual prevents another individual from consuming it. In other words, a good is considered to be a private good if there is competition between individuals to obtain the good and if consuming the good prevents someone else from consuming it. A private good is the opposite of a public good. Public goods are generally open for all to use and consumption by one party does not deter another party's ability to use it. It is also not excludable; preventing the use of the good by another is not possible. Many public goods can be consumed at no cost.

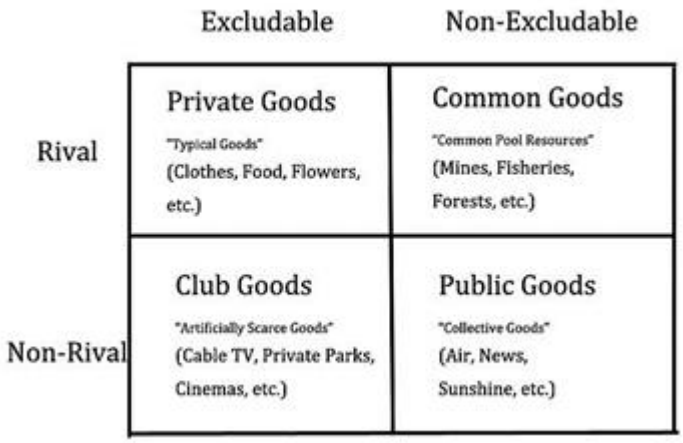


Figure 1. Public vs Private Goods Matrix. Public Domain. "Features of Goods." Wikimedia Commons. Wikimedia. 28 April 2012. Web. May 2018

Using the matrix, secure digital identity services fall into the "Public Goods" quadrant. Almost all public goods are considered to be non-rivalrous and non-excludable goods. Non-rivalry denotes any product or service that does not reduce in availability as people consume it. Non-excludability refers to any product or service that is impossible to provide without it being available for many people to enjoy. Therefore, a public good must be available for everyone and not be limited in quantity. However, not all digital identities are equal and, depending on the level of assurance, may or may not be deemed sufficient to allow access to a particular service. For example, being born in Canada entitles you to certain rights and access to certain services, but it is incumbent on the individual to provide evidence through a birth certificate or immigration documents. The conclusion is that Digital Identity fits the category of a quasi-public good, alongside libraries, museums and education since it is non-rivalrous and somewhat non-exclusive.

Appendix III- List of Working Group Participants

Co-Chair of Digital Identity Working Group
Jackie Stankey, Government of Alberta
Sophia Howse, Government of British Columbia

Team Leads
Roxanna Dehghan, Government of British Columbia
Sharon McLean, Government of British Columbia

Federal
Caroline Cossette, Service Canada
Elizabeth Dussault, Service Canada
Adam Hayes, Immigration, Refugees and Citizenship Canada
Allison Littlefortin, Immigration, Refugees and Citizenship Canada
Michelle Richardson, Immigration, Refugees and Citizenship Canada
Teresa Reeve, Immigration, Refugees and Citizenship Canada
Marie-Christine Rousseau, Immigration, Refugees and Citizenship Canada
Lieu Yen, Immigration, Refugees and Citizenship Canada
Tim Bouma, Treasury Board of Canada Secretariat
Ken McMillan, Treasury Board of Canada Secretariat

Provincial
Chantal Ritcey (also Lead of Communications), Government of Alberta
Scott Duff, Government of Nova Scotia
Roxana Azad, Government of Nova Scotia
Laura Offman, Government of Nova Scotia
Liane MacFarlane, Government of New Brunswick

Municipal
Norm Synnott, Municipality of Windsor