

Joint Councils of Canada
Digital Identity Priority Stream

Digital Identity
Governance
Framework

Version 1.0

Recommendations from in-person workshop
23-24 July 2019

Table of Contents

1. Background	3
2. Key Terms.....	3
3. Governance Framework Design Principles.....	5
4. Summary of Major Themes.....	6
5. Governance Framework for Digital Identities in Canada	6
6. Accountability Recommendations	10
7. Mapping to Existing Governance Structures.....	13
8. Other Recommendations	14
9. Next Steps	15
 Appendix I – Workshop Invitees and Attendees	 16
Appendix II – Survey Distribution, Respondents and Content	18

To the members of the Canadian Joint Councils

As the co-leads for the Digital Identity (DI) priority stream, we are pleased to present the following recommendations for a governance framework for digital identity in Canada.

Following Joint Councils' direction in February 2019, we issued a survey to both public and private sector organizations to gather input on the critical questions of:

- “**what**” should be governed;
- “**how**” it should be governed; and
- “**who**” should be given accountability for governing.

We received twenty-six detailed responses and found three major themes of **what** should be governed:

- **Setting the rules for onboarding:** establishing clear criteria for participation in the Pan-Canadian digital identity landscape;
- **Recognizing trusted entities:** the processes by which entities demonstrate compliance with the established rules and are, therefore, considered trusted;
- **Governing the operational processes:** oversight of the day-to-day services of creating, using and managing digital identities.

Accountabilities Recommendations

The three themes framed the discussions at the 1½ day in-person workshop in July and anchor the accountability recommendations:

Setting the rules:

- Public sector: enabling legislation that may be required for jurisdictions to issue DIs;
- Joint public and private sector forum: setting conformance criteria through the Pan-Canadian Trust Framework.

Recognizing trusted entities:

This is a highly complex area and accountabilities may be different depending on, for example, if the entities are public or

private sector. It was not possible to review each of these use cases and it is recommended:

- Joint public and private sector forum: define requirements for recognizing trusted entities.

Governing operational processes:

- Each trusted entity (public or private sector): develop internal policies, design their program and make technology and architectural decisions.

Structure Recommendations

Joint Public-Private Forum: refreshed DIACC

- DIACC to become the joint public and private sector forum, with the proviso that there are no financial barriers to the participation of all the jurisdictions.

Public Sector DI Lead: A new focus

- Each jurisdiction should designate a DI lead with the authority to represent the jurisdiction on digital identity and focus on how the jurisdiction will become an issuer of DI.

Public Sector Forum: A reframed IMSC

- IMSC should be re-framed to align with the role of the joint forum, focusing on jurisdictional readiness to issue Dis.

We offer sincere thanks to everyone who responded to the survey or participated in the workshop. We believe the recommendations will help accelerate progress towards unlocking Canada's growing digital economy for citizens.

Sophia Howse

Executive Director, Provincial Identity Management Program, Province of BC

Alexandre Bourque

Director of Engagement and Oversight, Cyber Security, Treasury Board of Canada Secretariat, Government of Canada

Digital Identity Governance Framework

Recommendations from In-Person Workshop 23/24th July 2019

1. BACKGROUND

Digital Identity (DI) remains a high priority for the Joint Councils (JCs) of Canada. In February 2019, the JCs recognized that significant progress has been made on the Digital Identity priority work-stream and acknowledged that ultimate success will require a strong governance framework for digital identity in Canada. JCs directed the co-leads of the Digital Identity priority work-stream to host an in-person workshop, with representatives of all key stakeholders, to develop recommendations for a governance framework for digital identities in Canada. (See Appendix I for list of invitees and attendees.)

Three key questions that the governance framework must answer were identified:

- **WHAT** are the areas that need to be governed?
- **HOW** should they be governed?
- **WHO** should be accountable and responsible?

Recognizing that many individuals and organizations had important input, a survey was broadly distributed to both public and private sector organizations ahead of the in-person workshop. Twenty six responses were received from federal and provincial governments, private sector and not-for-profit organizations. (See Appendix II for distribution, respondents and copy of the Survey).

The responses were used to frame the discussion at the workshop and focused on 3 major themes of what should to be governed in the Canadian digital identity landscape:

- the rules that organizations must comply with to onboard to the Pan-Canadian Digital Identity sector;
- the recognition of trusted entities (identity issuer, network provider and service provider);
- the operational processes of issuing, using and managing digital identities.

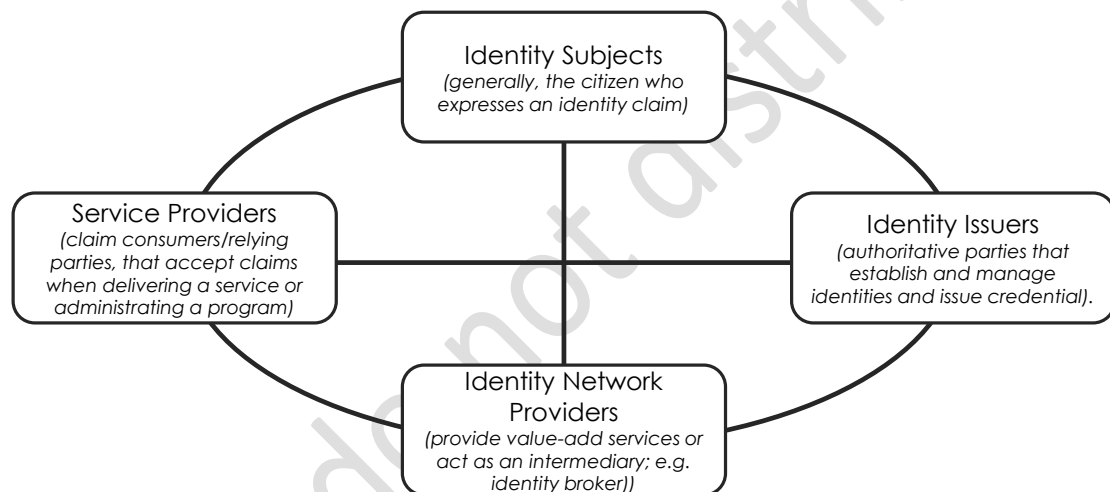
The in-person workshop took place 23-24th July 2019 in Toronto. It was led by an independent external facilitator and supported by the Digital Identity priority work-streams co-leads. As directed by JCs, invitations were sent to Federal government (Treasury Board Canada; Employment and Social Development Canada; Immigration, Refugees and Citizenship Canada), all Provinces, 2 Territories, Municipalities, Corporate Registries, Co-chair of JCs' Business working group, Co-chairs of Identity Management Sub-Committee, Drivers' Licences, Vital Statistics, Institute for Citizen Centred Service, Digital ID and Authentication Council of Canada, and representatives from Banking, Financial and Technology private sector organizations.

There was a high degree of openness and participation throughout the workshop and consensus was achieved on a series of recommendations, captured in this report, which will be presented to JCs at the September 2019 meeting.

2. KEY TERMS

The following terms are used to describe the key actors:

- **Identity Subjects:** generally, the citizen who expresses an identity claim, either as an individual or as a business.
- **Identity Issuers:** authoritative parties (public or private sector) that include organizations or individuals that establish and manage identities and issue credentials. Also known as claims providers, they may issue claims to Identity Subjects (the owner of the claim or their delegate) and/or relying parties depending on the ecosystem they are participating in.
- **Service Providers:** public or private sector organizations that consume claims as part of delivering a service or administering a program. (AKA as claims consumers or relying parties).
- **Identity Network Providers:** organizations that provide supporting and value-add services or act as an intermediary; e.g. identity broker.



- **“Entities”** is another term used in this document. It is used as collective term for Service Providers, Identity Issuers and Identity Network Providers. An entity becomes a **“Trusted Entity”** when it has been recognized as confirming to the standards and criteria that govern the digital identity ecosystem.

3. GOVERNANCE FRAMEWORK DESIGN PRINCIPLES

The surveys identified a number of possible principles for the design of the governance framework. The workshop also considered possible principles from other sources such as the JCs' Declaration on Digital Identities, the Public Policy Paper, the public sector profile of the PCTF and DIACC.

The key design principles that were surfaced at the workshop are described below. These were explicitly developed from the perspective how the governance framework should be designed. The workshop recognized there were other valid principles that co-exist and apply to other aspects of digital identities such as developing standards that are technology-agnostic and designing services that provide convenient and secure access for citizens.

The workshop also acknowledged that accountability for the issuance of foundational identities (birth and arrival in country records) must continue to lie with the Vital Statistics Organizations and Immigration, Refugee and Citizenship Canada.

The governance framework should

- *be sufficient to safeguard the integrity of digital identities.* The governance framework must ensure identity data is protected appropriately, but not be overly restrictive. The framework must be flexible enough to allow innovation that will enable Canada to be a leader. Rather than a heavy emphasis on rules, the framework should seek to maximize collaboration.
- *be a coalition of the willing and be authoritative to those who adopt.* The governance framework should recognize the importance of collaboration across all the digital identity sector, where there is a recognition of shared accountabilities, and work to set appropriate and fair structures and processes. Organizations choosing to be part of the DI sector must play within the agreed boundaries.
- *leverage existing frameworks to enable true interoperability.* The governance framework should seek to leverage existing bodies, frameworks and standards and minimize the possible duplication of effort. By leveraging existing standards and criteria the goal of interoperability will be more likely to be achieved and sustained.
- *ensure that individuals are in control of their own data to the limits of the law.* The governance framework should respect the critical components of notice and consent and ensure that citizens and businesses are in control of their own data and how it is shared and used.
- *allow service providers to determine who they will trust.* The governance framework should promote a common language and understanding of different levels of assurance. However, it should also respect that services providers will be responsible for determining what level of assurance they require for their service and which entities to accept data from.
- *be capable of evolving and scaling.* The governance framework established today must also be viable in tomorrow's digital landscape, which is poised to grow significantly.
- *use clear incentives to drive user behaviour.* The governance framework should acknowledge the interests of the different parties and put incentives in place to accelerate wide-spread adoption and acceptance.

4. SUMMARY OF MAJOR THEMES

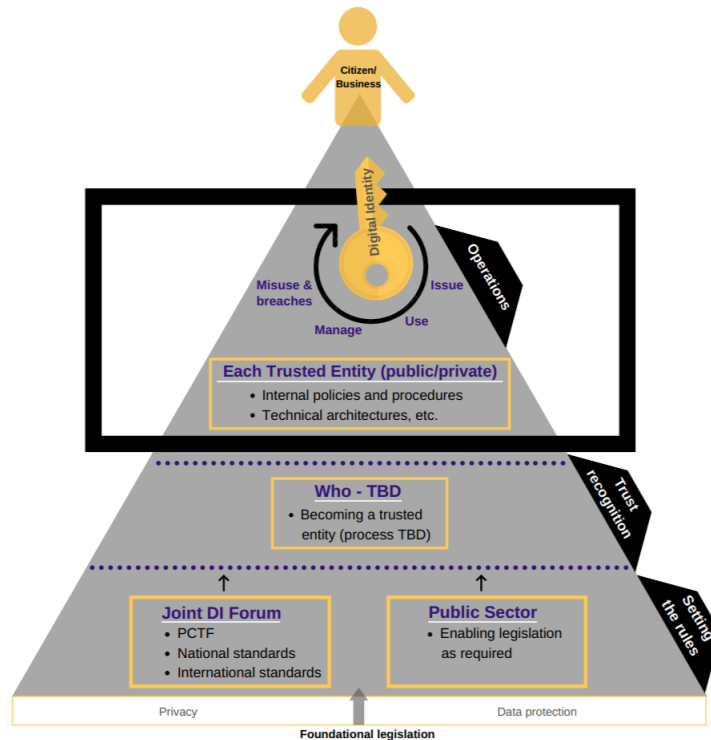
The survey responses identified 3 major themes, with 8 associated sub-themes, of **what** should be governed (see diagram below). These were used to frame the discussions at the workshop, and proved to be a useful partitioning. The three themes are used to anchor the recommendations in this document.

1. Setting the rules for onboarding	
Overarching standards & conformance criteria	core standards and criteria for Canadian digital identities
Privacy, notice & consent	authority to collect, record keeping, sharing data
Data management & protection	collecting, compiling, aggregating, storage & retention
2. Recognizing trusted entities	
Being an issuer, network provider or service provider	how organizations are recognized as trusted entities
3. Governing the operational processes	
Creating a digital identity	issuance, enrollment and ensuring equal access for all
Using a digital identity	authentication, authorization, attribute exchange, propagation
Managing digital identities	managing the digital identity lifecycle, complaints & revocation
Misuse & breaches	notification, remediation and penalties

5. GOVERNANCE FRAMEWORK FOR DIGITAL IDENTITIES IN CANADA

The governance framework shown below is based on the workshop discussions of the three major themes: “setting the rules”; “recognizing trusted entities”; and “the operational processes”. Proposals from the surveys were used to seed these discussions and the workshop considered how best each could be governed and where accountability and responsibilities should lie.

In the diagram below, these three themes are shown as separate tiers and illustrate the scope of **WHAT** should be governed. Within each tier the **WHO** and the **HOW** are shown within the yellow-edged-boxes.



- Existing legislation, such as Privacy and Data Protection, set the stage for digital identities. However, they lie outside the direct scope of the DI governance framework. No changes to accountabilities are proposed, but the legislation is reflected in the governance framework as a foundational part of the DI landscape.
- Public sector should be accountable and responsible for identifying and creating any enabling legislation that is required.
- A joint public-private sector DI forum should be accountable and responsible for establishing and maintaining the criteria for becoming a trusted entity in the Pan-Canadian digital identity ecosystem and work with accredited bodies to establish digital identity standards for Canada.
- The process of becoming a trusted entity should be determined by the joint public-private forum. Specifics of the process and responsibilities are to be developed and may include a form of self-attestation or a more formal accreditation process.
- Within the legal framework, trusted entities should be accountable and responsible for the day-to-day operations of issuing, using and managing digital identities. In exceptional circumstances, such as complaints, mis-use and breaches a joint public-private forum will have specific responsibilities.

Theme 1: Setting the “Rules”

The first major theme focused on setting the overarching rules for DIs in Canada. The surveys and the workshop recognized the importance of establishing clear criteria for participation in the Pan-Canadian digital identity landscape. Legislative requirements, policies, standards and conformance criteria were agreed to be part of this “strong front door”.

Pan-Canadian Trust Framework (PCTF)

The Pan-Canadian Trust Framework (PCTF) was identified as a key governance mechanism. The workshop recommended two new additions to the PCTF:

- guidance on transaction types and what attributes can be requested;
- levels of assurance definitions.

The workshop also identified the need for national standards. Specifically discussed was a trust scale with supporting definitions, schema, authorities, roles and accountabilities. This would be used to assess each entity and generate a clear and well understood level of identity trust that could be shared across the digital identity sector. Longer-term, the workshop considered that the PCTF may evolve to include not just conformance criteria, but also these stronger, explicit standards, including a standardized approach to defining levels of assurance across jurisdictional lines. However, in the short-term, the recommendation is to develop national standards that exist in parallel, but outside of, the PCTF.

Foundational Legislation: Privacy and Data Protection

Two critical areas of legislative requirements were identified: privacy and data protection (including mis-use and breaches). In both these areas, it was noted that existing legislation sets important parameters that must be complied with by all actors in the digital identity sector. No changes to existing accountabilities are anticipated, however, the workshop saw two specific roles for a joint public-private digital identity forum:

- assessing and monitoring legislative barriers and making recommendations for change to the existing governance bodies for privacy and data protection;
- providing interpretation of legislation and central policies with respect to the requirements for digital identities.

Key Assumptions

- Organizations wishing to conduct business in the EU will be accountable for their compliance with GDPR.
- No GDPR-like regulations for Canada anticipated at this time.

Theme 2: Recognizing Trusted Entities

Theme 2, “Recognizing Trusted Entities” focused on how entities are recognized as being trusted by other entities within the Pan-Canadian digital identity ecosystem. Options considered included self-attestation to meeting the published national standards and the criteria in the PCTF, or a more formal assessment and accreditation process that generates a trustmark. It was recognized that this is a highly complex area with multiple use cases: public sector versus private

sector identity issuers; foundational digital identities versus derived digital identities; self-sovereignty versus service provider to network provider versus service provider to identity issuer.

It was not possible within the time constraints of the workshop to review each of these use cases and develop recommendations. However, the concept of a trustmark issued after a formal accreditation process was considered most useful for private sector entities. Further consideration is required:

- Joint public-private DI forum to identify and assess the different use cases and define requirements for recognizing trusted entities.

Key Assumptions

- Service Providers determine who they will trust.

Theme 3: Governing the Operational Processes

This final theme considered the governance required for the day-to-day operations associated with issuing, using and managing digital identities. Within the context of the above noted “rules” and “recognition of trusted entities”, and aligned with key principles of applying governance only where it is required and minimizing rules, it was recommended that additional governance was only required for the exception processes of complaints and revocations, and misuse and breaches.

Recognizing how dynamic digital identities are, the workshop also recommended that the joint public-private DI forum be responsible for:

- sharing test/pilot results and emerging best practices;
- overall change management, taking a central role in ensuring all changes are communicated to all the key stakeholder groups.

Key Assumptions

- The legislation, policies, standards and conformance criteria are in place and that the entities operating in the landscape are known and trusted.
- The internal processes, policies, technology and architecture decisions of the trusted entities should be considered a “black box” by the governance framework.
- Identity issuers will be accountable for first response to complaints.
- Identity issuers will be accountable for revoking digital identities and claims.
- There are existing liability models that apply to the private sector.
- Existing legislation covers liabilities and specifies penalties for private sector.
- Police Services will continue to lead investigations of suspected criminal activity.

6. ACCOUNTABILITY RECOMMENDATIONS

The workshop explored all 8 sub-themes and identified specific accountability and responsibility recommendations. These are shown in the tables below.

Theme 1: Setting the “Rules”

HOW	Digital Identity Sector WHO
Overarching Standards and Conformance Criteria	
Pan-Canadian Trust Framework	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • develop, extend and maintain Pan-Canadian Trust Framework with the goal of ensuring inter-operability
National standards	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • define a “Trust Scale”, with schema and rules for assessing where each entity lies • define critical infrastructure standards to ensure cyber security, including liaising with Canadian Centre for Cyber Security and accredited standards setting body
International standards	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • ensure that international standards are leveraged in Canadian frameworks and that Canada appropriately influences emerging international standards
Privacy, Notice and Consent	
Legislation (legislation governed through existing structures)	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • assess and monitor for legislative barriers and make recommendations for change • provide interpretation of legislation and central policies • define “issuer” and determine if this must be included in legislation
Policies	<ul style="list-style-type: none"> • All trusted entities in DI sector: <ul style="list-style-type: none"> • develop supporting internal policies and privacy programs
Education and outreach	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • educate identity subjects (citizens) of best practices and risks
Data Management and Protection	
Legislation (legislation governed through existing structures)	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • assess and monitor for legislative barriers and make recommendations for change • provide interpretation of legislation and central policies
Industry-led initiatives	<ul style="list-style-type: none"> • All trusted entities in DI sector: <ul style="list-style-type: none"> • trigger specific initiatives to explore emerging trends or perceived issues
Education and outreach	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • educate identity subjects (citizens) of best practices and risks

Theme 2: Recognizing Trusted Entities

HOW	Digital Identity Sector WHO
Being a Digital Identity Issuer, Network Provider or Service Provider	
Further discussion required	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • maintain central registry of trusted entities, their roles and profiles, compensating controls etc.

Theme 3: Governing the Operational Processes

HOW	Digital Identity Sector WHO
Creating a Digital Identity	
<p><i>No additional governance required beyond the rules, criteria and recognition process established under themes 1 and 2. Once an entity is trusted, the operational process of creating a digital identity will be managed by the specific entity.</i></p> <p><i>(Noted that existing accountability for issuing foundational identities must continue to lie with Vital Statistics and Immigration, Refugee and Citizenship Canada)</i></p>	
Using a Digital Identity	
<p><i>No additional governance required beyond the rules, criteria and recognition process established under themes 1 and 2.</i></p>	
Managing Digital Identities	
<p><i>Assumed that each entity will be accountable for providing first response to complaints.</i></p> <p><i>Assumed that each entity will be accountable for managing the revocation of DIs and claims.</i></p>	
Collaborative review	<ul style="list-style-type: none"> • Joint public-private DI forum: <ul style="list-style-type: none"> • review escalated complaints and ensure a smooth experience for identity subjects (note, should include VSO and Registrars)
Transparency reports	<ul style="list-style-type: none"> • Organization receiving and responding to claims: <ul style="list-style-type: none"> • Prepare transparency reports
Misuse and Breaches	
Policy	<ul style="list-style-type: none"> • All trusted entities: <ul style="list-style-type: none"> • set internal policies that are aligned with legislation • Joint public-private DI forum: <ul style="list-style-type: none"> • establish network to send flash notifications across the ecosystem
Assurance reviews and investigations	<ul style="list-style-type: none"> • All trusted entities: <ul style="list-style-type: none"> • log and report suspected breaches, conduct assessments and response analysis • Network providers: <ul style="list-style-type: none"> • outreach and education on opportunities to improve on privacy and security • Notes: <ul style="list-style-type: none"> • <i>3rd Party: may be brought in to conduct assurance reviews and investigation, at discretion of the identity issuer, network provider or service provider.</i> • <i>Assumed that trusted entities will be required to demonstrate compliance with documented standards as part of the recognition process,</i>

Summary of Recommended Accountabilities and Responsibilities

The following table summarizes the recommended split of accountabilities and responsibilities between trusted entities, the joint public-private DI forum and the public sector.

Trusted Entities in the DI Sector (public and private)	Joint DI Forum (public and private)	Public Sector
<ul style="list-style-type: none"> Internal policies, privacy programs, technology and architectural decisions Industry-led initiatives, as required Transparency reports Log and report suspected breaches, conduct assessments and response analysis Network providers to explore opportunities to improve data protection and security 	<ul style="list-style-type: none"> Assess and monitor for legislative barriers Legislation and policy interpretation Pan-Canadian Trust Framework Central registry of trusted entities Critical infrastructure standards to ensure cyber security and interoperability International standards liaison Managing a network to send flash notifications on misuse and breaches Review escalated complaints Share test/pilot results and emerging best practices Overall change management, ensuring changes are communicated to all the key stakeholders <p>Preparatory Tasks</p> <ul style="list-style-type: none"> Definition of a “Trust Scale”, with schema and rules for assessing where each actor lies Definition of “issuer” and determination if this must be included in legislation Define requirements for recognizing trusted entities 	<ul style="list-style-type: none"> Assessing if enabling legislation is required to give jurisdictions the authority to issue digital identities and triggering follow-up, if required Liaising with existing legislation and policy governance structures to ensure barriers to DI are communicated and discussed VSOs and IRCC continue to issue foundational identities

7. MAPPING TO EXISTING GOVERNANCE STRUCTURES

In examining the existing governance structures, two bodies were identified as being affected by the recommended changes: DIACC and IMSC.

Joint Public-Private Forum: a refreshed DIACC

The workshop considered DIACC the best placed existing body to take on the responsibilities envisioned for the joint public-private DI forum, described in the previous section. The barriers to this being successful were noted as:

- All jurisdictions must be represented, and there should be no financial barriers to participation. It is understood that the DIACC board is currently discussing this.
- The public sector representatives must also represent Vital Statistics and Driving Licence programs within their jurisdictions. This may require new structures/communication channels to be established within each jurisdiction.

Public Sector DI Lead for each Jurisdiction: new

The workshop recognized that to ensure that progress continues to be made towards issuing digital identities in Canada, it will be important to have a designated lead within each jurisdiction. It is recommended that this single individual has the authority to represent the jurisdiction on digital identity covering, at a minimum, digital identity for clients of Health services, drivers licensing, and vital statistics. The person that is designated should be:

- undertake a policy and legislative review to understand how the jurisdiction can become an issuer of digital ID;
- able to represent the jurisdiction with the confidence of the jurisdictions' Joint Councils' members, and the Assistant Deputy Ministers and Executive Directors from Health services, drivers licensing, vital statistics and corporate registries;
- capable of addressing topics such as program delivery models, service delivery models, their enablement in legislation, policy and the logistics within the jurisdiction that would be associated with moving towards becoming an issuer of digital ID.

Public Sector Forum: a re-focused IMSC

The workshop recognized that there would be a need for a public sector only forum and saw a continuing role for IMSC. Should DIACC be able to remove the barriers noted above, its refreshed and extended mandate would result in a re-scoping and refocusing of IMSC to ensure there is appropriate representation from all jurisdictions. It is recommended that the IMSC is re-constituted to include the DI leads recommended above and that the mandate updated to align with the role of the joint public-private forum, with a focus on the challenges associated with jurisdictional readiness and ability to operate as an issuer of digital ID.

8. OTHER RECOMMENDATIONS

Legal identities

The workshop recognized the difference between legal (foundational) identities and derived identities (those that rely on the foundational identities for proof of identity) and recommended that the accountability for issuing legal identities continue to lie with Vital Statistics and IRCC.

The workshop noted that the existing paper-based foundational identities are open to mis-use (where an individual may be issued multiple identities that are then used by others). It was recognized that the closer a digital identity is to the foundational source, the less risk there is of this occurring. It is recommended that:

- VSOs and IRCC pursue issuing digital birth certificates and immigration documents and ensure that each individual only has one identity.

Assessment by Jurisdictions on Readiness to Issue

Embedded in the recommendations above is the recognition that privacy and data protection legislation varies by jurisdiction and updates to that existing legislation and/or new enabling legislation may be required to allow for the issuance of digital identities. Consistent with the recent joint councils Declaration on Digital ID, it is recommended that:

- each jurisdiction conducts an assessment of its readiness to issue digital identities, including a determination of whether the jurisdiction currently has the legislative authority to operate as an issuer pursuant to the verified persons component of the public sector profile of the Pan-Canadian Trust Framework.

ICCS Continuing Role

The workshop understood that the Institute for Citizen-Centred Service (ICCS) was created to support, advance and enable interjurisdictional efforts to improve citizens' satisfaction with public sector services. It was recognized that ICCS provides a neutral platform for information sharing and collaboration and is well suited to conduct and undertake interjurisdictional collaborative work in support of digital service integration.

As previously noted, the workshop supported leveraging DIACC to establish the required Joint Public-Private Forum. To make this a reality, DIACC has been requested to review the membership fee structure to enable barrier-free and active participation by all jurisdictions. It will be important to monitor progress and work together to make the required changes. As ICCS is the legal manifestation of the Councils, it is recommended that:

- ICCS is mandated to lead discussions with DIACC and negotiate changes to the cost structure on behalf of the Councils.

JCs Declaration on Digital Identities

The workshop felt that significant progress had been made and recommended that the JCs Declaration be reviewed and updated to reflect this significant step forward.

Continuing In-Person Workshops at this level

Participants overwhelmingly reported that the workshop had been successful in generating very open discussion on high profile issues. The recommendation is to continue this:

- Joint in-person workshop to be convened every quarter.

9. NEXT STEPS

With approval of the recommendations in this document, the next steps will be to pursue the implementation of the above-noted recommendations by:

Immediate

- Direct ICCS to negotiate with DIACC to establish a membership fee structure that is a barrier-free joint public-private forum
- Encourage each jurisdiction to assign a designated DI Lead
- Request VSO and IRCC to commence work towards issuing digital foundational identities
- Direct DI priority co-leads to organize an in-person workshop to build implementation plan and support assessments, with goal of reporting back at February JCs in-person meeting:
 - Establish a tiger team responsible for developing and managing a detailed plan;
 - Develop an engagement and communications strategy;
 - Meet with peers and chair of similarly configured pan-Canadian governance bodies such as the Canadian Council of Motor Transport Authorities (CCMTA) and Open Banking consortium;
 - Organize follow-up multi-stakeholder workshops to establish majority consensus on priorities and governance model.

When DI Leads identified

- Encourage each jurisdiction to conduct readiness assessments

When DI Leads and Re-framed DIACC in place

- Direct IMSC Co-chairs and DI priority co-leads to re-fresh IMSC ToR

Appendix I – Workshop Invitees and Attendees

	Name	Sector	Role	Notes
	Sophia Howse	Provincial (BC)	Digital ID work stream Co-Lead	Co-facilitating
	Alexandre Bourque	Federal (TBS – CTO/OCIO)	Digital ID work stream Co-Lead	Co-facilitating
	Marc Brouillard	Federal (TBS – CTO)	IMSC Co-Chair	DIACC Board Member
	Rob Devries	Provincial (ON)	IMSC Co-Chair	DIACC Board Member
	Colleen Boldon	Provincial (NB)		DIACC Board Member
	Igor Solesa	Provincial (ON)		
	Peter Watkins	Provincial (BC)		
	Sherry McCourt	Provincial (PEI)	Also represented Registrar	
	Arlene Williams	Provincial (NS)		
	Mark Healey	Provincial (NL)		
	Omar Subhani	Federal (IRCC)		DI for Immigration
Did not attend	Sean McLeish	Territory (YK)		
	Imraan Bashir	Federal (TBS)		Enterprise DI policy and oversight for the GC
Sub sent	Rob Frelich SUB: Janice Lobodale	Federal (Service Canada/ESDC)		DI for benefits delivery
	Pirth Singh	Federal (ISED)		DI for businesses
	Joni Brennan	DIACC President		
	Franklin Garrigues	Private Sector: TD BANK		DIACC Board Member
	Neil Butters	Private Sector: Interac		DIACC Board Member
	Andre Boyson	Private Sector: Secure Key		DIACC Board Member
	Dan Batista	ICCS Representative		
	Jack Shewchuk	Vital Stats Council of Canada Rep		From BC
Did not attend	Wynnann Rose	Drivers Licensing Rep		From ON

	Name	Sector	Role	Notes
	Sharon McLean	N/A	Lead Facilitator	
	Maria Luisa Willen	ICCS (Observer)		
	Cathy Kealey	ICCS (Observer)		
	Suezan Le Breton	Provincial (BC) (Observer)		
Regrets	Chantal Ritcey	Provincial (AB)		
Regrets	Cosanna Preston	Provincial (SK)		
Regrets	Manitoba	Provincial (MB)		
Regrets	Quebec	Provincial (QC)		
Regrets	Northwest Territories	Territorial (NWT)		

Appendix II – Survey Distribution, Respondents and Content

Distribution:

- All PSSDC and PSCIOC Members
- DIACC

Covering email asked that the survey be distributed within each organization.

Respondents:

Federal Government	
• Treasury Board Secretariat	• Immigration and Refugee Board of Canada
• Innovation, Science and Economic Development	• Public Services and Procurement Canada
• Employment and Social Development Canada	• Canada Revenue Agency
• Immigration, Refugees and Citizenship Canada	
Private Sector	
• DIACC	• Price Waterhouse Coopers
• Biometric Signature ID	• 2 keys
• Vancouver City Savings Credit Union (Vancity)	• Manulife
• Interac	
Provinces and Territories	
• Ontario * 2	• Nova Scotia
• British Columbia	• New Brunswick
• Alberta	• Northwest Territories
• Saskatchewan	• Quebec
• Newfoundland & Labrador	
Vital Statistics	
• VSO - BC	
Not for Profits	
• Canada Health Infoway	

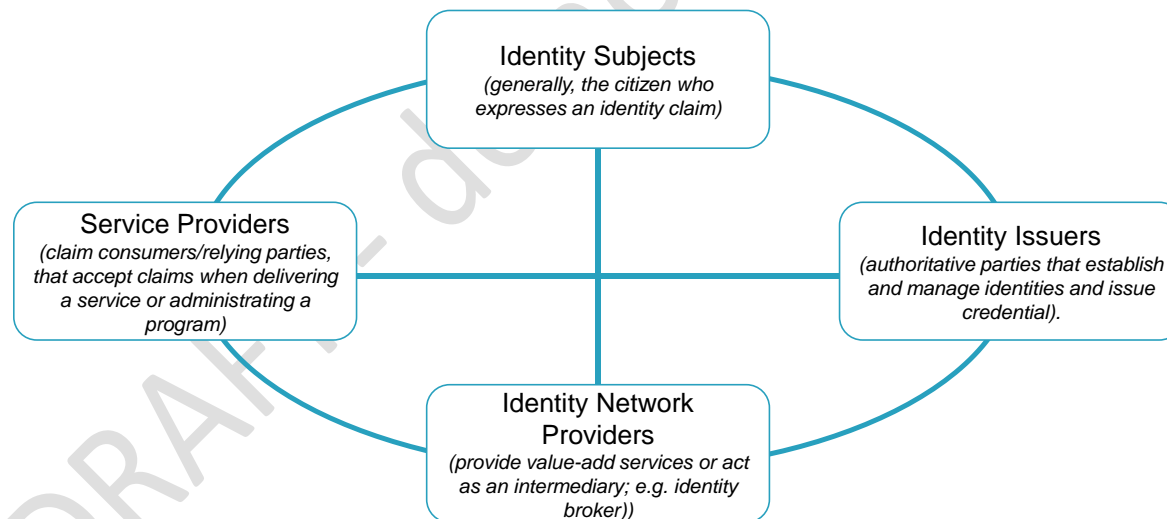
Digital Identity in Canada

Governance Survey, June 2019

Survey Introduction

The core of the survey is structured around the interactions between the four key stakeholder groups in the digital identity ecosystem:

- **Identity Subjects:** generally, the citizen who expresses an identity claim, either as an individual or as a business.
- **Identity Issuers:** authoritative parties (public or private sector) that include organizations or individuals that establish and manage identities and issue credentials. Also known as claims providers, they may issue claims to relying parties.
- **Service Providers:** public or private sector organizations that consume claims as part of delivering a service or administering a program. (AKA as claims consumers or relying parties).
- **Identity Network Providers:** organizations that provide supporting and value-add services or act as an intermediary; e.g. identity broker.



DEADLINE: Please return to Sharon.McLean@gov.bc.ca by 30 June 2019

Please contact Sharon at above email, if you have any questions

QUESTION 1:

Which stakeholder group(s) do you represent? (Identity Subject, Identity Issuer, Service Provider, Identity Network Provider)

QUESTION 2:

Please provide input on what things should be governed and your suggestions for how this could be done. It may be useful to consider the functions/services of the four stakeholder groups and the interactions between them to identify which areas need to be governed. Please comment on:

- **WHAT** are the areas that need to be governed? The areas should be at a relatively high level. For example, “Identity Issuance” – an interaction between an Identity Subject and an Identity Issuer – is an area that you may wish to consider.
- **HOW** should it be governed? (e.g., legislation, policy, PCTF, audits, assessments, certification)
- **WHO** should be accountable and responsible? (e.g., Federal provincial and/or territorial governments, private sector, independent third party, joint?) Please consider if the governance model is different depending if the organization is private or public sector. For example, if the Identity Provider is a provincial government, and the claim is issued to a different provincial government is the governance model different than if the identity provider is a bank and the service provider is another private sector organization.

(Please add additional lines, if required).

Topic or area to be governed (what?)	Governance option (how and who?)

QUESTION 3:

Are there any aspects of issuing and managing digital identities that you believe should **NOT** be governed?

QUESTION 4:

Are there any key lessons we should learn from how digital identities in Canada are governed today?

QUESTION 5:

Are there existing governance frameworks in other industries (e.g., financial or insurance) or other countries that you believe are comparable and worth learning from?

QUESTION 6:

Are there any external influences that should be considered in evaluating governance options – either now, or possible in the future?

QUESTION 7:

Do you have any other comments that you wish to share?

CONTACT DETAILS (OPTIONAL):

This is a complex subject area and during the collation of the results there may be follow-up questions on your submission. If you are comfortable, please provide your name and email address where Sharon McLean can contact you to clarify or discuss specific responses. This information will not be used to attribute comments in any published results.

Name:

Email: