Report | June 2024

Blueprint for Progress:

Strategic insights for safe, seamless and secure access to digital citizen services

Sponsored by:
Government of Yukon,
Department of Highways and Public Works

Written by:
Hadrien Seymour-Provencher
and Cosanna Preston-Idedia
of the Digital Trust Laboratory of Canada

Table of Contents

Copyright Notice & License

Written by:

Hadrien Seymour-Provencher

and Cosanna Preston-Idedia

of the **Digital Trust Laboratory of Canada (DTLab)**

Executive Summary

Many jurisdictions across Canada, from the federal government to provinces and territories to municipalities, are grappling with how to improve access to digital citizen services in a secure, privacy protecting, convenient and cost-effective manner. With over 3,500 governments in Canada, including municipal governments, there are a lot of opportunities to learn from emerging practices rather than figure it out from scratch over and over again. This report, authored by the Digital Trust Laboratory of Canada (DTLab) and sponsored by the Government of Yukon, aims to do just that by offering strategic insights into digital citizen service access management to all levels of government in Canada, their stakeholders and their execution partners.

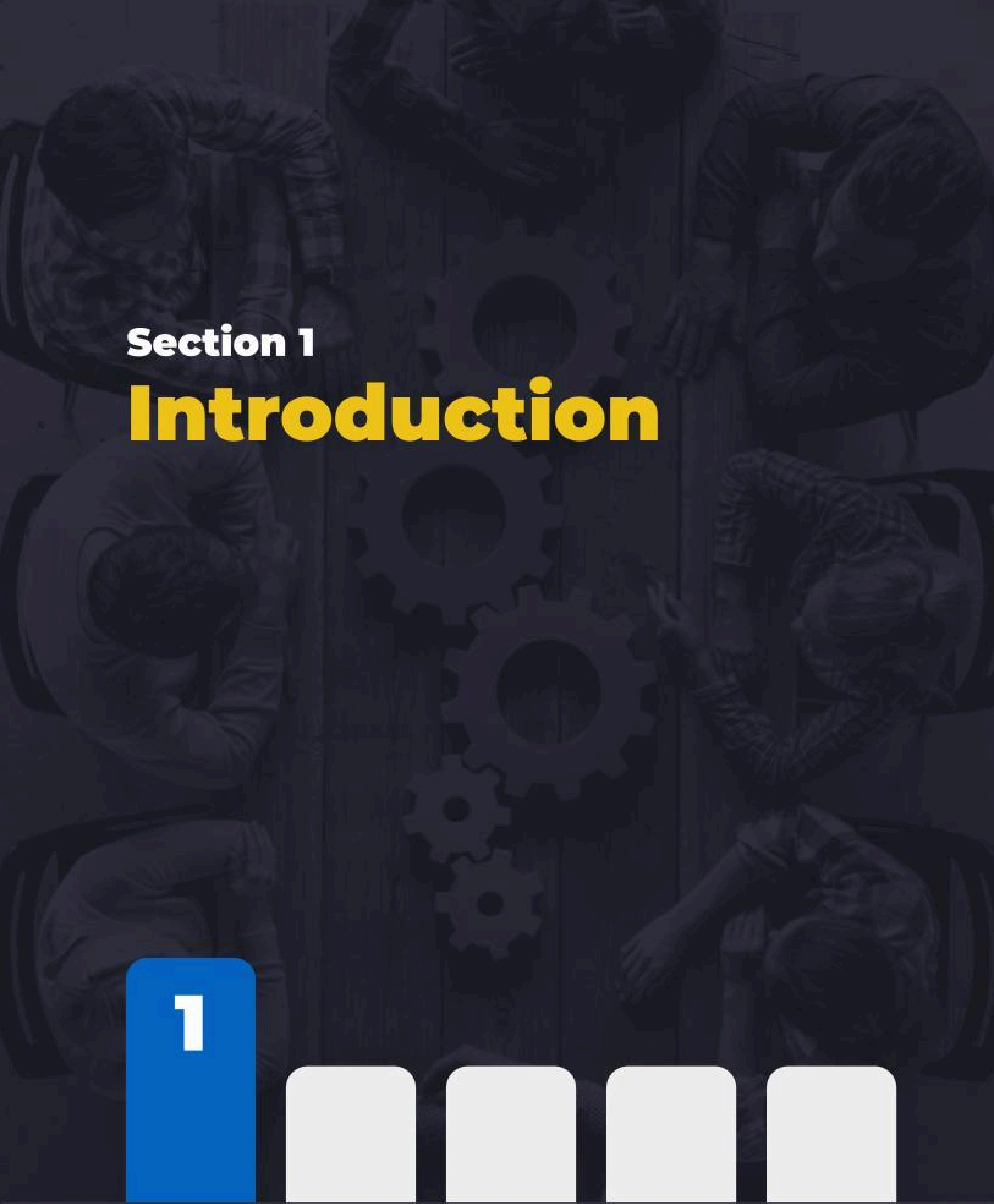
The approach to this report consisted of a jurisdictional analysis and market research scan involving secondary research and interviews with government representatives, privacy commissioners and solution providers. These interviews covered the following topics: progression from LOA1 to LOA3, data brokering, federation with federal and provincial/territorial governments, collaboration with privacy commissioners, and the adoption of digital credentials.

The report emphasizes aligning levels of assurance (LOA) for access to citizen digital services with federal standards, and prioritizing user experience by offering multiple options for authentication and identity verification. Additionally, this report highlights the importance of working effectively with privacy commissioners by engaging early and collaborating throughout the design, implementation and continuous improvement phases to ensure transparency and consent for users.

Overall recommendations include:

1. Take a program view to ensuring safe, seamless and secure access to digital citizen services
2. Develop a long-term program strategy
3. Develop a privacy framework
4. Centre the user in development and operations
5. Take a collaborative approach to procurement
6. Communicate precisely and build trust
7. Stay engaged in the community

By leveraging a collaborative and research-driven approach, DTLab has developed a blueprint that provides noteworthy perspectives and strategic guidance to support the ongoing progression of safe, seamless and secure access to digital citizen services.



Section 1

Introduction

1

Introduction

Many jurisdictions across Canada, from the federal government to provinces and territories to municipalities, are grappling with how to improve access to digital citizen services in a secure, privacy protecting, convenient and cost-effective manner. While the current focus tends to be on a centralized approach through single sign-on (SSO) platforms, decentralized models are starting to gain traction in Canada. These initiatives could pave the way for a pan-Canadian approach to offering Canadians digital credentials, not just for their government issued photo ID, like the driver's licence, but individual credentials for all their important documents such as business licences, professional certifications, employee ID, permits, etc.

With over 3,500 governments in Canada, including municipal governments, there are a lot of opportunities to learn from emerging practices rather than figure it out from scratch over and over again. This report, authored by the Digital Trust Laboratory of Canada (DTLab) and sponsored by the Government of Yukon, aims to do just that by offering strategic insights into digital citizen service access management to all levels of government in Canada, their stakeholders and their execution partners.

To accomplish this, the Digital Trust Laboratory of Canada (DTLab) was guided by the primary questions listed below.

Primary questions for investigation:

1. How does a jurisdictional government increase the level of assurance associated with access to citizen and business digital services??
2. Should single sign-on platforms for government digital service delivery support data brokering for relying parties within government, and potentially between government programs? And if so, how should this be done?
3. How can sign-on platforms used at the provincial and territorial level be enabled to access Federal Government services through federation?
4. How does a digital citizen services team best work with its privacy commissioner to ensure safe, seamless and secure access to digital citizen services?
5. How does a digital citizen services team plan for a future with digital credentials?

Advancing safe, seamless and secure digital service delivery

The value of offering services online to citizens is well established. Digital service delivery, done well, is cheaper for government, with the potential to be 20x cheaper than phone, 30x cheaper than mail, 50X cheaper than in-person service delivery.[1] Digital service delivery is also more convenient and inclusive for citizens as it provides 24/7 access to government, allowing citizens to complete their tasks anytime, and anywhere.

However, in parallel to this rise in convenient access to government services, Canada has also seen a rise in privacy breaches and identity fraud cases. Identity fraud is the number one type of fraud in Canada and cyber threats are soaring, with financial losses from fraud in Canada having more than tripled from $165 million in 2020 to $554 million in 2023.[2] Meanwhile, over a similar period 27 billion Canadian data records were exposed due to privacy breaches.[3] What this fraud prevalence and privacy breaches have demonstrated is that not all systems are created equally when it comes to security and protection of personal data.

While there are no silver bullets to preventing fraud and cyberattacks on digital citizen services access management systems, ensuring that they are operating with an appropriately high level of assurance - typically level of assurance 3 (LOA3) - is critical for safeguarding the most sensitive personal or high-value information. (See Progression from LOA1 to LOA3 for more detail on levels of assurance.)

Most importantly, LOA3 provides much greater assurance that the right person is accessing the right services. However, there are at least two remaining problems:

1. Most LOA3 authentication today is still offered through centralized systems, meaning this secure form of a citizen proving that they are who they say they are can only be used with the specific level of government offering the authentication or services they access through federation. Citizens cannot use this digital proof of their identity to complete other digital transactions such as: with a bank, or when renting or buying a home, or renting a car, or purchasing age-restricted goods. However, they can use their physical

[1] Central Digital and Data Office, Cabinet Office. 2012. "Digital Efficiency Report." Gov.UK. https://www.gov.uk/government/publications/digital-efficiency-report

[2] Canadian Anti-Fraud Centre. 2024. "Canadian Anti-Fraud Centre Bulletin". https://x.com/canantifraud/status/1747656665334165965/photo/1

[3] Statista. 2023. "Number of data records exposed due to data breaches in Canada from 1st quarter 2020 to 1st quarter 2023". https://www.statista.com/statistics/1324220/canada-number-of-leaked-records/

government issued photo ID (e.g. a driver's licence) to prove that they are who they say they are to whomever they choose.

2. LOA3-based login credentials only address one element of identity fraud - that you are who you say you are. They don't address other elements of identity fraud like fraudulently producing a permit, financial document or licence in someone else's name, which can easily be done with a document issued on a piece of paper or as a PDF.

To address these two problems, digital citizen services teams need to take a step further along their digital roadmap and implement digital credentials.

The value of digital credentials

Digital credentials represent a transformative approach to identity verification. Governments and organizations worldwide are exploring the potential of digital credentials to enhance security, while empowering individuals with greater control over their personal data.

Simply put, digital credentials can be defined by three main points:

1. **A digital credential is a digital representation of information found in the digital credential's physical counterpart -** such as a government issued photo ID, a permit, an employee badge, a financial statement, or a proof of business registration.
   - A digital credential can also represent information which is not readily available in a physical credential today, like proof of address.
   - It's more than just access TO this information. It IS the information.
2. **Digital credentials (aspire to be) compatible** (also known as interoperable). This effectively means that digital credentials are not tied to a single technology system or organization. Just like we can use any credit card with any point of sales terminal today, the goal for digital credentials is that any credential can be used with any verifying technology. The ongoing work in trust frameworks and interoperability testing amongst other initiatives continues to push the digital credential community to realize this vision.
3. **Digital credentials are cryptographically signed and verifiable.** Cryptographically signed means you can automatically tell whether any of the data contained in the credential has been tampered with. This gives the recipient the confidence to trust the data provided.

Digital credentials have a number of benefits. We highlight three of the most relevant:

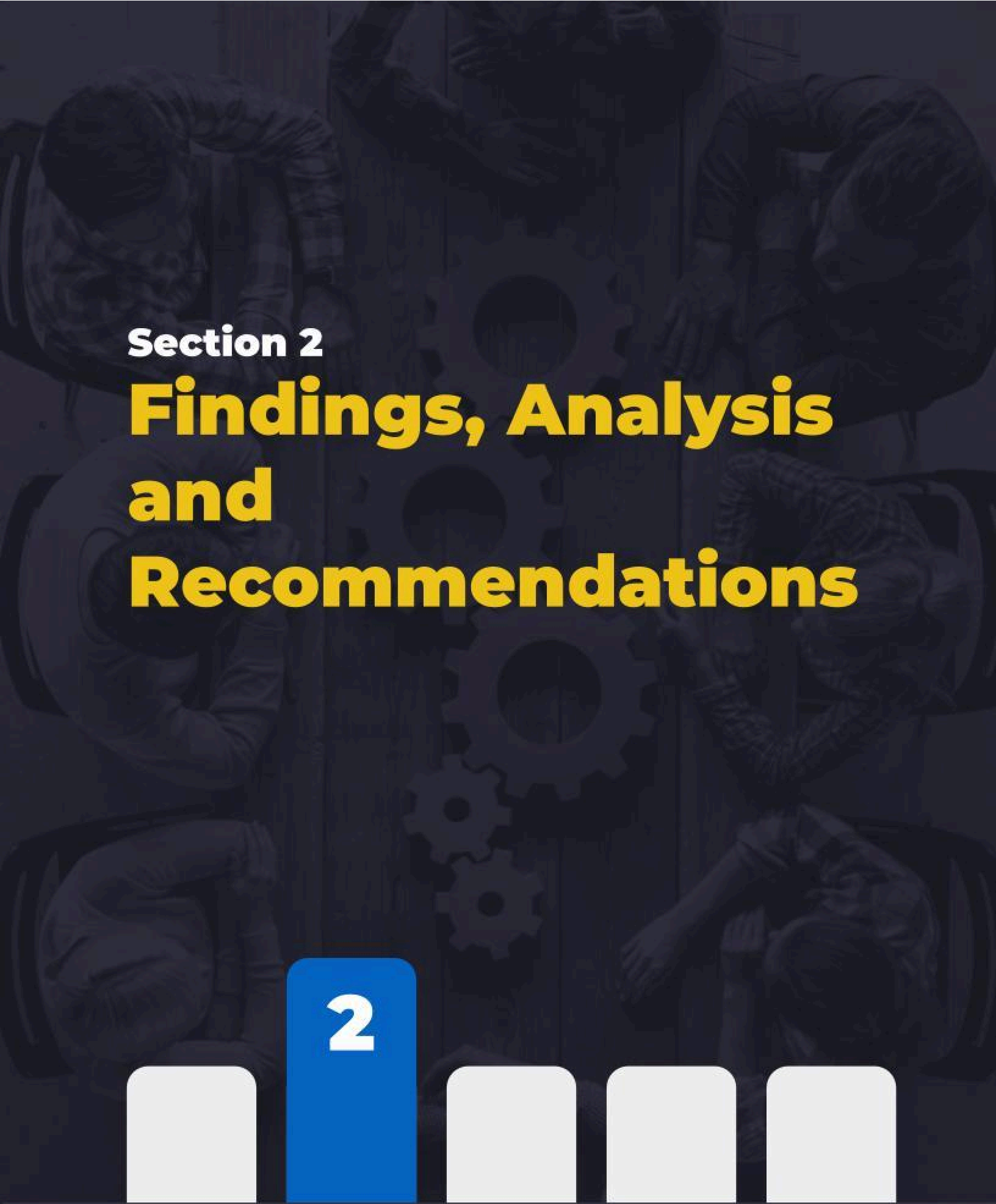
1. **It addresses the forgery risk of paper or PDF issued documents.**
   If a permit, licence or government issued photo ID is issued as a digital credential, it means that a citizen can carry this credential with them in a digital wallet, just as they would carry their important cards in a wallet or store important files in a drawer. The difference is a printed or PDF permit, as we've established, can be easily forged. Due to the cryptographic protections on a digital credential, this forgery risk is dramatically mitigated.
2. **It increases privacy and data protection.**
   Many types of digital credentials have the ability to selectively disclose information. So when a citizen chooses to share their permit licence or government issued photo ID with someone, for example sharing a fuel tax form with a financial institution to demonstrate compliance as part of a loan application, the financial institution may need to only know that the form has been filed, and not the details of the form. The individual sharing the information could choose to share just that one data attribute.
3. **Greater convenience and security**
   A digital credential that is a government-issued photo ID equivalent, can replace the username and password as the access key to government services and any other private sector service that chooses to accept this form of authentication. Think of it like swiping an employee card to access a building. This eliminates the frustrating and often cumbersome password reset workflow. The replacement of usernames and passwords with digital credentials also goes a long way to mitigate identity fraud and privacy breaches.

This is not to suggest that access management systems for digital citizen services must leapfrog immediately to digital credentials. Though that is one option, it's likely not cost effective for smaller jurisdictions.

Approach

The approach to this report involved a **jurisdictional scan and market research.** DTLab conducted interviews with individuals from the following stakeholder groups: Jurisdictions (7), Privacy Commissioners (4), Solution Providers (5), and a pan-Canadian government expert. These interviews were conducted between December 2023 and February 2024.

In addition to the research, DTLab has layered on its own analysis to develop this public report including findings and recommendations.



Section 2

Findings, Analysis and Recommendations

2

Digital citizen services access management systems and the progression from LOA1 to LOA3

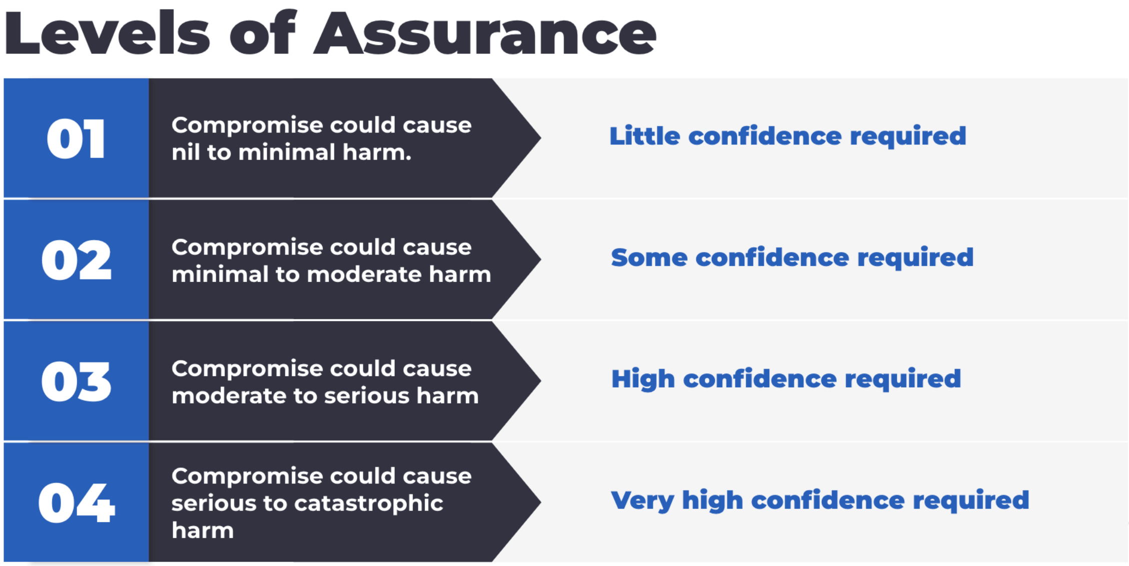
The primary question for this section was:

How does a jurisdictional government increase the level of assurance associated with access to citizen and business digital services??

Two of the key access management decisions for a digital citizen services team are determining how much rigour is needed at the time of issuing an account (or digital credential) to someone and determining how much rigour is needed at the time of authentication (when the person signs in) or verification (when the person uses their digital credential). For example, it's more comfortable to proceed with less assurance that someone is who they say they are when completing a transaction through Kijiji or Facebook Marketplace vs when someone is accessing classified information, confidential corporate information or a multi-million dollar contract.

This rigour is called a level of assurance (LOA). According to the federal government Guideline on Identity Assurance there are four levels of assurance that range from LOA1 to LOA4:

- LOA1 - little concern if the person or credential is real because access to the system or information would result in little to no harm
- LOA4 - there is need to be extremely sure that both the person and the identity or credential document presented are legitimate because access to the system or information risks catastrophic harm. Typically LOA4 is reserved for issues of national security.



Levels of Assurance

01	Compromise could cause nil to minimal harm.	Little confidence required
02	Compromise could cause minimal to moderate harm	Some confidence required
03	Compromise could cause moderate to serious harm	High confidence required
04	Compromise could cause serious to catastrophic harm	Very high confidence required

LOA3 is generally considered the highest level needed for government citizen services. The primary Government of Canada requirements for LOA1 and 3[4] are:

Requirement	Level 1	Level 3
Uniqueness	Define identity information Define context	Define identity information Define context
Evidence of Identity	No restriction on what is provided as evidence	**Two** instances of evidence of identity (At least one must be foundational evidence of identity)
Accuracy of Identity Information	Acceptance of self-assertion of identity information by an individual	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **and** Confirmation of the foundational evidence of identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source or inspection by trained examiner
Linkage of Identity Information to Individual	No requirement	At least **one** of the following: i. Knowledge-based confirmation ii. Biological or behavioural characteristic confirmation iii. Trusted referee confirmation iv. Physical possession confirmation

[4] Government of Canada. March 2016. "Guideline on Identity Assurance". https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30678&section=html#:~:text=Table%202.%20Minimum%20Requirements%20to%20Establish%20an%20Identity%20Assurance%20Level

The implementation model for achieving LOA3 is evolving and varies across digital citizen services programs. It includes both asynchronous and synchronous options and ranges from in-person, to teleconference-based validation, to experimentation with fully automated remote validation via facial verification.

Jurisdictional and market findings

Jurisdictions

General approach to identity verification and onboarding

Currently, there isn't a uniform method for managing identity verification across jurisdictional governments in Canada, and also often not within a single government either. It is not uncommon for each department within a government to interpret and implement authentication procedures within the context of its specific service. This fractured approach has led to challenges such as repetitive verification processes resulting in a fragmented user experience.

While security measures are essential, it's equally important to ensure that authentication processes are seamless and user-friendly to prevent user frustration and abandonment. Some provinces and territories provide single sign-on (SSO) platforms, which enable users to securely authenticate and log into a centrally managed account to access downstream integrated government services. Platform functionalities can include account creation, authentication, authorization, revocation, global logout, profile management, notification management, etc.

Some programs offer two levels: a “basic” account at LOA1 (email, first and last name) and a “verified” account at LOA2 or LOA3, with a specific emphasis on the latter due to its relevance in scenarios involving financial transactions or the exchange of sensitive information such as medical files.

For single sign-on platforms that start at LOA1 (sometimes with additional steps that could be referred to as LOA1.5) the onboarding process typically involves self-declared name and password or a verification against another source, such as online banking credentials. Downstream services may require additional information or verification, such as walking into a service point to register a first vehicle. LOA1 onboarding processes typically do not manage duplicate accounts. In these cases, a client can create as many accounts as they wish. They may want to have separate accounts for different services and can do so, allowing for flexibility. Typically, the only requirement is that each account must have a unique email address. Regarding duplicate applications or access to services, uniqueness is determined through other mechanisms, and the digital citizen services team can work with the ministry or department on their service specific requirements. Either ministries/departments can handle duplications in their downstream service, or onboarding requirements are configured to ensure a one-to-one linking of account records.

If the single sign-on platform's base LOA3, the norm is still verification by an agent at a service point. Individuals present themselves along with acceptable forms of identification for in-person verification, which may involve a query to a jurisdictional database, such as a motor vehicles registry, before being granted an LOA3 account. There are typically limitations in terms of verifying out-of-province/territory individuals that don't have ID from the province/territory. Duplicates are avoided due to the uniqueness requirements in registration.

Trust frameworks in the government context

These more elevated LOA programs also tend to focus on aligning with the Pan-Canadian Trust Framework Public Sector Profile (PCTF-PSP)[5], a set of guidelines designed to facilitate secure and trustworthy digital interactions within the Canadian public sector.

Government Spotlight

BC Services Card - a Canadian LOA3 example

To obtain government-issued BC Services Card, an LOA3 verified physical card, a resident's identity must be verified at a physical service desk, or by a government agent in rural areas. Identity is verified by presenting two pieces of identification. This typically includes a driver's licence, which can be cross-referenced to ensure uniqueness. The BC Services Card replaced the provincial health care card, and can also be combined with the BC driver's licence.

The BC Services Card can be used to create and access a BC Services Card Account, which is the BC government's primary single sign-on platform. Account setup is achieved using a mobile app or a username and password. This process requires verifying the individual's identity again, using their BC Services Card. Once verified, they can access their online account by registering an email address, and setting up a username and password. This results in an LOA3 account for online service access.

[5] Public Sector Profile of the Pan-Canadian Trust Framework | Cadre de Confiance pancanadien. https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_4

Roadmaps and visions can include an objective to attain LOA3, aligning with the guidelines outlined in the PCTF-PSP. However, to reach this level additional steps would be required, particularly in terms of collecting and validating foundational ID such as a person's birth certificate. The challenge is, birth certificates present their own security challenges, and provinces and territories can only verify birth certificates for individuals born in their jurisdiction, posing a challenge in achieving LOA3. To address this limitation and increase the level of confidence in identity verification processes, governments are exploring strategies to request additional information that can be verified online, remotely, or asymmetrically. This approach aims to enhance authentication procedures and move towards a higher LOA within the constraints posed by current verification methods. Accordingly, very few jurisdictional governments have been able to implement LOA3 to date, and it remains challenging.

Privacy Commissioners

Privacy commissioners advocate for a privacy-centric approach to access management for citizen digital services, stressing the need to strike a balance between security and authentication requirements, while safeguarding individuals' privacy rights. A higher LOA may enhance security and reliability in identity verification, but also poses challenges related to the collection and management of personal information. This applies both to the increased collection of personal data and in terms of understandability and transparency as it relates to consent.

To address privacy concerns associated with higher LOAs, a consistent message from privacy commissioners was that jurisdictions should involve their privacy commissioner early in the process and conduct thorough privacy impact assessments (PIAs) throughout the project (as opposed to one only at the end). This helps identify and mitigate potential risks linked to the collection, use, retention, and disclosure of personal information. Privacy commissioners recommend applying principles of consent and user control in a manner that is clear and user friendly. Collecting only the necessary amount of personal information for the intended, authorized and specified purposes allows jurisdictions to fulfill their obligations and adhere to relevant privacy laws and regulations, both federally and provincially/territorially.

Biometrics and emerging technologies

Concerns about data breaches, especially with the introduction of artificial intelligence (AI) and biometric technologies, highlight the necessity of stringent security measures and continuous evaluation of SSO platforms. However, how precisely to achieve this remains debated amongst privacy commissioners across the country, particularly when it comes to the use of biometrics. One privacy commissioner stated that “any time you have someone’s biometrics floating out somewhere in the cloud or elsewhere than your phone, that’s a problem because you can’t change your biometrics like you can a password, and with AI [rudimentary uses of some biometrics] could be faked.”[6]

On the other hand, another had a more positive outlook on the matter. Seeing the trend as inevitable, they stated that “there are risks and it’s a bit of a slippery slope. I think it’s inevitable that we use these technologies and the more data points we use the more reliable the verification becomes.”[7] In sum, biometric technology is a strong way to authenticate, but the reward must match the justification.

Solution providers

How to approach attaining LOA3

When it comes to attaining higher LOAs, solution providers offered thoughts on target levels, cross border considerations and the importance of both good technology and business processes. Some solution providers suggested that jurisdictions can skip LOA2 and focus directly on achieving LOA3 to gain the confidence that they’re talking to the right person. Solution providers also pointed out that LOA (Level of Assurance - Canadian) and IAL (Identity Assurance Level - American) standards are relatively similar across the board and are ultimately about determining the necessary level of confidence in verifying a person's identity. Accordingly, starting with the Canadian LOA guidance sets jurisdictions up for success to consider cross border uses down the road if desired. Lastly, solution providers stressed that technology itself is not the primary barrier to achieving higher confidence in online transactions. While advanced technology solutions can facilitate the implementation of LOA frameworks, the more difficult challenges emerge in adjusting business processes and aligning with established regulatory requirements.

In-person versus remote verification

Solution providers also weighed in on in-person vs remote verification. They recognized that in-person verification remains crucial for certain transactions and should be integrated into identity and access management solutions where necessary. But, they also cautioned that this can be time-consuming and poses

[6] A quote from the privacy commissioner interviews undertaken by DTLab in January and February of 2024.
[7] A quote from the privacy commissioner interviews undertaken by DTLab in January and February of 2024.

challenges in rural or remote areas where access to government services may be limited. Remote verification allows individuals to verify their identity online and can offer greater convenience and accessibility. Remote verification can leverage technologies such as biometric authentication, document scanning, and electronic signatures to verify identity. However, both come with trade-offs. While remote verification offers convenience, it may raise concerns about security and fraud prevention.

Analysis

Each of the provincial and territorial jurisdictions interviewed has its own SSO platform with varying offerings of LOAs and authentication methods. Different approaches exist for identity verification across jurisdictions, with ranges in terms of digital enrollment and authentication. While the jurisdictions' citizen digital services teams demonstrate aspirations to provide LOA3 verification for connected government services, challenges remain in fully complying with the federal government's Directive on Identity Management, particularly as it relates to the use of foundational identity.

Alternative verification methods

The Federal Standard on Identity and Credential Assurance requirements for LOA3 include requirements such a foundational instance of evidence of identity, cross-referencing assertions from an individual with a registry of records maintained by a recognized authority, inspection of identification by trained examiners, and alludes to the use biometric technology as a method of linking identity information.

This has opened the door to achieving LOA3 in unconventional ways that would broaden the pool of options to citizens looking for online verification, and increase accessibility and inclusion. Examples include asynchronous and synchronous options such as video teleconference-based approaches, and experimentation with fully automated remote validation via facial recognition and liveness detection. For those with mobility issues or residing in rural areas, this could prove exceptionally accommodating and dramatically increase accessibility and the inclusion of disparate and disadvantaged groups.

However, caution is needed when pursuing remote verification. Teleconferencing is increasingly risky with the rise in deep fakes and other forms of artificial intelligence technology. The ethical and legislative concerns surrounding the use of biometric technology for identity verification also haven't been fully examined, and resolution on the development of a rigorous framework is still evolving.[8] The impact of these emerging technologies on privacy, security, and safety remains to be determined and will shape their integration into the current approaches to identity verification for online government service delivery.

Building buy-in

Shifting government departments to an SSO platform and to LOA3 where necessary is not an easy task. Many jurisdictions have pursued a corporate mandate to push this forward but even those that receive one still need to prove the value of the platform to front line services. There seems to be no silver bullet from any jurisdiction: a mandate is helpful but not sufficient. Jurisdictions discussed the importance of demonstrating value, with some also stressing the importance of quick releases and continuous iterations. Offering LOA3 identity verification has been a draw rather than a deterrent for some, emphasizing the value of increased privacy protection and the opportunity to reduce validation burdens on front-line services.

Flexible approach to LOAs

While achieving LOA3 is considered a desirable goal, it's essential to recognize that the journey towards this higher level of assurance may vary depending on organizational priorities and constraints. Understand that the choice which LOA to apply to a given context needs to balance risk with user accessibility and may require a program area to accept a higher risk due to accessibility concerns.

For instance there are programs that should be LOA3 from a risk management perspective, e.g. financial assistance. However, due to infrastructure or accessibility constraints, programs may be downgraded to a lower LOA. Continuing with the financial assistance example, if the LOA were downgraded at the time of application, further identity proofing may be required at the time of issuing financial assistance.

Efforts towards making LOA2 more reliable instead of striving for LOA3 across the board could help address these challenges. Some citizen digital services programs are reaching for a higher level of assurance when they don't really need to be. Instead, one solution to more accessible verification and enrollment might be strengthening existing authentication processes by requiring multiple pieces of ID or implementing adaptive authentication models based on the level of risk associated with each transaction.

[8] The Office of the Privacy Commissioner of Canada. 2024. "Biometrics consultation – call for comments". https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-bio/

Strengthening processes, user experience and risk management

It's important that citizen digital services access management doesn't limit its focus to achieving a higher LOA. There are complementary ways to strengthen safe, seamless and secure access to citizen digital services that also need attention. These include addressing legacy systems that hinder the effectiveness of security measures, monitoring user behavior to identify areas for improvement, prioritizing the experience by aligning the user journey with the expected level of risk, or reducing complexity by standardizing processes and streamlining agreements to ensure scalability in service delivery. This can lead to improving authentication methods, enhancing identity verification procedures, and minimizing technical debt.

Recommendations

1. **Adopt a risk-based approach:** Adopt a risk-based approach to determine the appropriate LOA requirement for each service. Understand that not all services may require LOA3 and/or that concerns about citizen accessibility to a service may outweigh the associated risks (e.g. in terms of access to forms of financial aid). Involve downstream services and collaborate with them to determine their LOA requirements based on a risk assessment.

2. **Align to federal standards:** Align LOAs for access to citizen digital services with the Federal Directive on Identity Management and the supporting Guideline on Identity Assurance. Consider the need for LOA1 to 3 based on: the access constraints of the citizens, the sensitivity of the information being accessed and the risk of harm if a breach were to occur.

   Note: LOA4 is generally considered out-of-scope for citizen services.

3. **Choose a user-centric, multi-path, cost effective identity verification process:**

   Choose identity verification processes that match the requirements of the desired LOA while leveraging existing infrastructure, such as the provincial/territorial/municipal agents or existing verification infrastructure from another jurisdiction.

   - **Avoid single-path verification approaches.** Prioritize user experience by offering citizens multiple options for identity verification and authentication. Ensure that the processes are accessible both from a disability and socio-economic perspective, and easy to use across different devices and platforms.

    - **Monitor remote verification advancements.** Explore leveraging facial verification and liveness detection, and monitor the evolving Draft Guidance for processing biometrics – for public institutions from the Privacy Commissioner of Canada.

    - **Balance risk and access** Many LOA3 processes may limit the SSO platform to verifying only people residing in the province or territory. A program may need to accept a lower level of assurance for those residing outside the respective jurisdiction, pursue federations and/or explore other verification methods, such as credit bureau checks.

4. **Government Stakeholder engagement:** Strengthen the citizen digital services mandate for safe, seamless and secure access management to put all citizen-facing online services behind an SSO platform. However, recognize that even the strongest mandates do not eliminate the need to obtain and maintain departmental buy-in through education and relationship building. Demonstrate the benefits of improved citizen digital services, such as increased security, efficiency, and user experience.

SSO platforms as data brokers

As all levels of government across Canada continue to modernize their digital infrastructure to enhance citizen services, the concept of data brokering plays a significant role in facilitating seamless access to these services. Data brokering involves the exchange of information between different entities to enable personalized and efficient service delivery.

The primary question for this section was:

> Should single sign-on platforms for government digital service delivery support data brokering for relying parties within government, and potentially between government programs? And if so, how should this be done?

In the context of citizen digital services and SSO platforms, consent management and respecting privacy laws are essential for maintaining trust with citizens and ensuring compliance with regulatory requirements. There are two commonly contemplated scenarios:

1. Sharing what's typically called “phone book data” (e.g. name, email, sometimes address and/or birthdate, and any record of identity validation) from a single sign-on platform to a downstream service to ensure verified information and save the user the hassle of entering the same information in multiple locations.
2. To share information between two front line services such as sharing provincial/territorial or municipal tax information when applying for a grant.

In exploring data brokering we discussed both of these scenarios.

Jurisdictional and market findings

Jurisdictions

Some provinces’ SSO platforms share information with connecting government services after authentication, including attributes such as name, date of birth, documented sex, and address for identity verification. However, the sensitivity of each attribute varies, and the sharing of these attributes must be justified based on program requirements and collection authority. Some programs do not explicitly use the term "data brokering," but acknowledge the existence of data sharing arrangements.

Tell us once

The "Tell us once" model in government service delivery aims to simplify the process of updating personal information. It allows citizens to provide their details once to a central authority or agency, eliminating the need to repeat the same information across multiple government departments or services. There is no uniform approach across government services, and data brokering practices vary across services and departments. Each jurisdiction implements protocols based on its specific partnership agreements and collection authority. Through risk-based approaches, stakeholder engagement, and responsible use of available technologies, governments aim to balance citizen convenience and privacy rights when facilitating secure and efficient data exchanges for citizen services.

For example, a citizen digital services program might apply the following guidelines:

- For LOA1 connected government services are provided with unverified basic data fields such as first/preferred name, last name, email address, alongside the account identifier.
- For LOA2 and LOA3 connected services, attributes are typically verified before being sent. This could include a verified name, address, and birthdate verified off a driver's licence or health card, or at the respective card's source database, for example, in addition to the basic data fields.

Account linking

Account linking is a key consideration for government services that offered online service delivery prior to utilizing a single sign-on platform. In most cases, citizen digital services teams don't take on the migration of old accounts to the single sign-on platform. Instead they may use an account linking process, allowing citizens to link their new account to an existing file with a connected service. For example, a student loans program would have had its own login prior to leveraging a citizen digital services SSO platform. Rather than migrate their old account over, the SSO platform performs account linking by asking the student a few questions about their existing student loan application (such as name, dob, and SIN) and then student loans is able to link the SSO account with the existing student loans account in the student loans database. This enables continuity without having to get into the risks of data migration. The students have to agree to new terms of use.

Privacy Commissioners

Privacy commissioners converge on a cautious approach to data brokering for citizen digital services. There is also recognition that the practice of repeatedly requesting the same information from individuals across different government departments is seen as inefficient, wasteful, and a frustration to citizens.

Firstly, it entails the collection of personal attributes by government entities for the purposes of administering specific programs. This collection must be justified by the necessity of the information for the operation of the program, it should only be undertaken with the individual's consent, and it warrants careful scrutiny. For example, while certain information may be legitimately shared with other government agencies for specific purposes, such as tax reporting to the Canada Revenue Agency (CRA), there is concern when data is shared without clear justification or consent from the individual. Privacy commissioners were also concerned with data brokering if it involved government sharing data with external third parties. It's worth noting that no citizen digital services team reported sharing information collected via their SSO platform with third parties.

Sentiments from privacy commissioners can be aptly summed up as follows: "the potential for losing citizen trust is too immense. Be careful about those services ramping onto the [SSO system]. Put information sharing agreements, consent and reasonableness standards in place. It must be clear that the government has the authority to collect the data in question."[9]

There was also mention that "if it's government to government and involves a technology company contracted [to execute the brokering], the contract [between the government and the technology company] should be drafted in such a way that the information can only be used for government operations and when contract ends, delete everything and provide proof."[10]

Delegation of authority in the context of data sharing

Furthermore, privacy commissioners touched upon scenarios where data needs to be shared with someone acting on behalf of another person. While delegation of authority is not typically what comes to mind when considering data brokering, it was consistently raised by privacy commissioners and thus is worth reflecting in this report. The commissioners encouraged governments to collaborate with their

[9] A quote from the privacy commissioner interviews undertaken by DTLab between January and February 2024.
[10] Ibid.

privacy commissioner offices when considering delegation of authority and sharing information with a delegate (e.g. a parent, guardian or power of attorney).

For example, for someone such as a guardian acting on behalf of a child, there needs to be clear mechanisms in place for verifying the authority of the individual acting on behalf of another to ensure data is being shared with the right person. This may involve proving legal guardianship or obtaining explicit documented authorization from the individual in question (e.g. a power of attorney in the case of an elderly parent), depending on the context and legal requirements. Furthermore, once the necessity for someone to act on behalf of another is established, there must be provisions for transferring ownership or control back to the original individual when appropriate. This could involve clear procedures for revoking authorization or transferring access rights, ensuring that the individual's identity and privacy rights are protected throughout the process.

Solution providers

The perspective provided by the solution providers emphasized the importance of authority, consent, and privacy considerations related to data brokering. While the solution providers could not cover all potential and unforeseen consent requirements, they echoed the privacy commissioners stressing that early engagement of the respective office of the privacy commissioner would help ensure integration design concerns prior to system development and implementation.

Data brokering techniques

The solution providers highlighted the importance of quality control and auditing data brokering activities, touching upon mechanisms such as temporary storage of the data and limiting the scope of information collection.

They also stressed that while solution providers offer technology solutions and expertise to support these efforts, the responsibility of ensuring compliance with regulatory requirements in how information is shared across services ultimately rests with the programs.

Lastly, solution providers mentioned that digital credentials can put citizens in control of how data is shared, offering an innovative twist on traditional data brokering. Examples included sharing vaccination records, security clearances, and education certificates. These could be presented to connected government services with selective disclosure applied so that the government service only receives exactly what they need.

Analysis

Overall, data brokering practices must involve safeguarding privacy, obtaining consent, addressing complex scenarios, and ensuring that appropriate mechanisms are in place for managing such situations effectively and ethically.

While some provinces, territories and municipalities are advancing in areas such as enterprise-wide SSO solutions that facilitate data brokering, others lag behind, grappling with fundamental challenges in cybersecurity and digital service access management. If relying on large-scale procurement processes is proving to be slow or challenging, a focus on incremental progress and stakeholder engagement could be more sustainable towards achieving reliable and privacy-respecting data brokering across government services.

Consent management and collection authority

It's essential to prioritize consent and adhere to a reasonableness standard. Citizens must have a clear understanding of why and how their information is being collected, used, stored and shared, as well as the extent to which they can control and revoke consent. Additionally, it must be transparent that the government has the legal authority to collect and share the information in question.

Furthermore, while it may take more time and effort to implement data brokering practices, a meticulous approach is crucial for ensuring that citizen data is handled securely and ethically. Rushing into data brokering initiatives without thorough consideration and implementation could risk compromising privacy and trust.

Recommendations

5. **Adopt a "Tell Us Once" model:** Aspire to implement a "Tell Us Once" approach where citizens only need to provide and verify their phone book personal information once, and it is securely shared from the digital services management platform to relying government departments and services. This can streamline processes for citizens and reduce the burden of repeatedly providing the same information. Wherever possible, storage should remain with the source of truth and only be surfaced through the SSO platform, in keeping with data minimization.

6. **Ensure effective notice, consent, and justification:** Provide clear, concise and easy-to-understand notice and consent to citizens about how their personal information will be collected, used, disclosed, stored and shared.

Ensure this aligns with legal and regulatory requirements and follows the principle of data minimization. The SSO platform should provide:

- How citizens can voice concerns, ask questions or revoke consent.
- Consent receipts documenting what was consented to, and when.
- The ability to notify, and to re-consent, if terms of use have changed.

7. **Establish strong data sharing agreements:** Develop clear and encompassing data sharing agreements between the citizen digital services program and connected services. These agreements should outline the purposes for which data will be shared, ensure compliance with privacy laws, and establish protocols for data protection and deletion. For connected government services, these agreements should be standardized to streamline agreement management and ensure consistency across downstream services.

8. **Collaborate with other jurisdictions:** Learn from the experiences of other jurisdictions in implementing citizen digital services access management and data brokering initiatives.

9. **Keep delegated authority in view:** Evaluate and address delegated authority in digital service delivery, such as situations where individuals act on behalf of others (e.g., guardianship). Develop verification processes for confirming the delegated authority, clarity, accountability, and alignment with existing legal processes.

Federation

Federation involves establishing trust relationships between a SSO service provider and a relying party(ies) to enable seamless authentication and authorization across multiple systems. In the context of citizen digital services access management, federation refers to the ability for users to use their credentials from one trusted source to access services provided by other entities without needing separate login credentials.

Citizen SSO platforms are an example of federation, allowing citizens to sign in once and access connected services. The benefit is not needing to remember multiple usernames and passwords to access provincial/territorial or municipal services.

Enabling federation to Government of Canada services through a jurisdictional citizen SSO platform is another example. This currently exists for BC and Alberta residents and considerations for other jurisdictions looking to federate with the federal government is the focus of this section. The primary question for investigation was:

How can SSO platforms used at the provincial and territorial level be enabled to access Federal Government services through federation?

Federation enhances the user experience by enabling secure access to distributed services, improves security, and facilitates collaboration across different jurisdictions, programs and services.

Jurisdictional and market findings

Jurisdictions

Federation with the Government of Canada involves creating bi-lateral agreements based on Federal Government assessments of the province or territory, followed by a technical integration. It involves an assessment using the Public Sector Profile PCTF[11] as a way to map a service into the Government of Canada's policy framework using a common approach. A successful assessment results in a letter of acceptance from the Chief Information Officer (CIO) of Canada, which also describes findings and recommendations. Though there is no requirement for a service to meet a particular LOA, the federal government is mainly interested in identity and credential

[11] Public Sector Profile of the Pan-Canadian Trust Framework | Cadre de Confiance pancanadien. https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_4

assurance levels 2 and 3 per the Standard on Identity and Credential Assurance[12] and User authentication guidance for information technology systems (ITSP.30.031 v3).[13]

Past successes and alternative perspectives

As noted, British Columbia and Alberta have successfully implemented federation with the federal government, enabling their residents to log in to federal government services using their provincial single sign-on login information. The federation was grounded in a conformity assessment, collaboration, and of course the technical implementation.

Other jurisdictions have opted instead to utilize sign-on partner solutions, which the Federal Government also supports. So residents can already use the same credentials to log in to jurisdictional services and Government of Canada services. This approach meets the needs of residents and businesses without undertaking additional federation.

Privacy Commissioners

Privacy commissioners emphasized the importance of federating provincial and territorial sign-on platforms with the federal government to access federal government services. They also stressed the need for privacy protection, strong security measures, and establishing clear accountability through governance structures and implementing proper processes.

One privacy commissioner encouraged governments to pursue federation with the federal government, stating “what a waste it would be if a jurisdiction developed this great identity verification system and it didn’t integrate with the federal government to access services (online or otherwise).”[14]

Ensuring adequate training and user-friendly interfaces for citizens is essential, considering potential generational gaps and varying levels of access, particularly in rural communities which often have limited internet connectivity. They also highlighted that government programs must be careful to determine who will be accountable for what and provide proper training for citizens.

[12] Government of Canada. March 2016. “Guideline on Identity Assurance”. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32612

[13] Government of Canada. April 2018. “User authentication guidance for information technology systems (ITSP.30.031 v3)”. https://www.cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3

[14] A quote from the privacy commissioner interviews undertaken by DTLab between January and February 2024.

Solution providers

Solution providers stressed the importance of standardized service agreements and technical interfaces to facilitate integration processes across jurisdictions. They noted that the technical aspects of federation are considered less complicated, but underscored the challenges posed by legal and business considerations. They advocated for scalable agreements that could accommodate multiple jurisdictions without duplicating efforts.

Furthermore, solution providers suggested that jurisdictions, especially smaller ones, focus on tailored solutions that align with specific use cases and governance needs. Overall, solution providers emphasized the importance of collaboration, standardization, and strategic alignment in achieving successful federation initiatives.

Analysis

Federation can leverage existing SSO systems to improve cross-jurisdiction access to government services. While not explicitly explored in this report, federation between provinces and territories (e.g. one province or territory accepting another province or territories sign-in process) or between municipalities and provinces/territories (e.g. municipalities leveraging provincial or territorial sign-in processes to sign into municipal services) could improve access to government services, such as hunting licenses, for individuals who frequently travel. Federation could also reduce the username password burden, and in the case of municipalities leveraging provincial or territorial authentication mechanisms, limit the municipalities' need to establish their own LOA3 identity and access management service.

The evolving landscape of technology and its impact on federation strategies with government services is a current focus. Emerging technologies, such as digital credentials, may offer alternative approaches that could alleviate or complement traditional federation methods. As digital credentials could be used in place of a username and password, eliminating or at least reducing the need for point-to-point federation. This underscores the importance of remaining adaptable and responsive to technological advancements in the access management space for citizen digital services.

Recommendations

For those jurisdictions looking to federate with the federal government:

10. **Understanding federal government federation requirements:** Review the PCTF-PSP in detail along with the most recently published workbook, as this is the basis for the federal government assessment. Work with those in the federal government to better understand the formal federal assessment process and identify gaps. The federal government may have evolved its approach and moved past the latest published documents.

11. **Leverage past jurisdictional efforts:** There is a wealth of knowledge with the jurisdictions that have already gone through the federal federation process. As a citizen digital services program moves into its readiness and gap analysis phase for its identity and access management solution(s), it is highly recommended that it engage these jurisdictions.

For federal federations and any other type of federation the following would be important:

12. **Allocate appropriate resources:** Allocate necessary resources, including personnel and budget, to support the federation process. This initiative requires focused effort and is not recommended as a side-of-desk activity.

13. **Ensure your SSO platform and support structures are sufficiently documented:** Review the program's current definitions, processes, roles and accountabilities and ensure they are all documented.

    - **Define and document accountability and governance:** Clearly define and document accountability structures and governance processes within the program. Designing and documenting them with transparent reporting and oversight mechanisms from the beginning will help build trust among federating parties.

14. **Ensure transparency and consent with users:** Maintain transparency regarding the collection and use of personal data. Ensure it is stated clearly for citizens, who amongst the federation partners are collecting, using, storing or disclosing data, and what the data attributes are. Obtain explicit consent from users for data processing activities and clearly communicate the purposes for which their information is being collected, used, stored, and shared. The program should also provide users a way to easily access and update their consent preferences, promoting transparency.

How to work effectively with Privacy Commissioners

Through proactive engagement, transparent communication, and a commitment to privacy-respecting practices, government entities can effectively uphold privacy standards, protect citizen information, and ensure the success of digital initiatives.

The primary question for investigation for this section was:

> How does a digital citizen services team best work with its privacy commissioner to ensure safe, seamless and secure access to digital citizen services?

Drawing insights from interviews with government officials across Canada and its provinces/territories, the following are some key takeaways into the strategies, best practices, and considerations for fostering collaboration with privacy commissioners.

Jurisdictional findings

Early engagement is encouraged, but recognize that showing early work can turn into an investigation. So it is important that programs are designed to support an investigation down the line. Successful citizen digital services initiatives worked closely with their privacy commissioners balancing both education and consultation from the design of their SSO system all the way through launch and continuous improvement. Further consultation is particularly important when there are significant architectural changes, modifications to consent management, data brokering implications, or when experimenting with biometrics.

Integrating services

In order for a service to integrate with an SSO platform, they typically have to prove their collection authority and have to do their own PIA as an onboarding activity. These PIAs are often also of interest to the privacy commissioners and including the privacy commissioner in the onboarding process of a new service is generally recommended, even if it's not required.

Privacy commissioners

The collective advice emphasized a few key principles across three themes: early outreach, education and guidance, and privacy-by-design with user engagement.

Early outreach

The privacy commissioners encouraged early outreach in general. They emphasized the importance of early engagement with their offices, particularly in projects involving the collection of data and personal information. Departments and programs should proactively reach out for guidance and consultation, rather than waiting until later stages of development. Privacy commissioners recognized that there has been a fear in the past of not wanting to be shut down for engaging too early in a project. One privacy commissioner stated that “the earlier we are involved, the more likely we can get on the right track, ensuring that your project aligns with privacy regulations and best practices from the beginning.” and “don’t wait to have gone too far into development. Instead, employ privacy by design.”[15]

Involving the commissioner can be “an afterthought that is undertaken later than it could have been to check-off a check box on short notice.”[16] Privacy commissioners noted that this approach is something to avoid. If citizen digital services teams don’t engage with their privacy commissioners early enough, they don’t have time to build that feedback into their solution. Frequent consultations also build trust and promote transparency.

Education and guidance

Some privacy commissioners provide educational materials, workshops, and speaking engagements to help government departments understand privacy requirements and best practices. This helps to dispel fears about engaging with the privacy commissioner and encourages proactive collaboration.

Some privacy commissioner offices offer guidance on their websites for how to complete a PIA or consult with the office. Others have shifted to a more proactive approach focused on building relationships and adopting portfolio models with designated teams for certain project types. It is important for government program areas to learn how their respective privacy commissioner office is structured and how best to engage.

Privacy-by-Design and Public Engagement

Lastly, privacy commissioners stressed the importance of adhering to privacy-by-design principles, conducting thorough risk assessments, implementing

[15] A quote from the privacy commissioner interviews undertaken by DTLab between January and February 2024.
[16] Ibid.

strong privacy safeguards, and working with users as essential to ensuring compliance with privacy laws and regulations. Where possible privacy commissioners also encouraged public consultation.

Analysis

A common thread among these experiences is the emphasis on early outreach and engagement with privacy commissioner offices. For instance, reviews of each service connecting to an SSO platform and PIAs conducted throughout the SSO project lifecycle are important steps. Privacy-by-design principles are also important for an effective collaboration with privacy commissioners.

In summary, working effectively with privacy commissioners requires a proactive approach, education and guidance, understanding and adherence to existing methodologies, and meaningful public engagement. By embracing these fundamentals, government initiatives can navigate privacy considerations successfully and build trust with stakeholders and the public.

Recommendations

15. **Engage early and collaborate:** Establish early engagement with the privacy commissioner's office to ensure alignment with privacy principles and regulations. Keep them informed throughout design, implementation and continuous improvement and maintain close collaboration to address any concerns or issues proactively.

16. **Establish regular reporting intervals:** Establish regular reporting intervals and determine triggers, such as the onboarding of a new service to schedule additional consultations. This consistency will help to build transparency, trust and collaboration.

17. **Work with your privacy officer:** Involve the provincial/territorial privacy officer in establishing the cadence and approach to collaboration. It will be important to keep them up-to-speed on what the citizen digital services team is doing and they will have the most familiarity with how to effectively collaborate with their respective privacy commissioner.

18. **Work with your privacy commissioner on consent and transparency:** As a citizen digital services team prioritizes user consent and ensures transparency in data collection practices, it should work closely with their privacy commissioner to address any concerns or assumptions about data usage and privacy implications.

Moving towards digital credentials

As noted in the introduction, digital credentials represent a transformative approach to identity verification. While most government programs focus on the issuance of a verifiable person credential - which is a generic form of government-issued photo ID - DTLab wants to draw attention to the value of a digital credential program that exceeds just the person credential. From corporate registration documents to hunting licences to transcripts to permits and licences, investing in a digital credential program opens up a broad range of opportunities for citizens and businesses, while reducing fraud and offering better privacy protection.

Jurisdictional and market findings

Jurisdictions

Digital credentials are being contemplated across most of the jurisdictions interviewed for this report, which are at varying stages of maturity. British Columbia leads the pack with digital credentials in production for individuals (verified person), lawyers (proof of being a lawyer via the law society), business registration, and mining industry credentials such as ESG reporting and government permits.

Other jurisdictions are advancing in their journey, actively exploring the implementation of digital credentials and currently equipped with the necessary technology to issue them. However, before proceeding, they are conducting a comprehensive legal evaluation to determine the regulatory framework surrounding digital credential usage. This evaluation involves considering existing legislation and assessing whether modifications or new laws are required to provide the necessary legal backing for digital credentials.

Still other jurisdictions are at various stages of experimentation, exploring proofs of concept and pilots, and collaborating in pan-Canadian forums on digital credentials and cybersecurity. These jurisdictions may or may not have enterprise infrastructure in place. For these jurisdictions, getting started with targeted, small use cases seems to be the preferred path, with examples including employee cards for group management and exploration of credentials related to trade apprenticeships. One jurisdiction has embarked on a series of pilots focusing on digital credentials involving various stakeholders such as central agencies and banking institutions. A notable use case involves setting up a corporation online to open a commercial bank account and digital wallet. However, this had not resulted in a production solution at the time of publishing.

Beyond jurisdictional advancements there is also intra-jurisdictional collaboration on network infrastructure to enable sharing and interoperability across provinces and territories. The goal is to promote the adoption of standardized protocols and practices for digital credentials. Stakeholders emphasize the importance of having all provinces onboard the network, highlighting the need for cohesive standards and a unified approach to digital credentials across Canada.

Challenges

There is no doubt that transitioning from traditional paper-based or PDF credentials to digital credentials will require a significant period of adjustment, with multiple modes of authentication likely coexisting during the transition phase. Readiness for widespread adoption hinges on stakeholder engagement, technological integration, and acceptance across various highly representative sectors, such as healthcare.

In the meantime, there are some challenges to work through. The work on foundational national infrastructure to support cross-border credential exchanges remains nascent, though there have been some announcements about collaboration to attempt to move this forward.[17]

Technology stacks are varied with differing preferences across the country making interoperability more difficult, and while it's recognized that the country won't converge on a single technology stack, complexity from the outset does limit scalability.

Lastly, misinformation and disinformation continues to truncate constructive public conversations. The Saskatchewan Government program was paused due to public pressures[18] and other jurisdictions have also faced public pressure due to active mis and disinformation campaigns.[19,20]

[17] Newswire. Jan 2023. "Avancées importantes en matière d'identité numérique pour le Québec - Rencontre des ministres fédéral, provinciaux et territoriaux sur la confiance numérique et la cybersécurité". https://www.newswire.ca/fr/news-releases/avancees-importantes-en-matiere-d-identite-numerique-pour-le-quebec-rencontre-des-ministres-federal-provinciaux-et-territoriaux-sur-la-confiance-numerique-et-la-cybersecurite-869739478.html

[18] CTV News. 2022. "Plan to introduce digital identification system in Sask. put on hold". https://regina.ctvnews.ca/plan-to-introduce-digital-identification-system-in-sask-put-on-hold-1.5846948

[19] Digital Trust Laboratory of Canada. 2023. "Misinformation and Disinformation in Digital Identity". https://dtlab-labcn.org/en/misinformation-and-disinformation-in-digital-identity

[20] CTV News. 2022 "Ontario government won't comment on progress of digital ID program". https://toronto.ctvnews.ca/ontario-government-won-t-comment-on-progress-of-digital-id-program-1.5852732

Lessons learned

Key lessons learned from initiatives include the importance of leveraging existing resources and infrastructure, particularly through open source components. Additionally, partnering with reputable vendors possessing expertise in digital credentialing streamlines the implementation process and reduces time and effort.

One jurisdiction recommended starting small and focusing on implementing a minimum viable product with lower risk credentials. They advocate for a gradual growth approach, allowing for refinement and expansion of capabilities over time as the project matures and gains momentum.

Overall, a systematic approach to the adoption of digital credentials is important, ensuring that legal and practical considerations are thoroughly addressed before implementation.

Privacy Commissioners

The fundamental principles of privacy remain unchanged despite the advent of digital credentials. Privacy commissioners emphasized the importance of distinguishing between various types of digital credentials and ensuring that privacy and security considerations are paramount at every stage of their implementation. While technologies like facial recognition and biometrics offer potential avenues for authentication, they must be deployed with careful attention to privacy safeguards.

Additionally, one commissioner proposed framing such credentials as "verification", suggesting that the “verification label…goes down better than digital ID or digital credential,” in reference to the mis and disinformation that is plaguing the topic. Another kept it short and simple, stating that the emergence of biometric technology has “no impact” and that the “same principles apply.”[21]

The recurring themes of privacy and accountability echoed by the privacy commissioners are reinforced by a joint resolution, in which privacy commissioners and ombudspersons across the country align on key topics.[22] The resolution emphasizes that participation in a digital credential ecosystem should be voluntary and optional for individuals. Individuals should have control over their personal information and be provided with clear and informed consent mechanisms.

[21] A quote from the privacy commissioner interviews undertaken by DTLab between January and February 2024.
[22] Office of the Privacy Commissioner of Canada. September 2022. “Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada”.

The resolution underscores the importance of privacy, transparency, and individual rights in the design and operation of digital credential systems in Canada. This document outlines important characteristics of a digital credential ecosystem in order to gain trust and uphold the aforementioned principles, namely minimization and protection of personal information, auditability, and equitable access. It reflects a commitment to ensuring that digital credential initiatives benefit Canadians while upholding their privacy rights.

Collectively, the statements from privacy commissioners stress the imperative of gaining trust and considering the public's perception by employing and maintaining privacy and security measures in the development of digital credentials to ensure confidence in their use. Privacy commissioners acknowledge the potential benefits of digital credentials but also raise concerns about privacy implications and the need for clear legal frameworks to govern their use. Additionally, user privacy must be protected throughout the credential lifecycle.

Solution providers

Solution providers suggested starting small, with manageable digital credential projects, advocating for conducting tests and pilots before full-scale implementation. They advised following established standards and caution against attempting to build everything at once. One solution provider suggested jurisdictions "get started, set up tests/pilots, and be prepared for changes. Don't try to build it yourself."[23]

The definition and implementation of digital credentials vary among stakeholders, necessitating consensus-building to align understanding and expectations. "It can mean different things to different people, and take many shapes such as a diploma or licence. It's just a credential that can be digitally verified against an authoritative source." They explain that organizations have to "look at the business objective and what they're trying to achieve, then select the technology that makes sense in terms of scalability and security, and meets other business needs."[24]

Solution providers have experience integrating with digital wallets and anticipate governments becoming significant issuers of digital credentials. Collaboration between technical teams and marketing/communication teams is essential for successful digital credential projects, ensuring technological feasibility and effective communication with stakeholders. While challenges exist, solution providers remain confident in the value and potential of digital credentials despite occasional setbacks or detractors.

[23] A quote from the solution provider interviews undertaken by DTLab between January and February 2024.
[24] Ibid

Analysis

Digital credentials represent a potential paradigm shift in terms of privacy and surveillance within our systems. However, it's important to understand the intricacies of digital credentials. For instance, at the time of writing, the World Wide Web Consortium (W3C) Verifiable Credential Standard[25] is more cryptographically secure, but less privacy protecting than its Hyperledger counterpart, known as Anoncreds.[26]

To navigate this emerging technology, open collaboration and incremental progress is encouraged, with small teams working openly, collaborating with others, and demonstrating tangible proofs of concept to foster understanding and buy-in.

Current exploration efforts and pilot projects can position smaller jurisdictions to be not only more technologically capable, but build business readiness in anticipation of a wider adoption. While some may not be actively pursuing digital credentials, there is value in exploring their potential applications and implications, particularly given the privacy and fraud reduction benefits.

Next steps

Key considerations include defining use cases, addressing privacy concerns, and ensuring interoperability with other systems. To this last point, it is worth highlighting that a leading organization in the field has provided a high level roadmap to enable short term interoperability via participating jurisdictions all using the same network. The intention with this roadmap is to accelerate delivery in the short term. This recognizes that multiple technology stacks and vendors, and therefore more complex interoperability challenges, are likely to emerge over time.

Evaluating the progress of digital credentials across different regions reveals a rapidly evolving landscape characterized by diverse approaches, varying levels of readiness, and ongoing technological advancements. Establishing mechanisms for continuous monitoring of progress and trends can allow stakeholders to remain up-to-date with emerging technologies, standards adoption, evolving best practices, and regulatory developments. By being flexible and responsive, they can capitalize on new opportunities and ensure that its approach remains relevant. Adopting a proactive approach to monitoring progress by participating in community groups can help integrate innovation and enhance capacity to deliver secure and user-centric digital credentials.

[25] World Wide Web Consortium (W3C). March 2023. "W3C Verifiable Credential (VC) Data Model V1.1". https://www.w3.org/TR/vc-data-model/

[26] Hyperledger AnonCreds. November 2022. "AnonCreds Methods Registry V0.1 Draft". https://hyperledger.github.io/anoncreds-methods-registry/

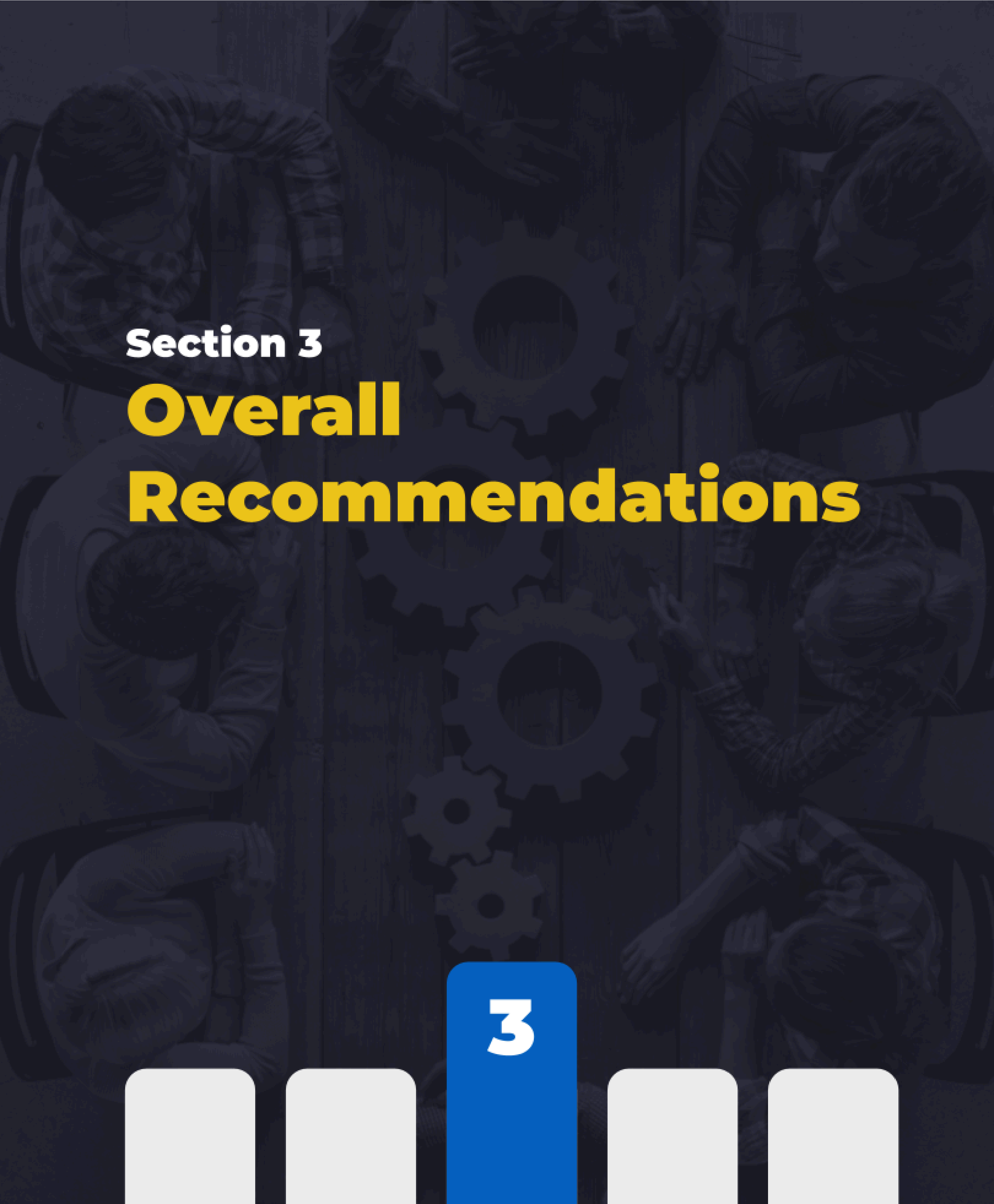
Recommendations

19. **Start with pilot programs:** Begin with small-scale pilot programs to test the effectiveness of digital credentials in specific use cases. These pilots can help identify potential challenges and opportunities while minimizing risks associated with broader implementation, and increase internal capability for future projects. Also seek opportunities to showcase these pilots, as this can generate significant feedback, and improve collaboration opportunities.

20. **Leverage pilot successes:** Leverage insights and lessons learned from pilot programs to inform future decision-making and scale up successful initiatives. Identify areas of improvement and iterate on pilot projects to refine processes, address challenges, and maximize the value derived from digital credentials across Canada. Adapt implementation strategies based on lessons learned and develop mechanisms to better collect and integrate feedback received from pilot participants and stakeholders, such as surveys and focus groups.

21. **Familiarize the team with established standards and frameworks:** Invest time in understanding the various frameworks, standards, and technical components and how they are evolving globally (refer to the Appendix). Monitor the evolution of standards and frameworks to support interoperability with industry. Ensure this knowledge lives with the team as a whole and not one person, as it has cross-functional implications.

22. **Monitor progress and trends:** Continuously monitor progress and trends in the field of digital credentials. Stay informed about emerging technologies, best practices, and regulatory developments to adapt implementation strategies accordingly and capitalize on new opportunities. Refer to the Appendix for a list of working groups for consideration.



Section 3

Overall Recommendations

3

Overall Recommendations

These recommendations are a reflection of the research done for this report and DTLab's existing expertise.

1. **Take a program view to ensuring safe, seamless and secure access to digital citizen services:** Design access management for citizen digital services as a program rather than an IT project. Develop a program vision that is citizen-centric, outcomes focused, and prioritizes stakeholder collaboration. Work towards staffing accordingly and establishing multi-year funding.

   Specifically:

   a. **Develop a program governance structure:** To ensure strong oversight and to build buy-in, create a governance committee (or leverage an appropriate existing committee) that would receive program updates at regular intervals and would be tasked with the highest risk or highest strategic value decisions. The governance committee should have representation from key stakeholders across government.

   b. **Build a cross-functional team:** The exact make-up may vary but for smaller jurisdictions this typically consists of a mix of a dedicated core team members with other resources assigned to the work as part of a larger portfolio of duties (e.g. a solution architect, security or privacy specialist) and still others aspects of the work outsourced to contractors or vendors. Team representation should include a program lead, a project or product manager(s), and a business analyst(s) alongside specialists in areas such as privacy, security, user experience/service design, communications, legal, architecture, client support, and representation from downstream services.

   c. **Invest in capacity building:** Digital credential and citizen-centric access management talent is hard to find. As a result, governments often focus on up-skilling internal people. Enhance internal capabilities related to citizen digital services access management, including training for the broad program team described above. Training should focus on ensuring each team member has the basics, that the team is speaking the same language, and building bridges between business and technical team members.

2. **Develop a long-term program strategy:** Develop a long-term strategy that aligns with the government's broader digital transformation initiatives. Ensure

that the strategy is flexible enough to accommodate future advancements in technology, changes in regulations, changes in user behavior and expectations.

Specifically:

a. **Prioritize the design and enhancement of an LOA3 single sign-on (SSO) solution that can be scaled up and future-proofed:** Having an LOA3-based SSO infrastructure is a foundational element of a citizen digital services program. Targeting LOA3 ensures that the program has strong risk management in place and doing this through an SSO is critical for supporting federation, data brokering and digital credential goals.

b. **Pilot and evaluate digital credential solutions:** Pilot digital credential solutions, technologies, and processes in controlled environments to assess their effectiveness and feasibility. Gather feedback from users and stakeholders to iteratively improve and refine practices. Start with low-risk use cases and gradually scale up based on the success of initial implementations and feedback from stakeholders, to be a fast follower.

c. **Stay flexible and adaptive:** Recognize that the citizen digital service landscape is continuously evolving, and remain flexible in response to changes in technology, regulations, and user needs. Regularly review and update the access management strategy for citizen digital services to adapt to emerging trends and challenges.

3. **Develop a privacy framework that:**

- **Is developed in collaboration** with a jurisdiction's respective Chief Privacy Officer and Privacy Commissioner.
- **Prioritizes privacy-by-design principles** and the delivery of privacy impact assessments throughout the design, development, implementation and continuous improvement of a citizen digital services program.
- **Identifies internal privacy policies and procedures** that enshrine privacy-by-design and ensures compliance with laws and regulations that align with legal obligations and principles outlined by a privacy commissioner.

- **Incorporates privacy safeguards**, such as encryption and data minimization, implementing access controls and establishing auditing mechanisms to protect users' sensitive information and maintain their trust in the credentialing process.
- **Designates a privacy liaison(s)** to serve as point of contact for citizen and stakeholder privacy-related inquiries and initiatives, to facilitate communication and collaboration with a privacy commissioner, and to monitor and report on the design, implementation, and operation of the privacy framework.

Consider resourcing the team with a dedicated privacy specialist to design and deliver the privacy framework and ensure that team members are aware of the policies and procedures within, and that they understand their role in design, decision making and safeguarding personal information.

4. **Centre the user in development and operations**

    a. **Prioritize user-centered design principles and components**, to ensure that the system meets the needs and expectations of residents. The Government of Canada has a library of design components that could be adapted as needed.

    b. **Iterative development:** Embrace an iterative development approach, frequently releasing updates and improvements to access management systems for citizen digital services. Use feedback from users and stakeholders to refine and enhance the system over time.

    c. **Ensure citizen-centric support** for your citizen SSO platform and the full citizen digital services program. Leverage expertise where possible to remain cost-effective.

5. **Take a collaborative approach to procurement** Involve solution providers in the course of your procurement development. While the traditional approach is a Request for Information (RFI) followed by a Request for Proposal (RFP), a consultative approach to developing an RFP is likely a better way to centre the user (the responding vendor) in the process.

    Evaluate vendors based on their track record, capabilities, alignment with your identity and access management strategy for citizen digital services and the vendor's ability to keep pace with emerging technology within the space. Proofs of concepts as part of the evaluation process are highly recommended.

Prioritize solutions that can be tailored to specific use cases, user populations, and regulatory environments. This also means having a solid understanding of existing capacity, a strong foundation of use cases and detailed processes.

6. **Communicate precisely and build trust:** As the Canadian landscape remains fraught with misinformation and disinformation regarding identity and access management for citizen digital services, communication needs to be targeted and intentional. While the best way to communicate in this climate remains elusive, the following are two valuable starting points:

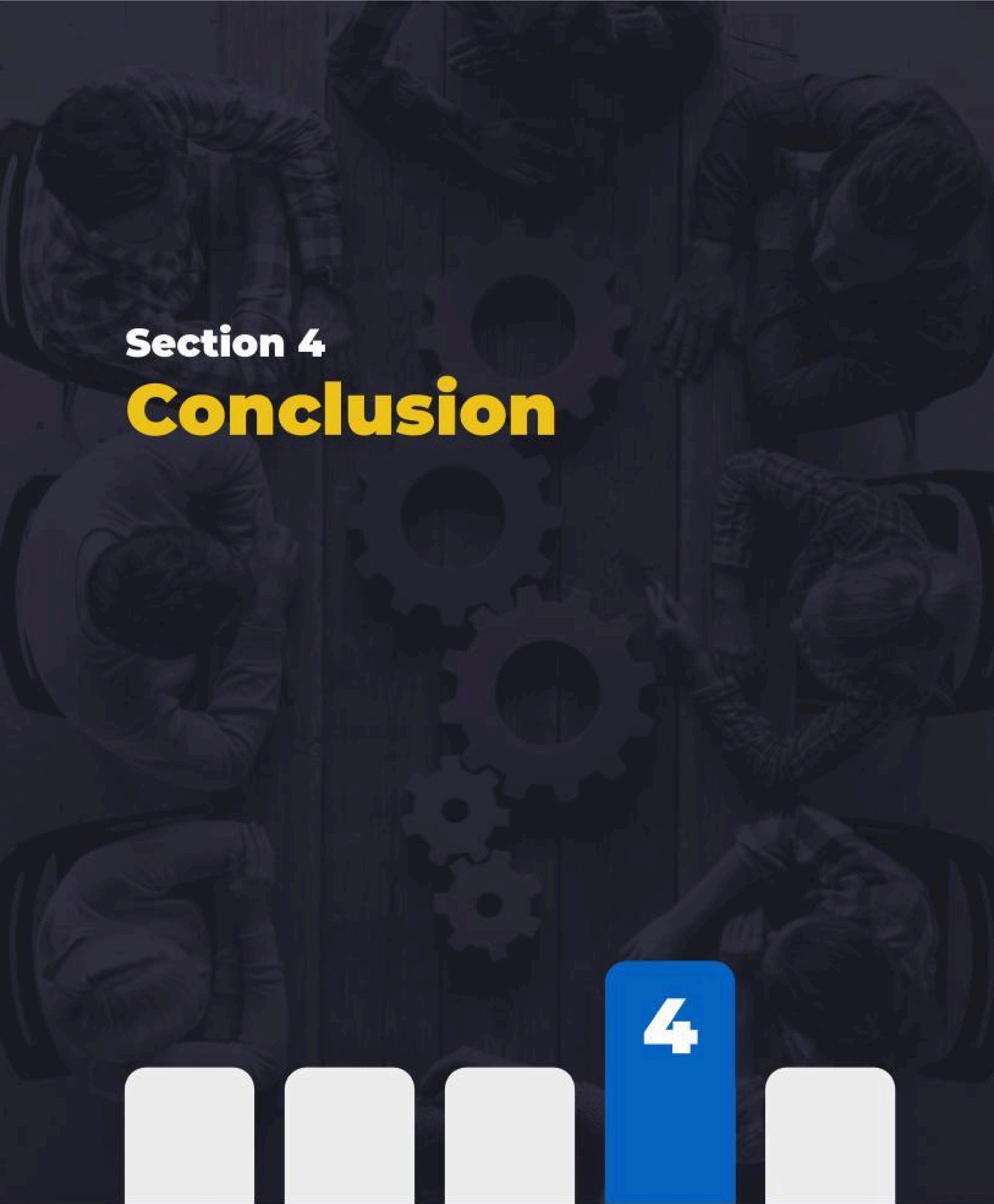
    a. **Build buy-in and understanding with internal influencers and at the political level.** Communicate the benefits of safe, seamless and secure citizen digital services and the long term strategy, while addressing any misconceptions or resistance from stakeholders.

    b. **Prioritize public engagement focused on gathering user needs** in a targeted way tied to use cases, rather than mass communication, and maintain clear, demonstrable messaging (backed up by program delivery) that stresses privacy, security, and convenience

7. **Stay engaged in the community**

    a. **Work collaboratively with external partners**, including identity and access management solution providers, other government jurisdictions, nonprofits and industry associations to share insights and best practices. Collaborative efforts can help streamline and accelerate processes and ensure interoperability.

    b. **Actively engage in standards and technology community organizations** to accelerate internal capacity building while contributing to the development of a more cohesive and interoperable digital credentials ecosystem across the country.



Section 4
Conclusion

Conclusion

Many jurisdictions across Canada face the challenge of advancing safe, seamless and secure access to their citizen digital services. The recommendations outlined in this report provide actionable guidance for governments at all levels across Canada, and their partners, that are looking to advance access to citizen digital services in a structured and impactful way. The recommendations of this report highlight the importance of prioritizing stakeholder collaboration, risk-based approaches, and a focus on the end-users.

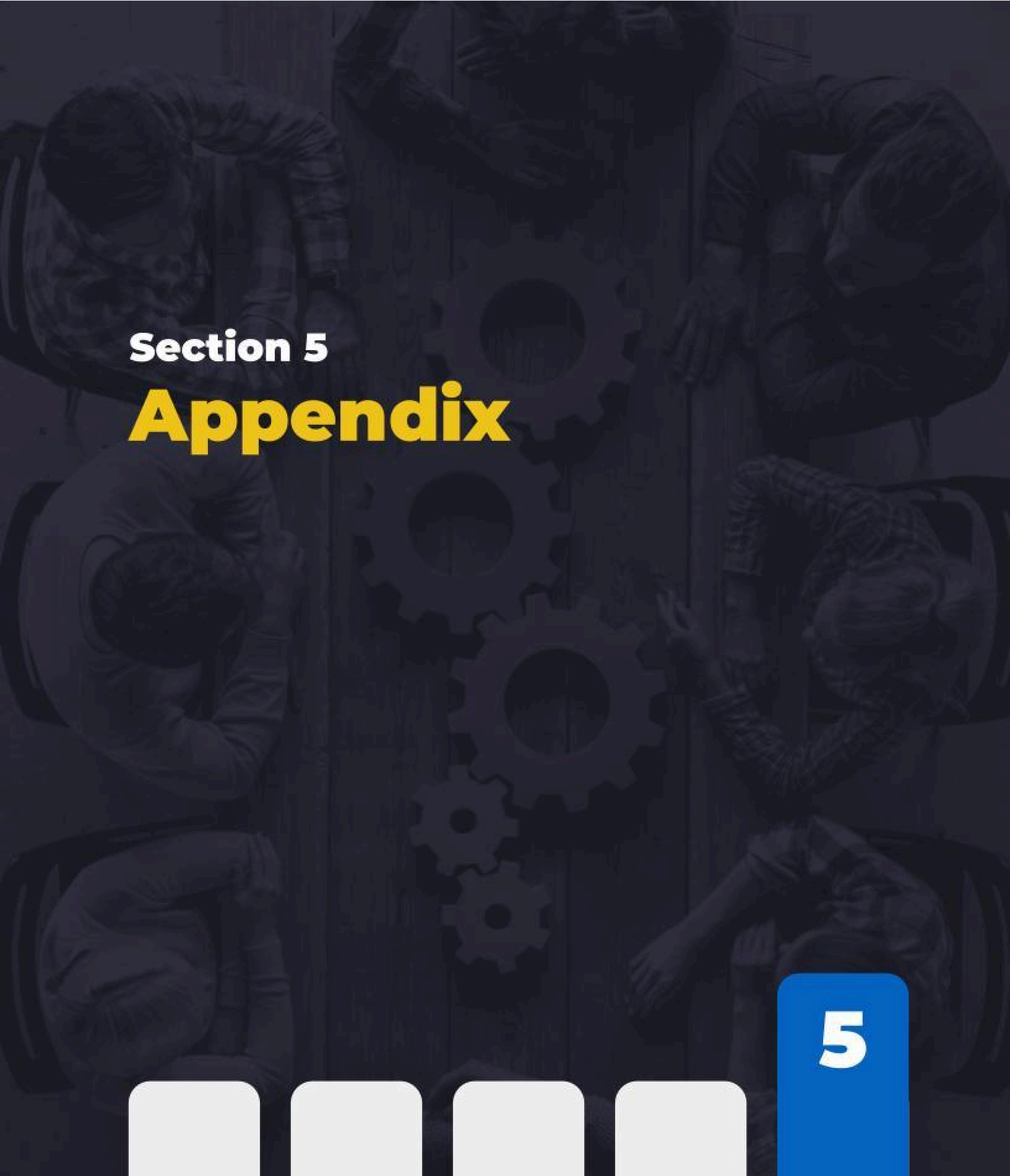
Ultimately, the report recommends being ready to move towards digital credentials through pilot programs, leveraging pilot successes to inform future decision-making, and continuously monitoring progress and trends. Adopt an iterative approach, prioritize collaboration, and build trust. Foremost, take a program view to ensuring safe, seamless and secure access to citizen digital services. It is not just another information technology (IT) project. Jurisdictions can then more effectively and continuously advance their citizen digital services program and contribute to a more cohesive, dependable and interoperable ecosystem for their citizens across Canada.

In summary, by applying the recommendations outlined in this report, governments at all levels across Canada can position citizen digital services access management programs as business and technology ready in the short and long-term. Keeping pace with current and emerging trends, being seen as a strong collaborator, while ensuring the security, privacy, and convenience of services will allow jurisdictional digital citizen services teams to be adaptable and effectively stay up-to-date while addressing evolving needs.

Ready to take the next step in your digital credential journey?

Reach out to us at DTLab to see how we can support you with:

- Capacity building and training
- Pilot projects
- Technology assessments



Section 5

Appendix

5

Appendix - Standards, Frameworks and Technology Working Groups

The following is a non-exhaustive, alphabetized list of standards, technology, and framework bodies that citizen digital services teams may want to monitor for digital credential advancements and broader discussions about identity and access management. It is never possible to participate in or monitor all organizations and some organizations are closed to national actor participation only. Where relevant, DTLab has provided notes on the organization to interest or potential participation.

1. Decentralized Identity Foundation (DIF) - DIF is an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interop between all participants.

2. Digital Governance Standards Institute (DGSI)- The Digital Governance Standards Institute, part of the Digital Governance Council is an accredited standards development body. The Institute enables greater trust and confidence in Canada's digital systems through developing technology governance standards collaboratively across a range of stakeholders.

   DTLab note: DGSI also has delegated authority from the Standards Council of Canada to develop digital identity standards for the country.

3. Digital Identification and Authentication Council of Canada (DIACC) - The Digital Identification and Authentication Council of Canada, known as the DIACC, is a non-profit coalition of public and private sector leaders committed to developing a Canadian framework for digital identification and authentication.

   DTLab note: Canadian companies are now actively working to certify their products against the DIACC's Pan-Canadian Trust Framework.

4. Hyperledger Indy Foundation - Hyperledger Foundation promotes interoperability and standardization, paving the way for the widespread adoption of secure and scalable blockchain and digital trust solutions across industries and sectors.

   DTLab note: Hyperledger Indy is the foundation for a network that some jurisdictions have been exploring as a potential option for their verifiable digital credential issuance and verification ecosystem.

5. International Telecommunication Union - ITU is the United Nations specialized agency for information and communication technologies (ICTs). It facilitates international connectivity in communication networks.

   DTLab note: ITU maintains the X.509 recommendation, which is the base for a majority of Public-key Certificate-based management system

6. Internet Engineering Task Force (IETF) - The IETF is the premier standards development organization (SDO) for the Internet. The IETF makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet.

   DTLab note: the IETF is responsible for the OAuth 2.0 Framework critical in many federation services.

7. IS0 Mobile Driver's Licence (mDL) - establishes interface specifications for the implementation of a driving licence in association with a mobile device. It also specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure.

   DTLab note: The ISO mDL standard is seeing significant interest and some uptake in the United States. It is not open to non-state actors.

8. The Open Identity Exchange (OIX) - OIX is a community for all those involved in the ID sector to connect and collaborate, developing the guidance needed for inter-operable, trusted identities Through our definition of, and education on Trust Frameworks, we create the rules, tools and confidence that will allow every individual a trusted, universally accepted, identity.

   DTLab note: OIX recently released an analysis of trust frameworks from around the world highlighting similarities and differences. DIACC's framework was included in the analysis.

9. The OpenID foundation - is a global open standards body committed to helping people assert their identity wherever they choose. They are a global vibrant community where identity peers and thought leaders convene to craft the identity ecosystems of tomorrow.

   DTLab note: the OpenID protocol is an authentication protocol, allowing users to log into a website while delegating authentication to a central authority. They are also responsible for OID4VC - OpenID for Verifiable Credential Issuance and Presentation.

10. Open Wallet Foundation - The OWF is a consortium of companies and non-profit organisations collaborating to drive global adoption of open, secure and interoperable digital wallet solutions as well as providing access to expertise and advice through our Government Advisory Council.

11. Organisation for the Advancement of Structured Information Standards (OASIS) - OASIS Open offers projects—including open source projects—a path to standardization and de jure approval for reference in international policy and procurement.

    DTLab note: OASIS helped foster SAML, the Security Assertion Markup Language, widely used in federated authentication models and PKCS 11: Cryptographic Token Interface Base Specification version.

12. Trust over IP Foundation - The ToIP Foundation works to promote global standards for confidential, direct connections between parties; leverage the opportunities for interoperable digital wallets and credentials; protect citizen and business identities by anchoring them with verifiable digital signatures; integrate the technical elements for digital trust with the human elements—the business rules and policies that govern collaboration in a successful digital trust ecosystem; and foster communication and knowledge sharing amongst Digital Trust experts.

13. W3C Verifiable Credentials Working Group - The mission of the working group is to make expressing and exchanging credentials that have been verified by a third party easier and more secure on the Web.

    DTLab note: Widely accepted as the gold standard for digital identity and credentials