DIACC CCIAN

Public Trust Forum Report

Committed to Building Trust Together - October 2023

Contents

1. The Challenge
- DIACC’s role
- A public trust gap

2. Recommendations
- All organizations
- DIACC’s commitment

3. Public Trust Forum
- Initiative objectives
- Key discussion takeaways

4. Forum Discussion Themes
- On public acceptance of digital trust capabilities
- Observed public behaviours
- Bolstering cybersecurity
- Importance of frameworks and standards
- No ‘one-size-fits-all’ approach

5. Our Commitment
- Building trust together

5. Appendix
- Sponsors
- Methodology
- Pre-forum report recommendations
- Forum participants

The Challenge

The Challenge

DIACC's role

Established in 2012, DIACC is a non-profit organization of **public and private sector members** committed to advancing full and beneficial participation in the global digital economy by promoting adoption and establishing a certification framework to verify the **assurance and trust** practices of services.

DIACC, and its members, prioritize personal data control, **privacy, security, accountability, and inclusive people-centred** design.

The Challenge

DIACC's role

DIACC's **Public Trust Forum** fosters debate to seeds **actionable recommendations** for public and private sector organizations committed to building public trust. This initiative builds on **people-centred policy universal design principles** detailed in a paper co-authored by DIACC and the Human Technology Foundation.

Source: https://diacc.ca/wp-content/uploads/2022/11/Universal-Digital-ID-Policy-Principles-to-Maximize-Benefits-for-People.pdf

The Challenge

Privacy and data control

Privacy and personal data control are powerful tools to help safely confirm a person’s identity. These tools are foundations of **digital trust** (i.e., a collection of technologies and methods used to verify a person or organization’s identity to enhance **privacy, security, and transparency using people-centred design** to operate digital credentials, digital wallets, networks, and modern authentication).

Digital trust capabilities are critical—and long overdue—to support a **secure and inclusive** digital economy and society.

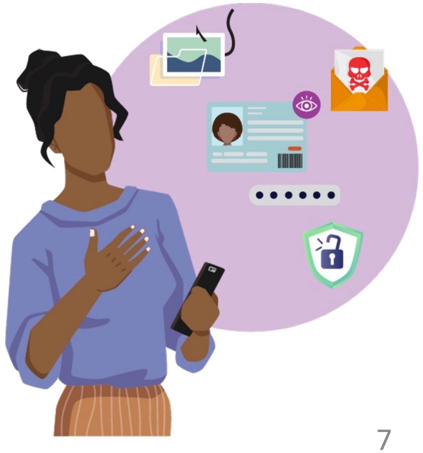
The Challenge

A public trust gap

Digital trust capabilities hold the **potential to put people in control** of their data, streamline processes, enhance security, and improve services access, yet our research indicates some people (23%) are **unsure or apprehensive** about the benefits.

People should **rightly** be concerned about **data privacy, security,** and potential **misuse of personal data**.

There are often **no easily understood rules** around where personal data lives, who owns it, or how others use it. High-profile **data breaches** and misuse of personal data **erode trust.**



Source: https://diacc.ca/wp-content/uploads/2023/04/DIACC-Canadian-Digital-Identity-Research-2022-Wave-4-1.pdf

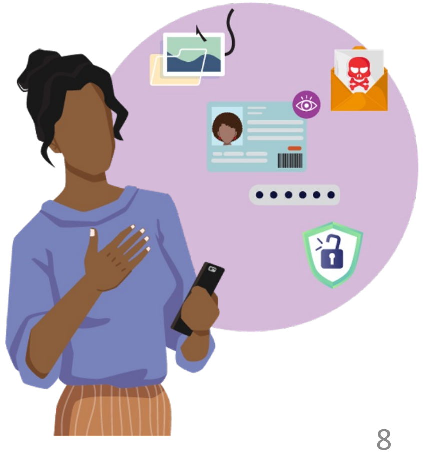
The Challenge

Data minimization

The words “digital ID” may **confuse people** and conjure **negative images** of Big Brother-type surveillance.

Some people think "digital ID" means constant authentication. But, in most cases, people can be **anonymous or pseudonymous** (use fake names) and access services using the **minimum information needed** to complete a task.

A bank needs to know **you are who you claim to be** to stop fraud. A beer store only needs to know that a **person meets the age of consent**. Typically, a retailer only needs to know that a **payment card is valid**.



The Challenge

A public trust gap

Organizations and governments must **act together** and **individually** to address the **diverse interests** of the public.

Organizations and governments must prioritize **transparency, robust data protection measures, and ethical data usage** while actively engaging with the public to address concerns and ensure that digital trust capabilities are developed and implemented to protect and enhance **individual privacy and security,** and **support organizations'** operational needs.

The Challenge

Most feel benefits

Simply put, digital ID is about enabling people with the **choice and control to use the credentials they already have** offline for their online activities**.**

And our research indicates that most people (55%) already feel the positive impacts of **secure, convenient, and privacy-enhancing** digital services.

DIACC CCIAN

Source: https://diacc.ca/wp-content/uploads/2023/04/DIACC-Canadian-Digital-Identity-Research-2022-Wave-4-1.pdf

Recommendations

Recommendations

For all organizations

Consider the following to support and inform public dialogue.

1. **Don’t wait for a universal public consensus on adopting digital trust capabilities because it will never come**. Commit and message that public adoption is voluntary. Individuals may choose to use digital trust services or not.

2. **Make significant public education investments** at municipal, provincial and federal levels and in the private sector to inform the public about the benefits of well-designed capabilities. Focus on easy use cases (i.e., digital parking or bus passes, obtaining a business licence).

3. **Reduce the temperature** by moving public messaging away from the confusing term “digital identity” in certain situations. Terms like “verify,” “authenticate,” and “credential” are more easily understood.

4. **Communicate importance for public safety** as scenarios where digital services reduce response pressure and help get resources faster to those in need. Pandemic-related personal safety concerns accelerated the demand for modern digital services.

5. **Break transformation down into manageable outcomes** rather than trying to boil the ocean with a national or universal strategy.

Recommendations

DIACC’s commitment

Consider the following to support and inform public dialogue.

1. Establish and facilitate a storytelling campaign among private and public sector entities and governments to amplify benefits. Address:

- links between privacy, transparency and control of personal and business information.
- cyber-safety and educate the public about modernization developments.
- real-world examples from sectors i.e., the aviation sector for example.
- tangible benefits and specific daily pain points that can be alleviated.
- modern workforce capacity development supporting universities and talent.
- Informing and building government security policy analysts awareness.

2. Continue work with collaborative bodies such as the joint councils of federal and provincial CIOs and public sector delivery leads to support synergies. Emphasize the value of frameworks and standards as central to the strategy as the private sector moves forward.

3. Build more visible partnerships with established institutions across sectors that interact with the public — i.e., universities, colleges in student settings, and banks.

4. Bring concepts to life peoples’ minds by depicting how capabilities are portrayed in policy debates, covering aspects of data privacy, security, related legislation, and access to information reform.

DIACC's Public Trust Forum

DIACC's Public Trust Forum

Initiative objectives

Seek forum participant consensus on the pre-forum report findings and recommendations on public trust gaps regarding digital trust capabilities.

Prioritize recommendations and discuss how to move them forward.

Identify high-level outcomes forum participants want to achieve to inform perceptions and build adoption of digital trust capabilities.

Inform the education and engagement work DIACC and its members conduct with in the public and private sectors.

Public Trust Forum Overview

Key discussion takeaways

> “If there is something of value people will adopt it. It is that simple.”
>
> ***Mel Crocker***
> *Chief Information Officer*
> *Air Canada*

Forum participants, with a variety of perspectives, discussed challenges, opportunities, and considerations, reaching consensus on the following:

→ **There will never be a universal consensus on acceptance of digital trust capabilities.** Universal acceptance should not be the goal.

→ **Use of government-issued digital credentials must be voluntary.** People must have the choice to opt-out, as they can opt-out in the private sector.

→ **There's no strong call to action from the public to advance digital trust.** This is partly due to a lack of education about what digital trust means, and most importantly, how it can benefit people.

→ **An effective communications strategy must focus on real-life success stories.** Use practical examples of how digital trust capabilities improve service delivery, such as in the aviation and financial sectors.

Public Trust Forum Overview

Key discussion takeaways

- **Though it's been around a long time, the term "digital identity" may be hindering acceptance** since it's politically charged.
  - Terms like "verify," "authenticate," or "credentials" may be easier to understand for those who are unsure about new technologies.
  - **DON'T** abandon the term "digital identity." It's a profession and a globally recognized definition; its use will depend on the audience and situation.
- **Digital trust systems must prioritize data portability** and the rights of citizens and residents to access and control their data. People should be in control of how their information is used and shared.
- **Governments must work together and with the private sector** to ensure digital trust services' interoperability, privacy, and security.
- **Jurisdictionally, with Canadian news removed from popular social media platforms** there may be a vacuum to spread mis and disinformation regarding digital modernization.

> "One of the things that we're working on is to help educate the public that when we increase trust and reduce fraud, then mechanically that reduces friction for the vast majority of consumers."
>
> ***Matt Charpentier***
> *VP, Global Head of Authentication & Identity*
> *VISA*

DIACC CCIAN

Forum Discussion Themes

Forum Discussion Themes

On public acceptance of digital trust capabilities

Forum participants unanimously agreed: universal public acceptance is unachievable and not required to modernize services on an economic and societal scale, stressing that capabilities must enhance privacy and security.

Discussion focused on the need for public education on multiple levels.

- Digital identity is a confusing concept. Jurisdictions making progress report that using a word like “credential” is more easily understandable.

Trust is local: There was recognition that acceptance of capabilities varies globally and often depends on localized public trust in governments.

- Some participants believed fears about digital modernization are being amplified disproportionately.
- In Europe, it’s perceived that this type of modernization is “barely a conversation.”

Participants stressed the opportunity to learn lessons from experiences.

- People welcome services that relieve frustrations. Air travellers accept ID verification as a security requirement. Still, air travellers are frustrated with carrying physical ID cards and prefer digital equivalents.
- Context matters. While there is widespread acceptance of digital verification in financial services, the sector encounters resistance to biometrics/facial recognition technologies to facilitate faster checkout.

Forum Discussion Themes

Observed public behaviours

Data sharing paradox: There was discussion about peoples' willingness to share personal information on social media platforms and in apps. People are more concerned about sharing personal information with governments even though governments may already have access to this same information.

- The consensus among forum participants was that public messaging should emphasize peoples' lack of transparency and control over their data rather than focusing only on fears about privacy today. Stress "We don't have control of our data" and explain what data control means in the context of privacy protection.

Lack of outcry: Anecdotally, people criticize the inconvenient current patchwork of website logins and lack of modern government digital services, yet there is no massive public outcry for transformation.

- "Everybody agrees [that the patchwork is a poor experience]. But there's that little spark [of vocal demand] missing," said Jonathan Kelly, Assistant Deputy Minister, Government Digital Transformation in the Government of Quebec.
- "We're focusing so much on the few that are making a loud noise…but…the rest of us…I don't know if we're okay with mediocre service...We're just quieter," said Giselle D'Paiva, Partner, Government & Public Sector Digital ID Lead at Deloitte.

Forum Discussion Themes

Observed public behaviours

Generational divide: Forum participants noted that older people may have a higher tolerance for visiting physical locations to shop and access government services, but exceptions exist. Younger people expect minimal friction and want every service on a smartphone.

- “In use cases where there is both an expectation of identity verification and the current process is incredibly cumbersome, then that's an easy win; you're going to face virtually zero pushback,” said Charpentier of VISA. “The challenge is when you start with use cases where friction is already pretty low, and the expectation that identity verification is low or non-existent, [it’s] incredibly hard to get those processes to change.”
- Chicken before the egg — experiences in other countries (i.e., New Zealand and Estonia) suggest that better experience in digital government services leads to greater trust in government to handle people’s information.

Alleviate pain points: There was consensus on the importance of identifying peoples’ biggest pain points to demonstrate how digital trust capabilities can help. This is an effective way to amplify benefits.

- “That's where we need to put a lot of our energy on because a lot of that noise, in my experience, goes away when the experience is a better choice,” Mel Crocker, Chief Information Officer at Air Canada.

Forum Discussion Themes

Bolstering cybersecurity

There's an urgency to increase cybersecurity and reduce data breaches. Every breach adds to public suspicion and concern. What that looks like will vary. Frameworks and standards could help.

Breaches erode trust: Participants agreed that frequent data breaches, including in public sector institutions, degrade trust and create more reluctance at the political level to address digital trust challenges and opportunities.

- "The public might not be as concerned, but government security policy analysts certainly are, and that's where a lot of the concern can get raised," said Gregory Natran, co-founder at Becker-Carroll.
- The level of concern varies by geography and by use case.

Focus on safety and benefits: Once the benefits and cybersecurity measures are widely understood, most people will likely come around to using digital trust services.

- Previous digital transformations followed a similar trajectory of suspicion followed by acceptance. People had confidence that their personal information would be safe and secure when the benefits became real.
- When e-commerce began, people were reluctant to use their credit cards online for fear of fraud. As the public saw the systems were secure, online transactions became the norm. The pandemic accelerated online shopping. We're going through the suspicion-acceptance cycle again with digital trust capabilities.

Forum Discussion Themes

Importance of frameworks and standards

Keeping up: The velocity of transactions in specific industries (i.e., aviation and financial services) necessitates an innovation pace governments struggle to match. Discussions focused on the need for widely adopted frameworks and standards to guide organizations' behaviours while industries anticipate government modernization.

- “Had there been a national standard or even agreement on provincial standards, [we could have used it]. We couldn't wait for that. So we adopted a standard, and then we're now using it,” said Crocker of Air Canada.
- “I don't think the industry collectively is doing a good enough job but coming up with those standards, and in parts of the world [that are], those are not designed with interoperability in mind, which is going to create challenges down the road,” said Matt Charpentier, Vice President, Global Head of Authentication and Identity at VISA.

Participants pointed to the vital work of Canadian representatives participation in W3C to push global standards.

Adoption: Wide adoption of a framework will be essential as the federal government revisits privacy legislation.

- “Trust is local, and designing made-in-Canada solutions for digital access and verification will help build consumer confidence, trust, and broad adoption,” said Neil Butters, VP Product, Interac Verified.
- He cited the example of bringing Apple Pay to the Canadian market. Having an existing framework for e-commerce ensured a smoother transition.

Forum Discussion Themes

No ‘one-size-fits-all’ approach

Participants discussed the need for a nuanced approach. Different provinces are at different points in the journey. There was consensus that the federal government is lagging.

- Essential public sector work is happening at joint councils of federal and provincial chief information officers and public sector service delivery leads.
- “It's all about continuous collaboration, and bringing the ministers into that dialogue is really important,” said Colleen Boldon, Director, Digital Lab and Digital ID programs at the Government of New Brunswick. “So the challenge with any given government is there's always way too many priorities and never enough money.”

Choice: People have different preferences. Some want different "digital wallets" for various activities. Some want one wallet for government-issued credentials and another wallet for shopping. Some want one single wallet for all.

- The public’s varied preferences are essential considerations to discuss in development circles and with policymakers. Who decides how systems will work is unclear, especially as providers develop different solutions in silos.

Building Trust Together

Please **use the Public Trust Forum recommendations to activate** discussions and actions in your organization.

DIACC will reconvene the Public Trust Forum at intervals to **review** developments, **address** critical themes and **continue** public literacy research **to pinpoint public perception** evolutions.

DIACC CCIAN

Appendix

Sponsors

Leadership Sponsors

We are grateful to the leadership organizations whose sponsorship helped DIACC secure resources and impartial facilitation expertise to produce this report.

Deloitte.

Interac

PORTAGE cybertech

VISA

Methodology

DIACC contracted the Compass Rose Group to host two Public Trust Forum Sessions on July 21, 2023 and September 15, 2023.

Forum participants reviewed a pre-forum report based on a series of interviews conducted in Spring 2023.

Participants for the interviews and forum were drawn from a target list developed and socialized across DIACC members and governance committees. Many participants in the sessions were interviewed for the pre-forum report, which was circulated in advance of the Public Trust Forum sessions. Participants came from the following areas:

- Academia
- National organizations
- Private sector companies
- Provincial/territorial governments

Former television news correspondent and Compass Rose Counsellor Shirlee Engel moderated the sessions, where questions were meant to guide an impartial and free flowing discussion among participants, who agreed to be identified in this report.

Pre-forum report recommendations

The following recommendations were made by respondents during their interviews with the Compass Rose Group.
As they are the opinions of various respondents, some recommendations may seem to contradict each other..

Canada-wide

- Don't wait for a consensus on digital identity, it will never come.
- Consider moving away from using "digital identity" as it has negative connotations.
- Advance jurisdictional privacy legislation to align with 21st-century realities; ensure adequate consultation.
- Incorporate digital identity literacy into school curriculums.

Public sector

- Jurisdictions must take a stand on digital identity and once a decision is made about proceeding, be as transparent as possible with citizens.
- Consider a royal commission on the future of the digital economy in Canada, with digital identity at the forefront.
- Ensure internet access in remote areas remains a top priority.
- Focus on advancing digital identity in smaller government programs, where people can see quick wins to build confidence.

Private sector

- Contribute to public education campaigns by sharing benefits and wins from systems already in place.
- Bolster government efforts to develop solutions by continuing to share best practices and supporting DIACC/civil society advocacy.
- Consider interoperability with future government-issued digital credentials when developing proprietary solutions.

DIACC/ Civil society

- Continue public sector advocacy regarding urgency to implement digital identity. Emphasize real-world experience rather than hypothetical or overly technical arguments.
- Launch storytelling campaign with positive, tangible examples to demonstrate value of digital identity. Consider partnering with government, banks, etc. on the initiative.
- Leverage power of influencers to counter MDM spread on social media.

Forum Participants

NAME	TITLE	ORGANIZATION
Joni Brennan	President	Digital ID & Authentication Council of Canada (DIACC)
Jonathan Kelly	Assistant Deputy Minister, Government Digital Transformation	Government of Quebec
Jacques Marcoux	Director of Research and Analytics	Canadian Centre for Child Protection
Gregory Natran	Co-Founder	Becker-Carroll
Matt Charpentier	Vice President, Global Head of Authentication and Identity	Visa
Rachel Dobrin-De Grace	Vice-President, Government Relations and Legislative Compliance	National Payroll Institute
Mel Crocker	Chief Information Officer	Air Canada
Neil Butters	VP Product Verification Solutions	Interac
Steve Waterhouse	Assistant Deputy Minister, Governmental Information Security and Cyber Security	Government of Quebec
Colleen Boldon	Director, Digital Lab and Digital ID programs	Government of New Brunswick
Serge Cayouette	Information Security Program Manager, IMTS	Royal College of Physicians
Giselle D’Paiva	Partner, Government & Public Sector Digital ID Lead	Deloitte
Sime Pavlovic	Interim National Digital ID Leader	Deloitte
Giles Sutherland	VP Business Development	Interac
Brenda McPhail	Acting Executive Director, Master in Public Policy in Digital Society program	McMaster University
Donna Barr	Assistant to Nadine Wilson, MLA, Saskatchewan Rivers	Government of Saskatchewan

Secure the Digital Economy

Join DIACC to **connect** insights, **drive** impact, **inform** decision-makers, and **educate** the public about digital trust **benefits** and the **risks** of inaction.

Contact info@diacc.ca for membership and general inquiries.

🌐 diacc.ca in /company/mydiacc