

Foundational ID: Restoring the Chain of Trust for Identity

DIACC Special Interest Group Insights

Table of Contents

About the DIACC	2
About DIACC Special Interest Groups	2
About the Author	2
Glossary	3
Introduction	4
Foundational ID: The Canadian Context	5
A Foundational ID Special Interest Group	6
Observations	6
Identity Silos, Contextual IDs, and De Facto IDs	6
Biometrics	7
Fraud	7
Service Delivery	8
Conclusions	8
Recommendations	9
Proposed Initiatives	10
Call to Action	14
Annex 1 – Additional Initiatives	15
Mutual Exclusion Tokens for program enrolment	15
Relationships as the DNA of an identity	16
Annex 2 – A Fraud Scenario	16
Annex 3 – Demonstrations	17



Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group.
To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca.
To join the DIACC community, visit www.diacc.ca.

About the DIACC

Created as a result of the federal government's Task Force for the Payments System Review recommendations, the [Digital ID & Authentication Council of Canada](#) (DIACC) is a non-profit coalition of public and private sector leaders who are committed to developing a Canadian digital identification and authentication framework that will secure Canada's full and secure participation in the global digital economy.

About DIACC Special Interest Groups

DIACC Special Interest Groups (SIGs) provide a mechanism through which to engage our stakeholder community in discussions around a specific interest. They provide an opportunity to connect subject matter experts from around the world, and to broaden conversations outside of our DIACC membership.

A DIACC SIG does not create intellectual property, but rather contemplates a specific question to make a recommendation to DIACC regarding the next steps that should be considered for incorporation into the DIACC strategy and roadmap.

About the Author

Bill A.V. Pezoulas is an IT consultant and entrepreneur with a particular interest in identity. In his consulting roles, he has focused on Technical and Solution Architectures and has been contracted by many Canadian Federal Government departments as well as a handful of private sector and NGO clients. Through his entrepreneurial and consulting work in developing software applications and frameworks, he became aware of the critical role that identity management plays in corporate, B2B, and B2C business contexts.

In the wake of the 2001 terror attacks on the World Trade Center (WTC), Bill was engaged in an effort to further secure the issuance of passports by developing a system for validating Birth Certificates at source. The prototype of this system evolved and was eventually deployed in every province and territory. This motivated Bill to explore identity from a societal context, which led to more projects involving foundational sources of identity, and then, with Narciso Zorzi, to the formation of Valid8ID Solutions Inc. to develop identity solutions.

Bill has been an active member of the DIACC since 2016, and has contributed to the Innovation and Trust Framework Expert Committees (IEC and TFEC). A frequent participant at Identity North, Bill has presented and led Unconference sessions. Finally, Bill moderated the DIACC SIG on Foundational ID and worked along with the DIACC team to produce this report. Additional contributions were made by both private and public sector organizations that participated in this SIG.

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

Glossary

Biometric anchor: A hypothetical approach, utilizing one or more biometrics that can be tested to ensure an identity is always associated to only one natural person, thereby “anchoring” an identity to that person.

Book of names: A colloquialism of the authoritative list of identities.

Contextual ID: IDs created for a specific (limited) business purpose within a narrow business context, as opposed to an ID that was created for a broad range of purposes.

De facto ID: IDs used for multiple purposes but not designed as such, and in many cases, has been prohibited for multiple uses (e.g., driver’s license, health card, employment ID). In these cases, the issuer strictly prohibits its use as an ID except for the specific purpose for which it was designed.

Foundational ID: An identity that's been established or changed due to a foundational event (e.g., birth, person’s legal name change, immigration, legal residency, naturalized citizenship, death). Defined in the [Public Sector Profile of the Pan-Canadian Trust Framework](#) (PSP PCTF)

Holder: A person, organization, or machine that controls, or is in the process of obtaining a digital representation in the digital identity ecosystem regulated by the [Pan-Canadian Trust Framework](#) (PCTF).

ID credential: A type of digital representation that describes a person’s set of attributes or properties. This information may exist on its own (e.g., as a credential that contains no personal information, only a unique string identifier) or be related to personal information.

Level of Assurance (LOA): A level of confidence that may be relied on by others. In the PCTF applied as a measure of certainty that a Subject is who or what they claim to be, or that a Subject has maintained control over an Authenticator, and that the Authenticator has not been compromised. In the context of the PCTF, Levels of Assurance are those defined by the [Government of Canada Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance](#). Defined in the [PCTF Glossary Final Recommendation V1.0](#).

Mutual Exclusion Token: A mechanism designed to prevent concurrent access to protected resources by more than one process or entity. In the context of this document it is used to prevent the enrollment of an identity into more than one program of a given type that needs to be mutually exclusive (e.g., a person can only be enrolled in one provincial health insurance plan at any given time).

Verifiable Credential: A Verifiable Credential can represent all of the same information that a physical credential represents. The addition of technologies (e.g., digital signatures) makes Verifiable Credentials more tamper-evident and more trustworthy than their physical counterparts. For a more in depth definition please refer to [Verifiable Credentials Data Model v1.1 \(w3.org\)](#).

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

Introduction

Trust is the assured reliance on the character, ability, strength, or truth of someone or something. Trust is the indispensable pillar of any highly functioning democracy, economy, and society. Security is a key enabler of trust. Trust erodes without security.

Trust removes the constraints that are applied to increase the level of assurance in a transaction. If those constraints are removed there is no limit to the opportunities, prosperity, and collective goals that people, companies and governments can achieve. With trust, contracts can be entered into, money can be lent, purchases can be made, services can be accessed, and information shared with confidence and security.

Without trust, opportunity is easily lost, economic growth contracts, and people can be left out or left behind. Without trust, no one can be certain that their plans, purchases, and information are safe and secure.

While trust has always been indispensable in economic and social relations, it is even more so in the digital economy, where irrevocable decisions can be made in the blink of an eye or the click of a mouse; where the buyer or lender isn't necessarily around the corner or down the block, but potentially on the other side of the globe; where information is more frequently shared online rather than in-person; where determined individuals manipulate weak identities and verification processes for their own nefarious purposes. Gaining Canadians' trust in the rapidly expanding digital ecosystem is even more challenging amid the rise in distrust of government and economic institutions among a growing segment of the Canadian population.



As Canada expands its participation in the digital economy, certain challenges relating to the existing trust environment, particularly with its jurisdictional silos of identities, have become apparent.

Developing a robust digital ID is an essential element in Canada's ability to establish digital trust and harness the potential of the digital economy of the 21st century. Governments and the private sector in Canada and globally know this, and have made significant advances in devising new, modern, standards-based digital identity networks/ecosystems that are robust and secure, and provide convenience, choice and user controlled access to, and use of, personal information. This important work will be incomplete and will likely create significant

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group.

To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca.

To join the DIACC community, visit www.diacc.ca.

problems unless the identified challenges with the jurisdictional silos of identities are addressed.

DIACC believes that the integration of foundational sources of identity into the evolving digital identity ecosystem is essential to meet these challenges, which is why it formed a SIG of identity experts to facilitate progress and focus work in this area.

This report lays out the SIG's observations, recommendations and proposed initiatives designed to help prepare the Canadian identity system for transition to a global digital identity ecosystem. It defines the requirements of a Trusted ID, the relative merits of existing IDs measured against these requirements, and lays out a national identity strategy.



Foundational ID: The Canadian Context

Canada does not have a national identity card, the reasons for which are rooted in the unique structure of our federation and the distribution of responsibilities between our national and provincial governments. Canadians are wary of a centralized government registry that can be used to track their activities, a fact that has been repeatedly upheld in the courts in relation to restricting the use of federal social insurance records (Social Insurance Number - SIN) and related identifiers for employment insurance and taxation purposes.

Historically, identity in Canada has been fragmented in multiple jurisdictional silos and as a result, Canada does not have a unique identifier that is used for identity. Silos of identity (Contextual IDs) have evolved in support of various purposes, such as driving permits (driver's licenses), employment insurance and taxation (SIN), government services (government services cards, health cards), immigration (immigration visas, permanent resident and citizenship documents), and travel (passports). While the organizations responsible for each of these silos have worked diligently to secure their own identity systems for their own purposes, none of these were designed to act as a robust and ubiquitous identity instrument. These are some of the accepted de facto forms of physical identity documents on which the Canadian identity system relies.

Foundational IDs are those established as a result of a foundational event (i.e., birth or immigration events) and are under the exclusive control of the Vital Statistics Organizations [VSOs] of the Provinces and Territories, and Immigration, Refugees, and Citizenship Canada [IRCC] respectively.

A "Chain of Trust" based on examination of physical identity documents and an imperfect matching of names is commonly used to resolve identities between these silos, however,

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

Foundational IDs are not consistently incorporated into this Chain of Trust to link Contextual IDs to their foundational counterparts.



Biometrics have also been layered into these forms of identity, most commonly facial photographs, to aid in verifying identities. Yet the facility to verify those with the issuer are generally only available to a select few within the issuing silo. The use of these forms of biometrics outside the issuing silo has been by manual inspection, with few assurances that the biometric appearing on the physical ID is the right one.

Great advances have been, and continue to be, achieved in Canada and globally in devising new, modern, standards-based digital identity networks/ecosystems that are robust and secure, and provide convenience, choice, and control of personal information. Unfortunately, in Canada these advanced new identity networks are being populated with identities that have been established within this broken Chain of Trust, further amplifying the harms of the past.

The basic premise behind this report is that this Chain of Trust is **broken**, despite the introduction of biometrics and other advancements over the years. This reality is producing serious and growing economic losses for the Canadian economy due to identity-related fraud and service delivery inefficiencies, but also threatens the integrity of the digital identity ecosystems that have been rapidly evolving over the past few years. These challenges, if left unresolved, will have a more pronounced impact on Canada's economy and will continue to impede Canadians' participation in the exponential growth of the worldwide digital economy.



This report contains a range of observations and recommendations, the sum of which make a persuasive case for the development and implementation of a national identity strategy. Together, they also make the case for additional initiatives to restore the Chain of Trust for Identity and pave the way for the evolving digital identity ecosystem.

A Foundational ID Special Interest Group

Over the course of 2021 and early 2022, the DIACC worked with a SIG to explore how the integration of Foundational IDs into the digital identity ecosystem could improve identity resolution between silos, introduce new efficiencies in service delivery, and reduce fraud. Members of the SIG included representatives from provincial Vital Statistics agencies and

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

digital identity initiatives, Immigration, Refugees and Citizenship Canada (IRCC), representatives from the Canadian financial and insurance sectors, as well as additional participants from the private and public sectors. The SIG members took part in 14 working sessions to explore work streams across various topics including birth records, impacts on service delivery and fraud, and roadmapping. In addition, the SIG Moderator and some of the members prepared a series of five technology demonstrations ([see listing and links in Annex 3](#)) to illustrate the business concepts of some of the proposed initiatives (as referenced in the sections below).

This section of the report outlines observations, conclusions, and recommendations including a list of 12 proposed initiatives that may be considered as a method to address and resolve some of these challenging issues facing our community today.

Observations

Birth and immigration records document the events that witness and create a legal identity. These records are foundational to an individual's identity in Canada and contain unique identifiers. Provincially, the Vital Statistics Agencies and federally, IRCC, are the authoritative sources for these Foundational IDs.



Birth records were instituted for statistical and other public health-related purposes. Immigration records were instituted to manage and control immigration. Legislation (provincial in the former case and federal in the latter) focuses on the original purposes of these registries, however, both are used as a form of ID in certain unique contexts. The provincial Vital Statistics Act and the Immigration and Refugee Protection Act do not recognize or support the ubiquitous use of the issued documents and underlying data sets as valid forms of ID in the generalized case.

The unique identifiers, in association with the legally-recognized names in these registries, have the potential to be used to efficiently resolve an identity between silos.

Identity Silos, Contextual IDs, and De Facto IDs

Many public and private sector silos in Canada capture and maintain contextual identity data. Each silo has traditionally issued and maintained Contextual IDs for its own program and/or service and jurisdiction or for commercial purposes (e.g., health cards, driver's licenses, passports, student IDs, employer-issued identity cards, etc.). The silos do not generally foresee

or plan for the use of their IDs in other silos and do not validate those identities for other relying parties. The consequences of this siloed structure include:

- Redundant processes and costs to create and maintain IDs
- Variable features and characteristics of an ID, especially security and privacy features
- Variable eligibility requirements for an ID
- Variable identity establishment processes, required evidence of identity, exceptions, and workarounds
- IDs containing unique identifiers that are resolvable only within one context and/or silo

Most Contextual IDs are not anchored to any external globally-unique identifier. Even when a Foundational Identity was used as evidence of identity in the issuance process, its unique identifier is not incorporated into the Contextual ID.

Some Contextual IDs have become accepted as *de facto* forms of ID in other silos (e.g., driver's licenses, passports, health cards, permanent resident cards, etc.). This has happened despite the fact that:

- There is no universal infrastructure for validating those IDs or for receiving notifications of status changes (i.e., document expiry, revocation, lost/stolen) or a change of name and/or death
- The issuing organization has made disclaimers regarding the uses of the ID for purposes other than those for which it was originally issued
- Forgeries of physical IDs can easily be obtained or created

Many government benefits and regulatory programs find it difficult to increase the Level of Assurance (above LOA2) of their IDs, given the lack of verifiable and incorruptible forms of evidence of identity.

Biometrics

Biometrics are sometimes used within given silos for verifying the identity of an individual. However, biometrics are not systematically used beyond the silo for which the identity was captured.

There is no “cradle to grave” biometric captured at birth that can be effectively used for identity verification through a person's lifetime, and there is no biometric that is actively captured at birth. Without this biometric anchor, identities are vulnerable to fraud as every enrolment process presents another opportunity for another person's biometric to be associated with an identity.

While facial photographs are widely used on printed IDs, there is no ubiquitous infrastructure for systematically verifying a person's identity against the authoritative source using this biometric. In many cases, human inspection is used against these printed photo IDs to verify identities, but this method is unreliable, and most attempts to automate this facial recognition from printed IDs (thereby using it as a biometric) only compare the holder's live image with the printed image, allowing fake IDs to pass the test.

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group.

To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca.

To join the DIACC community, visit www.diacc.ca.



Fraud

Identity fraud-related crime is significant and growing. Organized crime and determined criminals use fraudulent identities for the following purposes:

- Theft
- Evading criminal consequences
- Evading immigration processes/entry requirements
- Social benefits fraud
- Parental kidnapping
- Money laundering
- Financing and hiding the proceeds of crime
- Obfuscation of beneficial ownership of corporations for securities and tax fraud
- Terrorism (domestic and international)



Identity fraud-related crime is easy and lucrative for perpetrators because:

- A person's identity information can be obtained relatively easily by collecting information found on social media platforms or by accessing readily available (on the dark web) data exposed by the continuing data breaches of corporate and government databases
- A synthetic identity can be created relatively easily
- A biometric can easily be associated with a stolen or synthetic identity
- Resolving identities between identity silos is problematic because of:
 - The reliance on imperfect name-matching methodologies
 - The lack of unique identifiers that can be used on a national scale
 - The lack of infrastructure for validating all forms of ID
 - The ease with which false identity documents can be created
 - The ease with which a false or stolen identity can be enrolled in a legitimate program, creating a valid Contextual ID

Comprehensive and detailed information on the impacts of fraud in Canada is not readily available. The following information is not openly shared across all sectors:

- The frequency of identity fraud-related crime
- The most common attack vectors
- The amounts of losses by sector
- Other impacts (e.g., loss of reputation and trust at the local, national, and international levels)

Service Delivery

Each program/service, jurisdiction, or commercial enterprise incurs significant costs to capture, validate, and maintain the identity information of their clients/stakeholders. These identity-proofing processes rely on Contextual IDs from other silos, and most rely on name-matching methodologies to resolve identities.

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

The lack of unique identifiers and tamper-proof, verifiable identity documents increases the risk for these organizations, compelling them to mitigate the increasing effort and cost to discharge their mandate.

Programs that have a mutual exclusion requirement (e.g., an individual can only be enrolled in one provincial health insurance plan) cannot effectively detect multiple enrolments.

Service delivery would benefit from trusted digital ID credentials.

Conclusions

The siloed identity system that has evolved in Canada over the past decades lacks certain unifying integrations leaving many gaps, inconsistencies, and vulnerabilities amongst and between the silos, which we have characterized as a *broken Chain of Trust* in identity. This has, and continues to result in, significant service delivery inefficiencies and identity-related fraud.



Identities established through this broken Chain of Trust are lacking one or more of the following characteristics of a “Trusted ID”:

- Resolves to a single individual **at the national level**
- Easily proven to be authentic
- Is tamper-proof, and is impossible to make unauthorized changes to the identity information
- Contains safeguards to prevent its misappropriation
- Enables changes to the contained information (names, death) and status (revoked, lost/stolen, expired) to be expediently dispatched to relying parties
- Enables the holder to be reliably verified as the Subject of the ID in conformance with legislation, policy, and regulations within a specific context
- Enables the holder to maintain control of the ID, enhancing privacy and security
- Book of names must not contain undiscovered fraudulent or erroneous records

Canada’s siloed identity system is further lacking:

- A strategy for identity resolution between existing silos
- Common standards for core components (ie credentials, authentication, sharing/interoperability)
- A roadmap on how to create, both physical and digital, Trusted IDs as described above, where these IDs would be:
 - Properly supported in legislation
 - Backed by a national-scale infrastructure
 - Universally accepted

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

- Knowledge sharing between all interested and invested parties on identity fraud and related crime to identify:
 - The size of the problem
 - Its root causes
 - Mitigation strategies
- A methodology for continually testing and improving our identity system

In spite of ongoing progress in building a robust digital identity ecosystem, we are populating this ecosystem with identities that were established through this broken Chain of Trust, and in doing so, we are entrenching and amplifying the harms of the past and creating new risks.



Recommendations

As the digital identity ecosystem continues to grow and evolve at an increasingly rapid pace, we must simultaneously work to restore the Chain of Trust by establishing a Trusted ID at a pan-Canadian scale. A Trusted ID, that is created, maintained and consumed independently of any silo, can be achieved by:

1. Developing a National Identity Strategy for Trusted IDs.
2. Formalizing the concept of Foundational ID such that it can be incorporated into the applicable policy frameworks, regulations, or legislation.
3. Transforming Birth Certificates and immigration documents into true Foundational IDs, such that they:
 - Recognize the rights of holders to use them as IDs, which will require changes in the related policies and legislation
 - Enhance security and privacy by issuing them in a digital format
 - Adopt best practices when issuing IDs in physical forms
 - Identify and close gaps in processes to issue and maintain these artifacts as true Foundational IDs (instead of birth certificates or immigration documents).
 - Provide the holder with the ability to control who sees and uses the identity information
4. Leveraging Foundational ID unique identifiers to improve identity resolution for Contextual IDs
5. Implementing mutual exclusivity detection/enforcement for programs that have that mandate (e.g., driver's license, health insurance, etc.). See Annex 1 below for a further discussion of this recommendation.

The identity system and the economy as a whole will benefit from a Trusted ID in:

- Reducing duplication and cost

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

- Standardizing the level of trust afforded to any ID by using standard Levels of Assurance
- Having a single source of identity-related notifications such as change of name, death, identity theft, change of status (e.g., expiration, revocation, lost/stolen, fraudulent activity detected) of identity instruments
- Allowing program administrators to focus more on an applicant eligibility and less on ID-proofing



Holders of the Trusted ID will benefit by:

- Making it more difficult to forge Foundational ID documents
- Reducing the value of forged Foundational ID documents
- Making it more difficult to misappropriate Foundational ID documents
- Providing a mechanism for all relying parties to validate Foundational ID documents
- Detecting and preventing the multiple (fraudulent) uses of a legitimate identity
- Receiving notification of when/where their ID is being used (much like some online accounts e.g. Google)
- Making it more secure and enhancing privacy

Trusted ID will improve the ability of any relying party to resolve an identity to a single person by:

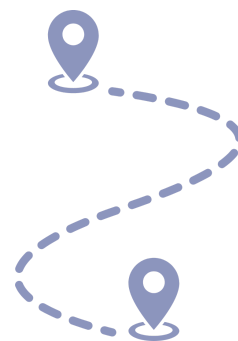
- Leveraging unique identifiers from foundational sources for all forms of identity
- Consolidating and improving legal change of name processes, including for marriage use cases
- Leveraging biometrics and defining the life cycle of an ID with associated biometrics to achieve a cradle-to-grave biometric anchor

The next section lists proposed initiatives that would implement the above recommendations.

Proposed Initiatives

The proposed initiatives are distributed over a number of years starting in 2023 (Year 1). The description of the initiatives contain links to demo application videos that are illustrative to a proposed initiative. Additional detail for these initiatives can be found in the [broader roadmap](#). Two additional initiatives that were only briefly explored in the SIG working sessions are included in Annex 1.

The authors recognize the significant challenge of proposing such far-reaching cross-jurisdictional initiatives, so the dates proposed



Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

are hypothetical and represent target years and a sequencing of initiatives for maximum impact.

1. **Develop a national identity strategy:** Develop, or enhance, a national identity strategy for all major Foundational and Contextual IDs, including recognizing their status/use as ubiquitous IDs and holder's rights and expectations, ID services, proper identity resolution between silos, etc. There should be a particular focus on strengthening ID verification and proofing processes.

- Goals:
 - To recognize the fundamental nature of Foundational ID and entrench the *de facto* use of certain Contextual IDs outside their original silos
 - Support holder's rights and expectations in their use of these IDs
 - Provide a more coherent and integrated identity system
 - Support the transition to a digital identity ecosystem
- Stakeholders:
 - CIO Strategy Council
 - Provincial identity initiatives
 - Government service card issuers
 - Treasury Board of Canada Secretariat
 - Public and private sector issuers of Contextual IDs
 - Public and private sector relying parties
- Timeframe: Immediate and ongoing



2. **Improve the security of our identity system:** Establish an open dialogue on identity fraud and security among stakeholders and develop/implement a pan-Canadian regime to improve security.

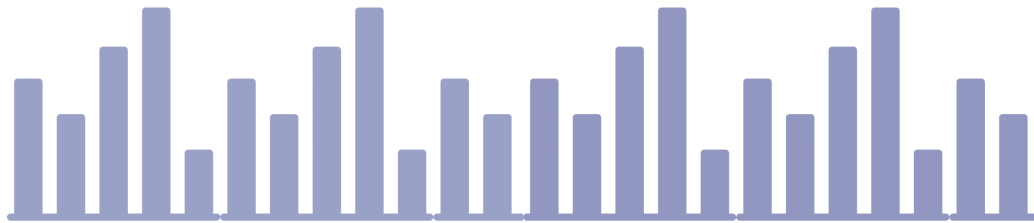
- Goals:
 - Increase the security of the identity system
 - Reduce opportunities for fraud
- Stakeholders:
 - Royal Canadian Mounted Police National Cybercrime Coordination Unit (NC3)
 - Provincial police forces
 - Canadian Anti-Fraud Centre
 - Financial Action Task Force (FATF)
 - Financial institutions
 - Canada Border Services Agency (CBSA)
 - Immigration, Refugees and Citizenship Canada (IRCC)

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

- Public sector issuers of identities, including provincial issuers, Vital Statistics Agencies, etc.
 - Timeframe: Immediate and ongoing
-

3. **Vital statistics central validation:** Deploy a central validation service for birth certificates that provides an authorized relying party the ability to validate a birth certificate issued in any Canadian province or territory ([demo #1](#)).

- Goals:
 - Leverage unique identifiers binding to legal name
 - Lessen reliance on name-matching for identity resolution
- Stakeholders:
 - All Vital Statistics Agencies
- Timeframe: As soon as possible (in parallel with Vital Stats modernization efforts), initial deployment year 1, onboarding relying parties years 2 and 3.



4. **Vital statistics death and legal change of name notification:** Deploy a death and legal change of name notification service from vital stats for all relying parties ([extension of demo #1](#)).

- Goals:
 - Reduce the opportunity for identity-related fraud
- Stakeholders:
 - All Vital Statistics Agencies
- Timeframe: Immediately following Vital Stats Central Validation (in parallel with Vital Stats modernization efforts), initial deployment year 2, onboarding relying parties years 3 and 4.

5. **Immigration validation:** Deploy a validation service for immigration documents (permanent resident, temporary resident, citizenship). ([extension of demo #1](#)).

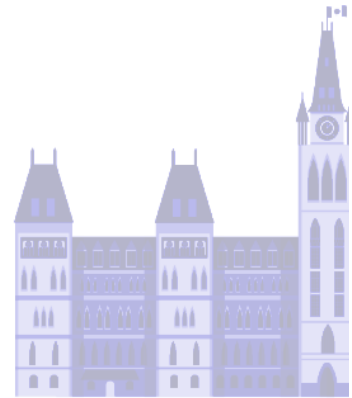
- Goals:

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

- Leverage unique identifier binding to legal name
- Lessen reliance on name-matching for identity resolution
- Stakeholders:
 - Immigration, Refugees and Citizenship Canada (IRCC)
- Timeframe: As soon as possible, initial deployment year 2, onboarding relying parties years 3 and 4.

6. **Contextual ID Central Validation:** Deploy a central validation service for other key Contextual IDs, primarily driver's licenses, and potentially health and government services cards. ([extension of demo #1](#)).

- Goals:
 - Reduce the opportunity for identity-related fraud
- Stakeholders:
 - Canadian Council of Motor Transport Administrators (CCMTA) and individual Ministries of Transportation
 - Health and Government Services
- Timeframe: As soon as possible, initial deployment year 1 and 2, onboarding relying parties years 3 through 5.



7. **Anchor Contextual IDs:** Embed Foundational ID unique identifiers in major Contextual IDs, primarily driver's licenses, health and government services cards.

- Goals:
 - Reduce the opportunity for identity-related fraud
- Stakeholders:
 - Individual Ministries of Transportation
 - Health and Government Services
- Timeframe: Immediately following Vital Stats & Immigration Central Validation, deployment to initial Contextual IDs year 2 and 3, onboarding remaining IDs years 3 through 5.

8. **Central Birth Certificate Verifiable Credentials Issuance:** Deploy a central service that uses the National Routing System (NRS) validation services in all provinces and territories to issue a birth certificate Verifiable Credentials automatically by validating existing shared secrets ([enhancement of demo #2](#)).

- Goals:

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

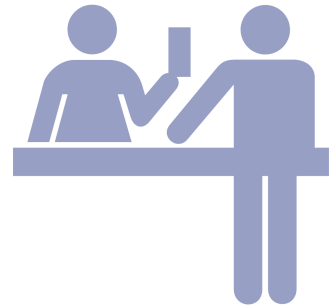
- Accelerate onboarding of population to a digital wallet infrastructure
- Strengthen relationship between Vital Statistics Agencies as issuer and person (opportunities for future transactions)
- Agency to the holder, provide better convenience for proving one's identity
- Increase Level of Assurance in combination with other Verifiable Credentials
- Reduce the opportunity for identity-related fraud



- Stakeholders:
 - All Vital Statistics Agencies
- Timeframe: Immediately following Vital Stats & Immigration Central Validation, deployment to initial Contextual IDs year 2 and 3, onboarding remaining IDs years 3 through 6.

9. **Notification of Validation to Holder:** Deploy a notification service to notify holder of a Verifiable Credential when validation of traditional birth certificate or immigration document is validated ([extension of demo #2](#)).

- Goals:
 - Earlier detection of fraud by holder, reduce impact of fraud
- Stakeholders:
 - All Vital Statistics Agencies
 - Immigration, Refugees and Citizenship Canada (IRCC)
- Timeframe: Year 4 after Verifiable Credentials are issued and Contextual IDs are anchored to Foundational IDs.



10. **Foundational ID Authoritative Source Verifiable Credentials Issuance:** Vital Stats and immigration agencies to each implement the issuance of Foundation ID Verifiable Credentials, including birth certificates, permanent and temporary resident, and citizenship Verifiable Credentials ([extension of demo #4](#)).

- Goals:
 - Strengthen relationship between Vital Statistic Agencies as issuer and citizen (opportunities for future transactions)
 - Agency to the holder, provide better convenience for proving one's identity
 - Increase LOA in combination with other Verifiable Credentials
 - Reduce the opportunity for identity-related fraud



Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

- Stakeholders:
 - Individual Vital Statistics Agencies
 - Immigration, Refugees and Citizenship Canada (IRCC)
- Timeframe: Result of Vital Statistics and Immigration modernization for identity. Years 4 through 6, onboarding population years 6 through 10.

11. CPIC reporting of lost or stolen IDs: Leverage the Canadian Police Information Centre (CPIC) for issuing Contextual IDs/Foundational ID issuers to report lost or stolen IDs.

- Goals:
 - Strengthening the security of the identity ecosystem
- Stakeholders:
 - Royal Canadian Mounted Police
 - All Vital Statistics Agencies
 - Immigration, Refugees and Citizenship Canada (IRCC)
 - All Contextual ID issuers
- Timeframe: Year 2



12. Monitoring for fraudulent uses of an identity: Use (in a privacy-respecting manner) the correlation between a Foundational ID and its uses to detect/prevent fraud. For example, if an identity is resident in one province, but then it appears out of the blue for very specific use cases somewhere else, it could be flagged as fraudulent.

- Goals:
 - To make it harder for someone to claim and use another's identity
- Stakeholders:
 - Vital Statistic Agencies
 - Immigration, Refugees and Citizenship Canada (IRCC)
 - Canada Border Services Agency (CBSA) as holders of unique identifiers
 - Major Contextual ID issuers
- Timeframe: Years 4 and 5 - Can be implemented once Contextual IDs are anchored to Foundational IDs



Call to Action

The scope, pace, and complexity of the global digital economy places a premium on trust and protection against fraud and hacking as never before.

With trust, the sky's the limit for what Canadians, governments, and the private sector can achieve to promote economic growth, attract investment, create jobs, strengthen service delivery, and enhance citizen engagement.



Without trust, the consequences could be deep and long-lasting, relegating Canada to the status of a global digital afterthought.

With these high stakes, the DIACC believes that Canada requires greater attention on the infrastructure required to foster this trust.

This report demonstrates conclusively that the siloed identity system that has evolved in Canada over the past decades is fractured and contains many gaps, inconsistencies and vulnerabilities, which has and continues to result in significant service delivery inefficiencies and significant identity-related fraud. Further, these gaps and vulnerabilities are widely distributed, deeply entrenched, and their effects are migrating to the evolving digital identity ecosystem.



The DIACC calls on governments and the private sector to work collaboratively to develop a comprehensive national identity strategy that fully integrates foundational sources of identity and to take measured steps over the next few years to restore the Chain of Trust for identity and secure Canada's digital future. We are ready to provide any assistance to help move Canada toward this critical goal.

Annex 1 – Additional Initiatives

The below initiatives were discussed briefly at the SIG but were not studied adequately and are therefore not among the DIACC's recommendations. These are included here for completeness sake, but would require additional study.

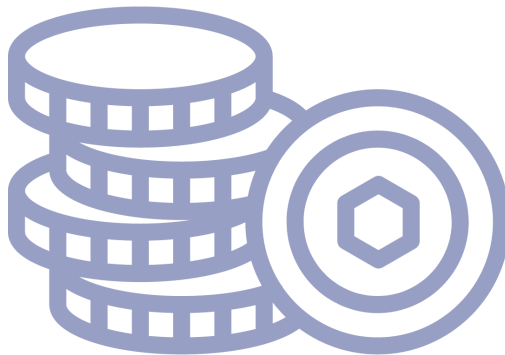
Mutual Exclusion Tokens for program enrolment

Certain programs and permits have legislated requirements limiting enrollment to one jurisdiction. Examples include:

- Driver's license, limited to one province or territory
- Provincial health insurance, limited to one province or territory
- Canada Revenue Agency allows an individual to only declare one province or territory of residence

Members of the SIG would like to explore the creation of a "Mutual Exclusion Token" or similar mechanism in a Verifiable Data Registry that would ensure that a unique identity (Foundational ID) could only be enrolled in one program of a given type (e.g., provincial health insurance plan) within Canada.

This would protect the program against fraud and the individual against identity theft, as it would catch the use of a unique identity (Foundational ID) in multiple jurisdictions. The task would be to identify one or more mechanisms to implement the Mutual Exclusion Token within technologies currently in use and to address any issues that may arise. A key design principle for such a mechanism would be to enforce these requirements without resorting to a traditional registry that could be misused as some form of surveillance or be a target for a data breach or other attack that would compromise a person's privacy.



Relationships as the DNA of an identity

In this time of data breaches and social media, there are few items of personally-identifiable information that aren't discoverable. Knowledge-based proofs of identity (such as "Mother's

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group.
To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca.
To join the DIACC community, visit www.diacc.ca.

maiden name”, or the “name of a pet”) are becoming more unreliable as a means of identity verification, given the amount of data that has been breached or posted willingly to social media. Social engineering of these “secrets” is becoming easier.

Throughout an individual's life experience, they develop associations/relationships with other people, places, and things. Some of the key associations start with the association to mother and father (which is captured in an individual's foundational birth record), places of residence, schools attended, job positions held, spouses, children, and even long-lasting friendships. This collection of relationships is like the DNA of an individual's identity, and could conceivably be tested as a way to verify that identity.

Members of the SIG would like to explore the application of “Verifiable Relationships” to maintain and use this identity DNA in the context of a unique (foundational) identity for the purposes of establishing a high level of identity assurance.

Annex 2 – Fraud Scenarios

This Annex includes scenarios that highlight the ease with which synthetic identities can be produced in using established identity proofing processes and identity documents in Canada. Bad actors take advantage of these vulnerabilities to commit identity theft and fraud which can cause significant economic losses to the individuals, companies and governments that accept the synthetic identity resulting in significant stress and hardship for those affected.

Let's start by introducing the main character that will be involved in the different scenarios:

Wally is the target of identity theft. He:

- Is 26 years old
- Lives in Vancouver B.C., where he was born and grew up
- Studied marketing at UBC, obtaining a Bachelor of Commerce
- Works part-time as a waiter in a bar
- Has a decent credit score at 620

The lawful scenario shows the typical steps for obtaining identity documents. In the unlawful scenarios, we show some of the ways the gaps between the silos of identity can be exploited to steal an identity and create a synthetic identity, and then to subsequently perpetuate financial crimes.

Scenario 1: Lawful - Wally moves to a different province

In this scenario, Wally moves to Toronto, Ontario for a high-paying job with a tech start-up. Because he now lives in Ontario, Wally needs to get an Ontario Driver's licence (required after living in Ontario for 60 days) and register for the Ontario Health Insurance Program (OHIP) (required to get free health services in Ontario). Wally also wants to open a new bank account at the local neighbourhood branch of a chartered bank. He is not a customer of this bank and was attracted by their \$500 promotion for new customers who open an account with them.

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.

To exchange his BC driver's license for an Ontario driver's license Wally will need to:

- Apply in-person at a DriveTest centre or a ServiceOntario location
- Take an eye test
- Bring originals of his accepted identity documents showing his legal name, date of birth and signature
- Bring his original, valid out-of-province/foreign driver's license
- Bring any original supporting documents that show proof of his driving experience
- Pay the applicable fees
- Fill out an application form where he will state how long he has been driving

Source: [Drivers License | Exchange out of province drivers license](#)

Scenario 2: Unlawful – A fraudster obtains some of Wally's information and uses it to obtain a fraudulent loan

Fred, one of the casual labourers hired by the moving company to move Wally's possessions to Ontario occasionally frequents the bar where Wally works part time, so he strikes up a conversation with Wally on his break. The conversation turns to Wally's father who recently passed away and Wally shows him the obituary that he just posted to his social media.

When Fred gets home, he searches Wally's Facebook page and finds the obituary, where he notes the following information about Wally's parents:

- City/Province of birth
- Surname (maiden name for his mother)
- Given names

Fred takes that information along with Wally's date of birth that he found in some documents that he handled when working at Wally's house and proceeds to order 2 copies of Wally's birth certificate using the [BC Vital Statistics online ordering page](#). He also orders 2 different BC driver's licenses from the dark web using photos of individuals that are vulnerable due to their addictions and who have been enticed into criminal activity. Fred sends one of the false driver's licenses and a copy of the birth certificate to his partner in crime, Jay, who operates out of Winnipeg.

Fred uses the one false identity to quickly open a bank account in Wally's name and apply for a \$25,000 loan in Penticton. He gives the vulnerable person \$500 of that money and they part ways. Fred takes the \$24,500 that is left and takes a trip to Las Vegas, where he lives la vida loca for a weekend.

Scenario 3: Unlawful - A slightly more sophisticated gift

Jay, on the other hand, is slightly more sophisticated. He takes the birth certificate and false driver's license and applies for a Manitoba driver's license. Jay proceeds to exchange the false BC driver's license for a Manitoba driver's license as follows:

- Visits any Autopac agent or Manitoba Public Insurance Centre

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group.

To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca.

To join the DIACC community, visit www.diacc.ca.

- Brings originals of his [accepted identity documents](#) showing a legal name, date of birth and signature. Jay presents:
 - the fake BC driver's license and Service Card
 - the stolen BC birth certificate
- Brings his original, valid out-of-province/foreign driver's license
- Brings any original supporting documents that show proof of residency. Jay presents:
 - a fake Residential Lease Agreement
 - a fake employment letter
- Pays the \$65 fee

Source: [Manitoba Public Insurance | Get A License | New To Manitoba](#)

Jay receives the Manitoba driver's license in 45 days. Before he does anything with this identity, he processes a Legal Change of Name to reduce the chance that someone connects the identity to the rightful owner. Jay proceeds as follows:

Jay completes the Application for a Legal Change of Name form and sends the completed form to the Vital Statistics office via registered mail. He includes:

- The original stolen BC birth certificate
- A copy of the new Manitoba driver's license
- \$120 fee

Vital Statistics will send the Manitoba Legal Change of Name and Fingerprinting Information Sheet with additional information and instructions on how to complete civil fingerprinting for a legal change of name.

Jay signs a waiver and brings the Manitoba Legal Change of Name and Fingerprinting Information Sheet to a fingerprinting agency who submits his fingerprints to the RCMP to search whether his fingerprints match an entry in its National Repository of Criminal Record Information.

If a match is found in the criminal records, the new name is added to that record as an additional name for the individual. Regardless of this result, Manitoba Vital Statistics processes the legal change of name application and mails the certificate of change of name to the applicant within ten business days of receiving confirmation from the fingerprinting agency.

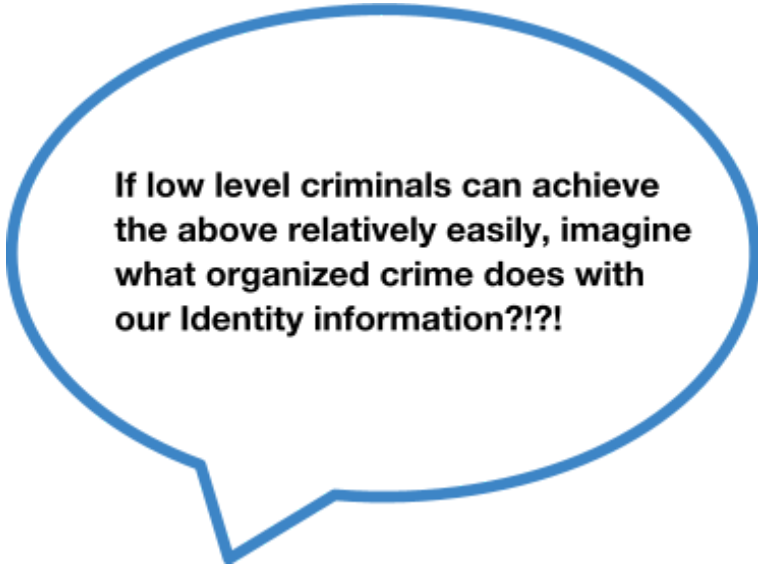
Source: [Legal Change of Name | Manitoba Vital Statistics Branch | Province of Manitoba](#)

Jay takes the change of name certificate and updates his Manitoba driver's license. He gets a cell phone and opens a bank account in the new name. Over the next three years armed with the birth certificate, change of name certificate, and updated driver's license, Jay opens additional bank accounts and credit cards, buys and sells cars (starting with a beater but moves up to more and more expensive cars over time), and generally lives under the assumed

name while making regular payments on his credit accounts. He fills the bank accounts with proceeds of his drug dealing, making it appear as legitimate employment income.

In the 4th year he uses his three years of credit history and 800 credit score to:

- Run up credit card debts to \$125,000
- Sells the synthetic identity for \$5,000 to an illegal immigrant who needs medical care
- Disappears to do it all over again in another jurisdiction with another synthetic ID



**If low level criminals can achieve
the above relatively easily, imagine
what organized crime does with
our Identity information?!?!**

Annex 3 - Demonstrations

Video	Description	Contributors
Demo #1: Relying Party Validation	Demo #1 is a traditional Document Validation use case, where a subject applying for a service would present an identity document to a private or public sector service provider to prove their identity and receive a benefit.	<ul style="list-style-type: none"> • Valid8ID Solutions • Axiell
Demo #2: Proxy Issuer of Electronic Birth Certificate	Demo #2 is a Birth Certificate Verified Credentials issuance use case, where a subject would obtain an electronic version of their Canadian Birth Certificate from a central proxy service. The proxy service validates the Birth Certificate information against the appropriate provincial Vital Statistics database and issues a corresponding Verifiable Credential to the Subject's Digital Identity Wallet.	<ul style="list-style-type: none"> • Valid8ID Solutions • Interac • Axiell
Demo #3: Birth Certificate Verifier-Health Card Issuer	In Demo #3, the Ontario Ministry of Health verifies an out-of-province Electronic Birth Certificate without connecting it to its issuer and issues a health card Verifiable Credential to the applicant's wallet. This is an example of a Contextual ID based on the evidence of a Foundational ID.	<ul style="list-style-type: none"> • Valid8 ID Solutions • Interac
Demo #4: Authoritative Issuer Demo	Demo #4 is a demonstration of a Verifiable Credential issuance from the province of Manitoba Vital Statistics. It leverages existing online ordering processes to order an electronic birth certificate as a Verifiable Credential to an Self Sovereign Identity (SSI) wallet belonging to a citizen born in Manitoba.	<ul style="list-style-type: none"> • Axiell • Northern Block
Demo #5: Age/Date of Birth Verification	Demo #5 is a demonstration of a proof request from Law Firm Ottawa, an external organization (Verifier) used to verify the authenticity of the presented Verifiable Credential.	<ul style="list-style-type: none"> • Northern Block

Contents of this paper have been submitted by the DIACC Foundational ID Special Interest Group. To learn more about the findings or to explore collaboration opportunities, contact info@diacc.ca. To join the DIACC community, visit www.diacc.ca.