DIGITAL IDENTITY – A VISION FOR CANADIAN PROSPERITY AND INCLUSION

Digital ID and Authentication Council of Canada

JONI BRENNAN
Présidente
DIACC

DIACC

CYBER SECURITY CONFERENCE 2020

VIRTUAL EDITION

DIACC

$48-97 Billion

3-6% +GDP

Economic Impact of Identity in Canada

Source: McKinsey & Co https://www.mckinsey.com/featured-insights/innovation-and-growth/the-value-of-digital-id-for-the-global-economy-and-society

Digital Identity

Digital Identity

is a foundation of digital transformation

Canadians need to know what **data** exists **about them**

DIACC

Canadians need to know what **data** exists **about them**

Citizens, governments, & businesses need **tools to manage sharing**

DIACC

What do Canadians think about digital identity?

Canadians’ Perspectives on Identity and Privacy

DIACC

Source: https://smartcityprivacy.ca/survey-results/

Canadians’ Perspectives on Identity and Privacy

88% Concerned at some level about their privacy in the context of smart cities.

Source: https://smartcityprivacy.ca/survey-results/

Canadians’ Perspectives on Identity and Privacy

88% Concerned at some level about their privacy in the context of smart cities.

72% For-profit sale of personal data related to smart cities should be prohibited.

DIACC

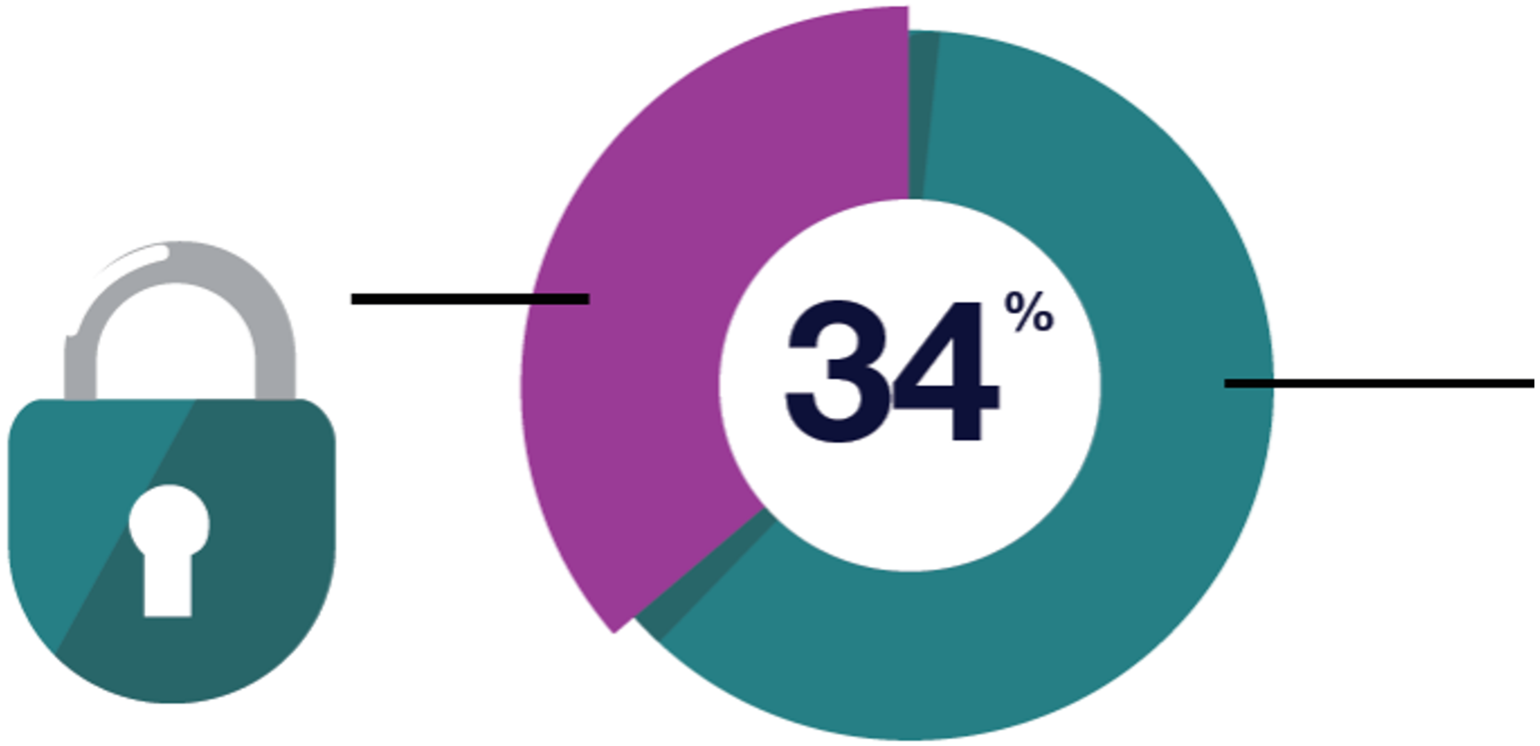
Source: https://smartcityprivacy.ca/survey-results/

Canadians’ Perspectives on Digital Identity

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians’ Perspectives on Digital Identity

Canadians are concerned with how social media sites use their personal information; **Just one-third** trust social media sites to keep their personal information **safe and secure.**

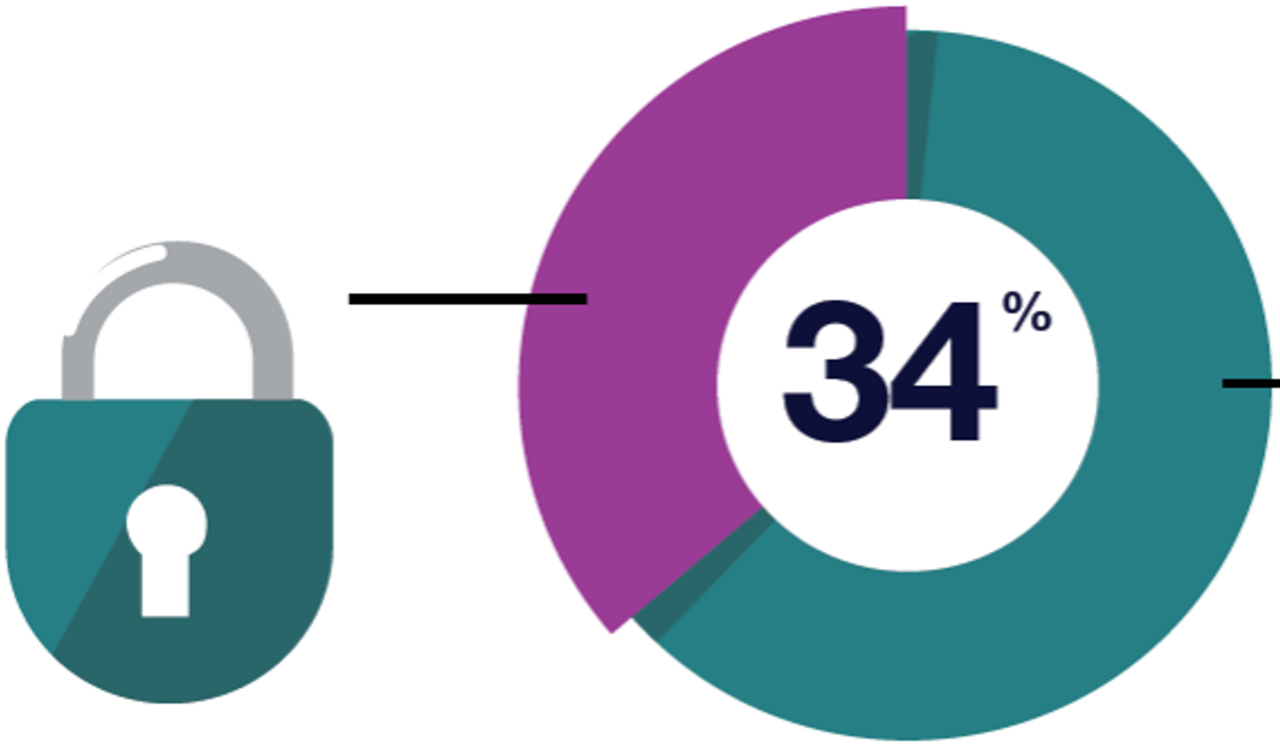


DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians’ Perspectives on Digital Identity

Canadians are concerned with how social media sites use their personal information; **Just one-third** trust social media sites to keep their personal information **safe and secure.**



compared to ~4-in-5

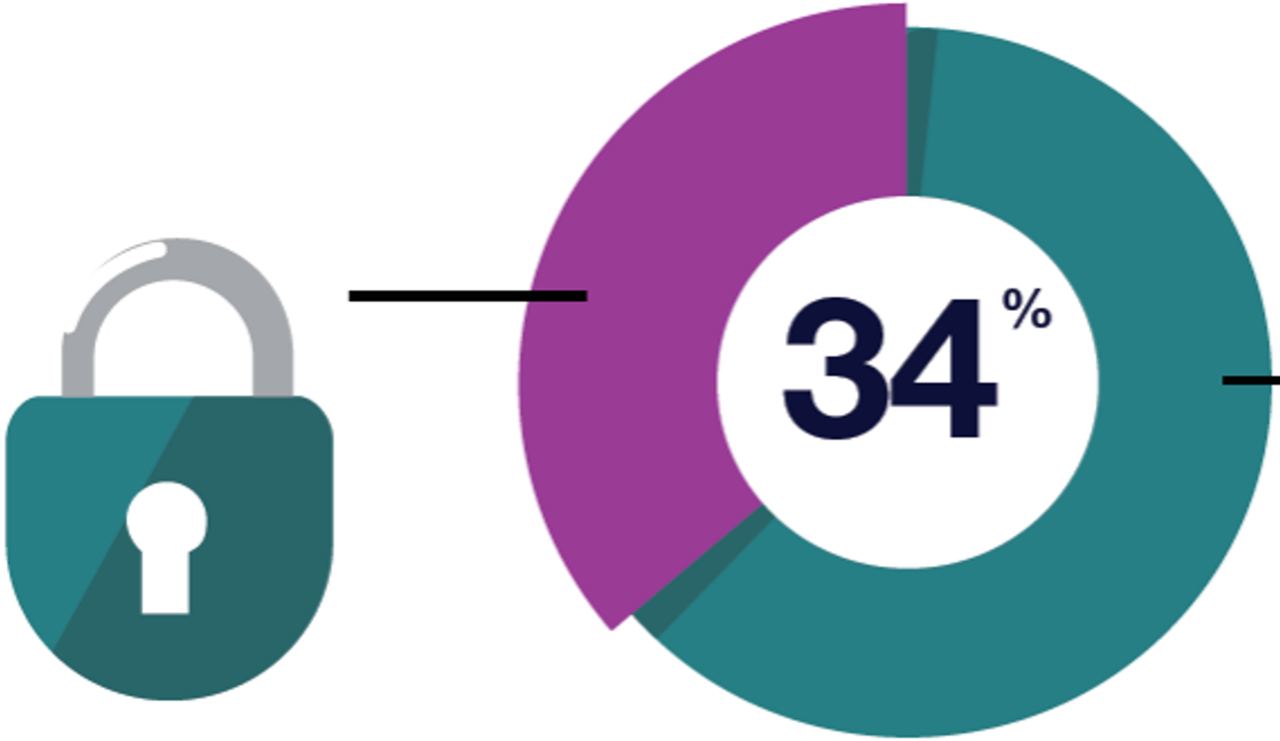
83% trusting the government

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians’ Perspectives on Digital Identity

Canadians are concerned with how social media sites use their personal information; **Just one-third** trust social media sites to keep their personal information **safe and secure.**



compared to ~4-in-5

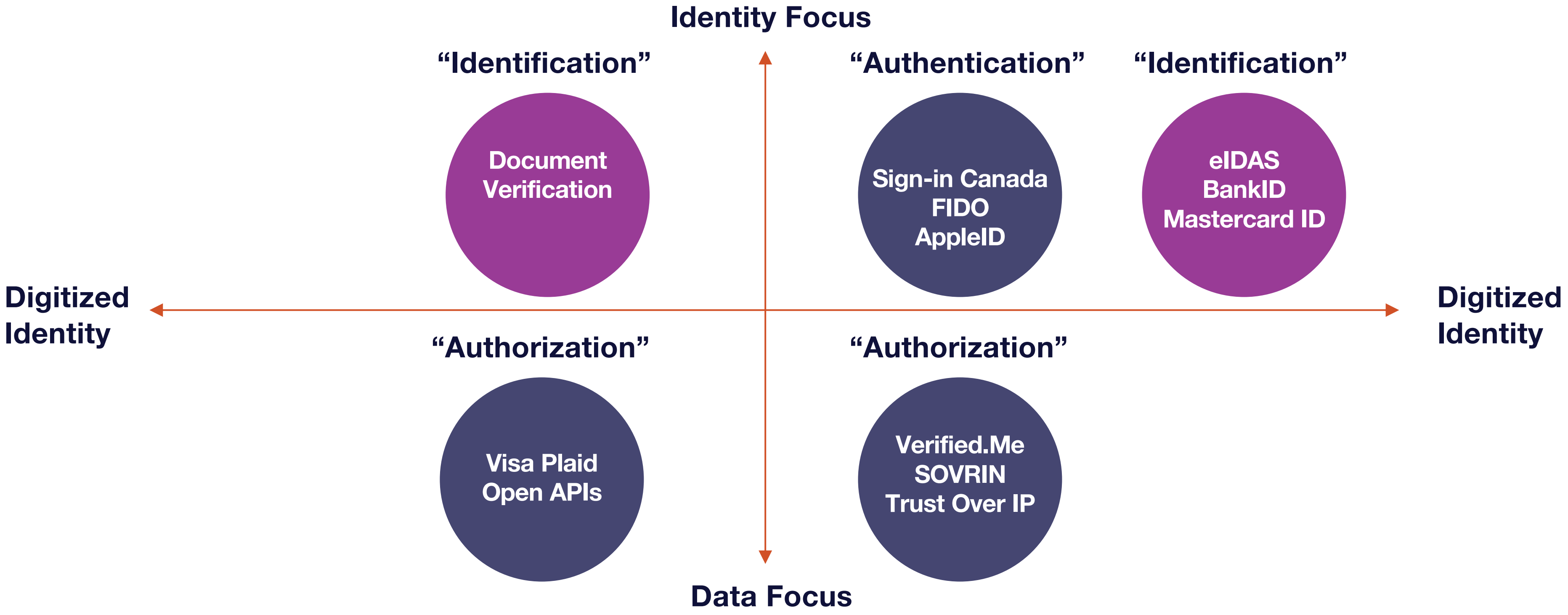
83% trusting the government

81% trusting financial institutions

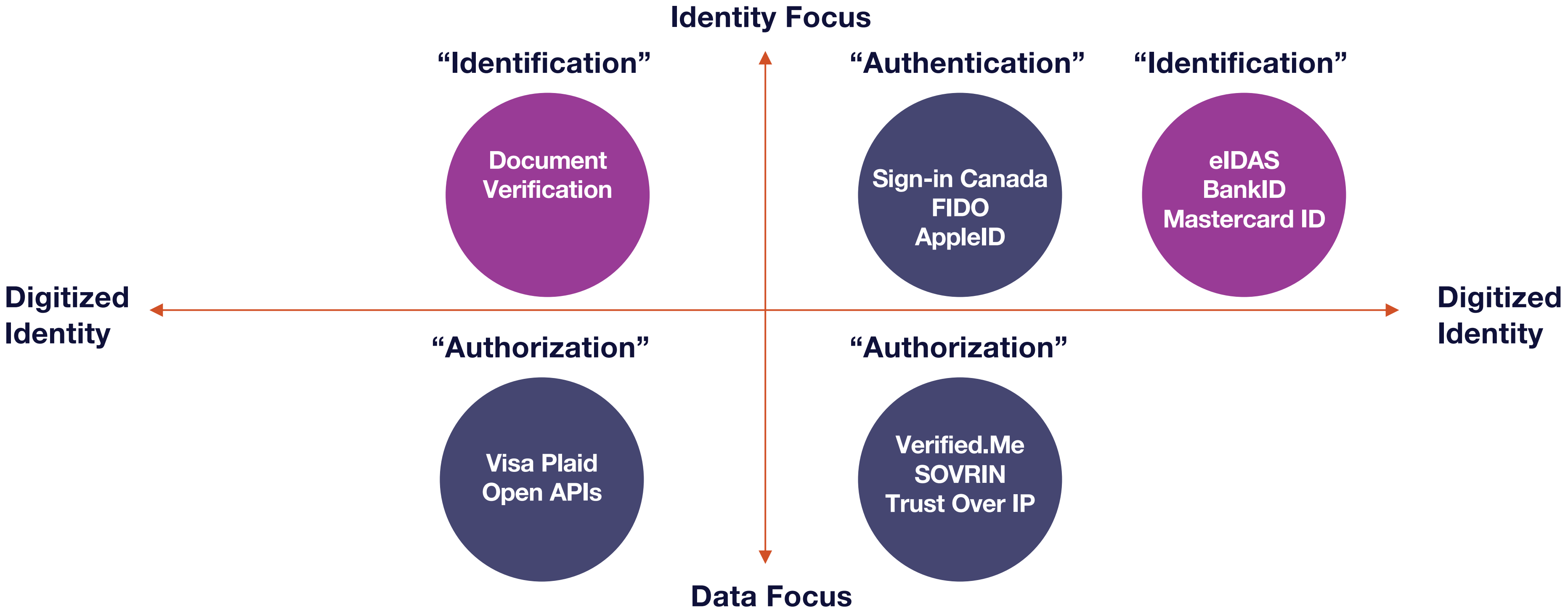
Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

What does digital identity look like today?

What does digital identity look like today?



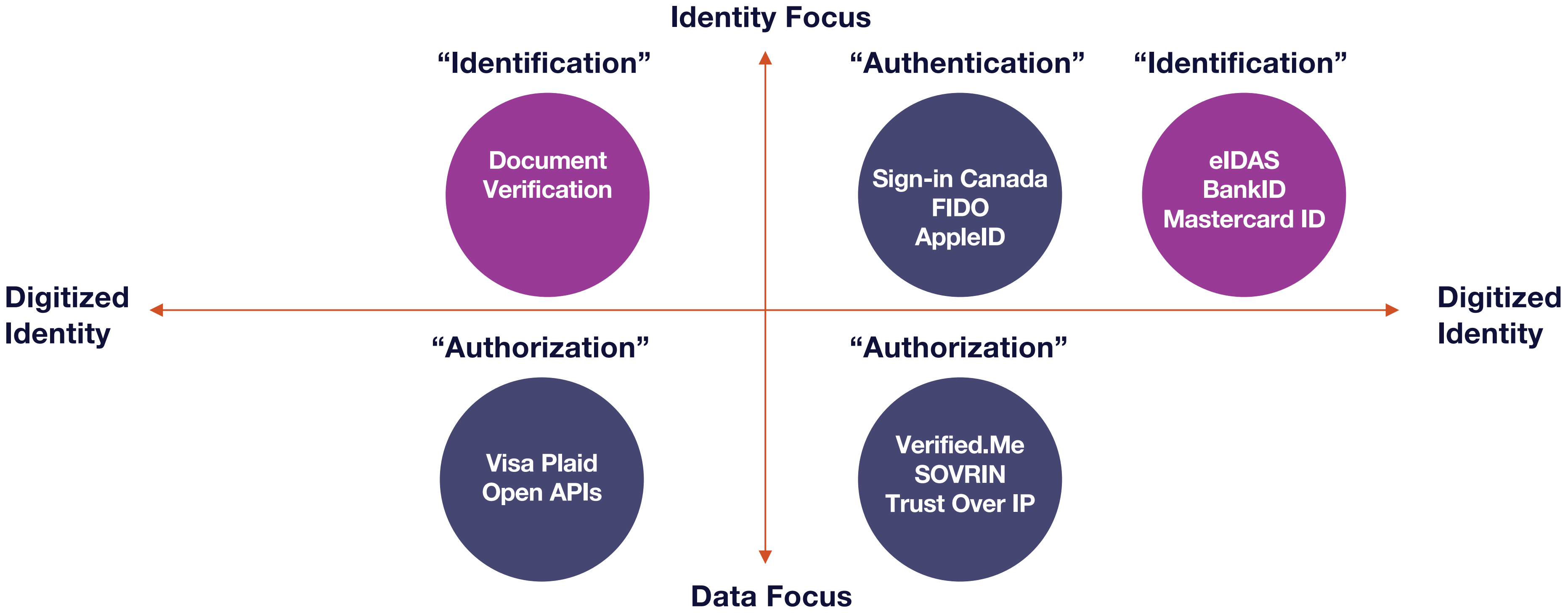
What does digital identity look like today?



Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

What does digital identity look like today?



Theme: Identity vs Identification

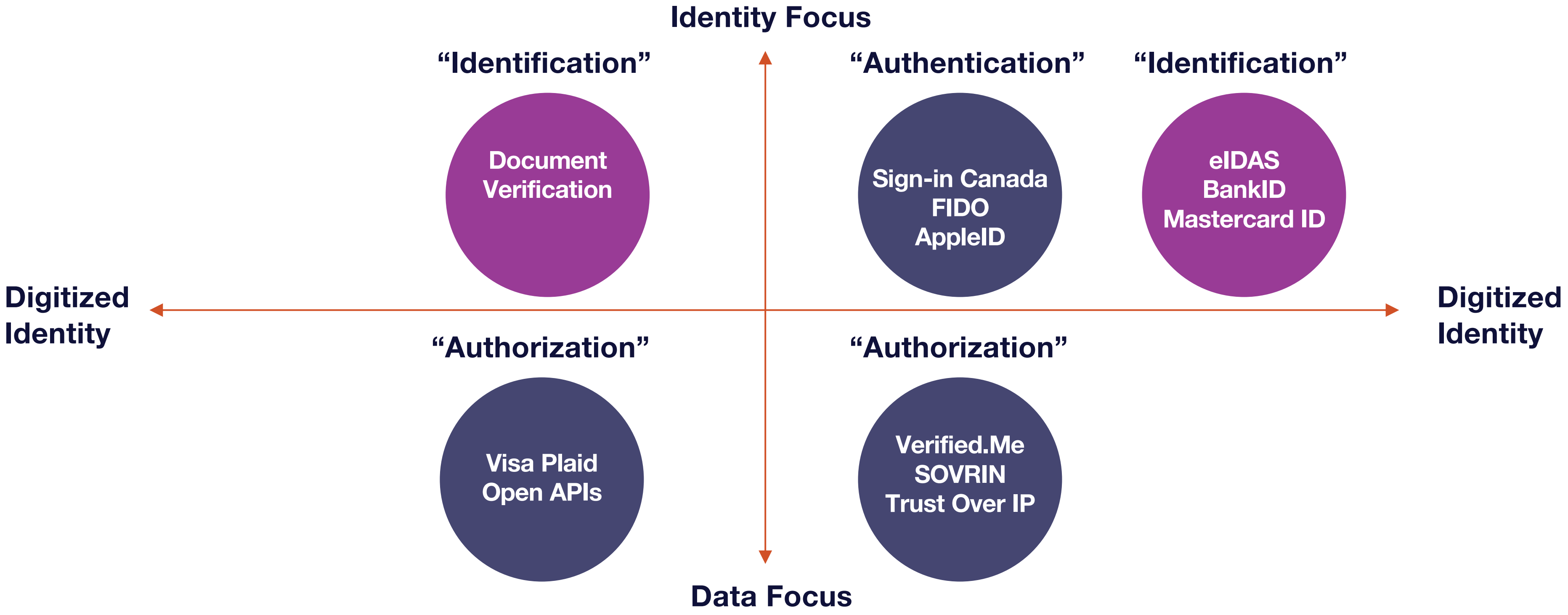
Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

Theme: Identity vs Data

Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

Big tech companies that have amassed huge data are also increasingly dabbling with identity.

What does digital identity look like today?



Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

Theme: Identity vs Data

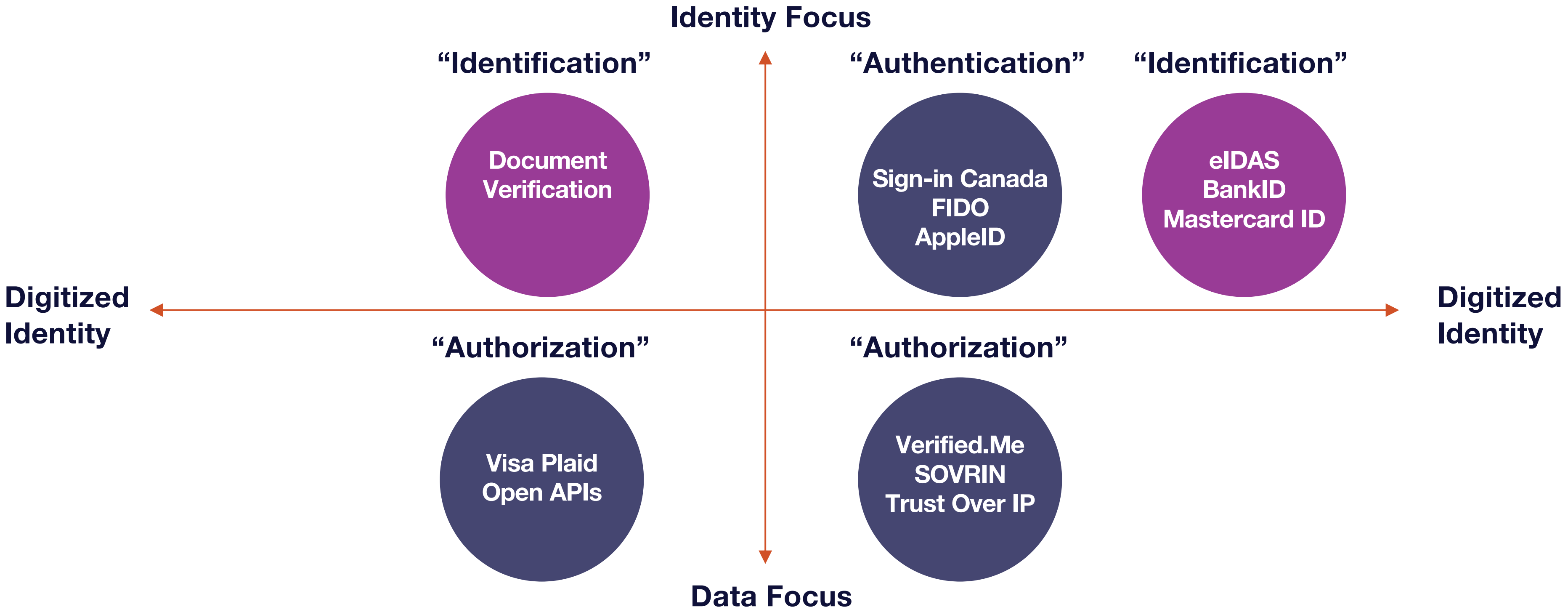
Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

Big tech companies that have amassed huge data are also increasingly dabbling with identity.

Theme: Data Integrity

Ensuring the integrity of data is key to trusted digital identity. This has brought cryptography to the fore, especially in the development of Verifiable Credential standards.

What does digital identity look like today?



Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

Theme: Identity vs Data

Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

Big tech companies that have amassed huge data are also increasingly dabbling with identity.

Theme: Data Integrity

Ensuring the integrity of data is key to trusted digital identity. This has brought cryptography to the fore, especially in the development of Verifiable Credential standards.

Theme: Governance

Decentralized identity standards enable the rails. Trust frameworks are needed to set the rules.

On the internet, nobody knows you're a dog

Possible future scenarios

Possible future scenarios

Platform Identity

Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.

“On the internet still no one knows you’re a dog”

Possible future scenarios

Platform Identity

Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.

“On the internet still no one knows you’re a dog”

Operator Networks

To sign up and use secure digital services, users need to provide reliable information about their identity. Users trust regulated organizations to provide services like banking and protected internet access. It’s natural to look to the same organizations to help with digital identity. Secure identity exchange networks help responsible organizations to share user information, with the user’s consent. It may not work everywhere but it helps for services where identity matters the most.

“How can you be a dog if you’ve got a bank account and mobile phone?”

Possible future scenarios

Platform Identity

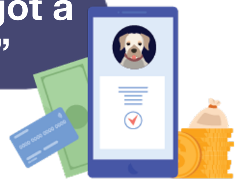
Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.

“On the internet still no one knows you’re a dog”

Operator Networks

To sign up and use secure digital services, users need to provide reliable information about their identity. Users trust regulated organizations to provide services like banking and protected internet access. It’s natural to look to the same organizations to help with digital identity. Secure identity exchange networks help responsible organizations to share user information, with the user’s consent. It may not work everywhere but it helps for services where identity matters the most.

“How can you be a dog if you’ve got a bank account and mobile phone?”



Self-Sovereign Identity

Users and businesses realize a need to fundamentally change personal data management. For businesses, personal data is a liability due to data protection risks. Users see the value of being able to hold data and take it where they need it. For this to work, data presented by users needs to be reliable and trustworthy. Some have started to use cryptographic wallets to collect and share signed data. Users need to look after their data, much like they look after their money.

“On the internet you can now prove you are a dog.”

Possible future scenarios

Platform Identity

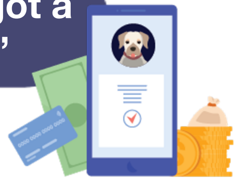
Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.

“On the internet still no one knows you’re a dog”

Operator Networks

To sign up and use secure digital services, users need to provide reliable information about their identity. Users trust regulated organizations to provide services like banking and protected internet access. It’s natural to look to the same organizations to help with digital identity. Secure identity exchange networks help responsible organizations to share user information, with the user’s consent. It may not work everywhere but it helps for services where identity matters the most.

“How can you be a dog if you’ve got a bank account and mobile phone?”



Self-Sovereign Identity

Users and businesses realize a need to fundamentally change personal data management. For businesses, personal data is a liability due to data protection risks. Users see the value of being able to hold data and take it where they need it. For this to work, data presented by users needs to be reliable and trustworthy. Some have started to use cryptographic wallets to collect and share signed data. Users need to look after their data, much like they look after their money.

“On the internet you can now prove you are a dog.”

Open APIs

Organizations across the economy have been forced to open APIs allowing services to access user data (with the user’s consent) from other places. Users link together different services as the need arises. It is down to the individual service to piece together all the data it collects into something meaningful for the particular user. Most individual users don’t remember all the connections and links they have set up.

“We don’t know if you are a dog, but we can see you like doggy treats.”

What are the key challenges that need attention?

DIACC's role in scenarios

How well would scenarios align with the values of DIACC members?

Requirement	Platform	Operator Networks	Self-Sovereign	Open APIs
Participation	L	H	M	M
Transparency	L	M	H	L
Accountability	L	H	M	L
Confidentiality	L	H	H	H
Integrity	L	H	H	M
Availability	M	H	H	M

What influence does the DIACC currently have?

Platform	Operator Networks	Self-Sovereign	Open APIs
None	Good	Good	Limited

The above high-level evaluation of each of the scenarios is based on the governance and operational requirements as described in DIACC's whitepaper "Making Sense of Identity Networks", which reflects DIACC member values and expectations for identity networks. More detail behind the intent of each requirement is included in the appendix of this document.

This evaluation demonstrates that the self-sovereign and operator network scenarios are best aligned with DIACC member values, with the open APIs scenario providing challenges particularly in governance, and the platform scenario being the least aligned.

What key challenges are common across future scenarios?

What key challenges are common across future scenarios?

Creating Market Conditions

Standards

The source of authority for digital identity standards across the economy is unclear due to parallel working body efforts across Canada.

Regulatory

Government has an important role to play in digital identity. The provinces and territories are primary sources of foundational identities. Regulation needs to allow digital identity solutions, including the controlled opening up of data.

What key challenges are common across future scenarios?

Creating Market Conditions

Standards

The source of authority for digital identity standards across the economy is unclear due to parallel working body efforts across Canada.

Regulatory

Government has an important role to play in digital identity. The provinces and territories are primary sources of foundational identities. Regulation needs to allow digital identity solutions, including the controlled opening up of data.

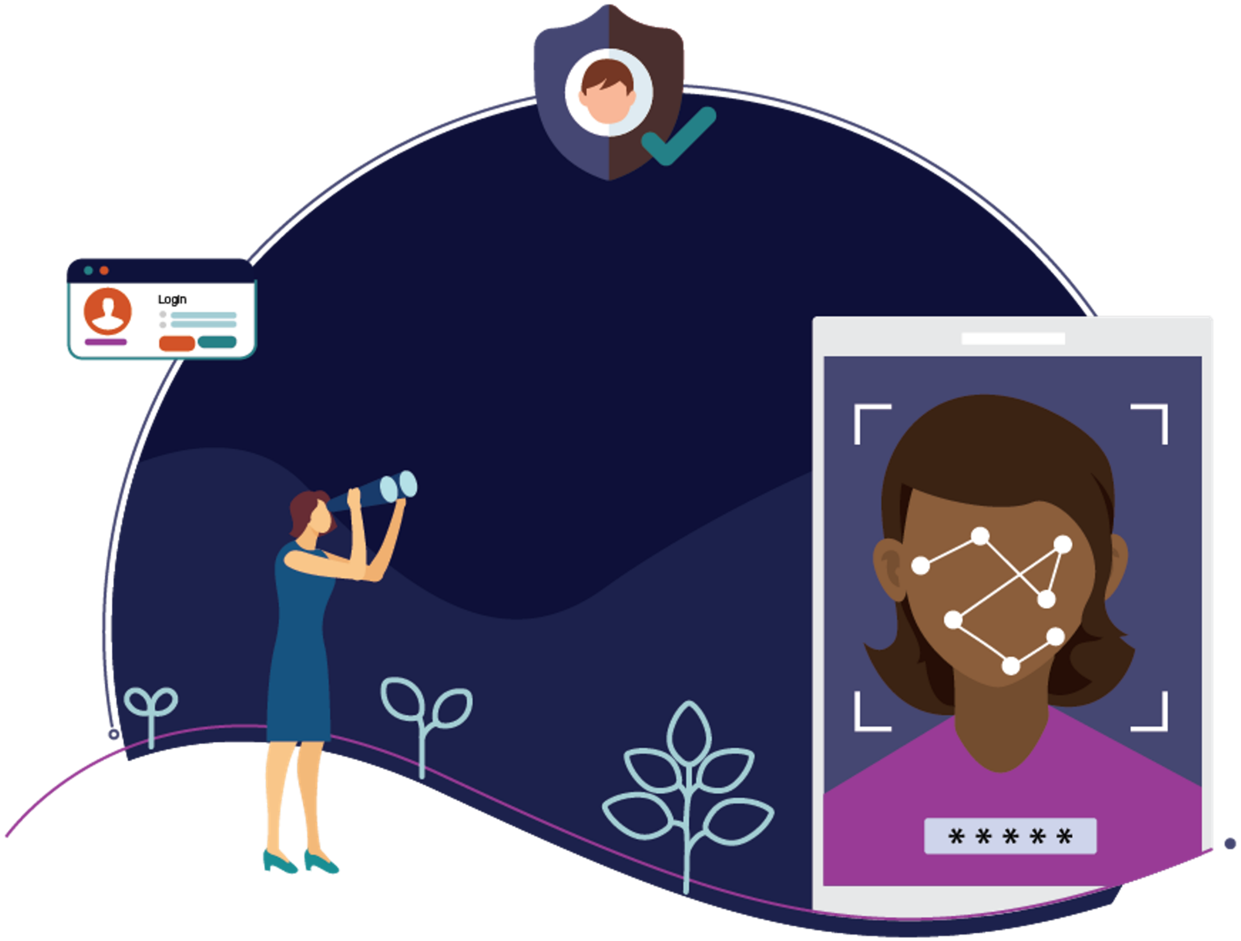
Promoting Market Growth

Sustainability

While each scenario provides a varying perspective, commercial sustainability and viability are either unclear, underdeveloped, or unproven. Considerations for liability should also be included in this category of challenges as the responsibility around personal data exchanged needs to be carefully examined.

Inclusion

Ensuring that a critical mass of providers and users adopt digital identity products is significant across all scenarios, while also ensuring those that are typically excluded can get access to services or can be provided with better experiences than those that exist today.



How do we ensure that identity will respect citizens and consumers?

Canadians’ Perspectives on Digital Identity

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians’ Perspectives on Digital Identity

70%

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians’ Perspectives on Digital Identity

70%

feel that a collaboration between the government and the private sector is the **best approach to creating a pan-Canadian digital ID framework**.

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Bill 64: Overhaul of Quebec’s Privacy Law Regime

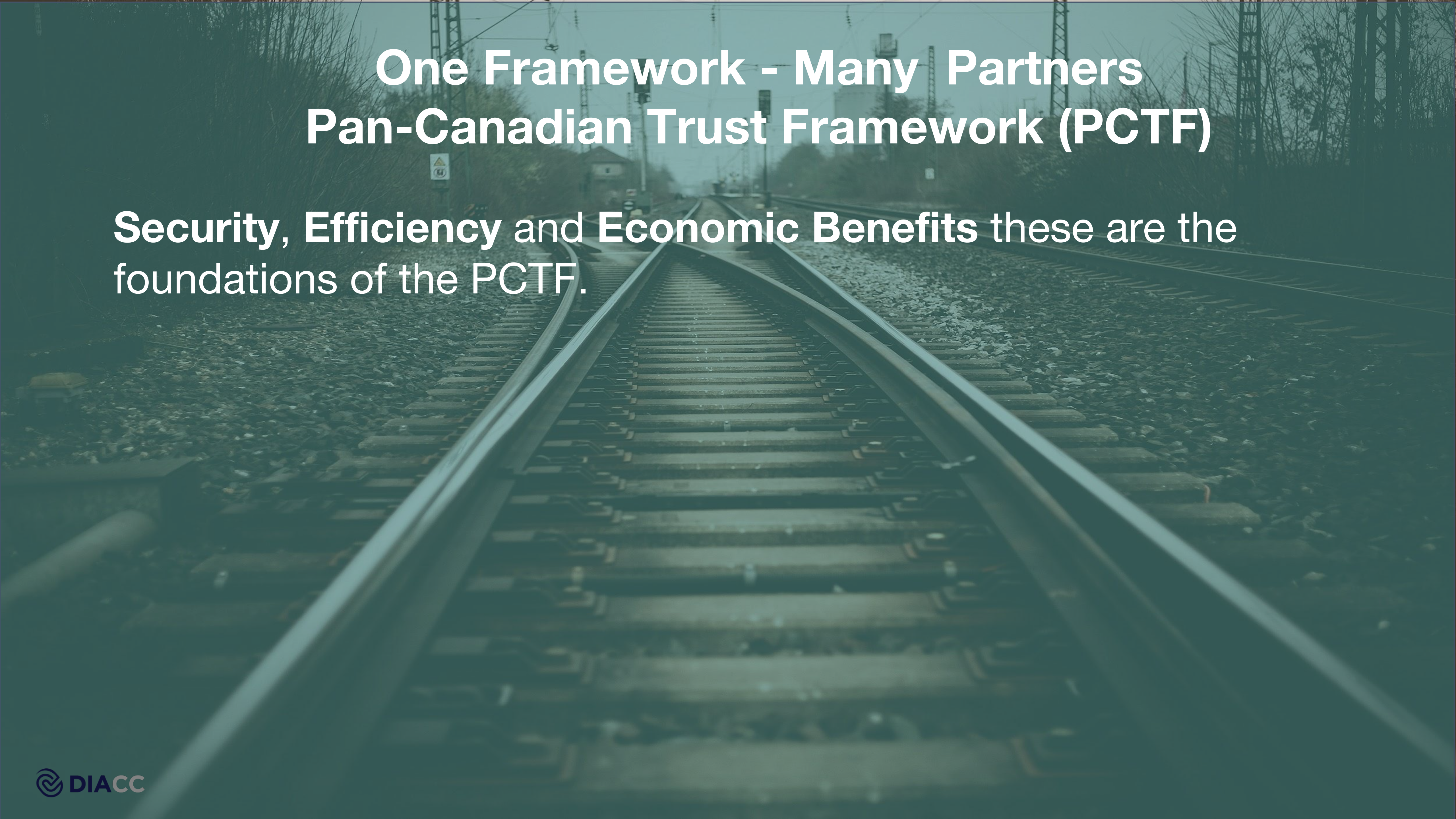
- Significant sanctions may be imposed by Commission d'accès à l'information (“**CAI**”) up to $10 million or 2% of worldwide turnover, whichever is greater, and penal sanctions up to $25 million or 4% of worldwide turnover.
- Possibility for a company to be sued for damages.
- Requirement to appoint a Chief Privacy Officer and establish governance policies and practices.
- New obligations when a data breach incident occurs.
- New rights for individuals for data portability, right to be forgotten and right to object to automated processing of their personal information.
- Creation of exception allowing disclosure of personal information in the course of a business transaction without prior consent of individuals concerned.
- Remove for businesses the possibility of communicating, without the consent of persons concerned, nominative lists and new rules governing the use of personal information for commercial or philanthropic prospecting purposes.
- Obligation for companies to ensure pre-established settings for technology products and services ensuring highest levels of confidentiality by default. (privacy by design)

DIACC

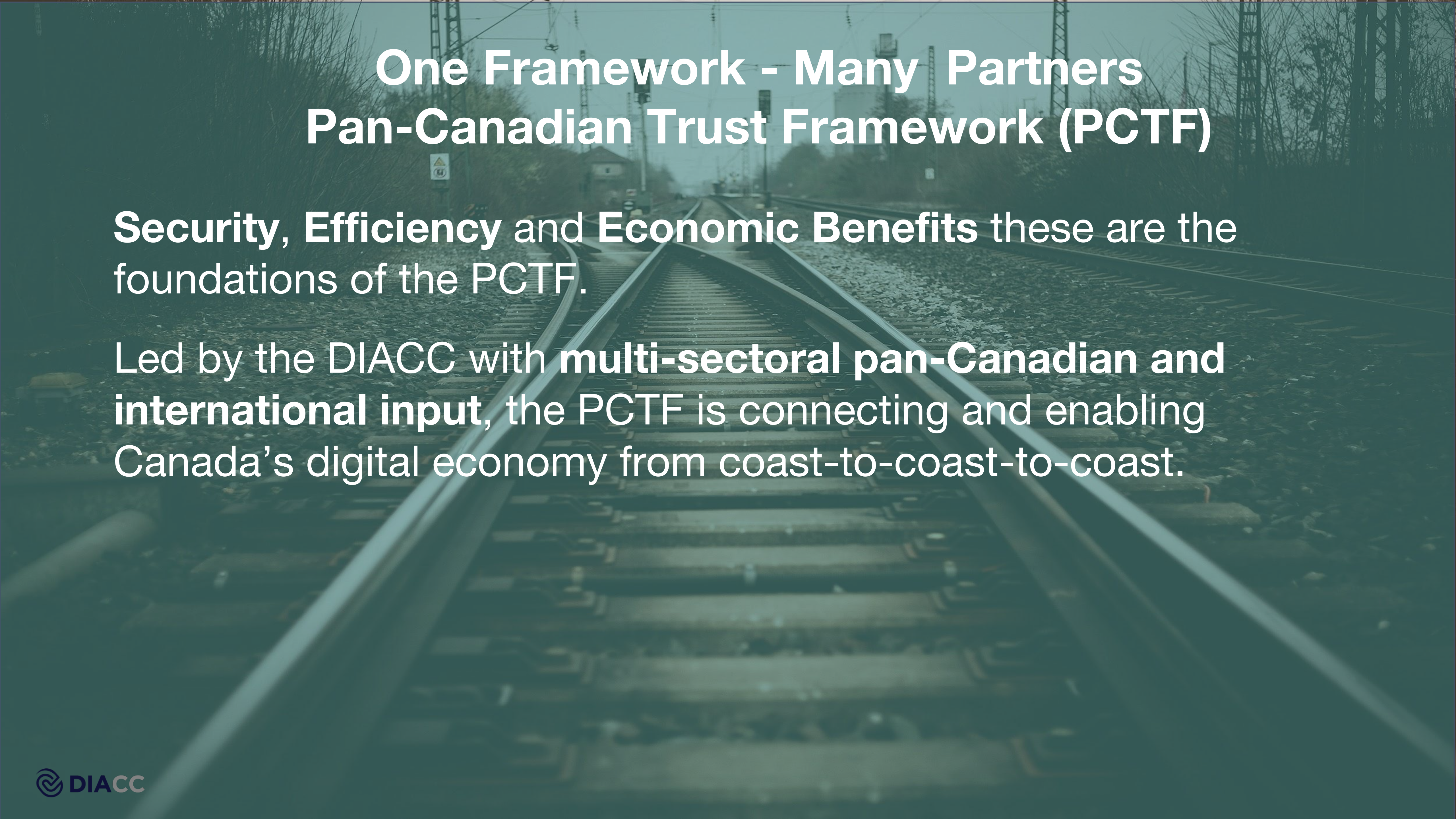
Source: https://www.mccarthy.ca/en/insights/blogs/techlex/bill-64-overhaul-quebecs-privacy-law-regime-implications-business

One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)



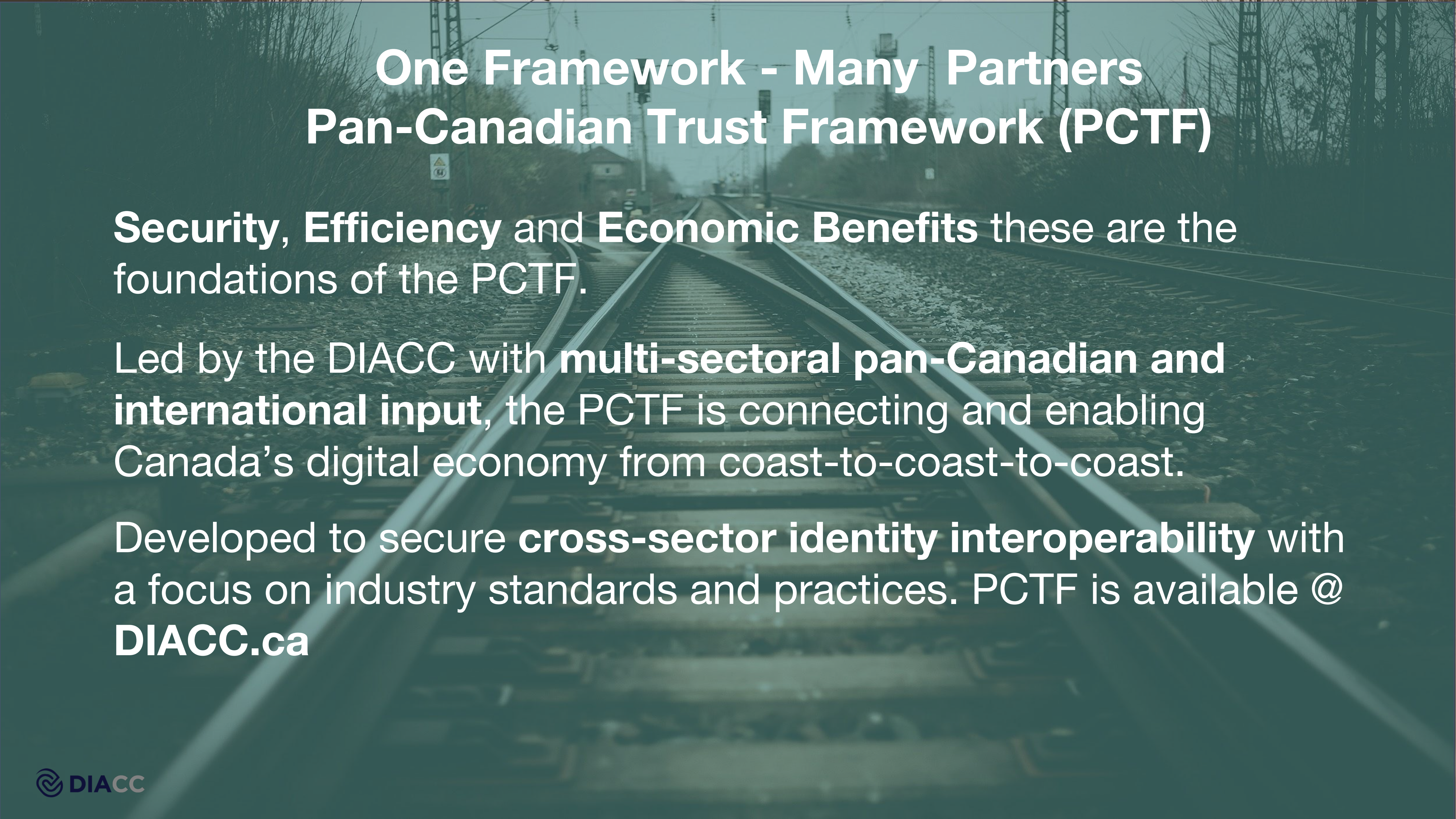
Security, **Efficiency** and **Economic Benefits** these are the foundations of the PCTF.



One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

Security, **Efficiency** and **Economic Benefits** these are the foundations of the PCTF.

Led by the DIACC with **multi-sectoral pan-Canadian and international input**, the PCTF is connecting and enabling Canada’s digital economy from coast-to-coast-to-coast.



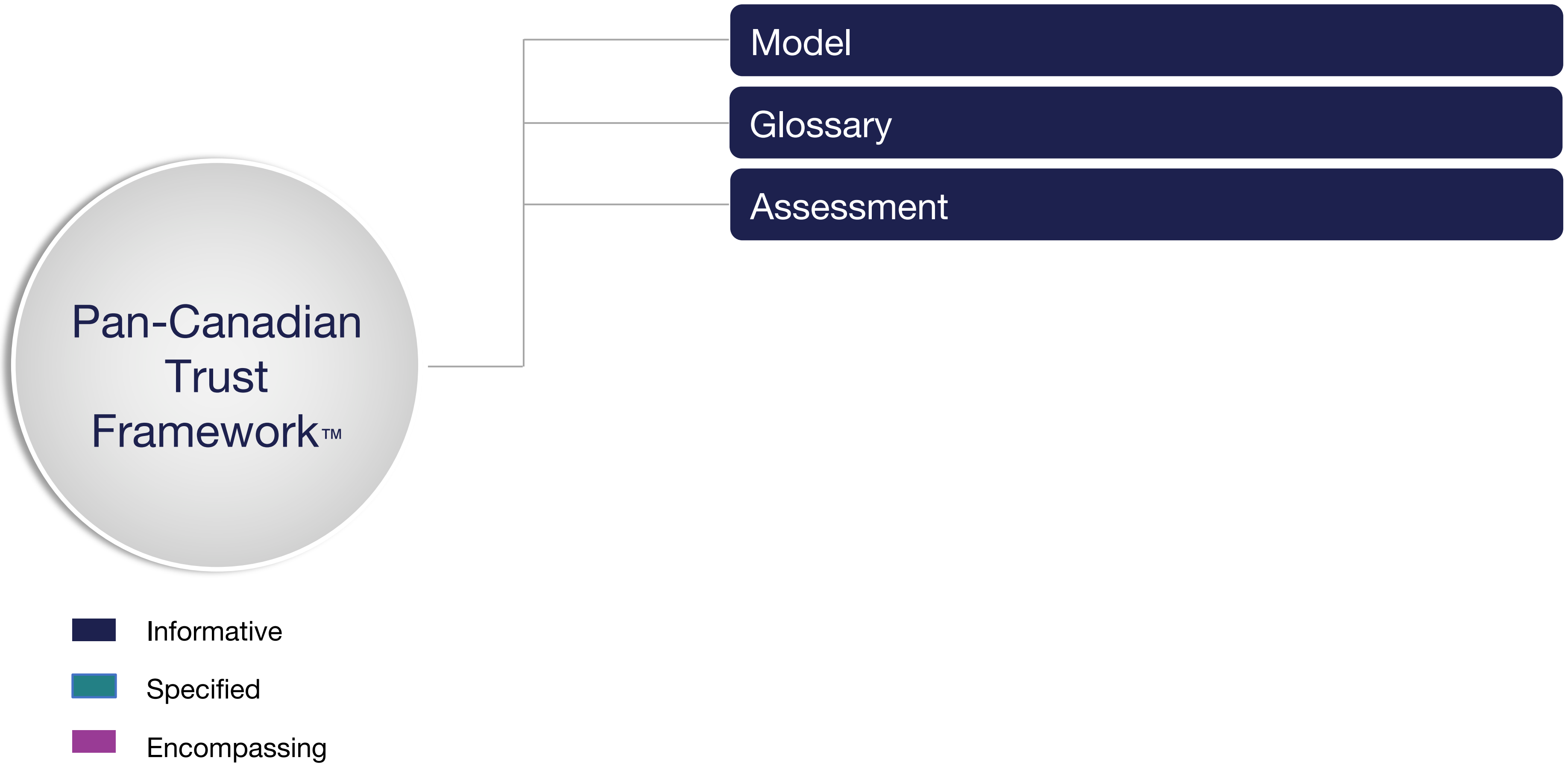
One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

Security, **Efficiency** and **Economic Benefits** these are the foundations of the PCTF.

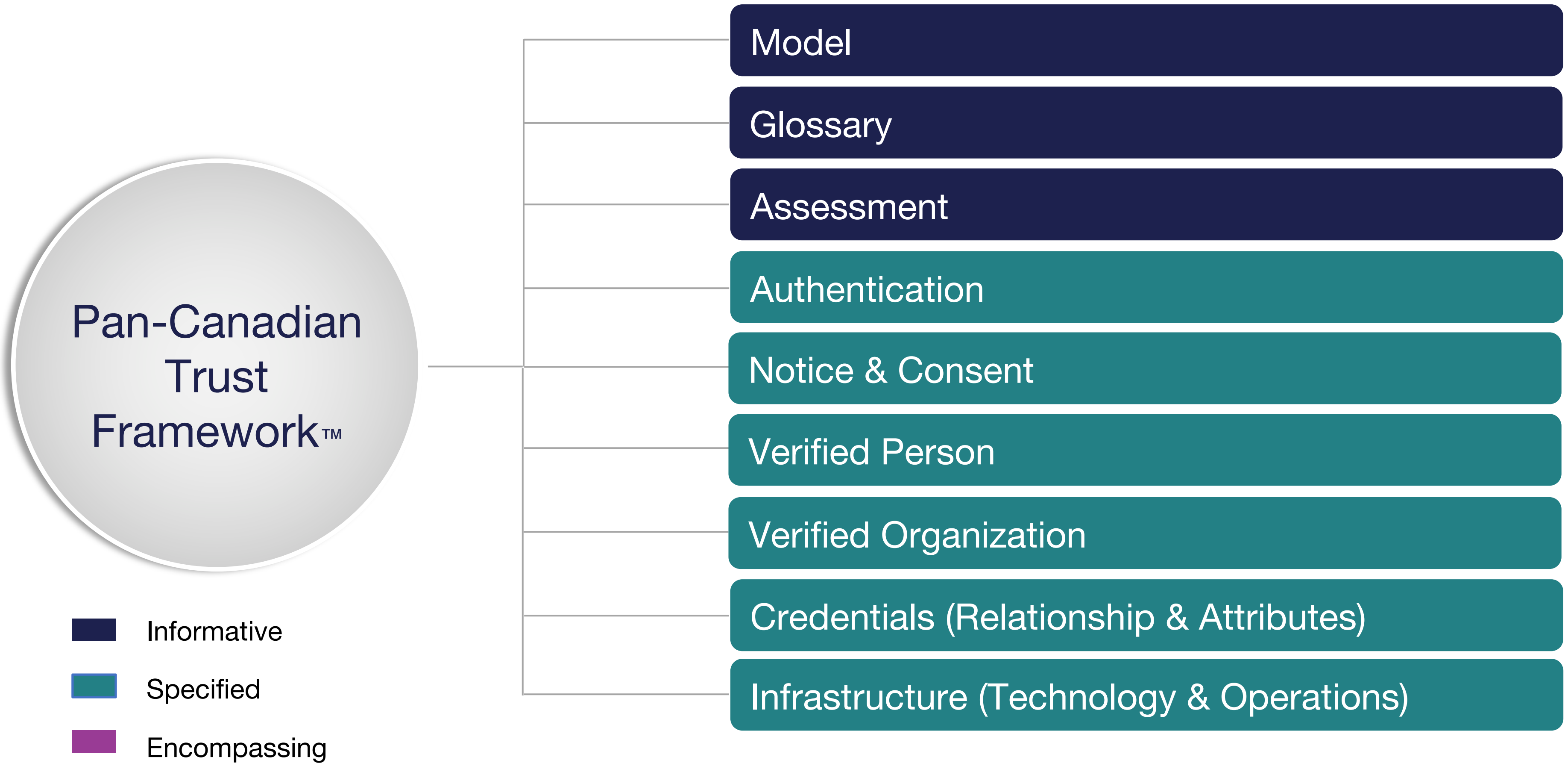
Led by the DIACC with **multi-sectoral pan-Canadian and international input**, the PCTF is connecting and enabling Canada’s digital economy from coast-to-coast-to-coast.

Developed to secure **cross-sector identity interoperability** with a focus on industry standards and practices. PCTF is available @ **DIACC.ca**

A Pan-Canadian Trust Framework for Digital Services



A Pan-Canadian Trust Framework for Digital Services



Pan-Canadian Trust Framework™

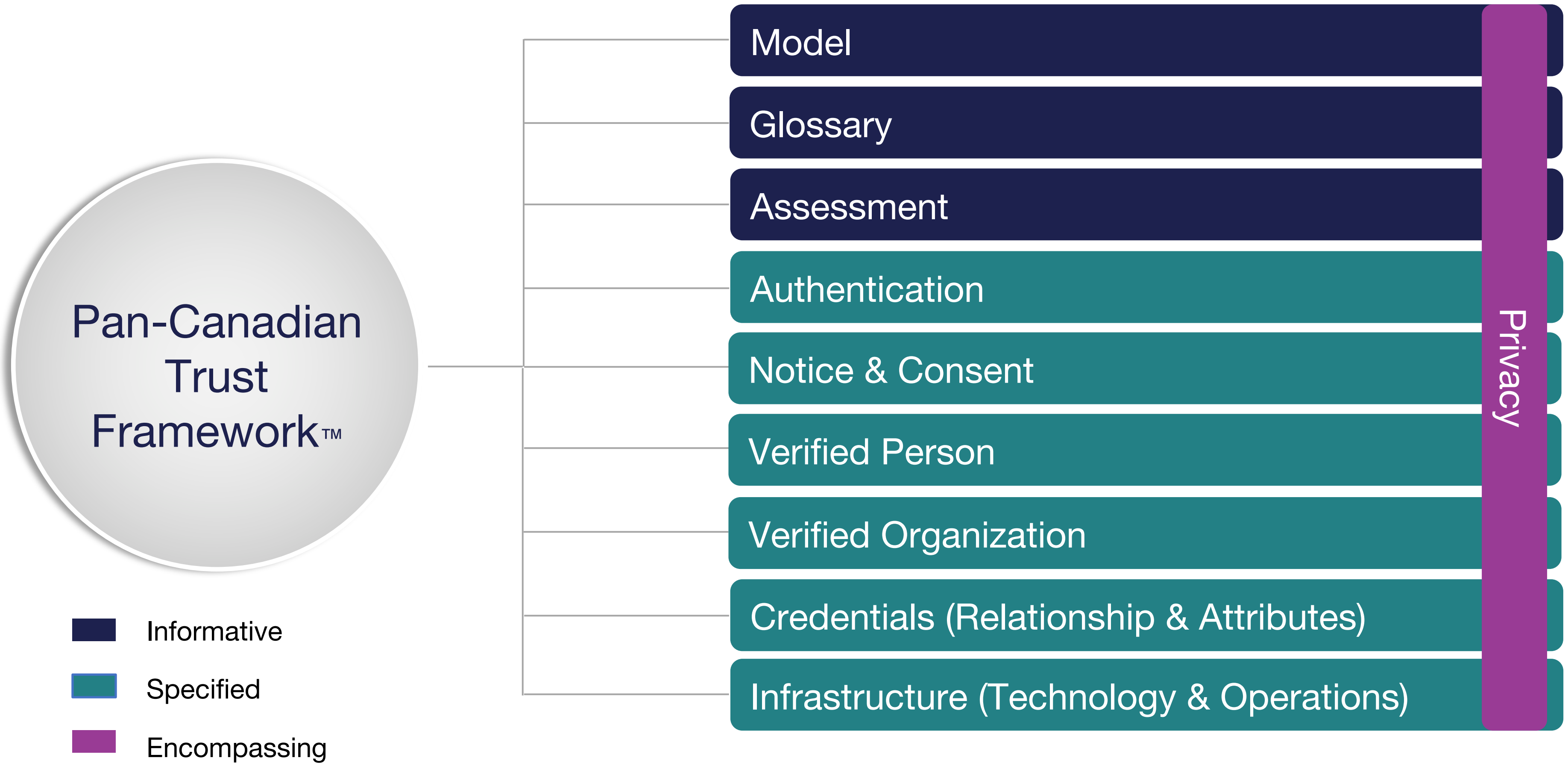
- Model
- Glossary
- Assessment
- Authentication
- Notice & Consent
- Verified Person
- Verified Organization
- Credentials (Relationship & Attributes)
- Infrastructure (Technology & Operations)

🟦 Informative

🟩 Specified

🟪 Encompassing

A Pan-Canadian Trust Framework for Digital Services



Pan-Canadian Trust Framework™

Model

Glossary

Assessment

Authentication

Notice & Consent

Verified Person

Verified Organization

Credentials (Relationship & Attributes)

Infrastructure (Technology & Operations)

Privacy

■ Informative

🟩 Specified

🟪 Encompassing

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

Verified Data

DIACC

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

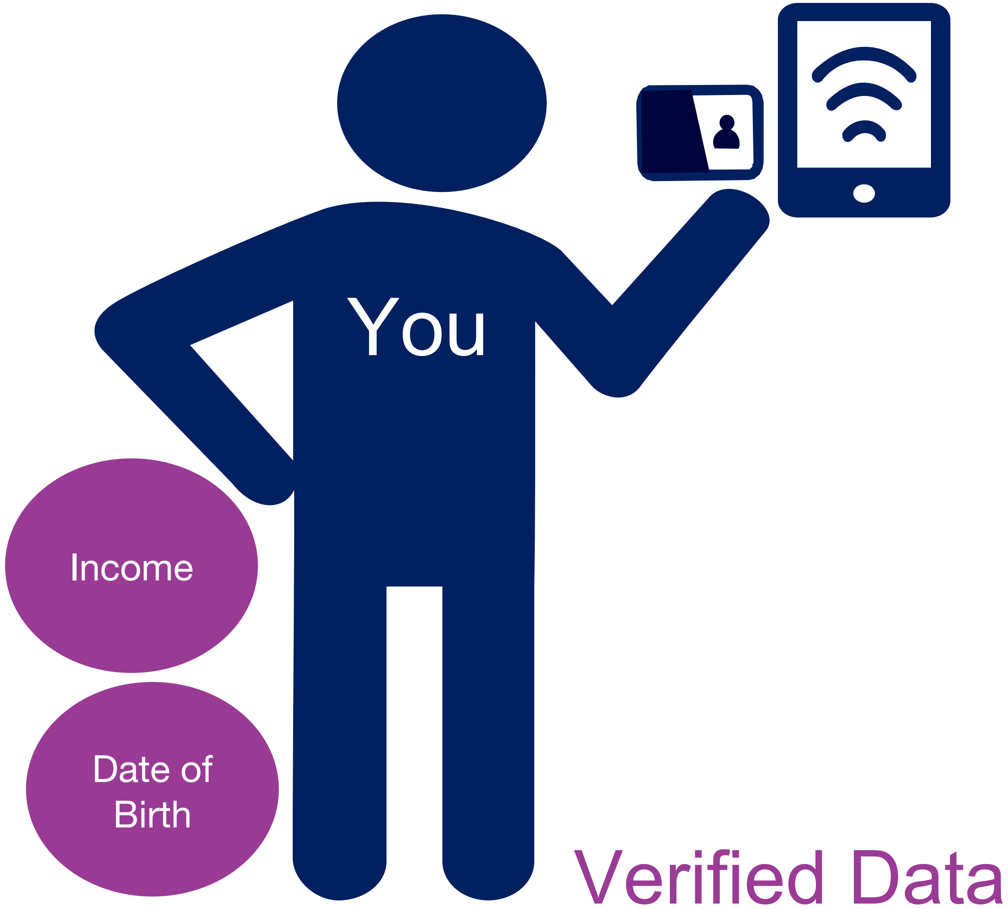
DIACC

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More



Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

DIACC

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

You
Income
Date of Birth
Address of record
Verified Data

Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

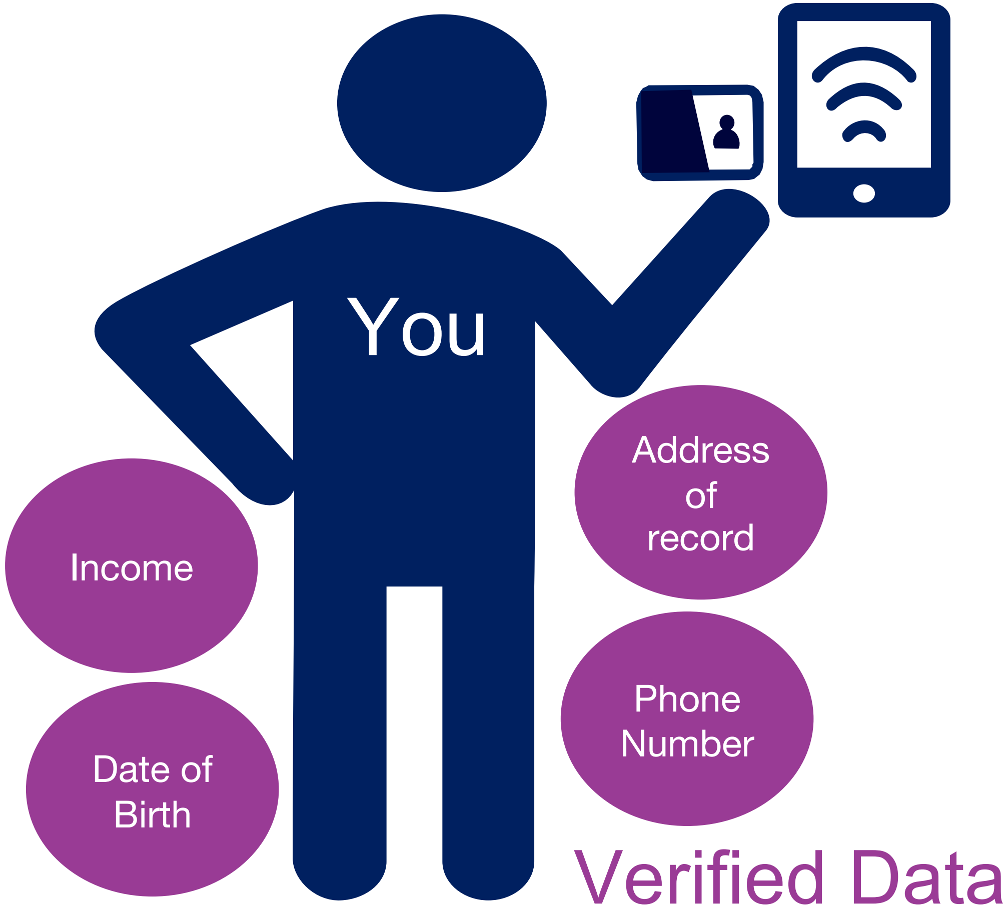
DIACC

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More



Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

DIACC

How would digital identity be used?

Digital Identity Use Cases: Government Services

Public Service/Policymakers can:

- Increase efficiencies in a highly regulated system by replacing the printing and resubmitting of forms from separate government departments with a digital ID-powered system
- Improve integrity of communication (phone calls, emails), as digital ID dramatically increases the certainty that the government is interacting with the correct person.
- Provide a more client-centric approach to serving the public by putting Canadians at the centre of digital ID solutions so that the government can change how interactions with Canadians are designed.
- Have less frequent data entry errors and higher data quality. Digital ID consent mechanisms that enable the sharing of data for research would lead to better policy direction and outcomes.
- Be innovative, by creating new ways of providing services to Canadian citizens and businesses and transform how government policies work.

Businesses can:

- Overcome cumbersome manual processes (such as business registration, licensing, permitting and inspections) for more efficient interactions with local, provincial and federal government departments.

Citizens can:

- Access services they need quicker and more efficiently by providing consent to share their data across departments. This can decrease in-person appointments and paper application processes and increase accessibility for those living in rural and remote communities by mitigating needs for commutes.
- Navigate the government administrative processes with more confidence and ease. With a unique digital ID, citizens can “log into” government services, similar to how they log into a bank account and access their services all in one place.

Digital Identity Use Cases: Health Care

Patients can:

- Seamlessly and securely access health documents in one place
- View test results, giving control over personal records and increased ability to advocate
- Integrated and unified health care records that enable more efficient and error-free point of care
- Access to health services any time, anywhere, securely authenticating identity to connect to health professionals on any device

Practitioners & Organizations (clinics, hospitals, paramed, medical research) can:

- Enhance operational efficiencies, including those related to records management and reporting, and care management.
- Reduce chances of prescription fraud with enhanced digital association between identity, prescription, and pharmacy fulfilment. Prescriptions for drugs like opioids and other controlled substances can have increased validation and verification requirements in order to fill the prescription.
- Access quality information about patients. Gated and segmented health records can be shared digitally between health professionals with a patient's permission for a robust medical history.
- Increase time for doctors and clinical researchers by decreasing the time needed to log in and out of applications to verify practitioner identity

Policy-makers (Government) can:

- Develop better informed policy decisions with the access of higher quality data, which can improve accuracy of future health care research and ensure actions taken are truly patient-first.

Digital Identity Use Cases: Commerce

Consumers can:

- Easily facilitate transactions by connecting their payment services provider to retailers.
- Minimize their risk of identity theft and privacy breaches with data minimization established - consumers provide their information on an as-needed basis, protecting their privacy and preserving anonymity.

Businesses can:

- Improve processes for remotely conducting transactions from distant geographic locations.
- Benefit those working in the 'gig economy' (i.e. freelancers and Uber drivers) with remote authentication across digital channels. With one click, platforms like Uber can verify these workers, and they could be trusted by both the platforms and customers.

E-commerce Businesses can:

- Reduce their risk for customer fraud or breaches by accessing only need-to-know details.
- Have the ability to perform Know Your Customer (KYC) checks to satisfy regulator requirements is key for providers. KYC procedures are also a legal requirement in order to comply with Anti-Money Laundering (AML) laws. KYC refers to the steps taken to establish customer identity, understand the nature of their activities and assess AML risks. Having a digital ID system in place would enable this.
- Conduct peer-to-peer sales more securely with verified identity, such as on eBay or AirBnB.
- Minimize administrative customer issues, which can impact their productivity and bottom line, such as minimizing the number of people calling in for password resets and errors in delivery logistics.
- Increase their probability of customer loyalty and retention by providing customers with a more structured and secure sales process.

Retailers (in-person) can:

- Accurately and securely verify the shopper's age when selling restricted goods and content.
- Reduce commercial transaction times and/or costs with automation (i.e. faster interactions at the check out), resulting in increased efficiency.

Digital Identity Use Cases: Finance

Financial Institutions (FIs) can:

- Streamline their business processes, from customer registration and transaction monitoring, to credit risk assessment, ultimately offering an improved service delivery. A more streamlined authentication process can also result in increased sales of goods and services, helping with customer retention.
- Increase their cost savings through reduced fraudulent activity, as digital ID can make it easier to verify and trust FI's customer bases.

Clients and consumers can:

- Place greater trust in their FIs knowing that a secure digital ID system has been adopted.
- Have more control over their data and identity, as data that is shared will be on a need-to-know basis.
- Gain greater accessibility to financial services that are currently hindered by lack of documentation, distance to financial institutions, and cost of financial services for many people worldwide.
- Save on transaction costs, with fewer or no service fees, as well as an elimination of the need for physical proof and exchange of paperwork in financial transactions.
- Access their services with speed and ease as a streamlined and efficient process makes for a faster turnaround time for verification and authentication.

Digital Identity

Digital Identity
done right requires
public and private sector
collaboration

The Digital ID & Authentication Council of Canada

Leading Canada’s **full and beneficial global digital economy participation** by delivering a **digital identity and authentication interoperability framework.**

The DIACC is a **Non-profit coalition** of **public and private sector members** created as a result of federal government’s Electronic Payments System Task Force.

DIACC Board

Treasury Board of Canada Secretariat

BRITISH COLUMBIA

Ontario

New Brunswick Nouveau

BMO

CIBC

CANADA POST POSTES CANADA

Desjardins

ForgeRock®

Interac

Manulife

SECUREKEY

TD

TELUS

Sustaining Members

cdic sadc
Canada Deposit Insurance Corporation
Société d'assurance-dépôts du Canada

RBC

Saskatchewan

Sustaining Members

mastercard

EQUIFAX

Vancity

Sustaining Members

1KOSMOS BlockID

2KEYS Cyber Security | Digital Identity

acuant

Affinity Credit Union

applied recognition

ApplyBoard

ARUCC Commitment Dedication

Auth0

bc Land Title & Survey

BECKER-CARROLL A CONVERGE COMPANY

boloro

catallaxy

CCUA Canadian Credit Union Association

Canada Health Infoway Inforoute Santé du Canada

DIGIDENTITY

celero

central 1

Convergence.tech

consult hyperion securing tomorrow's transactions

Digital Identity Laboratory

DIGITAL TECHNOLOGY SUPERCLUSTER

EQUITABLE BANK

Folio

Gambit GROUP OF COMPANIES

GET NORTH AMERICA GROUP

Innovation, Science and Economic Development Canada

Innovation, Sciences et Développement économique Canada

HYPERSECU

KUMA

iCOMPLY

Mavennet

CROWD ID

IdentityNORTH

IDENTOS

IF

iproov

JUMIO

Lenovo

LEAGUE DATA

Libro CREDIT UNION

ModoHR

Screening Canada

Northern Block

notarius

OneSpan Be bold. Be secure.

onfido

OARO

Outlier

PAYMENTS CANADA

peer

Peoples Group

Prodigy Labs

Quartech

SAIT

Smart Species

simeio

stash

TreeFort

Trulioo

VALID8ID SOLUTIONS

vlinder

VIVVO

WORLDREACH software

YOTI

Adopter Members: Canadian Council of Motor Transport Administrators, Niagara Health

Join the Conversation!

Adopt the Pan-Canadian Trust Framework to secure the foundation of digital identity that will secure Canada's digital transformation.

Contact us to join the conversation info@diacc.ca

diacc.ca   @mydiacc   in /company/mydiacc   f /mydiacc