

Update on Pan-Canadian Identity Management

Joint Councils
February 24, 2016

Identity Management Sub-Committee (IMSC)

IMSC Co-Chairs:

**Fred Pitt, Province of Ontario, Treasury Board Secretariat
Rita Whittle, Government of Canada, Treasury Board Secretariat**

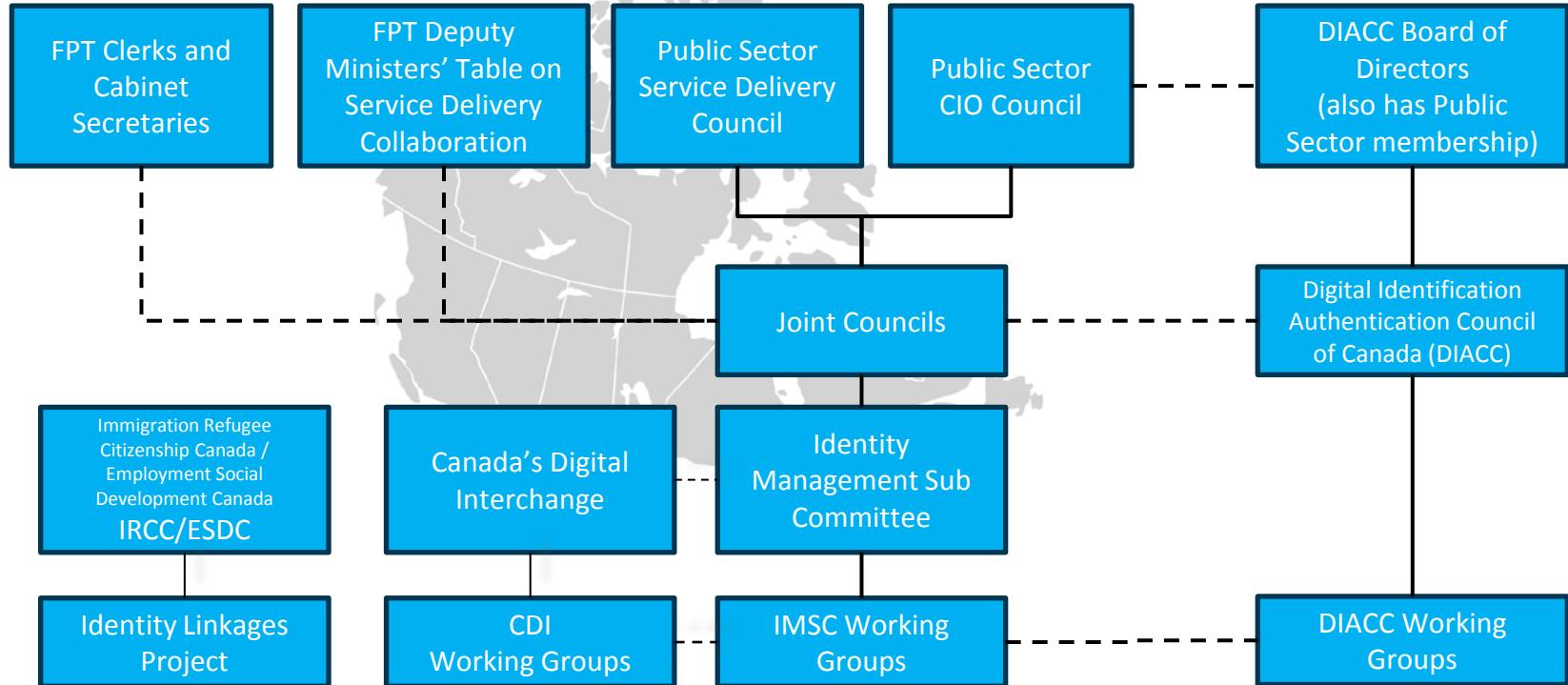
Objectives

- Provide an overview of Pan-Canadian context
- Give a progress update on development of the Pan-Canadian Identity Trust Framework
- Discuss where we go from here

Pan-Canadian Context

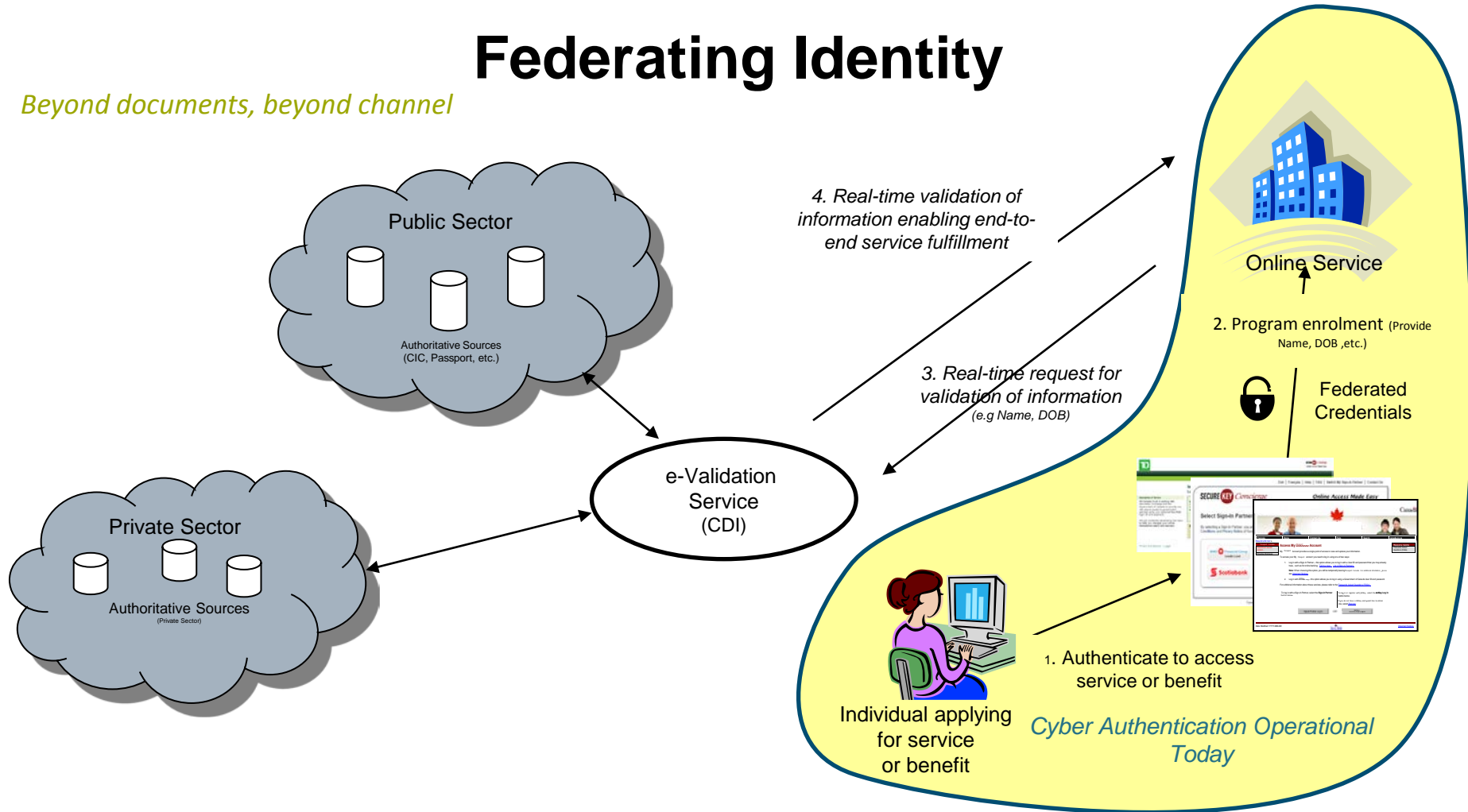
Public Sector

Private Sector/ Industry Initiatives



Federating Identity

Beyond documents, beyond channel



Federating Identity: Milestones and Initiatives

Milestones/Deliverables

- ✓ 2004: Secure Channel, including its epass authentication service, operational
- ✓ 2007: Identity Management & Authentication (IATF) Task Force Report
- ✓ 2008: Cyber Auth Report on Future Requirements for the Government of Canada
- ✓ 2009: TBS Directive on Identity Management
- ✓ 2009: ITSG-31 Authentication Guidance
- ✓ 2010: Pan-Canadian Assurance Model
- ✓ 2010: BC Identity Assurance Standard
- ✓ 2010: BC Evidence of Identity Standard
- ✓ 2010: BC Electronic Credential & Authentication Standard
- ✓ 2010: CIC (Passport Program) Facial Recognition capability operational
- ✓ 2010: Cyber Auth RFP 1/RFP2/RFP3
- ✓ 2011: Federating Identity for the Government of Canada: Backgrounder¹
- ✓ 2011: IMSC Pan-Canadian Approach to Trusting Identities
- ✓ 2011: National Routing System (NRS) Data Exchanges Standard
- ✓ 2012: Cyber Authentication Technical Specification
- ✓ 2012: Guideline on Defining Authentication Requirements
- ✓ 2012: Federating Identity Broker Architecture
- ✓ 2013: GC Federated Credential operational
- ✓ 2013: Standard on Identity and Credential Assurance
- ✓ 2013: Cyber Auth Close Out Report
- ✓ 2013: ePassport operational
- ✓ 2013: Issuing new BC Services Card commenced
- ✓ 2013: Service Quebec now responsible for clicSÉCUR
- ✓ 2013: Ontario approves Electronic Identification, Authentication and Authorization (IAA) policy
- ✓ 2014: Pan-Canadian Identity Validation Standard
- ✓ 2015: GC Guideline on Identity Assurance
- ✓ 2015: BC Identity Information Standard
- ❑ 2016: Pan-Canadian Identity Trust Framework

*Lessons
Learned*

*Strategic
Alignment*

Initiatives/Oversight

National Routing System

- 2004-2006: Pilot
- 2006-Present: In Production

Cyber Authentication Renewal

- 2008: Creation of DM Cyber Auth Committee
- 2008-2010: Consultation & Strategy
- 2010-212: Procurement & Transition
- 2012: Services Operational: (SecureKey Concierge & GCKey)
- 2013 Conclusion (DM membership incorporated in DM SFI)

Federating Identity

- 2010: GC Guideline on Defining Authentication Working Group
- 2011: GC Guideline on Identity Assurance Working Group
- 2013: GC Pilot Projects (Individuals/Businesses)
- 2013: GC Policy & Legal Implications Working Group
- 2014 Canada's Digital Interchange
- 2015 Identity Linkages Project

Task Force for Payments System Review

- 2012: Recommendation to create Digital Identification and Authentication Task Force (DIAC)
- 2015: DIACC Trust Framework Working Group

Identity Management Sub-Committee (IMSC)

- 2012: Changed Reporting Structure to Joint Councils
- 2013: IMSC Working Group

International

- 2013-2015: Identity Summits
- Involvement in Kantara, ISO & ANSI Standards

DM Committee on Service and Federating Identity (SFI)

- 2013: Inaugural meeting

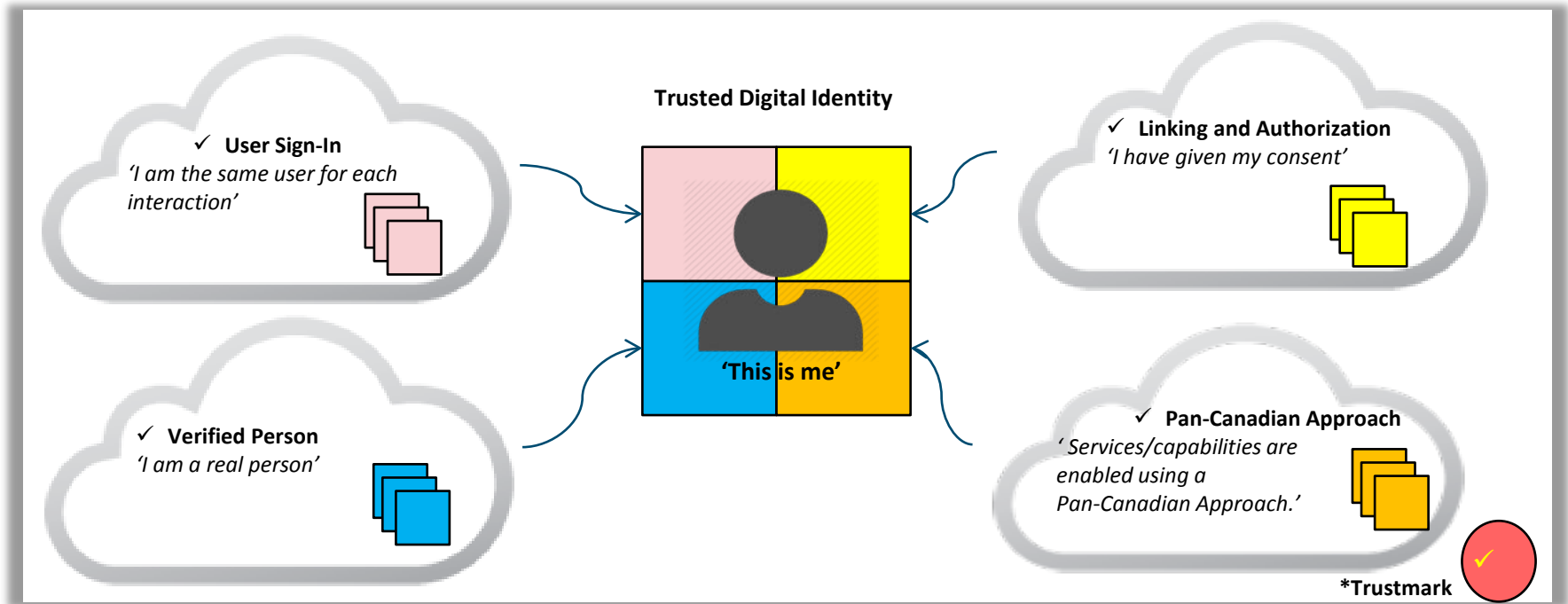
Related Arrangements & MOUs

- Citizenship Certificate Validation (CIC & Provinces)

Objective: Trusted Digital Identity

'A trusted electronic representation of who I am.'

A trusted digital identity consists of four main components:



*Trustmark

*being examined



Pan-Canadian Identity Trust Framework

Trusted Digital Identity

Trusted electronic representation of who I am



Including Public Sector Considerations and Private Sector Considerations

Is it the same person?

User Sign-In Component

The set of trusted processes that ensures that a user is securely signed-in and acting on his or her own behalf

- ☐ Credential Issuance
- ☐ Credential Authentication
- ☐ Credential Recovery
- ☐ Credential Revocation

Is it a real existing person?

Verified Person Component

The set of trusted processes that uniquely identifies a real and existing person, ensures that identity information is accurate and up-to-date, and that claims and actions can be attributed to this person.

- ☐ Identity Resolution
- ☐ Identity Establishment
- ☐ Identity Validation*
- ☐ Identity Verification
- ☐ Identity Maintenance*

Has the user given consent ?

Linking and Authorization Component

The set of trusted processes that links a user sign-in to a verified person and manages authorization (consent) as granted by this person.

- ☐ Credential Determination
- ☐ Identity Linking
- ☐ Owner Authorization

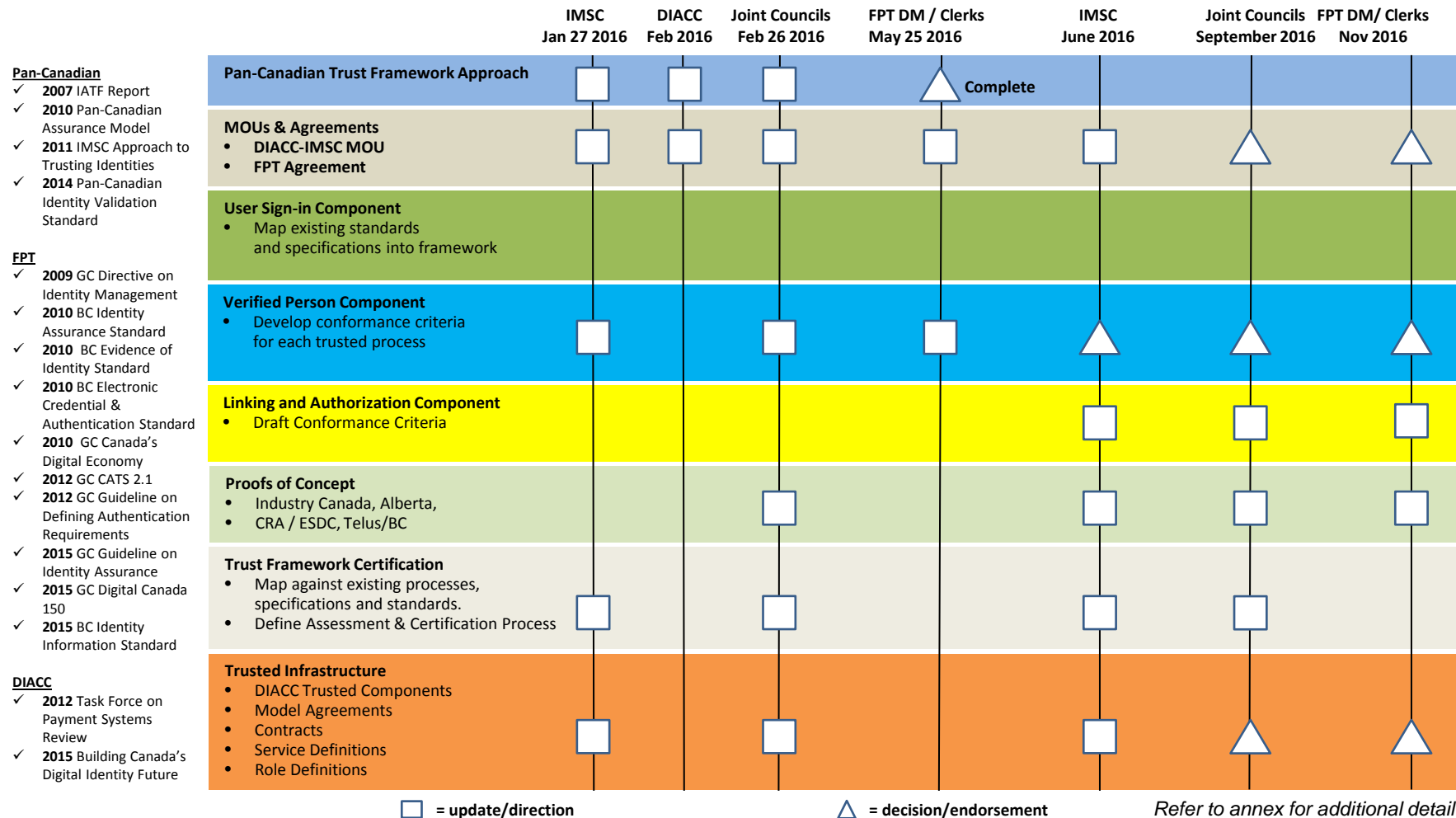
Pan-Canadian Infrastructure Component

Technical Standards, Specifications, Certifications Privacy, Security, Service Delivery, Organizational

**Canada's Digital Interchange (CDI)'s goal is to achieve these components*

PAN-CANADIAN IDENTITY TRUST FRAMEWORK: CRITICAL PATH

Pan-Canadian Identity Trust Framework



FPT

- ✓ 2009 GC Directive on Identity Management
- ✓ 2010 BC Identity Assurance Standard
- ✓ 2010 BC Evidence of Identity Standard
- ✓ 2010 BC Electronic Credential & Authentication Standard
- ✓ 2010 GC Canada's Digital Economy
- ✓ 2012 GC CATS 2.1
- ✓ 2012 GC Guideline on Defining Authentication Requirements
- ✓ 2015 GC Guideline on Identity Assurance
- ✓ 2015 GC Digital Canada 150
- ✓ 2015 BC Identity Information Standard

DIACC

- ✓ 2012 Task Force on Payment Systems Review
- ✓ 2015 Building Canada's Digital Identity Future

Pan-Canadian Trust Framework: Progress since September 2015

- **November 2015:** Pan-Canadian Trusted Identity Forum in Ottawa
 - Agreement in Principle with DIACC on developing one framework
- **December 2015:** Developed Critical Path
 - Milestone and Reporting Dates
 - Progress to Date on Trust Framework Components
- **January 2016:** Trust Framework Development
 - Draft IMSC-DIACC MOU
 - Draft Trust Framework Charter
 - DIACC Working Group Engagement

Pan-Canadian Trust Framework

Next Steps...

1. IMSC

- Finalize IMSC-DIACC MOU and Trust Framework Charter
- Identify additional stakeholders (e.g., Intergovernmental affairs)
- Develop trust framework conformance criteria
 - User Sign-in, Verified Person, Linking and Authorization
- Update Joint Councils (PSSDC/PSCIOC) during March/April teleconference calls

2. Digital Service Strategy

- Anchor Identity Management effort in pillar of digital government/service strategy

3. FPT DM Table

- Present progress regarding Pan-Canadian Identity Trust Framework in May 2016

4. DIACC

- Engage in monthly board meetings
- Contribute to DIACC Trust Framework Working Group

Discussion

Annex Slides

Pan-Canadian Vision

Pan-Canadian Vision (2014):

Citizens and businesses enjoy simple, convenient and secure access to services in a manner they choose and manage



Business Value

- *Enables a whole-of-government approach for seamless e-service delivery*
- *Improves client experience and user convenience by supporting a “tell-us-once” approach*
- *Enables jurisdictions to trust and leverage each other’s identity management and assurance processes*
- *Reduces the risk that the individual is not who they claim to be.*
- *Reduces identity-related administration costs*
- *Strengthens program integrity*

Business and User Value

Business and user value of a trusted digital identity is realized by the participants in the roles of **authoritative party**, **relying party** or **person (user)**

Government Program Authority



Business Value

*'As an **authoritative party** we can provide a trusted digital identity to service providers.'*

✓ **Business Value:**

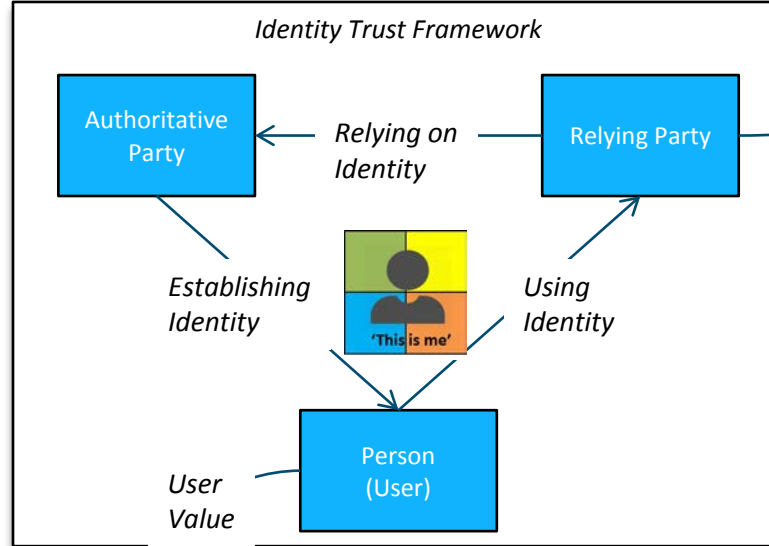
Opportunity to provide high value services to a broader service delivery community

Individual Client



*'As a **user**, I can prove myself once, and with my consent, use my identity information with multiple service providers.'*

✓ **User Value:** Easier access to high value services in a trusted, secure, and privacy-enhanced way.



Government Service Provider



Business Value

*'As a **relying party**, we can enhance and streamline our service experience by using a trusted digital identity that is based on trusted processes.'*

✓ **Business Value:** Improved service delivery through increased integrity, better efficiencies, and streamlined user experience.

Pan Canadian Trust Framework: Component 1 - User Sign-In

Processes that ensure that a user is securely signed-in and acting on his or her own behalf

PROGRESS TO DATE:

User Sign-in Component	Federal Public Sector	Pan-Canadian
Developing Policies, Standards, Guidelines and Specifications <ul style="list-style-type: none">✓ CATS 2.1,✓ ITSG-31✓ Directive Identity Management✓ Standard on Identity and Credential Assurance✓ Guideline on Defining Authentication Requirements	In Place	Development
Operationalizing User Sign-In Component <ul style="list-style-type: none">✓ Credential Issuance✓ Credential Authentication✓ Credential Recovery✓ Credential Revocation✓ Onboarding/Offboarding Credential Service Providers	In Place	Development
Mapping existing standards and specifications into framework	Initiating	Initiating

Status

Not Started

Initiating

Development

In Place

Pan Canadian Trust Framework- Component 2 - Verified Person

The set of trusted processes that uniquely identifies a real and existing person, ensures that identity information is accurate and up-to-date, and that claims and actions can be attributed to this person.

PROGRESS TO DATE:

Verified Person Component	Federal Public Sector	Pan-Canadian
Policies, Standards, Guidelines and Specifications <ul style="list-style-type: none"> ✓ Directive Identity Management ✓ Standard on Identity and Credential Assurance ✓ Guideline on Defining Authentication Requirements 	In Place (Federal)	Development
<ul style="list-style-type: none"> ✓ (New) Guidelines on Identity Establishment 	Development	Development
Verified Person Component <ul style="list-style-type: none"> ✓ Develop conformance criteria for each trusted process <ul style="list-style-type: none"> - Identity Resolution - The establishment of the uniqueness of a person within a program/service population - Identity Establishment – The creation of an authoritative record of identity that is relied on by others - Identity Validation - Confirmation of the accuracy of the identity information about a person as established by an authoritative party. - Identity Verification - Confirmation that the identity information being presented relates to the person making the claim. - Identity Maintenance - Ensuring identity information is as accurate, complete and up-to-date as is required. ✓ Validate against existing processes (e.g. AB) ✓ Develop conformance criteria for each trusted process ✓ Develop new standards and guidelines as required. 	Development	Development

Status

Not Started

Initiating

Development

In Place

Pan Canadian Trust Framework –

Component 3 - Linking and Authorization

The set of trusted processes that links a secure sign-in to a verified person and manages authorization (consent) as granted by this person.

PROGRESS TO DATE:

Linking and Authorization Component	Federal Public Sector	Pan-Canadian
Developing Policies, Standards, Guidelines and Specifications (New) User Consent / Authorization - Attribute Release Policy*	Not Started	Not Started
<ul style="list-style-type: none"> ✓ Kantara/IEEE: User Managed Access (UMA) ✓ OAuth 2.0 	Initiating	Initiating
Operationalizing Linking and Authorization Component <ul style="list-style-type: none"> ✓ Credential Determination ✓ Identity Linking ✓ Owner Authorization 	Initiating	Not Started
<ul style="list-style-type: none"> ✓ Support pilot projects /reference implementations ✓ Participate in consent management consultations ✓ Develop new standards and guidelines as required ✓ Determine service enrolment, program registration, or account management process <u>International</u> <ul style="list-style-type: none"> ✓ Explore Electronic Identification and Trust Services (eIDAS) – EU Regulations 	Initiating	Not Started

* Carried out separately by programs, services, jurisdictions

Status

Not Started

Initiating

Development

In Place

Pan Canadian Trust Framework –

Component 4 – Infrastructure

The set of services or capabilities required to operate the trust framework in a secure, privacy-enhancing and trustworthy manner.

PROGRESS TO DATE:

Infrastructure Component	Federal Public Sector	Pan-Canadian
Developing Policies, Standards, Guidelines and Specifications <ul style="list-style-type: none"> ✓ Privacy Protection policy direction ✓ Security ✓ Reporting, Auditing and Logging ✓ Standards Specifications Certification 	Development	Development
Infrastructure Component <ul style="list-style-type: none"> ✓ Service Delivery and Organizational 	<i>Not Started</i>	<i>Not Started</i>
<ul style="list-style-type: none"> ✓ Support pilot projects ✓ Participate in consent management consultations ✓ Develop new standards and guidelines as required 	<i>Initiating</i>	<i>Initiating</i>

Status

Not Started

Initiating

Development

In Place

Published/Approved Pan-Canadian Documents & FPT Policy Instruments (2007-present)

Year	Originator / Jurisdiction	Description
2007	IMSC	IATF Report - Developed initial Pan-Canadian vision, strategy and framework.
2009	GC	Directive on Identity Management – Ensures effective identity management practices for individuals, organizations and devices.
2009	GC	IT Security Guidance (ITSG)-31 - User authentication guidance for IT systems.
2010	BC	Identity Assurance Standard - Provides a framework for establishing trust and confidence between parties issuing and receiving identity claims
2010	BC	Evidence of Identity Standard - Provides a framework for establishing trust and confidence between parties issuing and receiving identity claims
2010	BC	Electronic Credential & Authentication Standard - Specifies requirements for issuing, managing and authenticating electronic credentials to differing levels of strength.
2010	IMSC	Pan-Canadian Assurance Model - Detailed model describing how jurisdictions can formalize trust relationships.
2011	IMSC	IMSC Pan-Canadian Approach to Trusting Identities - Describes approach for trusting identities between jurisdictions.
2012	IMSC	Cyber Authentication Technical Specification (CATS) 2.1 - Technical interface standard for credential assurance.
2012	GC	Guideline on Defining Authentication Requirements Detailed guidance to assist in conduction assurance level assessments and defining authentication requirements.
2013	BC	PERSONAL IDENTITY INFORMATION DIRECTION - Identity Proofing Direction
2013	GC	Standard on Identity and Credential Assurance - Ensures that identity risk for individuals, organizations and devices is managed consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors.
2014	IMSC	Pan-Canadian Identity Validation Standard - standardizes identity information and personal information validation requests and responses between federal, provincial, territorial, and municipal government organizations
2015*	IMSC	Guideline on Identity Assurance - detailed guidance to support the implementation of the Standard on Identity and Credential Assurance (*in publishing)
2015*	BC	Identity Information Standard - sets out the rules and methods by which data on identity credentials accepted during an identity proofing procedure is recorded in a standardized and consistent form (*not yet available)

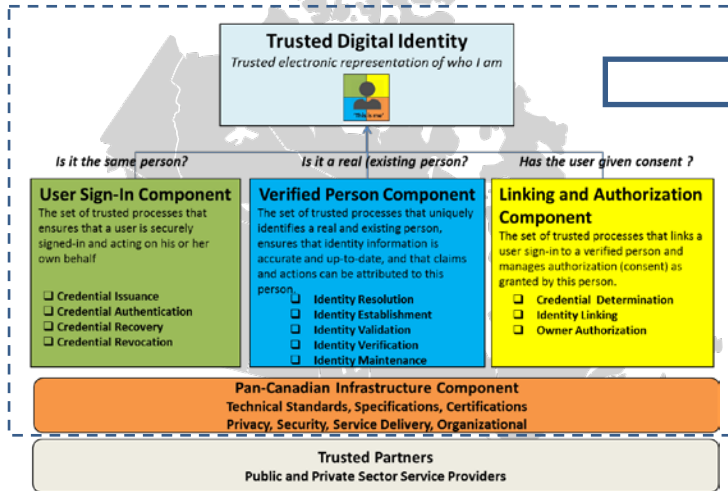
Trust Framework Deliverables: Detailed Description

Deliverable	Description	Lead
Trust Framework Approach	Pan-Canadian agreement on overall approach of trust framework. Includes strategic direction, project management, communications/briefing material as required.	<i>Joint Councils/ Identity Management Sub-Committee</i>
DIACC-IMSC MOU	Agreement outlining roles and responsibilities of DIACC and IMSC working groups and governance processes.	<i>Identity Management Sub-Committee</i>
FPT Agreement	Agreement detailing adoption and implementation of Pan-Canadian Identity Trust Framework. May include governance, business model and funding considerations.	<i>Identity Management Sub-Committee</i>
User Sign-In Trusted Component	User Sign-In Conformance Criteria Concept of Operations User Sign-In Assessment Methodology	<i>Identity Management Sub-Committee</i>
Verified Person Trusted Component	Verified Person Conformance Criteria Concept of Operations Verified Person Assessment Methodology	<i>Identity Management Sub-Committee</i>
Linking and Authorization Trusted Component	Linking and Authorization Conformance Criteria Concept of Operations Linking and Authorization Assessment Methodology	<i>Identity Management Sub-Committee</i>
Trust Framework Validation Business Process Mapping	Mapping to existing (and planned) business processes Validation of trust framework components (user sign-in, verified person, and linking and authorization)	<i>Identity Management Sub-Committee</i>
Proofs of Concept	Pilots/Demos Lessons Learned/Best Practices Application of Technical Standards	<i>ISED, CIC-PPT ESDC, CRA Telus/BC</i>
Trusted Infrastructure Component	Standardized Commercial Service Definitions Model Agreements/Contracts Business Role Definitions	<i>DIACC</i>

Mapping to eIDAS

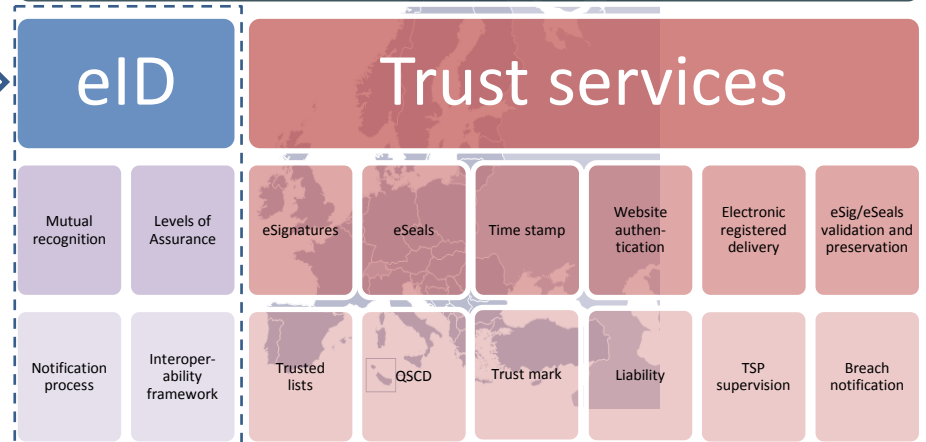
Pan-Canadian Governance (TBD)

FPT Agreement

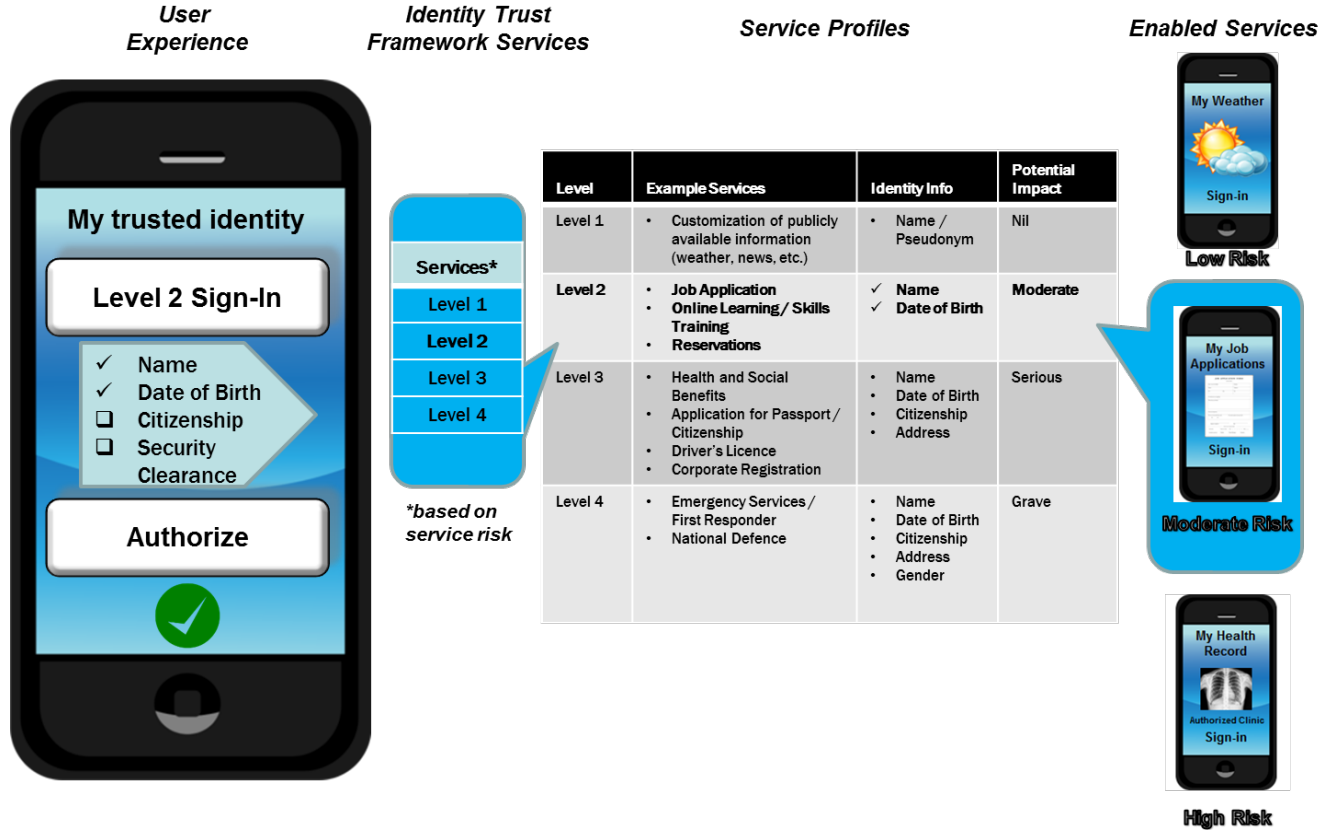


European Parliament
Council of the European Union

eIDAS Regulations



Example Services



Trusted Component Definitions

Trusted Service Category	Trusted Service Definitions	Considerations
User Sign-In: The set of services that ensure that the current user is the same person as established previously	Credential Provisioning – issuance, revocation and destruction of credentials.	<ul style="list-style-type: none"> These services together are usually considered as Credential Management Services may be offered together by a single provider, may be separated across multiple providers.
	Credential Storage – storage of credentials	
	Credential Authentication - process of generating a credential assurance.	
Verified Person: The set of services that ensure the current user is a real person	Identity Resolution the ability to uniquely distinguish a person from all other people.	<ul style="list-style-type: none"> These services, when provided together, are usually considered as Identity Management Services may be offered together by a single provider, may be separated across multiple providers.
	Identity Validation confirmation of the accuracy of the identity information.	
	Identity Notification notification that identity information has been established, changed or has been exposed to risk factors.	
	Identity Verification confirmation that the identity information relates to a specific individual making the claim.	
	Identity Establishment - Creation of the initial identity record of a person.	
Linking and Permission: The set of services that links together a user sign-in to a verified person and records permissions granted by the person indicating consent and/or authorization	Linking & Permission – The linking together of a user-sign-in to a verified person and recording permissions granted by the person indicating consent and/or authorization.	<ul style="list-style-type: none"> Can be part of a service enrolment, program registration, or account management process Consent can be relation to a specific credential; a user may have several credentials each with different consents

Standardized Identity Assurance Levels

Source: TB Standard on Identity and Credential Assurance <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776>

Level	Description
4	Very high confidence required that an individual is who he or she claims to be. <i>Compromise could reasonably be expected to cause serious to catastrophic harm</i>
3	High confidence required that an individual is who he or she claims to be. <i>Compromise could reasonably be expected to cause moderate to serious harm</i>
2	Some confidence required that an individual is who he or she claims to be. <i>Compromise could reasonably be expected to cause minimal to moderate harm</i>
1	Little confidence required that an individual is who he or she claims to be. <i>Compromise could reasonably be expected to cause nil to minimal harm</i>

Standardized Credential Assurance Levels

Source: TB Standard on Identity and Credential Assurance <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776>

Level	Description
4	Very high confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised. <i>Compromise could reasonably be expected to cause serious to catastrophic harm</i>
3	High confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised. <i>Compromise could reasonably be expected to cause moderate to serious harm</i>
2	Some confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised. <i>Compromise could reasonably be expected to cause minimal to moderate harm</i>
1	Little confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised. <i>Compromise could reasonably be expected to cause nil to minimal harm</i>

Establishing Identity Assurance Level: Minimum Requirements (1/2)

Source: TB Standard on Identity and Credential Assurance <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776>

Requirement	Level 1	Level 2	Level 3	Level 4
Uniqueness	Define identity information Define context			
Evidence of Identity	No restriction on what is provided as evidence	One instance of evidence of identity	Two instances of evidence of identity (At least one must be foundational evidence of identity.)	Three instances of evidence of identity (At least one must be foundational evidence of identity.)
Accuracy of Identity Information	Acceptance of self-assertion of identity information by an individual	Identity information acceptably matches assertion by an individual and evidence of identity and Confirmation that evidence of identity originates from appropriate authority	Identity information acceptably matches assertion by an individual and all instances of evidence of identity and Confirmation of the foundational evidence of identity using authoritative source and Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source or inspection by trained examiner	Identity information acceptably matches assertion by an individual and all instances of evidence of identity and Confirmation of the foundational evidence of identity using authoritative source and Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source or inspection by trained examiner

Establishing Identity Assurance Level: Minimum Requirements (2/2)

Table continued from previous slide...

Source: TB Standard on Identity and Credential Assurance <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776>

Requirement	Level 1	Level 2	Level 3	Level 4
Linkage of Identity Information to Individual	No requirement	No requirement	At least one of the following: i) Knowledge-based confirmation ii) Biological or behavioural characteristic confirmation iii) Trusted referee confirmation iv) Physical possession confirmation	At least three of the following: i) Knowledge-based confirmation ii) Biological or behavioural characteristic confirmation iii) Trusted referee confirmation iv) Physical possession confirmation

Applicable Frameworks and Standards

Jurisdiction / Sector	Standard or Framework
Canada	<ul style="list-style-type: none">• IATF Report (2008)• Pan-Canadian Assurance Model (2010)• Pan-Canadian Identity Validation Standard (2014)<ul style="list-style-type: none">• TB Standard on Identity and Credential Assurance (2012)• TBS Guideline on Defining Authentication Requirements• CSEC User Authentication Guidance for IT Systems
US	<ul style="list-style-type: none">• OMB M04 – 04 (2003) E-Authentication Guidance for Federal Agencies• NIST SP 800 – 63 Electronic Authentication Guideline• FICAM TFPAP• ANSI/NASPO IPDV
UK	<ul style="list-style-type: none">• GPG-44 Authentication Credentials in Support of HMG Online Services• GPG-45 Identity Proofing and Verification of an Individual (2013)• tScheme
NZ	<ul style="list-style-type: none">• Evidence of Identity Standard• Authentication Key Strength Standard
EU	<ul style="list-style-type: none">• Electronic Services and Trust Services Regulation (2014)
AUS	<ul style="list-style-type: none">• National e-Authentication Framework• National Identity Proofing Guidelines
Industry	<ul style="list-style-type: none">• Kantara Identity Assurance Framework• OIX
Financial/Payments	<ul style="list-style-type: none">• EMV Standard
ISO	<ul style="list-style-type: none">• ISO 24760 – Security – A Framework for Terminology and Concepts: Part 1