

**Update on :  
Pan-Canadian Trust Framework  
Joint Councils  
September 14, 2016**

**Identity Management Sub-Committee  
(IMSC)**

**IMSC Co-Chairs:**

**Rob Devries, Province of Ontario, Ministry of Government and Consumer Services**

**Rita Whittle, Government of Canada, Treasury Board Secretariat**

# Objectives

---

## **1. Provide an overview of Pan-Canadian Trust Framework**

- Trusted Digital Identity: Key Concepts
- Pan-Canadian Context
- Trust Framework: High-Level components

## **2. Progress update on deliverables:**

- Progress against critical path
- Key milestones since last update
- Progress of trust framework deliverables
  - Examples

## **3. Next Steps and Discussion**

# TRUSTED DIGITAL IDENTITY

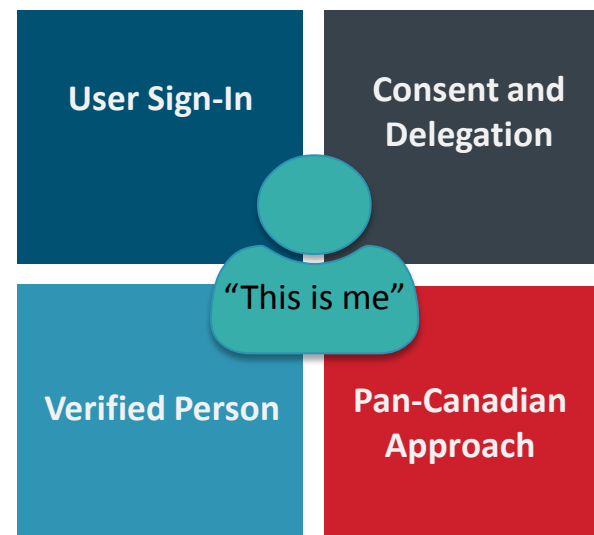
## A Trusted Electronic Representation of Who I am

A key building block for digital service



An electronic representation of a person, used exclusively by them to receive valued services and carry out transactions with trust and confidence.

### A Trusted Digital Identity consists of four main components:



1

**User Sign-In**

*'I am the same user for each interaction'*

2

**Consent and Delegation\***

*'I have given my consent'*

3

**Pan-Canadian Approach**

*'Services/capabilities are enabled using a Pan-Canadian Approach'*

4

**Verified Person**

*'I am a real person'*

# Pan-Canadian Trust Framework

## PAN-CANADIAN TRUST FRAMEWORK

An enabler for  
digital service



A set of agreed on definitions, principles, conformance criteria, and standards used consistently to ensure individuals and business are who they say they are.

### Trusted Digital Identity



Including Public Sector and Private Sector Considerations

*Is it the same person?*

*Is it a real existing person?*

*Has the user given consent ?*

#### User Sign-In Component

Set of trusted processes to ensure a user is securely signed-in and acting on his or her own behalf

#### Verified Person Component

Set of trusted processes to uniquely identify a real person, ensure identity information is accurate and up-to-date, and claims /actions are attributed to them

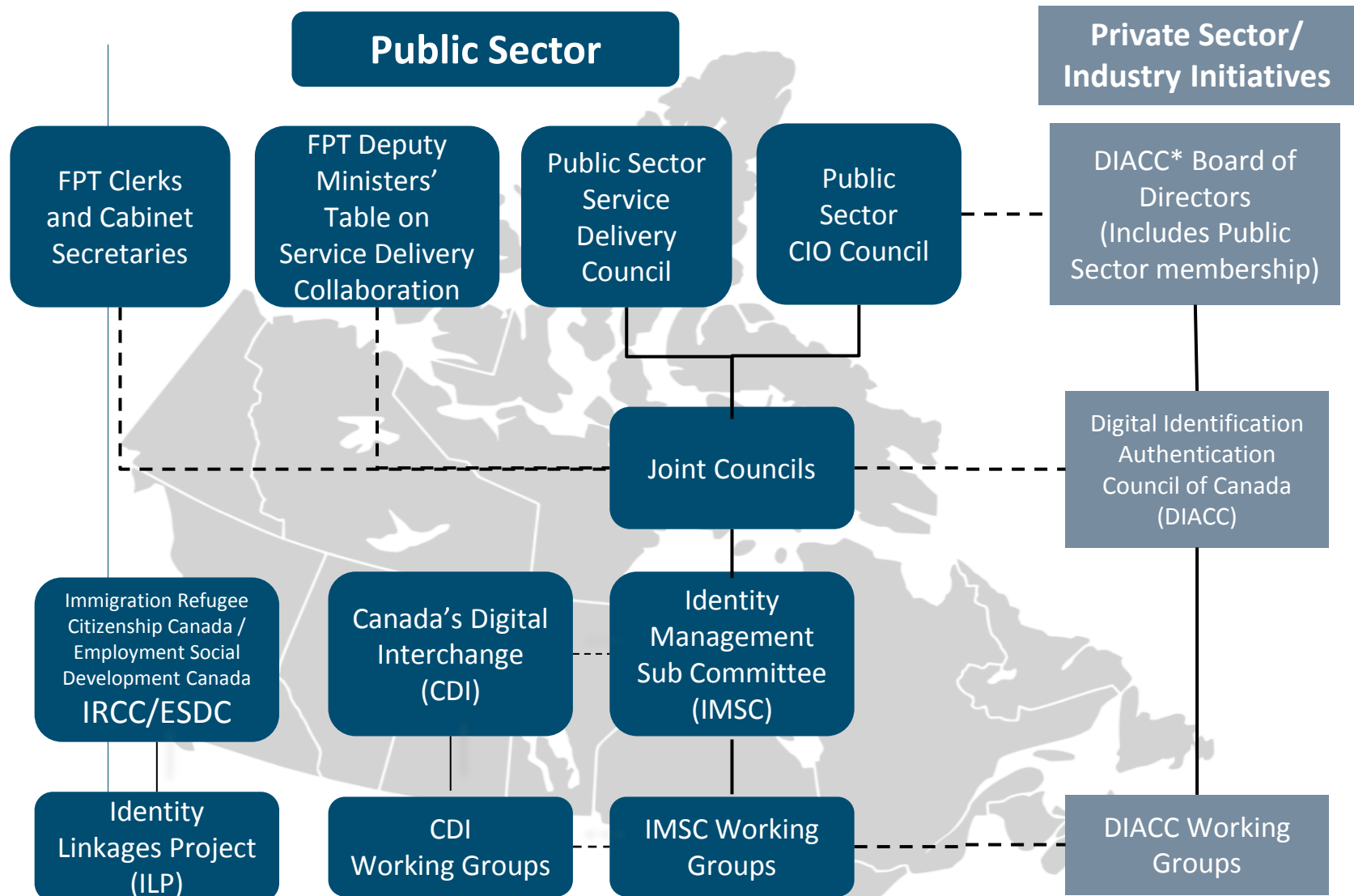
#### Consent and Delegation Component

Set of trusted processes to link a user sign-in to a verified person and manage consent as granted by them

### Pan-Canadian Infrastructure Component

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

# Pan-Canadian Trust Framework: Context



## Other Initiatives Underway

- Death Notification Project
- Business Number or Expedited Business Start
- DIACC Proof of Concept for Residency

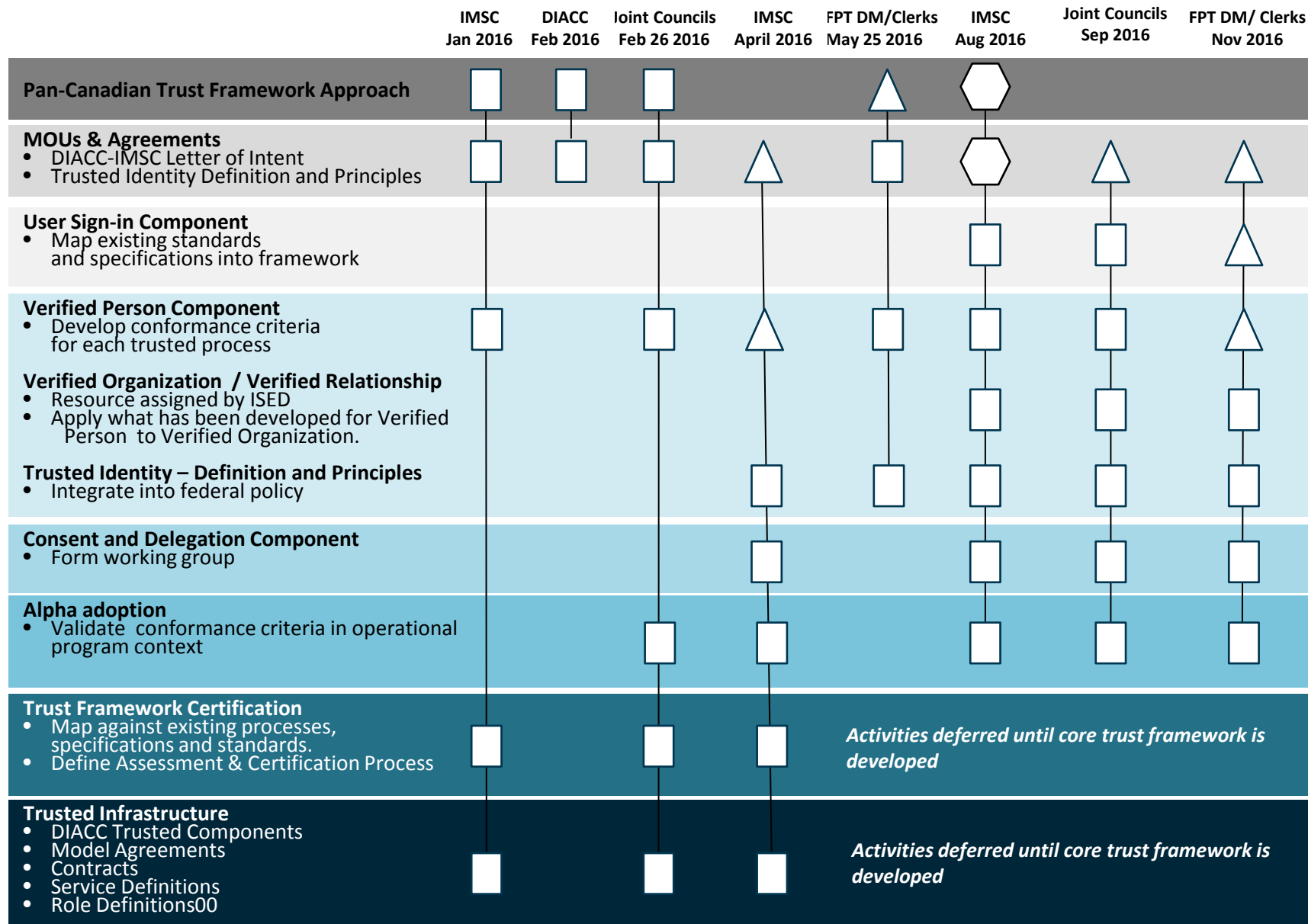
*\*Digital Identification and Authentication Council of Canada*

# Pan-Canadian Trust Framework Components



\*Focus of IMSC and DIACC Working Groups

# Pan Canadian Trust Framework: Critical Path



= update/direction



= decision/endorsement



= completed

# Key Milestones since last update (February 2016)

## 1. April 2016: IMSC Meeting

- Trusted Identity Principles endorsed by IMSC
- Letter of Intent signed between IMSC and DIACC

## 2. May 2016: In-Person Workshop

- In-Person meeting held in Ottawa

## 3. July 2016: Working Group Activities

### IMSC :

- Creation of Verified Organization Sub-Working Group
  - Engaged Business Number Working Group and Corporate Registrars
  - Call for participation
- Initiated Policy Discussion Paper (Public Sector and Private Sector Roles in Digital Identity)
- Engaged Death Registration & Notification Working Group
  - Consideration of death registration and notification as trusted processes within the framework

### DIACC:

- Creation of Trust Framework Expert Committee (formerly Trust Framework Steering Group): Leading development of User Sign-In Component

## 4. August 2016: DIACC Trust Framework Overview

- Finalized and published on DIACC website: <https://diacc.ca/2016/08/11/pctf-overview/><sub>8</sub>



# Trust Framework: Progress on Deliverables

Pan-Canadian Trust Framework	Deliverable(s)	Status	Est. Date	Lead(s)
<b>MOU &amp; Agreements</b>	<ul style="list-style-type: none"> <li>Letter of Intent</li> </ul>	Complete	Apr 2016	IMSC/DIACC
<b>Trust Framework Overview</b>	<ul style="list-style-type: none"> <li>Pan-Canadian Trust Framework Overview</li> </ul>	Published	Aug 2016	IMSC/DIACC
<b>Verified Person Component</b>	<ul style="list-style-type: none"> <li>Verified Person Component Overview</li> <li>Identity Establishment Conformance Criteria</li> </ul>	WG Draft	Nov 2016	IMSC
<b>User Sign-In Component</b>	<ul style="list-style-type: none"> <li>User Sign-In Component Overview</li> </ul>	WG Draft	Nov 2016	DIACC
<b>Consent and Delegation Component</b>	<ul style="list-style-type: none"> <li>Consent and Delegation Overview</li> </ul>	Not Started- see next steps	TBD	TBD
<b>Verified Organization Component</b>	<ul style="list-style-type: none"> <li>Verified Organization Component Overview</li> </ul>	WG Draft	Feb 2017	IMSC
<b>Verified Relationship Component</b>	<ul style="list-style-type: none"> <li>Verified Organization Component Overview</li> </ul>	Initiated	Feb 2017*	TBD
<b>Standards and Specifications</b>	<ul style="list-style-type: none"> <li>PCIM Validation Standard</li> <li>PCIM Notification Standard</li> <li>PCIM Retrieval Standard</li> <li>PCIM Information Exchange Specification</li> </ul>	Released Versions	July 2017	IMSC
<b>Discussion Papers</b>	<ul style="list-style-type: none"> <li>Digital Identity: Roles and Responsibilities of the Public and Private Sector</li> </ul>	Initiated	Nov 2016	IMSC

# Pan-Canadian Trust Framework Deliverables

## Overview and Discussion

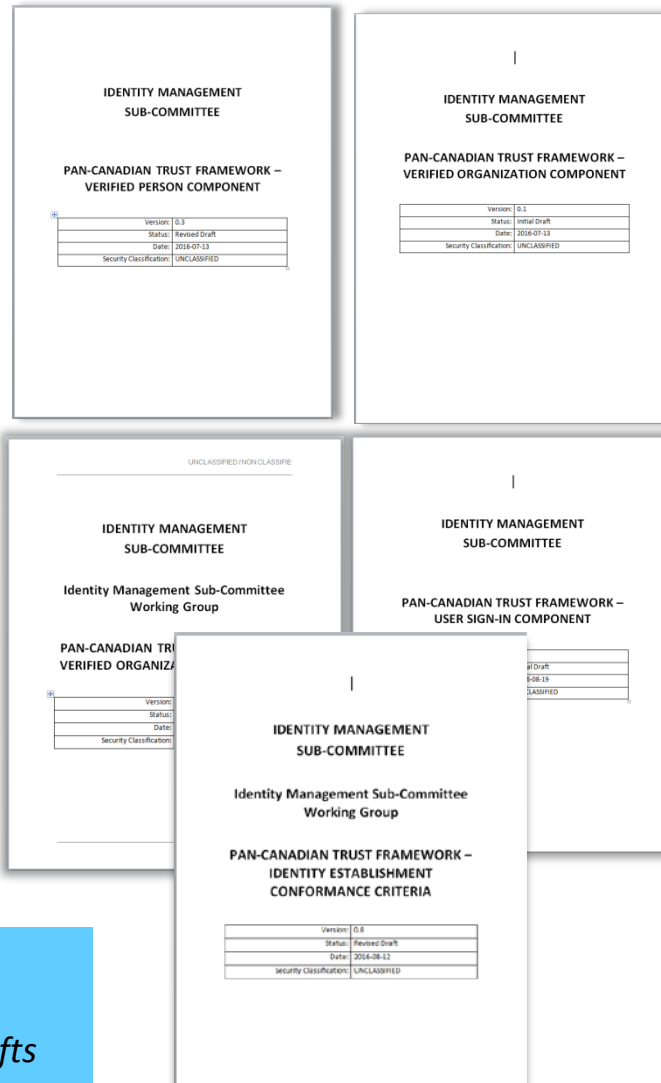


### IMSC Discussion Paper:

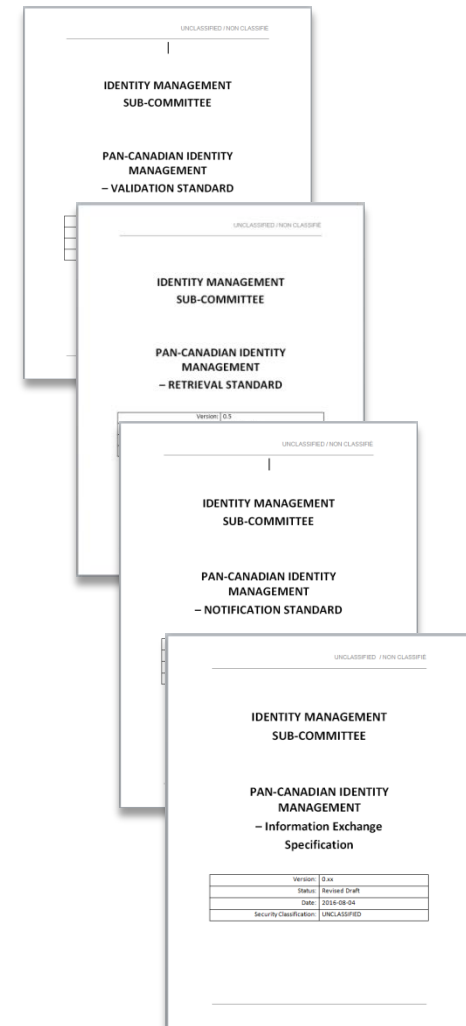
Digital Identity: Roles and Responsibilities of the Public and Private Sector

Currently the Pan-Canadian Trust Framework suite consists of 11 documents: 1 published, and 10 drafts

## Component Overviews and Conformance Criteria



## Standards and Specifications



# Example: Verified Person Component

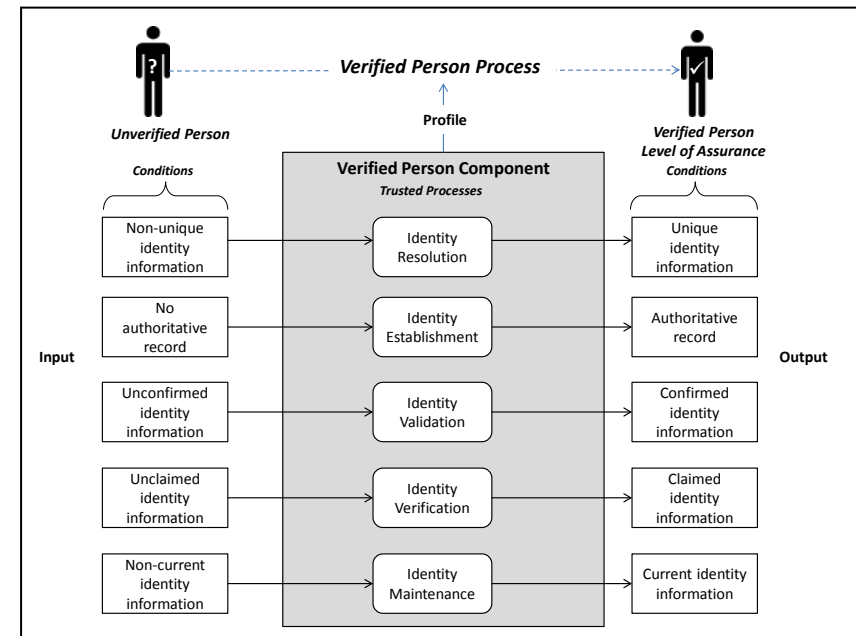
*Selected excerpts from draft deliverable:*

## Overview

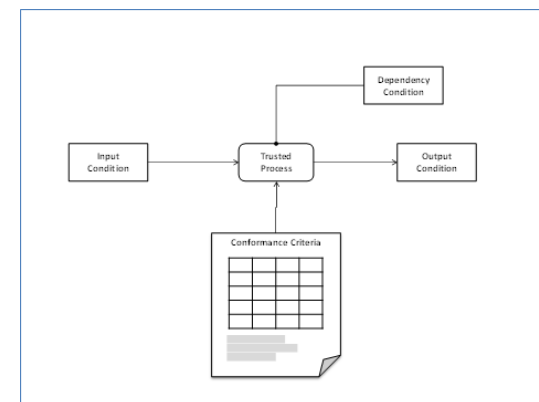
The Verified Person Component defines a set of processes used to verify that an individual is real, identifiable, and truthfully claimed who he or she is. The processes ensure identity information relating to the individual exclusively resolves to the individual only, is confirmed as accurate, is rightfully claimed by the individual (i.e., not being used by an imposter), and is up-to-date.

The Verified Person Component consists of elements that include the following:

- **Trusted Processes** – the set of processes that conform to criteria (conformance criteria) specified by the trust framework and on which may be relied by others
- **Conditions** – the particular states or circumstances relevant to verifying a person
- **Inputs** – into trusted process – an unverified person
- **Outputs** – outputs resulting from trusted processes – a verified person and the qualifier, level of assurance
- **Dependencies** – relationship between trusted processes
- **Profiles** – profiles used to ensure consistency of implementation, specify additional criteria, and facilitate trust framework certification.



## Verified Person Trusted Processes



## Trusted Process and Conformance Criteria

# Next Steps and Discussion

## 1. IMSC and DIACC Working Groups

- Continued development of Pan-Canadian Trust Framework deliverables in IMSC and DIACC working groups.
  - Develop Trust Framework Conformance Criteria and Profiles
- Coordinate efforts with other working groups
  - Canada's Digital Interchange
  - Death Registration & Notification
- Begin testing of trust framework conformance criteria
  - 'Alpha Adoption' Program
- Initiate Consent and Delegation working group
  - Reach out to Privacy and Service Delivery communities to lead this work.

## 2. FPT DM Table (November 2016)

- Present progress regarding Pan-Canadian Trust Framework in November 2016
- Seek endorsement on: Verified Person, Verified Organization, User-Sign-in components

## 3. Other Activities

- International Identity Meeting, Ottawa, November 1-3, 2016
- DIACC Industry Day, Ottawa, November 2-3, 2016

# Additional Slides

## IDENTITY : FUNDAMENTAL TO CANADIAN SOCIETY

**Identity is fundamental to Canadian society as it is the starting point of trust and confidence in interactions between the public and governments and government to government**

Pan-Canadian Trust Framework

Trusted Digital Identity

Canada's Digital Interchange (CDI)

Key to improve  
digital service  
and enhance  
security

### All jurisdictions and sectors have a role to play to advance this priority

- ✓ PTs are the authoritative sources of identity information for persons born in Canada in their respective jurisdictions
- ✓ The federal government is the authoritative source of identity information of persons born abroad

# 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***

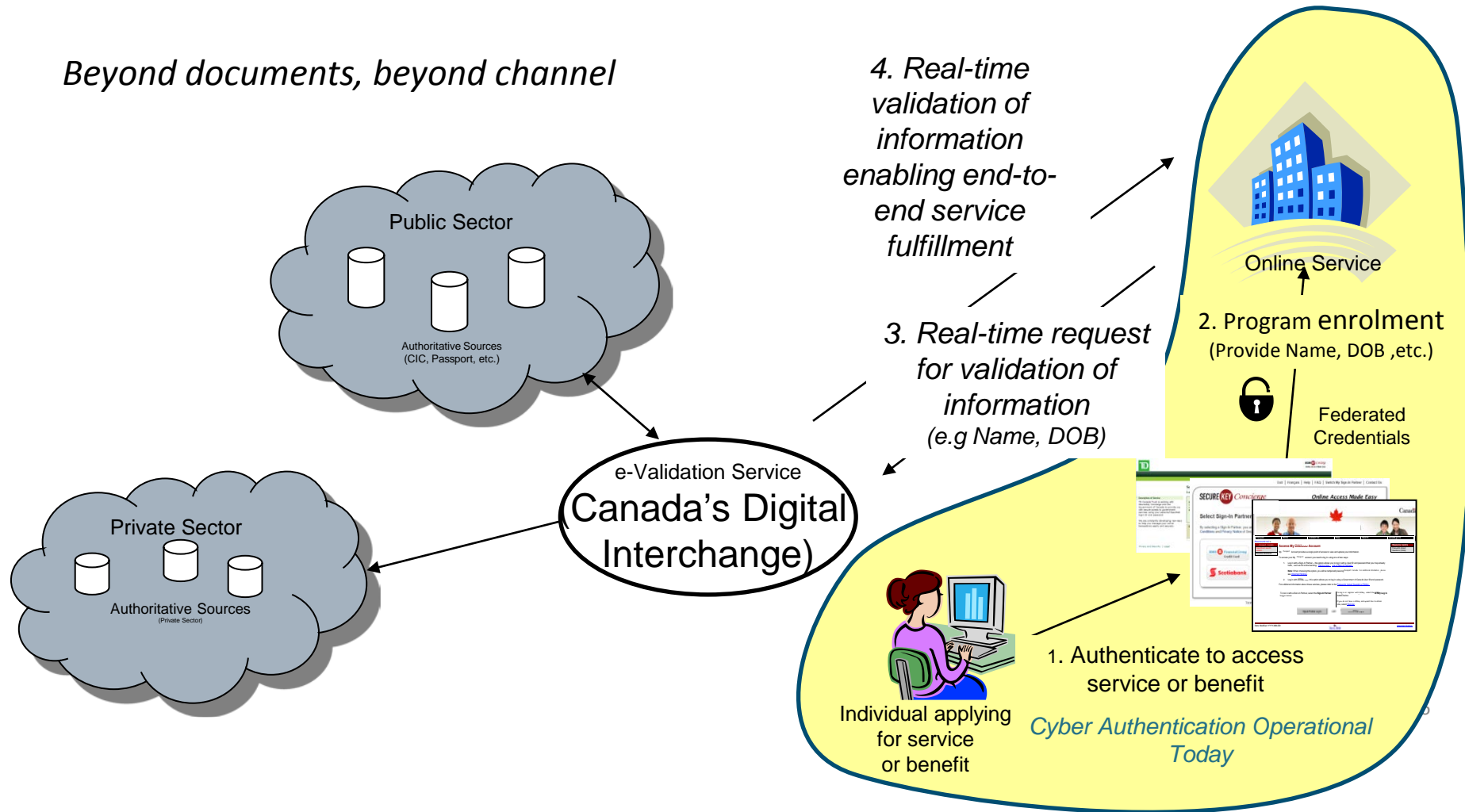


### ***Business Value***

- ***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***

# Federating Identity

*Beyond documents, beyond channel*





# Identity Management

Key to improve  
service and  
enhance security

## Identity Management

**Identity is fundamental to Canadian society as it is the starting point of trust and confidence in interactions between the public and governments and government to government**

Governments need to know that their **clients are who they say they are...**

- **Documents alone cannot provide assurance** of identity for digital delivery
- **Electronic means of validating identity is required** for secure online transaction

Governments need ways to **trust identity information that travels across jurisdictional boundaries**

- Need to ensure that **identity information remains up to date**
- Need to provide Canadians with a more **streamlined and secure** way to interact with governments

**All jurisdictions and sectors have a role to play to advance this priority**

- ✓ PTs are the authoritative sources of identity information for persons born in Canada in their respective jurisdictions
- ✓ The federal government is the authoritative source of identity information of persons born abroad

# 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)

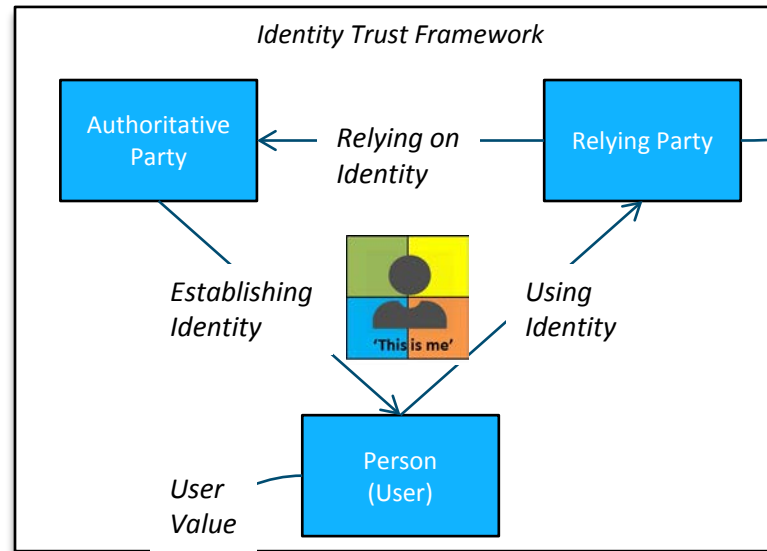
## Government Program Authority



### *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



## 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.

## 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.

# Federating Identity: Milestones and Initiatives

## 2004-2016

### 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: Background<sup>1</sup>
- ✓ 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 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

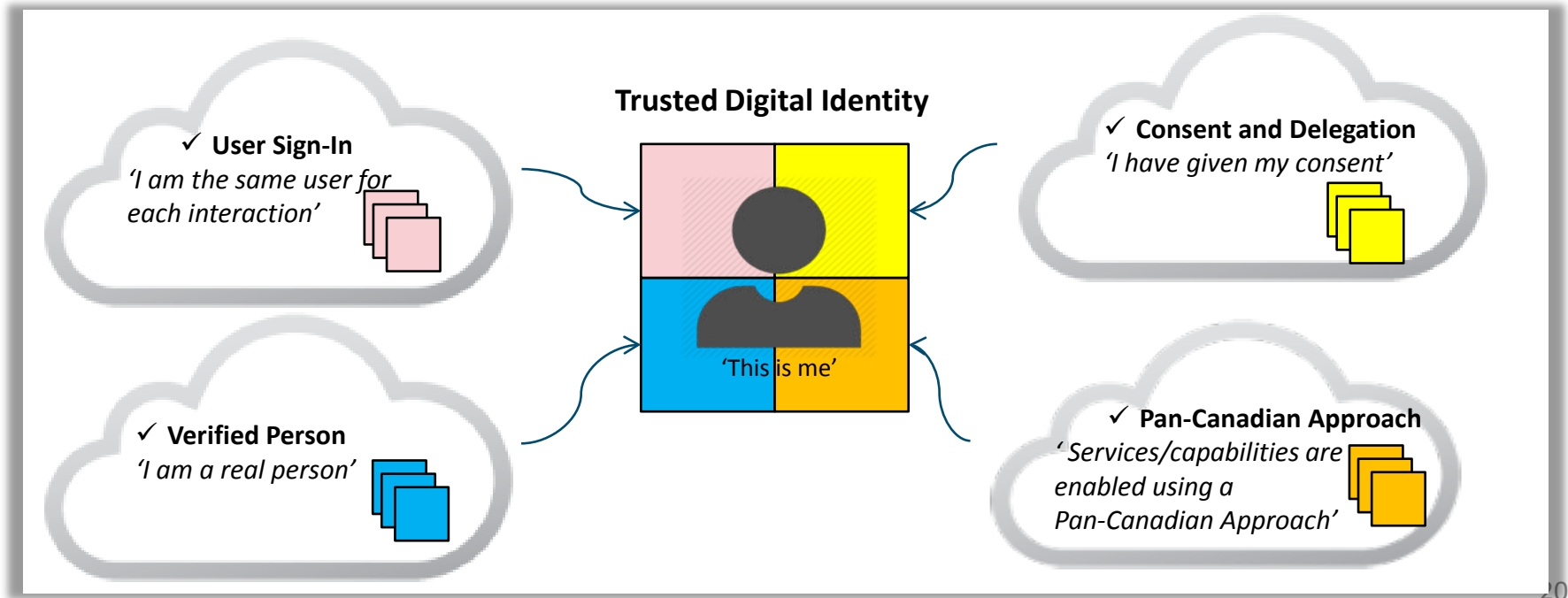
#### **Related Arrangements & MOUs**

- Citizenship Certificate Validation (CIC & Provinces)

# Trusted Digital Identity

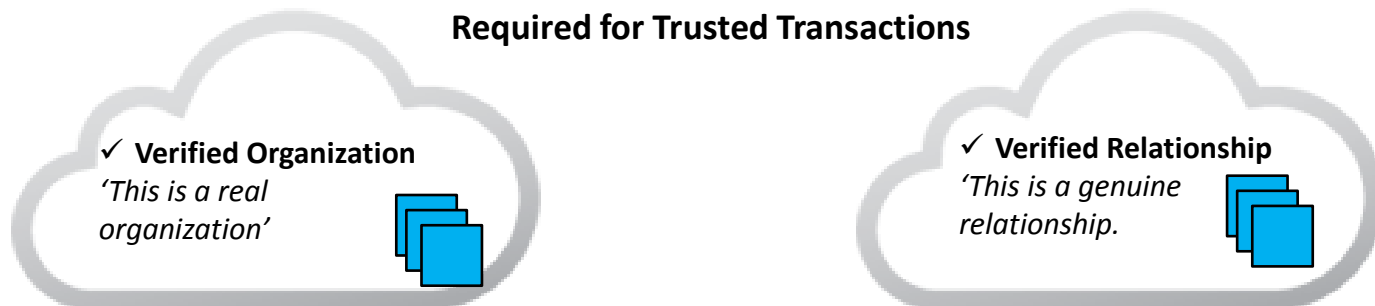
*'A trusted electronic representation of who I am.'*

A trusted digital identity consists of four main components:



20

## Required for Trusted Transactions



20

# IMSC Members

## **Federal**

Rita Whittle, IMSC Co-Chair  
Anik Dupont  
Natalie McGee  
Patti Pomeroy  
Caitlin Imrie  
Cynthia Leblanc  
Silvano Tocchi

## **BC**

Ian Bailey  
Patricia Wiebe

## **Alberta**

Roy Enslev  
Jackie Stankey

## **Saskatchewan**

Allison Daku

## **Manitoba**

Shannon Roe  
Patrick Hoyer

## **Ontario**

Rob Devries, IMSC Co-Chair

## **Quebec**

Guy Gagnon

## **New Brunswick**

Julie Mason

## **Nova Scotia**

Glen Bishop  
Arlene Williams

## **PEI**

Tim Garrity

## **Newfoundland and Labrador**

Jamie Hutchings

## **Yukon**

Chris Bookless  
Sean McLeish

## **Northwest Territories**

Linda Maljan