Update on:
Pan-Canadian Identity Trust Framework
&
Pan-Canadian Identity Validation Standard

Joint Councils

March 4, 2015

Identity Management Sub-Committee
(IMSC)

Objectives

To provide an update on progress made since our last meeting in September 2014 on:

A. Pan-Canadian Identity Trust Framework
B. Pan-Canadian Identity Validation Standard

A. Update on Pan-Canadian Identity Trust Framework

Progress since September 2014

- **October 2014:** Working model developed in Pan-Canadian Trusted Identity Workshop held in Ottawa

- **November 2014:** Provided update to FPT Deputy Ministers' Table on Service Delivery Collaboration

- **January 2015** – Framework presented to the FPT Clerks and Cabinet Secretaries as component of the Priority on Identity Management (see additional slides)
- Regularly-scheduled IMSC Working Group Calls
  - Refinement of framework
  - Vital Statistics members are now regular attendees

Alignment to Vision & Business Value

Pan-Canadian Vision (2014):

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

Business Value

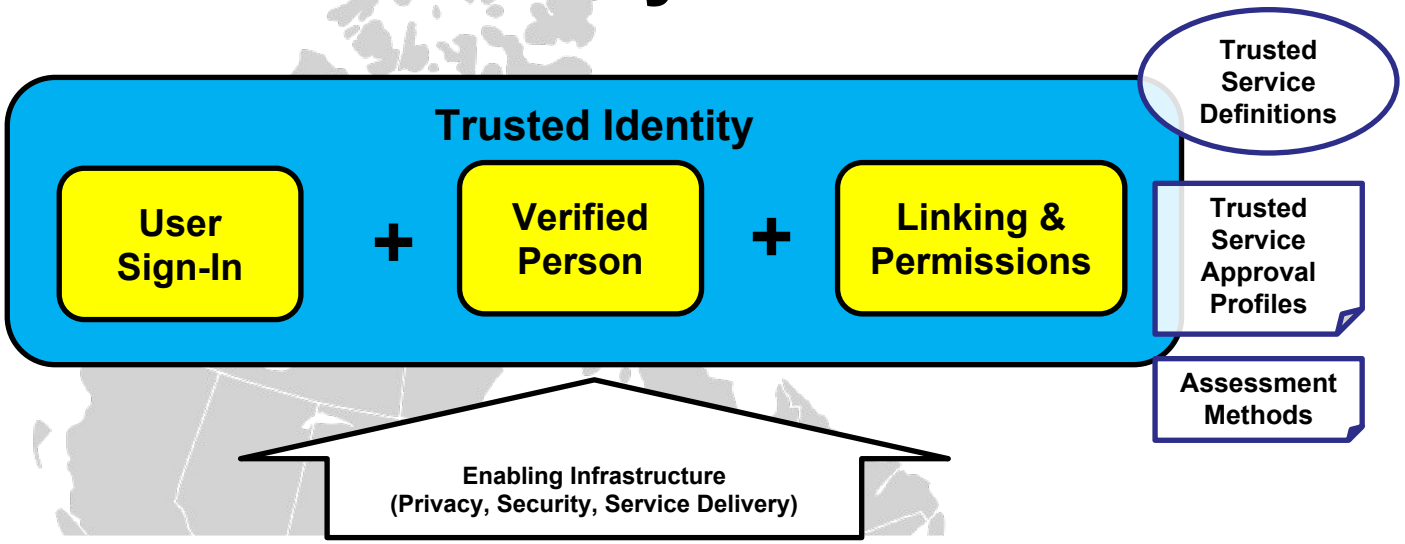
- *Enables a whole-of-government approach for seamless e-service delivery*
- *Improves client experience and user convenience by supporting a "tell-us-once" approach*
- *Enables jurisdictions to trust and leverage each other's identity and assurance processes*
- *Reduces the risk that the individual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

Pan-Canadian Identity Trust Framework

Enables a trusted identity to be relied on as a digital alternative to an in-person or document-based process

Pan-Canadian Identity Trust Framework

Current working group version



User Sign-In

1. Credential Provisioning
2. Credential Storage
3. Credential Authentication

Verified Person

1. Identity Resolution
2. Identity Validation
3. Identity Notification
4. Identity Verification
5. Identity Establishment

Linking and Permissions

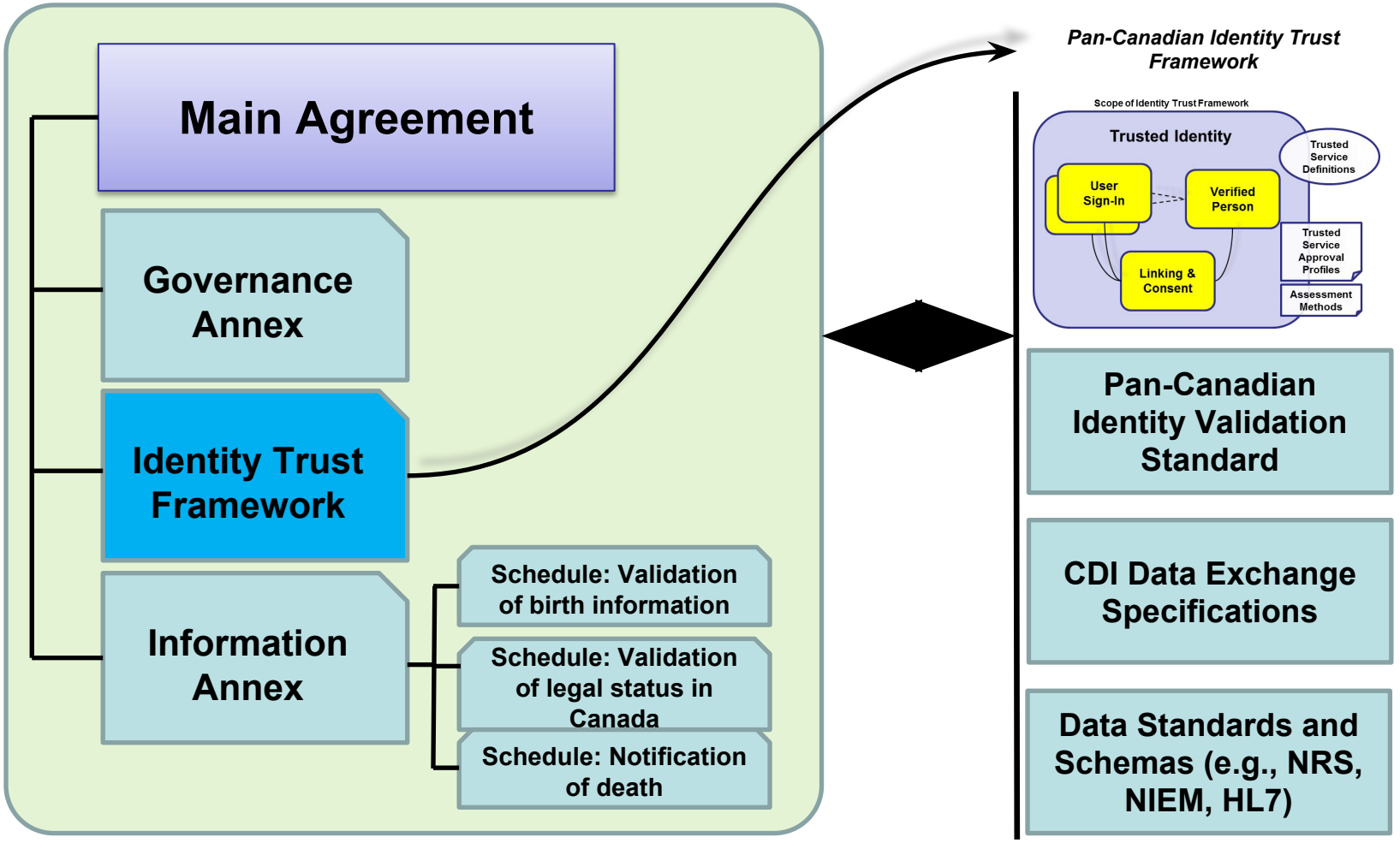
1. Linking and Permissions

These services may be delivered independently by different providers across different jurisdictions but must work together according to a Trusted Service Profile.

Detail on Trusted Service Definitions and Trusted Service Approval Profile can be found in the additional slides

Pan-Canadian Identity Trust Framework

The identity trust framework is an important component to an MOU or FPT Agreement



Pan-Canadian Trust Framework
Next Steps

1. Expand participation in development of trust framework (i.e., include wider scope of participants, i.e., business/program owners, service delivery)
   - Call for broader participation

2. Working Group to develop detailed service definitions and approval profiles
   - **Service Definition:** a detailed description of the trusted service.
     - Use existing CDI Service Definitions for Identity service definitions
     - Develop Linking and Permissions service definitions.
   - **Approval Profile:** an agreed-on set requirements and criteria used to approve a trusted service
     - Initial Focus: Identity Validation and Identity Establishment
3. Report to FPT DM Table in May 2015
   - Provide update to Joint Councils (PSSDC/PSCIOC) in March/April teleconference calls.
   - Present draft framework

B. Update on Pan-Canadian Identity Validation Standard

Progress since September 2014:

- **November 2014:** Updates provided to PSCIOC and PSSDC
- **November 25, 2014** Version 1.0 of Standard was approved by the Federal, Provincial and Territorial (FPT) Deputy Ministers' Table on Service Delivery Collaboration (Version 1.0)
- **January 2015** – Standard presented to the FPT Clerks and Cabinet Secretaries as component of the Priority on Identity Management (see additional slides)

- **Implementation of Standard**
  - Providing support to CDI Team and other projects
  - Revisions to correct minor errors, improve readability and presentation, and clarify concepts.
  - Currently incorporating revisions into subsequent draft.

Pan-Canadian Identity Validation Standard: Next Steps

1. Continue to support jurisdictions and project implementations

2. Finalize proposed revisions
   - Mature the application and adoption of the Standard

3. Report to FPT DM Table in May 2015
   - Provide update to Joint Councils (PSSDC/PSCIOC) in March/April teleconference calls.

Additional Slides for Pan-Canadian Identity Trust Framework

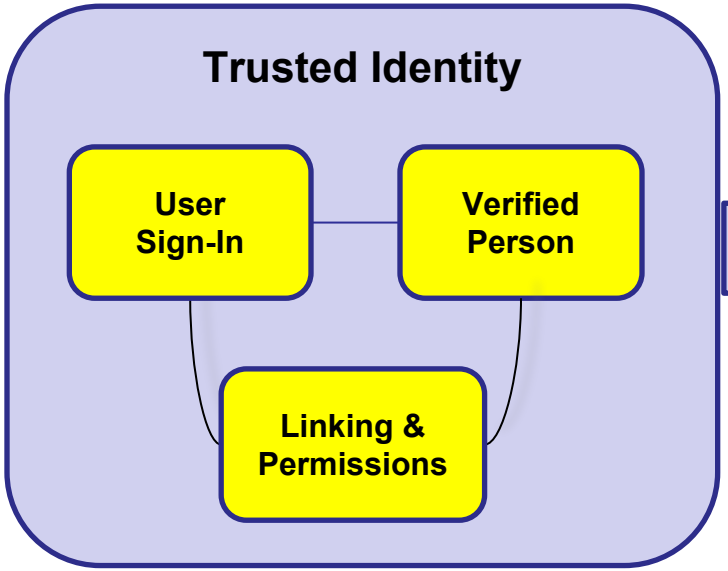
What Makes Up a Trusted Identity?

A trusted identity is made up of three sets of trusted services working together:

1. **User Sign-In:** The set of services that ensure that the current user is the same person as established previously. User Sign-In Services include: **credential provisioning**, **credential storage** and **credential authentication** services. .
2. **Verified Person:** The set of services that ensure the current user is a real person. Verified Person Services include: **identity resolution**, **identity validation**, **identity notification**, **identity verification**, and **identity establishment** services.
3. **Linking and Permission Services:** 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.

SpiderMan99/P3T3rP%RK#r

✔ **"My credentials"**



Digital Identity

✔ **"This is me"**

A digital identity cannot be assumed to be a trusted identity

✔ **"I agree"**

These services can be provided together, or separately within a larger ecosystem of trusted services

Ecosystem of Trusted Services

*Enabled by **Trusted Service Profiles** (to be defined in detail)*

Trusted services may be provided by public or private sector service providers (or both)

Trusted services are subject to privacy and security requirements (using applicable frameworks)

Service Category	Trusted Service	Trusted Service Profiles			
		Level 1	Level 2	Level 3	Level 4
User Sign-In	Credential Provisioning				
	Credential Storage				
	Credential Authentication				
Verified Person	Identity Resolution				
	Identity Validation				
	Identity Notification				
	Identity Verification				
	Identity Establishment				
Linking and Permissions	Linking-Mapping				
	User Consent				
Privacy	Privacy Protection	*Applicable Privacy Framework*			
Security	Security	*Applicable Security Framework*			
		elivery Framework			

Legend	*Commercial and/or Public Sector Providers*	*Public Sector Providers Only*	*Specialized Providers (e.g. Law Enforcement)*

*Each cell represents an agreed-on **Trusted Service Approval Profile** (see following slide)*

Trusted Service 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.	• 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.	• 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.	• 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

Trusted Service Approval Profile

- The set of agreed-on requirements and criteria necessary to approve a trusted service
  - Similar to:
    - UK tScheme Approval Profile http://www.tscheme.org/profiles/IdP_digest_2.html
    - US FICAM TFPAP http://www.idmanagement.gov/approved-identity-services
- Trusted Service Approval Profiles are used to
  - specify who can (or can't) provide the trusted service
  - map against existing or applicable frameworks (e.g. TFPAP, Kantara, etc.)
  - Specify additional constraints in using the service.
  - Assess a service before it can participate in the larger ecosystem

Applicable Frameworks and Standards

Jurisdiction / Sector	Standard or Framework

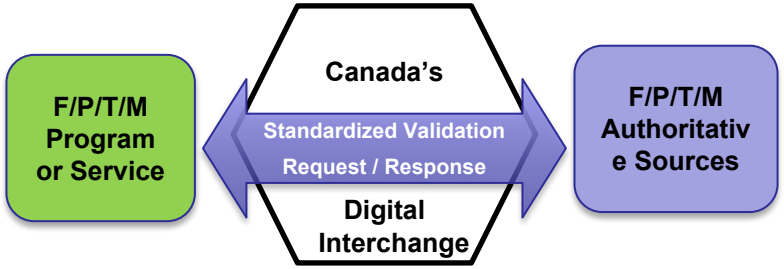
Canada	• IATF Report (2008)
	• Pan-Canadian Assurance Model (2010)
	• Pan-Canadian Identity Validation Standard (2014)
	  • TB Standard on Identity and Credential Assurance (2012)
	  • TBS Guideline on Defining Authentication Requirements
	  • CSEC User Authentication Guidance for IT Systems

US	• OMB M04 – 04 (2003) E-Authentication Guidance for Federal Agencies • NIST SP 800 – 63 Electronic Authentication Guideline • FICAM TFPAP • ANSI/NASPO IPDV
UK	• GPG-44 Authentication Credentials in Support of HMG Online Services • GPG-45 Identity Proofing and Verification of an Individual (2013) • tScheme
NZ	• Evidence of Identity Standard • Authentication Key Strength Standard
EU	• Electronic Services and Trust Services Regulation (2014)
AUS	• National e-Authentication Framework • National Identity Proofing Guidelines
Industry	• Kantara Identity Assurance Framework • OIX
Financial/Payments	• EMV Standard
ISO	• ISO 24760 – Security – A Framework for Terminology and Concepts: Part 1

Additional Slides for
Pan-Canadian Identity Validation Standard

Slide as presented to FPT Clerks and Cabinet Secretaries in January 2015

PRIORITY 1: Identity Management
Pan-Canadian Identity Validation Standard



Standardized Validation of Personal Information

1. Name
2. Date of Birth
3. Sex, Gender or Documented Sex
4. Place of Birth
5. Date of Death
6. Place of Death
7. Assigned Identifiers
8. Status
9. Address
10. Associated Person

Standard is now available

Table Priority: Identity Management

Recent Progress:

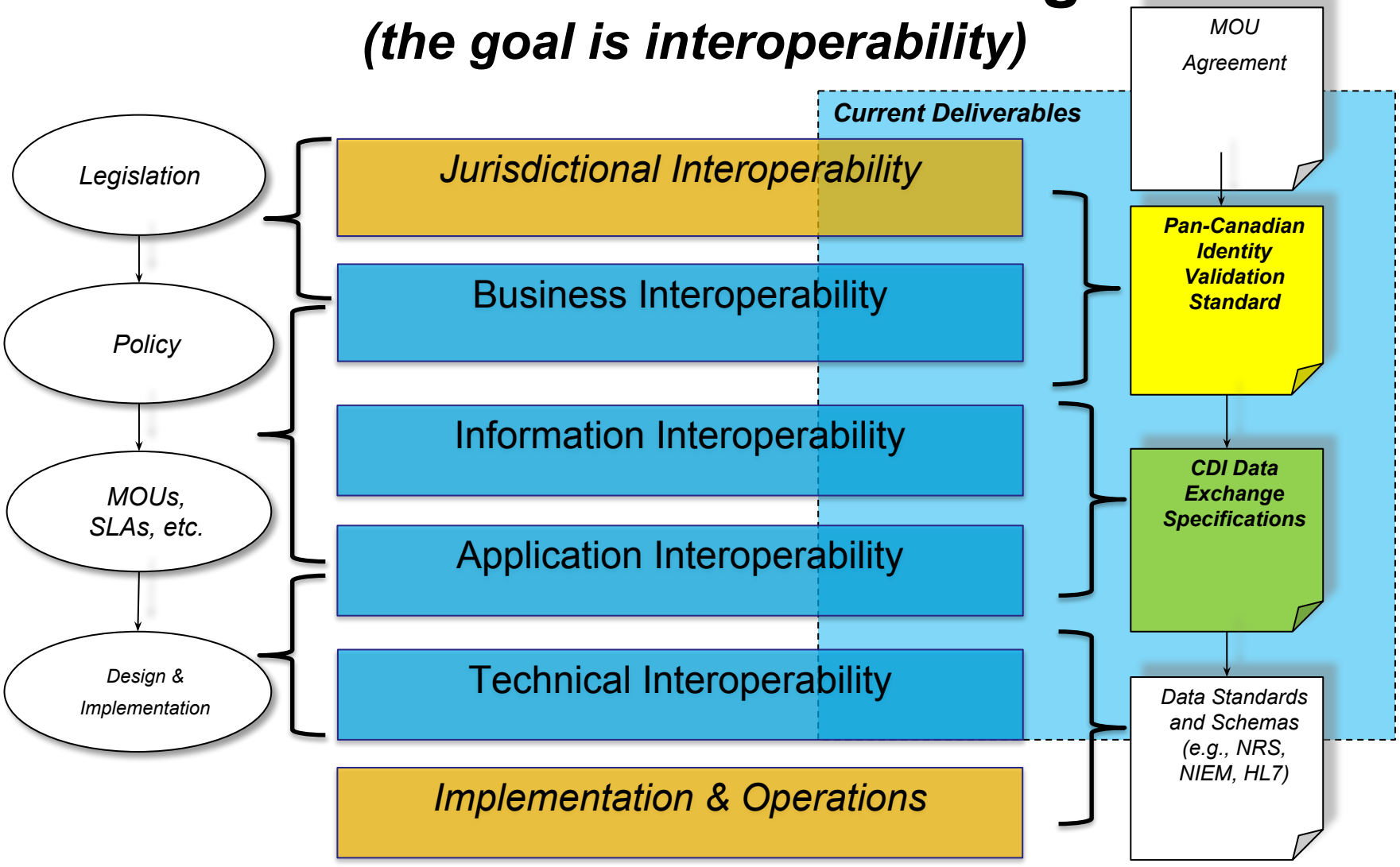
- **May 2014:** Update to F-P/T DM Service Delivery
- **May-Nov 2014:** Ongoing Interjurisdictional
- **Sept 2014:** Update to Joint Councils
- **Oct 2014:** Finalized draft of Standard
- **Nov 2014:** FPT DM Approval

Planned Work:

- Continued engagement in jurisdictions
  - Scheduled WebEX sessions
  - Application of Standard to Pilot Projects

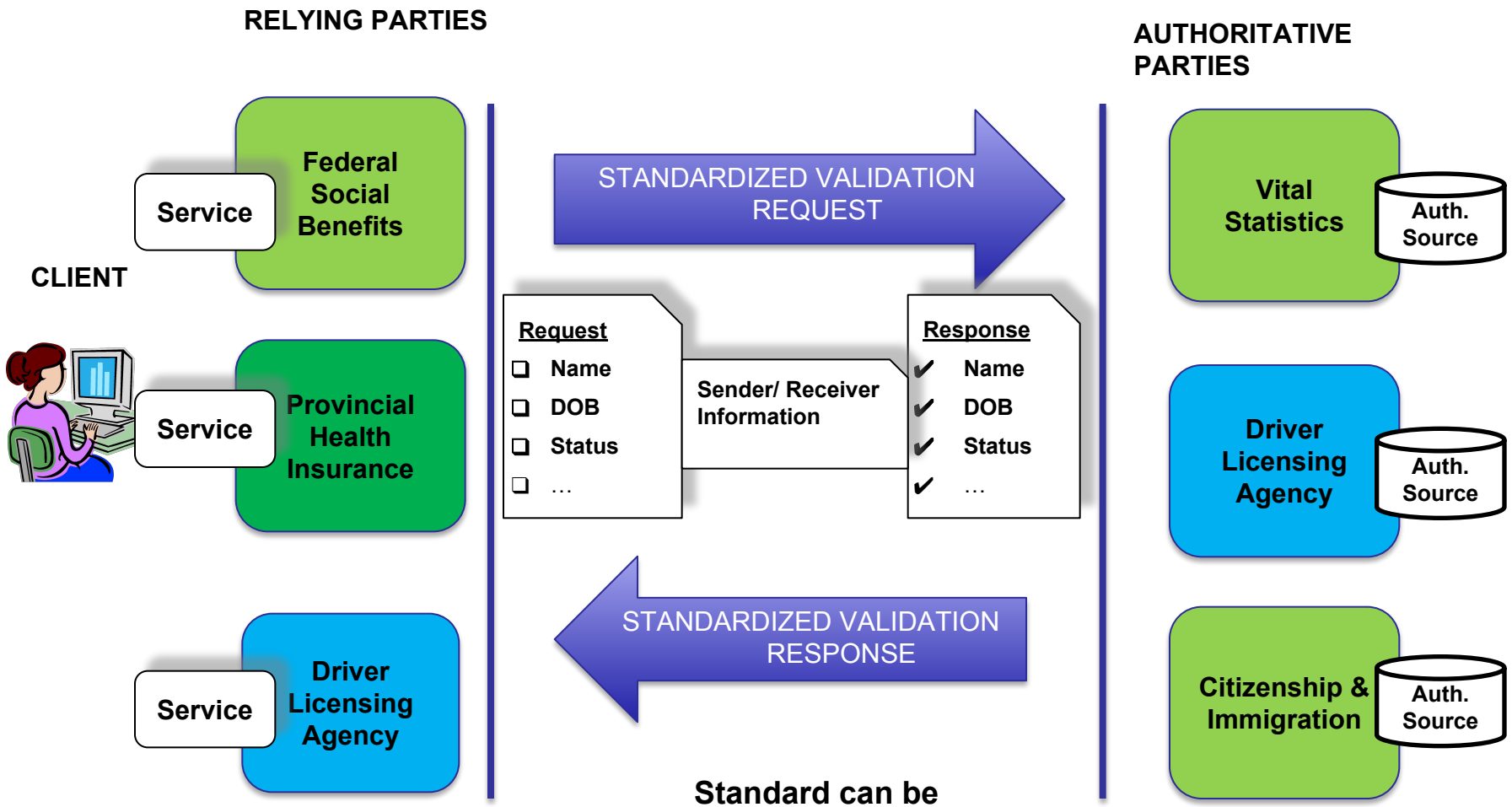
How the Standard fits in the Big Picture

(the goal is interoperability)



*GC Interoperability Framework

Generic Identity Validation Use Case



Implementation Example

Standard provides jurisdictions with a flexible framework to: 1) specify validation and matching requirements for 2) specific categories of personal information

Joe Public

Collect

RELYING PARTY F/P/T/M Program or Service

Digital Interchange

Validation Request / Response

Implementation

AUTHORITATIVE PARTY F/P/T/M

Validate

Auth. Source

Vital Stats

Prov. DL

Fed. CIC

e.g. (not exhaustive),
Vital Statistics
Driver's Licensing
Citizenship & Immigration

Validation Requirements

1. **Identity Information Validation:** validation of information used to uniquely identify an individual (e.g. name, date of birth, etc.)
2. **Personal Information Validation:** validation of information used for program and eligibility purposes (e.g. address, citizenship, status, etc.)
3. **Additional Identity Information:** personal attributes that may be provided as part of validation request to assist in resolving to a unique individual.

Validation of Personal Information

1. **Name**
2. **Date of Birth**
3. **Sex, Gender or Documented Sex**
4. **Place of Birth**
5. **Date of Death**
6. **Place of Death**
7. **Assigned Identifiers**
8. **Status**
9. **Address**
10. **Associated Person**

Trust Framework Based on Assurance Levels