Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Better government: with partners, for Canadians

Government of Canada Update

Municipal CIO Summit

April 10-12, 2014

Banff, AB

Canada

Outline

- Government of Canada Update
  - Road Map & Policy Architecture
- Cyber Authentication Statistics
  - Usage Statistics to date
- Identity Management Sub-Committee Update
  - Pan-Canadian Identity Validation Standard
- Pan-Canadian ID Hub Network
- Questions and Discussion

Government of Canada Update

Identity is the Starting Point for High Value Services, Benefits and Entitlements

Today, identity is managed separately by each sector…

Financial Sector

Who are you?

How will you pay?

Identity risks

Sector Issues

- Financial fraud
- Money laundering
- Higher transaction fees

Public Sector

Who are you?

Are you eligible for a government benefit?

Identity risks

Sector Issues

- Benefits fraud
- Longer processing times
- Redundant processes

Healthcare Sector

Who are you?

What is your medical history?

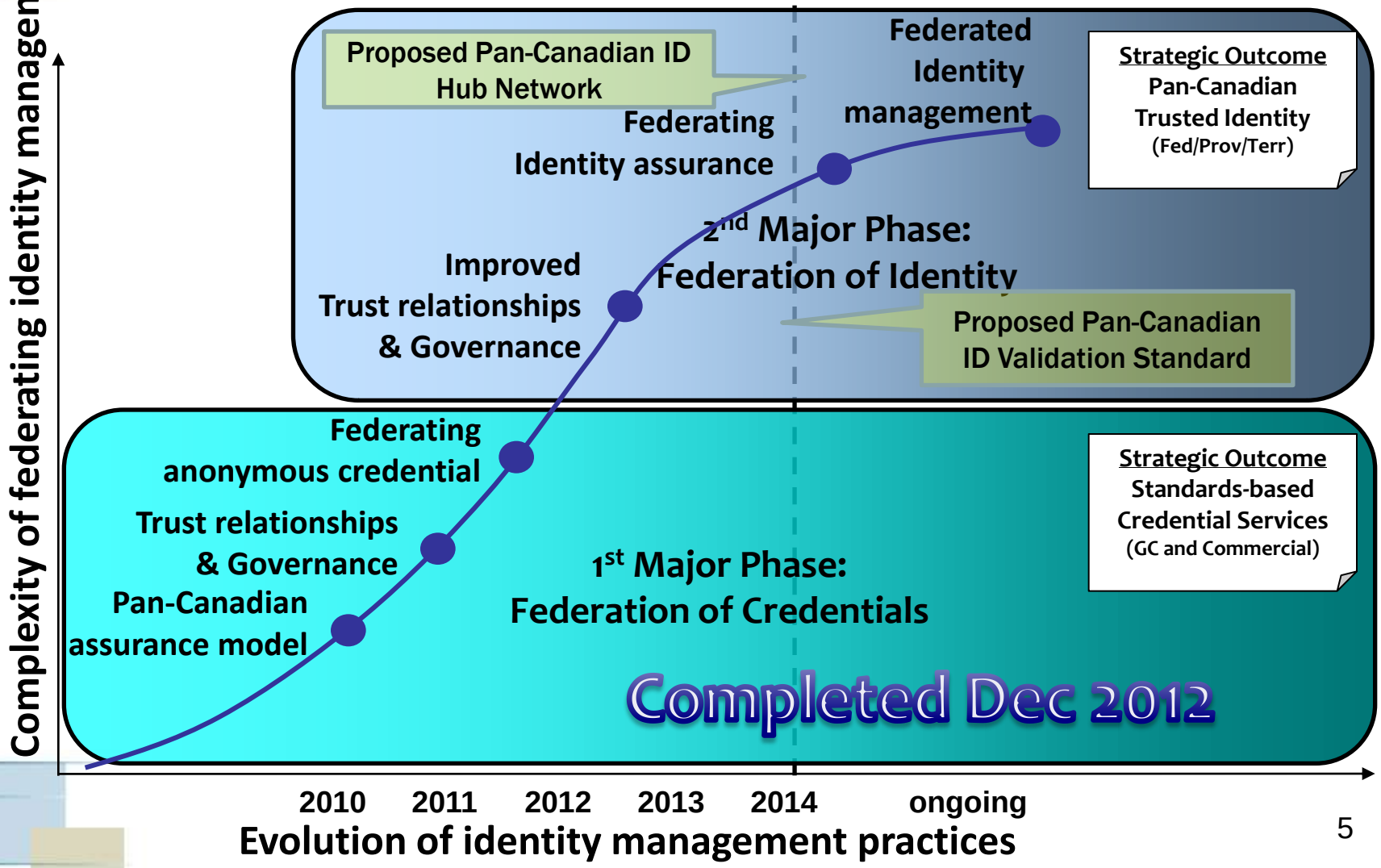
Identity risks

Sector Issues

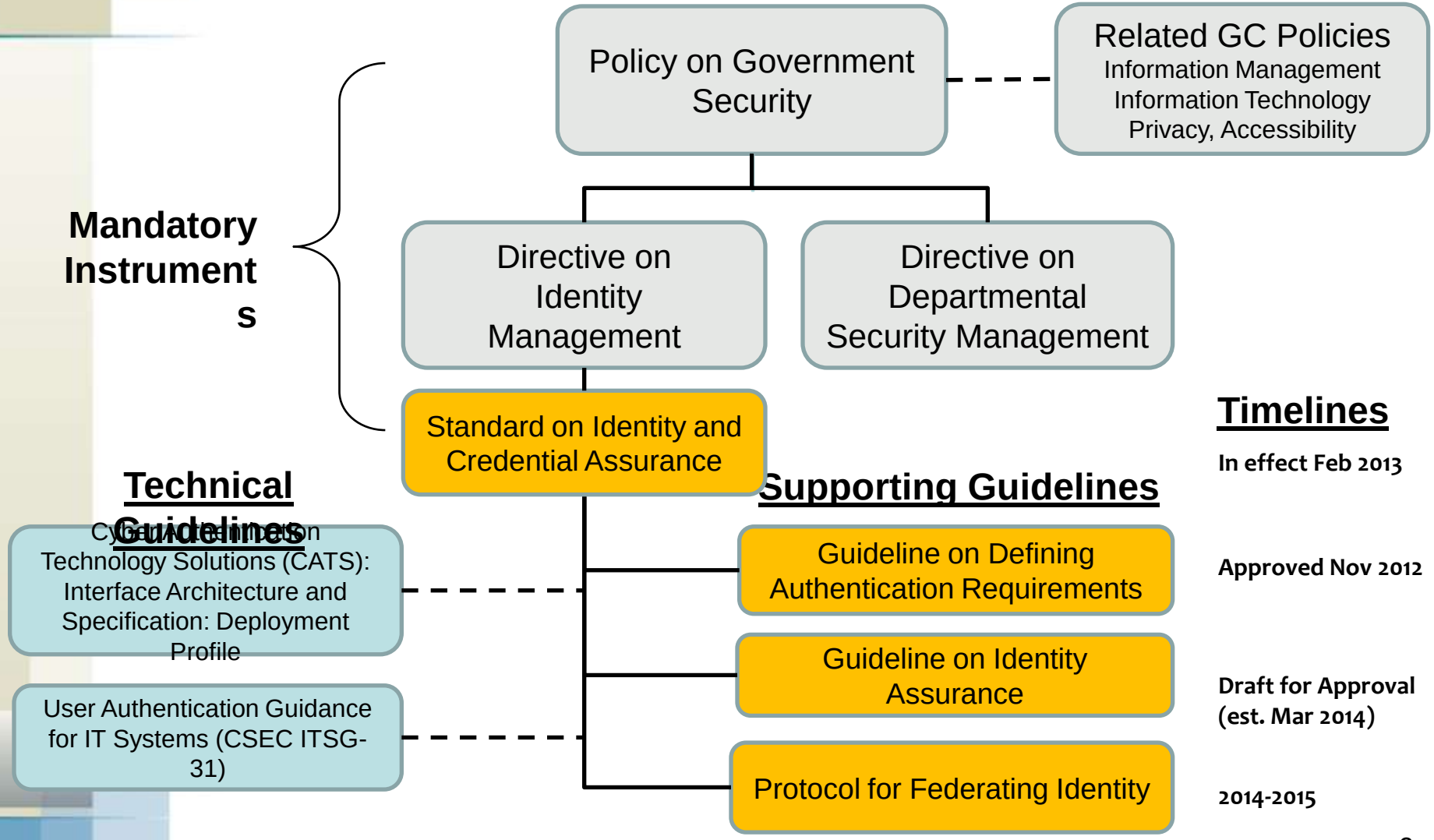
- Prescription fraud
- Patient Privacy
- Record integrity

… but the impacts are felt by everyone

Federating Identity Road Map: Major Phases



Treasury Board Policy Architecture



Cyber Authentication Renewal

- **Client choice for single, secure sign in to Government of Canada online services**
  - Foundational to the GC's Federating Identity Strategy
  - Leverages private sector investment in secure infrastructure
    - Enhanced service to Canadians
    - Cost efficiency

Cyber Authentication Renewal

- **4.7M clients accessing services from 26 Government of Canada departments**
  - Sign In Partners (BMO Financial, CUETS (Credit Union Electronic Transaction Services), ING Direct, ScotiaBank, TD Bank Group): **approx. 1.02M credentials issued to date**
  - GCKey (GC issued credential): **approx. 3.7M credentials issued to date**

Identity Management Sub Committee Update

Approach to Developing Pan-Canadian Identity Validation Standard

In May 2013, FPT Deputy Ministers of Service Delivery agreed to the following:

- Develop a Pan-Canadian Identity Validation Standard, so that all jurisdictions use consistent terminology in the validation of key identity information and related attributes.

Build upon National Routing System (NRS) Data Exchanges Standard

- NRS is a "Made in Canada" standard agreed to and is used in practice by jurisdictions.
- Established community familiar with the NRS standard.
- Existing systems and services in production using the NRS standard
- NRS standard has in place a conceptual framework that can be extended (validation, notification, etc.)

Extension to Identity Validation includes:

- Definition of identity information
  - Core identity attributes, other personal attributes, additional matching Criteria
- Incorporation of assurance level concept
- Developing "rules: for providing and using identity validation services, e.g.,
  - Use of permitted identifiers, matching attributes, etc.

Pan-Canadian ID Validation Standard

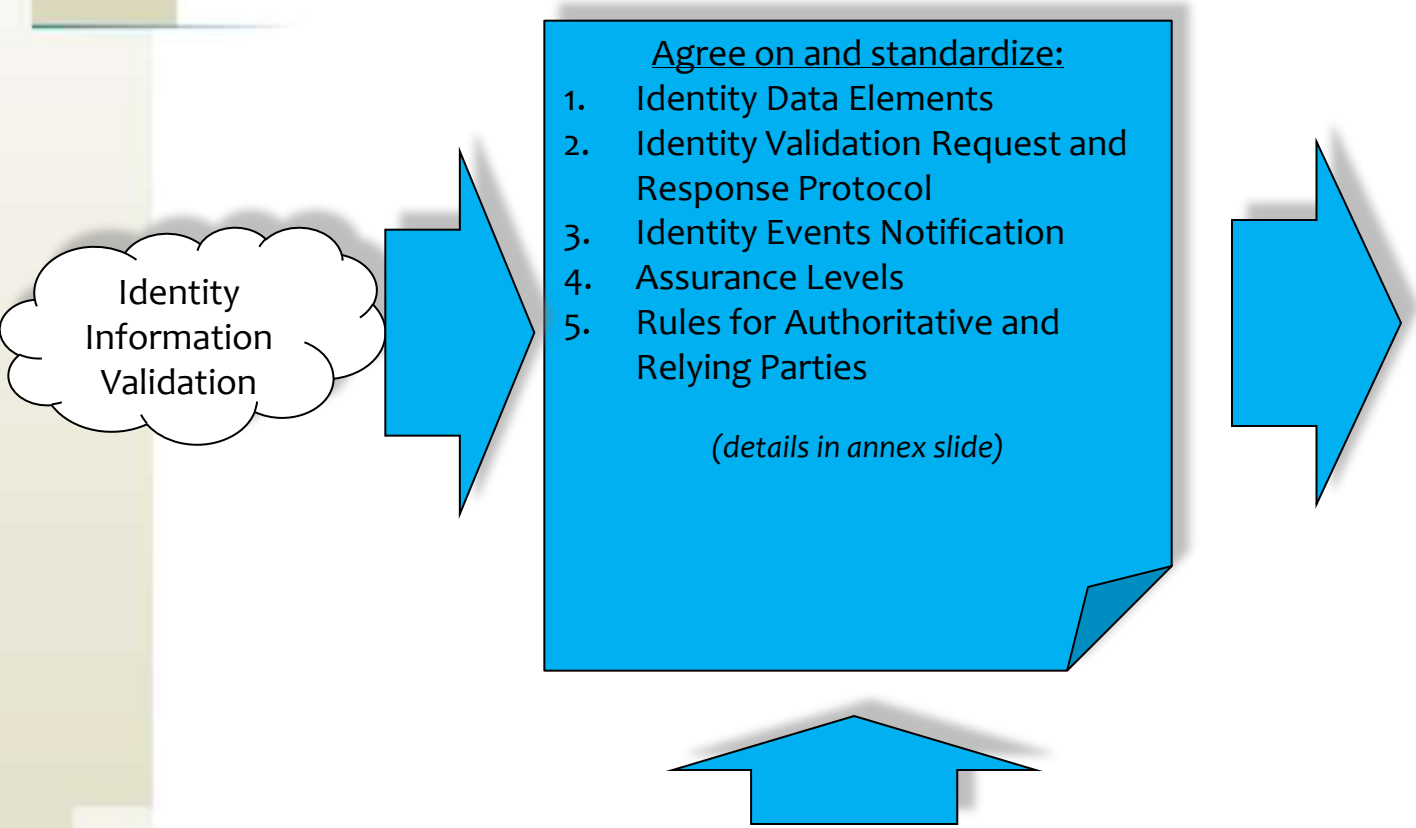
Initial requirements developed at IMSC In-Person Workshop Nov 7-8, 2013

- **Needs to be flexible: which attributes can be used for identity validation**
- **Develop an identity validation profile; specify a subset of NRS Data Attributes that can be formed as part of:**
  - Permitted identifiers that may be used as part of a query (e.g., DL number, document number etc.)
  - Identity attributes (e.g., name, dob, etc.)
  - Status attributes (citizenship, residency, etc.)
  - Address attributes (out of scope for now)

- **Each jurisdiction would be responsible for:**
  - Specifying a profile of identity attributes that are core, mandatory, optional (similar to schema used in existing National Routing System (NRS) implementations)
  - Determining what can be provided as an authoritative party or use as a relying party

Pan-Canadian ID Validation Standard

Components of Standard



Key Enabler for:

- Pan-Canadian ID (Status) Validation Hub
- Government, Industry and International Standards
- Inter- Jurisdictional and Multilateral MOUs
- Technical Interoperability Standards

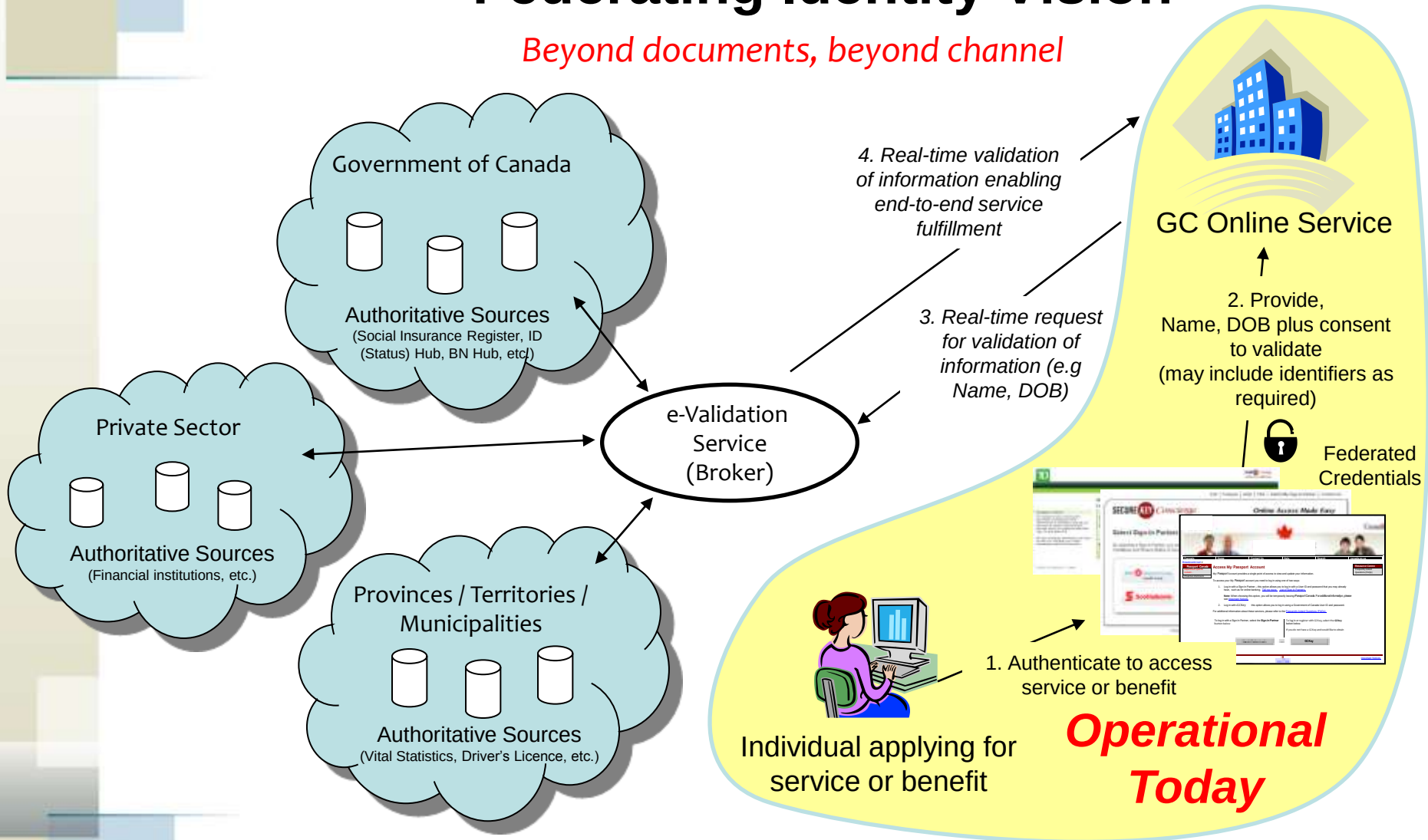
Developed by:

- IMSC Pan-Canadian ID Validation Working Group

Pan-Canadian Identity Hub Network Update

Federating Identity Vision

Beyond documents, beyond channel



Horizontal Enablers:

- Identity Policy architecture (Policy on Government Security, Directive on Identity Management, Standard on Identity and Credential Assurance, Guideline on Defining Authentication Requirements and Guideline on Identity Assurance (being finalized).
- Federated Credentials

Example Future Use Case:
Improving Service Delivery for Clients

SCENARIO

John and Zara recently moved to Canada from Australia.

John was born in Canada, but moved to Australia (he has dual citizenship) with his parents when he was a child. His wife Zara is an Australian citizen, and a Canadian permanent resident.

ONLINE LOGIN

Secure online login
CYBER-AUTHENTICATION

Zara and John registered for their GC Key when they submitted Zara's permanent residence application to Citizenship and Immigration Canada (CIC). Their identity was linked to their Australian passports.

Zara and John each login to Service Canada's (SC) website using their existing GC Key.

"Tell us once" Identity Enrollment: Zara and John provided significant personal information and documentation to CIC which was used to register and confirm their identity. Their original passports were seen and verified by a Canada Border Services Officer when they arrived in Canada and when Zara was landed by the CBSA agent. John's Alberta birth certificate was validated by CIC with the Alberta Vital Statistics Registry using the HUB.

IDENTITY ASSURANCE

Identity assurance from authoritative sources

John and Zara would like to apply for their Social Insurance Numbers.

They provide SC with their names, dates of birth, and status document numbers. John provides his birth certificate number, and Zara provides her PR Card number.

John and Zara are given a list of options for proof of "existence." John provides his new Alberta driver's license (which is validated against the Alberta DL database), and Zara provides her Australian Passport information, which is validated with CIC, as it was seen by the CBSA officer at landing, and the passport number is recorded in GCMS.

John and Zara give consent for SC to obtain the required information for their SIN application directly from CIC.

The SC system sends a query to CIC, and the information returned to SC appears on the screen for John and Zara to review. They update the information with their new Canadian address, and press "submit."

AUTHORIZATION

Validation of age, status in Canada, etc. to verify eligibility or **authorization** to obtain service

As Service Canada has obtained the required assurance of:

a) *John and Zara are the individuals they are dealing with online,*
b) *their identity information is correct,*
c) *evidence of existence was confirmed with a second source; and*
d) *they are entitled to a Social Insurance Number based on their status in Canada;*

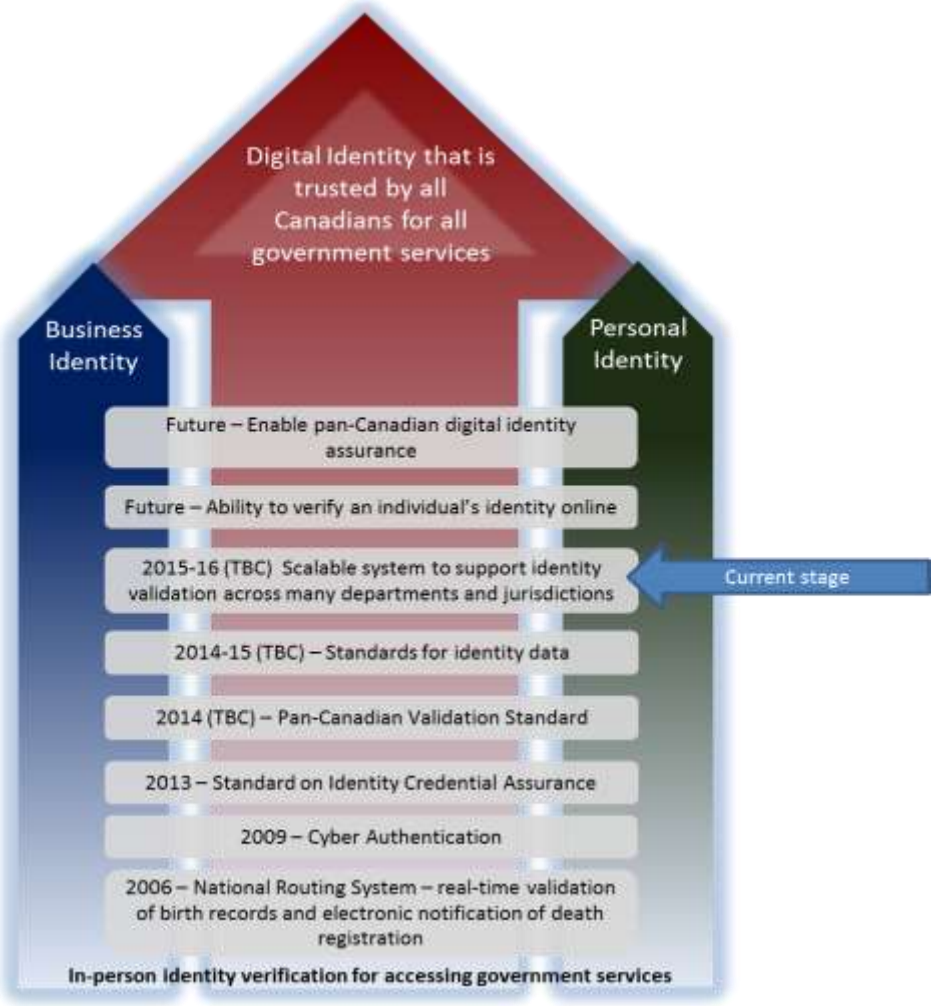
*John and Zara are given their Social Insurance Numbers while they are **online.***

Proposed Pan-Canadian Identity Hub Network
(Feasibility Study in Progress)

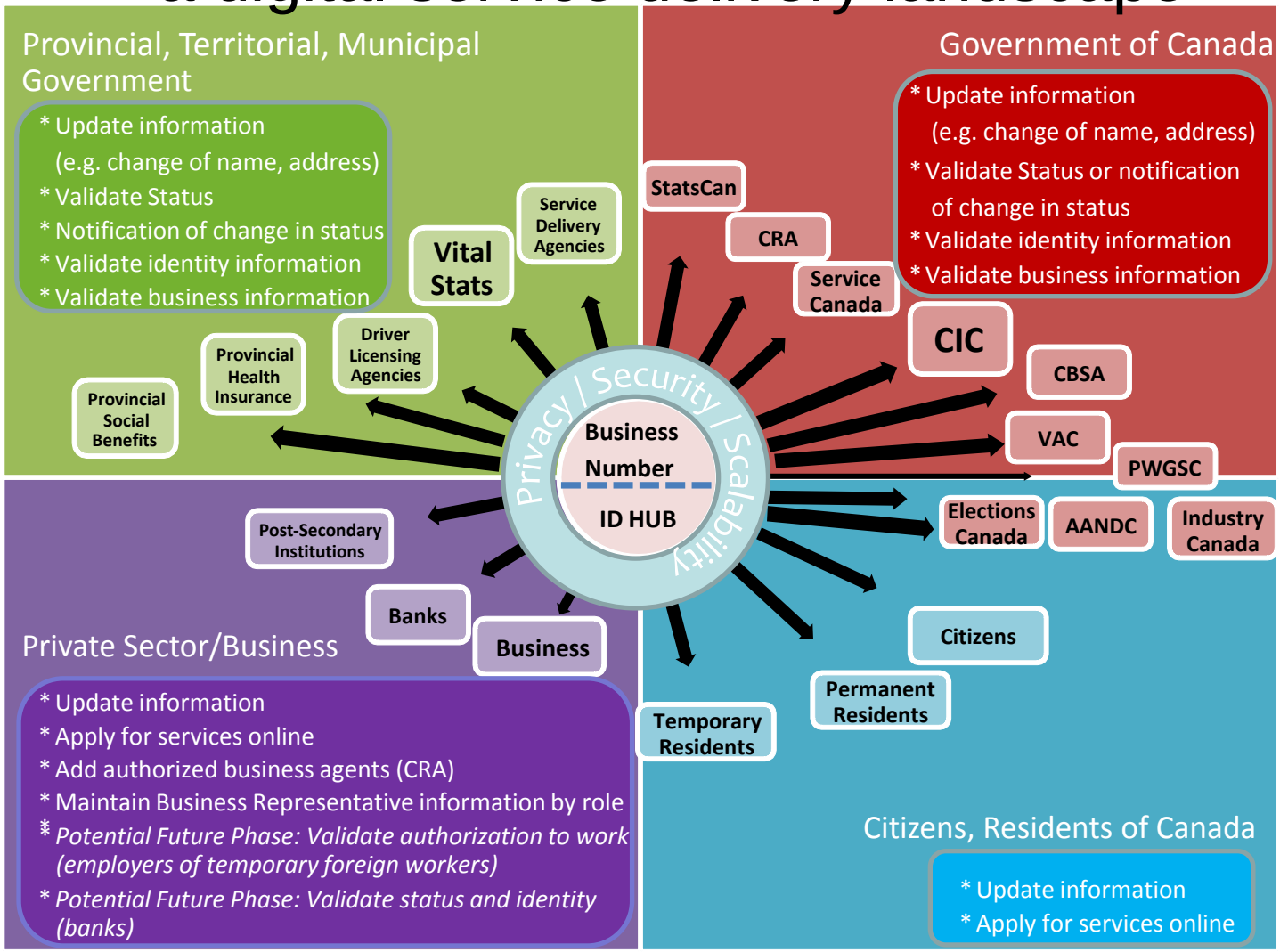
- **A real time, cost-effective service that enables the secure confirmation of identity information at the right place and at the right time for federal, provincial, territorial and municipal (FPTM) partners. The service will be facilitated by a single, multilateral MOU among FPTM partners that would govern the sharing of identity information**
- **Scope includes:**
  - the **electronic validation** of identity attributes (e.g. birth, death, immigration status) across multiple databases, and
  - the **notification** of a change in identity attributes to facilitate rapid update of FPTM databases
- **An essential step towards fully online service delivery**

Federating Identity…

An essential step towards full online service delivery…



Proposed Pan-Canadian ID Hub Network in a digital service delivery landscape



* For illustration purposes only

Pan-Canadian ID Hub Network Timeline

	Governance	Infrastructure	Pilot Project	Standard
2014	Confirm Business Case and decision to move forward	Options analysis	Initiate multi-jurisdictional pilot	Approval of identity validation standard
2015	Set up multi-jurisdictional governance	Procurement	Lessons learned	Implementation of standard
2016	Refine as required	Implementation of scalable, secure multi-jurisdictional infrastructure		Review standard and add components

Questions and Discussion