Identity Management and Federation of Identity in a National Service Delivery Model

3rd Annual Privacy, Access and Security Congress
October 4, 2012
HRSDC and its service delivery arm, Service Canada, are responsible for the delivery of many programs and services that impact on the lives of Canadians including:

- Employment Insurance (EI);
- Canada Pension Plan (CPP);
- Canada Education Student Loan Program;
- Child Tax Credit;
- Grants and Contributions; and,
- The Social Insurance Number (SIN) Program.

A coherent and consistent identity management approach is essential to assist HRSDC in delivering to the right person/organization the right access, service or benefit, in the right amount, at the right time and for the intended purpose.

Identity management is the foundation for all programs, benefits and service delivery processes in HRSDC.
The Importance of Identity Management to Service Delivery

- Integrated identity management allows for improved service delivery, better privacy protection practices and increased program integrity which in turn, enables the achievement of HRSDC’s service delivery objectives.

- The trust that is established between the client and the government, as soon as identity information is captured becomes the starting point of an improved service delivery experience.

- Efficient identity management is essential to meet the expectations of Canadians for:
  - electronic interactions,
  - tell us once,
  - increased quality of service, and
  - rigorous safeguards for personal and organizational security and personal information
The Importance of Identity Management in Prevention

- HRSDC dispenses over $100 billion in benefits per year
  - Occasionally overpayments/underpayments can occur due to improper identification of individuals

- The identity of an individual or an organization with whom HRSDC is dealing must be managed effectively to mitigate the risks related to:
  - identity theft;
  - fraudulent use of identity documents;
  - improper granting of entitlements;
  - inappropriate allocation of benefits and services;
  - financial losses to affected parties; and,
  - the breach of an individual’s right to privacy.
HRSDC’s Identity Management Program

- HRSDC has developed the foundation for an Identity Management Program - a centralized and rigorous identity proofing policy suite for all programs and services within the national portfolio.

- The elements of the Identity Management (IdM) Policy Suite are:
  - IdM Framework
  - IdM Policy
  - Identity Assurance Standard
  - Evidence of Identity (Proof of Identity) Standard

- IdM Policy Suite supports the Department to:
  - achieve an integrated, coherent and consistent approach to IdM in HRSDC
  - enable implementation of business transformation initiatives (new service offerings, Cyber Authentication, bundling of services)
The IdM Framework and Policy

Framework
- Describes the strategic context and direction for IdM:
  - Sound IdM practices across services, channels (in-person, phone, mail, on-line) and organizations mandated to deliver services, benefits or programs on behalf of HRSDC
  - Management of identity is guided by the following principles: consistency, privacy, security, transparency and the highest quality service

Policy
- Supports consistent treatment of IdM across all channels
  - Integrates identity management requirements at all stages of planning, implementation and evaluation of programs/services
  - Ensures coherence and consistency in identity activities
  - Ensures that IdM practices support registration, authentication and validation and address legal, security, privacy issues
  - Provides guidance and tools for IdM to staff
Identity Standards

Identity Assurance Standard
• Provides risk-based approach to identifying clients and how to register, authenticate and validate in consistent and rigorous fashion
  • Registration: collecting individual’s identity attributes (e.g. names; date of birth; Canadian citizenship, Aboriginal or foreign status; sex; SIN) or organization’s identity attributes (e.g. name; status - owner-operated, partnership, corporation, etc.; date of creation)
  • Authentication: establishing confidence that an identity claim made by a client (individual or organization) is true
  • Validation: verifying client (individual or organization) identity attributes with appropriate source

Evidence of Identity Standard
• Sets out requirements for the evidence that supports Identity Assurance:
  • Acceptable evidence of identity (documents/credentials) to authenticate each identity attribute requested during registration, based on assurance levels
  • Two types of evidence required: existence (e.g. birth certificate); linkage of applicant to existence (e.g. driver’s licence)
**HRSDC’s Standardized Approach**

| **Registration:** | Standardizing how we collect identity attributes:  
| Names: | - legal name only - no ‘nicknames’ or preferred names  
| - all legal names - given name, family name, mother’s maiden name  
| Date of Birth: YYYY/MM/DD - format standardized to be interoperable across channels, jurisdictions, organizations and internationally |
| **Authentication:** | Standardizing the process that establishes confidence in the validity of an identity claim or credential submitted in support of an identity claim (authenticating identity attributes collected at registration) |
| **Validation:** | Standardizing the verification of identity attributes and evidence of identity presented by the client |
| **Organizations:** | Standardizing the verification to identify an organization (registration, authentication, validation) |
| **Representatives:** | Standardizing and clarifying the link between clients and representatives |
| **Evidence of Identity:** | Streamlining acceptable evidence to authenticate a client’s identity  
| - reduce from 71 to far fewer authentication tools/credentials  
| - evidence that links identity to an individual for lower risk transactions  
| - evidence that proves existence for higher risk transactions |
HRSDC IdM Program and Federation of Identity

Key components of HRSDC’s IdM Program:

- Vital Events Linkages agreements signed with provinces for the secure electronic validation of birth certificates of Canadians, as well as enable the Social Insurance Register to be up to date on birth and deaths occurring across Canada.
- SIN@Birth (newborn registration)
- Agreements with other government departments such as CIC, CRA, DoJ to confirm identity attributes and status in Canada.
- Secure Key – provides the ability for clients to use their bank card to authenticate their identity.

The IdM program will support new e-services and proactive services for Canadians
- eSIN
- Death bundling of services
- CPP/OAS auto enrolment
- SIN@ arrival

HRSDC’s IdM Program will be a key part of a broader public/private partnership.
HRSDC IdM Program and Federation of Identity

HRSDC IdM Program: 90% completed

Enabling IdM Federation beyond the GoC

Legend

GoC
Provinces Territories Municipalities
Private Sector
Agreements
completed
In progress
Future

Proactive Services
- Bereavement
- Historical Birth/CPP-OAS auto-enrolment
- SIN@arrival

eServices
- ePassport
- eVeterans
- eSIN
- eAboriginal Card
- eLanding

Municipalities
Employers
Other Provincial Departments
Banks
Credit agencies
Insurance Companies
Law enforcement
Other Goc programs
IdM Assurance Standard
SIN SIR
IdM Policy Suite
Federation of Identity

- Federation of Identity proposes leveraging different sources of identity and personal information to assist GoC departments in electronically validating the identity of clients for program administration and service delivery.

- Validation, instead of exchanges of information, ensures there is no requirement to create a central repository or database, or to store information beyond the moment of validation.

- The Social Insurance Number (SIN)/Social Insurance Register (SIR) is a significant component of identity validation and confirmation.

- The use of a variety of existing sources of information to validate identity will allow for end-to-end electronic transactions and improved client service.

- The Federation of Identity will facilitate the migration of services online and allow the GoC to realize both costs savings and service delivery efficiencies as part of the service delivery transformation agenda.
Registration and Authentication

- To respond to requests from Canadians for easier access to on-line services HRSDC has developed a new process called the Enterprise Cyber Authentication Solution (ECAS) that will simplify use and increase security when clients use their online My Service Canada Account (MSCA).

- The ECAS system authenticates an individual’s identity information against a program information source, usually the Social Insurance Registry (SIR) database, before an online service can be accessed.

- When a client first registers for a MSCA their identity credential information is matched with an anonymous identifier so that when they return, we can easily confirm they are the same user.

- If the client comes in with a new credential that we don't recognize, we will ask the client to revalidate their identity with ECAS or use their previous credential.
Conclusion

• IdM is essential to good governance in Canada and is key to Service Canada’s vision of achieving better outcomes for Canadians through service excellence.

• Ultimately, IdM allows the Department to foster a climate of trust with citizens by ensuring privacy of personal information and security of access for citizens, employers and organizations.
“On the Internet, nobody knows you’re a dog.”