IDENTITY MANAGEMENT SUB-COMMITTEE

PAN-CANADIAN IDENTITY MANAGEMENT – VALIDATION STANDARD

Version:	1.9
Status:	Revised Draft
Date:	2016-08-04
Security Classification:	UNCLASSIFIED

Document Version Control

Version Number	Date of Issue	Author(s)	Brief Description
0.1	2014-04-28	IMSC Working Group	Consultation draft
0.2	2014-05-09	IMSC Working Group	Consultation draft
0.3	2014-05-15	IMSC Working Group	Consultation draft
0.4	2014-05-22	IMSC Working Group	Consultation draft
0.5	2014-05-28	IMSC Working Group	Consultation draft – presented to the FPT DMs
0.6	2014-08-18	IMSC Working Group	Consultation draft – presented to the Joint Councils
0.7	2014-10-10	IMSC Working Group	Revised draft
0.8	2014-11-04	IMSC Working Group	Revised draft – presented to the Joint Councils
1.0	2014-11-20	IMSC Working Group	Revised draft – presented to the FPT DMs
1.1	2014-12-12	IMSC Working Group	Revised draft
1.2	2015-02-04	IMSC Working Group	Revised draft
1.3	2015-03-11	IMSC Working Group	Revised draft
1.4	2015-04-08	IMSC Working Group	Revised draft
1.5	2015-04-20	IMSC Working Group	Revised draft
1.6	2015-06-03	IMSC Working Group	Revised draft
1.7	2016-06-21	IMSC Working Group	Revised draft
1.8	2016-07-14	IMSC Working Group	Revised draft
1.9	2016-08-04	IMSC Working Group	Revised draft

Table of Contents

LIST OF TABLES

LIST OF FIGURES

1 Purpose

The purpose of this document is to standardize identity information and personal information validation requests and responses between federal, provincial, territorial, and municipal government organizations.

2 Audience

This document is intended for:

- Federal/Provincial/Territorial/Municipal business program and service owners
- Organizations that intend to be providers of standardized identity information and personal information validation services (authoritative parties)
- Organizations that intend to be consumers of standardized identity information and personal information validation services (relying parties)
- Implementers who design, build, or provide standards-based technical solutions

3 Application and Authority

The *Pan-Canadian Identity Management Validation Standard* ("the Standard") shall be applied in accordance with the respective agreements, legislation, policies, and regulations. The Standard does not confer additional authority.

The Standard delineates the boundaries of what constitutes Pan-Canadian Identity Management (PCIM) validation for government organizations. The nature and extent of the personal information that will be exchanged between participating organizations may be further constrained by information sharing agreements, legislation, policies, regulations, and operational considerations. The Standard should not be construed as a depiction of what is, but rather, of what is possible.

The Standard and its companion Standards – the *Pan-Canadian Identity Management Retrieval Standard* and the *Pan-Canadian Identity Management Notification Standard* – are the primary inputs to the *Pan-Canadian Identity Management Information Exchange Specification* document.

This document will be refined as required, subject to the consensus of the participating Federal/Provincial/Territorial/Municipal stakeholders.

4 Scope

4.1 In Scope

4.1.1 Current Scope

The following items are in scope for the current release of the Standard:

- The Standard specifies the use of personal information for the purposes of:
  - **Identity resolution** – The establishment of the uniqueness of a person within a program/service population through the use of identity information
  - **Identity information validation** – The confirmation of the accuracy of identity information about a person as established by an authoritative party
  - **Personal information validation** – The confirmation of the accuracy of personal information about a person as established by an authoritative party

4.1.2 Future Scope

The following items are out of scope for the current release of the Standard. These items may be considered for future releases of the Standard:

- Validation of information related to organizations
- Inclusion of other personal information attributes to support a broader range of programs and services

4.2 Out of Scope

The following items are out of scope for the Standard:

- Identity information retrieval – The disclosure of identity information about a person by an authoritative party to a relying party that is triggered by a request from the relying party (This is specified in the *Pan-Canadian Identity Management Retrieval Standard*)
- Personal information retrieval – The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by a request from the relying party (This is specified in the *Pan-Canadian Identity Management Retrieval Standard*)

- Identity information notification – The disclosure of identity information about a person by an authoritative party to a relying party that is triggered by the establishment of the person's identity, a change in their identity information, or an indication that their identity information has been exposed to a risk factor (e.g. the death of the person, use of expired documents, a privacy breach, fraudulent use of the identity information) (This is specified in the *Pan-Canadian Identity Management Notification Standard*)
- Personal information notification – The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by the establishment of the person's identity or a change in their personal information (This is specified in the *Pan-Canadian Identity Management Notification Standard*)
- Identity verification – The confirmation that the identity information being presented relates to the person who is making the claim
- Document information notification – The notification about a document where there is no personal information attached as in the case of missing or stolen document stock
- Document authentication – The confirmation of the genuineness of a document by verifying security features, etc.
- Specification of authorities required by a relying party or an authoritative party to apply the Standard. (This is governed by legislation and/or specified in an applicable MOU)
- Certification or accreditation of parties in the use of the Standard. (This is specified in an applicable trust framework)
- Methods of communication of validation requests and responses (security, encryption, etc.)
- Specification of technical protocols or architectures
- Specification of rules for the routing of validation requests and responses (e.g. through an intermediary, or hub)

5 Terms and Definitions

Definitions of various terms used in this document can be found in *Appendix A: Terms and Definitions*.

6 Background and Context

6.1 Introduction

In May 2013, the development of an identity validation standard was proposed at the annual meeting of the Federal, Provincial, and Territorial (FPT) Deputy Ministers of Service Delivery. The Deputy Ministers agreed in principle that the Identity Management Sub-Committee (IMSC) reporting to the Joint Councils would develop a *Pan-Canadian Identity Management Validation Standard*. The goal of the Standard is to ensure that all jurisdictions use consistent terminology and procedures in the validation of identity information and related personal information. The FPT Deputy Ministers noted that the Standard is considered to be a cornerstone component to federating identity.

In April 2014, it was recognized that two companion standards – the *Pan-Canadian Identity Management Retrieval Standard* and the *Pan-Canadian Identity Management Notification Standard* – should also be developed by the IMSC. These two additional Standards would ensure that all jurisdictions use consistent terminology and procedures in the retrieval and notification of identity information and related personal information. The three Standards constitute the first steps toward the development of a set of standardized Pan-Canadian identity management processes.

6.2 Value of Standardized Identity Management Processes

Standardized identity management processes provide business value in several ways:

1. **Better delivery of services** – Standardized identity management processes can be used to improve identity-proofing processes between jurisdictions. From a client's perspective, these result in the better delivery of services and increased client satisfaction and uptake of services.
2. **Increased integrity of government programs and services** – Standardized identity management processes can increase the integrity of program and service delivery. The consolidation of processes can help to reduce fraud by implementing electronic processes that can benefit all programs and services.
3. **Improved efficiency and reduced costs** – Standardized identity management processes can minimize operational costs, where appropriate, by reducing the need for the inspection of physical documents or the requirement for in-person visits. Fraud-related costs are reduced by enabling real-time validation and retrieval within a registration/enrolment process or, in the case of detecting fraud, providing immediate notification to other participants within the federation. Standardization also enables trusted services to be leveraged across jurisdictions, enabling seamless digital service delivery to all Canadians.

4. **Enabling innovation and transformation** – Once in place, standardized identity management processes require minimal incremental investment to achieve substantial economies of scale and scope.

6.3 Enabling a Pan-Canadian Approach

The *Pan-Canadian Identity Management Validation Standard* is crucial to enabling a Pan-Canadian approach and is a next step toward the realization of *federating identity*. Federating identity will enable Federal, Provincial, Territorial, and Municipal (F/P/T/M) partners to fulfill program and service requirements by leveraging trusted processes carried out in other jurisdictions.

The Standard provides consistent terminology and procedures in the validation of identity information and related personal information. The Standard is a key enabler for initiatives implementing a Pan-Canadian approach.

The Standard has been developed to accommodate different implementations or arrangements that can exist within a Pan-Canadian context. These include:

- **Bi-lateral or point-to-point arrangements** where there is a specific agreement between two parties and a direct connection between systems (i.e. no intermediary or broker is involved)
- **Multi-lateral or federated arrangements** where there is a broader agreement between several parties and the connection between systems are intermediated by a hub or a broker
- **Application or adoption of trust frameworks** that use standardized assurance levels, assessment processes, and accreditation schemes

6.4 Supporting Canada’s Digital Interchange Services

The *Pan-Canadian Identity Management Validation Standard* has been developed to enable key services for Canada’s Digital Interchange (CDI). The Standard addresses the following service definitions[1] developed by CDI:

- **Identity Information Validation** – Identity information validation is the process whereby, if identity resolution is achieved based on the identity information of a person as supplied by the relying party in an identity information validation request, the authoritative party will confirm (via an identity information validation response) the accuracy of the relying party’s identity information about the person.
- **Personal Information Validation** – Personal information validation is the process whereby, if identity resolution is achieved based on the identity information of a person as supplied by the relying party in a personal information validation request, the authoritative party will confirm (via a personal information

[1] See *Canada’s Digital Interchange – Service Definition* for more information.

validation response) the accuracy of the relying party's personal information about the person.

This *Pan-Canadian Identity Management Validation Standard* does not address the following CDI services:

- **Identity Information Retrieval** – Identity information retrieval is the process whereby, if identity resolution is achieved based on the identity information of a person as supplied by the relying party in an Identity information retrieval request, the authoritative party will disclose (via an identity information retrieval response) identity information about the person to the relying party. Identity information retrieval is specified in the *Pan-Canadian Identity Management Retrieval Standard*.
- **Personal Information Retrieval** – Personal information retrieval is the process whereby, if identity resolution is achieved based on the identity information of a person as supplied by the relying party in a personal information retrieval request, the authoritative party will disclose (via a personal information retrieval response) personal information about the person to the relying party. Personal information retrieval is specified in the *Pan-Canadian Identity Management Retrieval Standard*.
- **Identity Information Notification** – Identity information notification is the disclosure of Identity information about a person by an authoritative party to a relying party that is triggered by the establishment of the person's identity, a change in their identity information, or an indication that their identity information has been exposed to a risk factor (e.g. the death of the person, use of expired documents, a privacy breach, fraudulent use of the identity information). Identity information notification is specified in the *Pan-Canadian Identity Management Notification Standard*.
- **Personal Information Notification** – Personal information notification is the disclosure of personal information about a person by an authoritative party to a relying party that is triggered by the establishment of the person's identity or a change in their personal information. Personal information notification is specified in the *Pan-Canadian Identity Management Notification Standard*.

6.5 Ensuring Privacy and Minimal Disclosure

Canadians value their privacy and the protection of their personal information. All jurisdictions are committed to protecting the privacy of individuals and recognize that the protection of personal information is an essential element in maintaining public trust. An important principle of ensuring privacy is minimal disclosure – a relying party should only request the minimum amount of personal information required to support a program or deliver a service. Conversely, an authoritative party should only provide the minimum amount of personal information required to fulfill a validation request.

The Standard is intended to work within existing privacy and program legislation and augment privacy principles such as Privacy by Design[2] and minimize the disclosure of personal information. The Standard provides a framework that enables jurisdictions, acting in the role of a relying party or an authoritative party, to specify how personal information is used and disclosed in relation to validation. This framework can be used to facilitate legislative compliance and to specify detailed requirements in MOUs.

6.6 Federations and Trust Frameworks

The Standard may be applied within the context of federations and trust frameworks. A federation is a cooperative agreement between autonomous entities that have agreed to work together. A federation is supported by trust relationships and standards to support interoperability. A federation can consist of public and private sector organizations, different jurisdictions, or different countries.

Federations, as they evolve, develop formalized assessment processes, contractual agreements, service agreements, legal obligations, and dispute resolution mechanisms. These components, together, are referred to as trust frameworks.

Several industry trust frameworks are currently in use, including:

- **Kantara Initiative** is an independent non-profit organization formed to work on various aspects of digital identity.
- **InCommon Federation** operates the identity management federation for U.S. research and education, and their sponsored partners. The federation provides a common framework for trusted shared management of access to online resources.
- **Open Identity Exchange (OIX)** is a non-profit trade organization focused on internet identity solutions. OIX's goal is to enable the expansion of online services and adoption of new online products through the development and registration of trust frameworks.
- **Safe/BioPharma** is a non-profit association that manages digital identities and the digital signature standard for the global pharmaceutical, biotech, and

[2] Privacy by Design principles can be found at: http://www.privacybydesign.ca/

healthcare industries.

Governments have developed trust framework adoption processes that are used to recognize and adopt industry trust frameworks for use by government organizations. These include:

- US FICAM **Trust Framework Provider Adoption Process (TFPAP)**[3] for all levels of assurance defines a process whereby the US Federal Government can assess the efficacy of external trust frameworks for federal purposes. Currently adopted trust framework providers include, Kantara, InCommon, OIX, and Safe/BioPharma.
- UK **tScheme**[4] is an independent, industry-led, self-regulatory scheme set up to create strict assessment criteria used to approve trust services. This scheme is used by the UK Identity Assurance Programme.

Canada is currently developing a Pan-Canadian Trust Framework which will include a trust framework adoption process.

[3] TFPAP web site: http://info.idmanagement.gov/2013/04/ficam-tfs-tfpap-updated.html

[4] tScheme web site: http://www.tscheme.org/

7 Identity Management Overview

This section provides a general overview of specific topics in identity management that are relevant to identity information and personal information validation. Additional information can be found in the *Guideline on Identity Assurance*.

7.1 Identity

Identity is defined as a reference or designation used to distinguish a unique and particular person, organization, or device.

An identity must be unique[5]. The uniqueness requirement ensures the following:

- that persons can be distinguished from one another and, when required, uniquely identified;
- that a service can be delivered to a specific person (e.g. the same person from a previous registration or enrolment process); and
- that a service is delivered to the right person; uniqueness reduces the possibility of the wrong person receiving a service or benefit (i.e. a service or benefit intended for someone else).

7.2 Defining the Population

Those persons who fall within the legislated mandate of a program or service constitute the population of the program or service[6]. In Canada, the population universe is first partitioned between political jurisdictions (i.e. national, provincial/territorial, municipal) and then within those boundaries the population is further divided by degree of program coverage (i.e. universal vs. criteria-based).

The following are some examples of program/service populations in Canada:

- Persons who were born in Alberta
- Persons who are required to file a federal income tax return
- Persons who are licensed to drive in Quebec
- Persons who are military veterans
- Persons who were not born in Canada
- Persons who are covered by provincial health insurance in Ontario
- Persons who have Indian status in Canada

[5] This is one of the requirements for establishing an identity assurance level. See Appendix C of the *Standard on Identity and Credential Assurance*.

[6] The characteristics of a program/service population are a key factor in determining identity context. See the next section.

- Persons who receive social assistance benefits in British Columbia

7.3 Defining the Identity Context

In delivering their programs and services, government organizations operate within a certain environment or set of circumstances, which in the domain of identity management is referred to as the identity context. Identity context is determined by factors such as mandate, target population (i.e. clients), and other responsibilities prescribed by legislation or agreements.

Understanding and defining the identity context assists government organizations in determining what identity information is required and what identity information is not required. Identity context also assists in determining commonalities with other government organizations or jurisdictions, and whether identity information and assurance processes can be leveraged across contexts.

The following considerations should be kept in mind when defining the identity context of a given program or service:

- Intended recipients of a service – recipients may be external to government (e.g. citizens, non-Canadians, businesses, non-profit organizations), or internal to government (e.g. employees, departments)
- Size, characteristics, and composition of the client population
- Commonalities with other services (i.e. across government)
- Government organizations with similar mandates
- Use of shared services

7.4 Determining Identity Information Requirements

A property or characteristic associated with an identifiable person is referred to as an *identity attribute* or an *identity data element*. Examples of identity attributes include *name*, *date of birth*, and *sex*. For any given program or service, identity information is the set of identity attributes that is both:

- Sufficient to distinguish between different persons within the program/service population (i.e. achieve the uniqueness requirement for identity); and
- Sufficient to describe the person as required by the program or service.

When determining the sufficiency of identity information for a program or service, government organizations need to distinguish between identity information and program-specific personal information, as these can overlap. For example, *date of birth* can be used to help achieve identity uniqueness (i.e. it is used as identity information) – but *date of birth* can also be used as an age eligibility requirement (i.e. it is used as program-specific personal information). When overlap between identity information and program-specific personal information occurs, it is a good practice to describe both purposes. This is to ensure that the use of identity information is consistent with the original purpose for which the identity information was obtained and that it can be managed separately or additionally protected by appropriate security and privacy controls. Government organizations are advised to reduce the overlap between identity information and program-specific personal information as much as possible.

7.4.1 Identifier

The set of identity attributes that is used to uniquely distinguish a unique and particular person within a program/service population is referred to as an *identifier*. This set of attributes is usually a subset of the identity information requirements of a program or service.

Different sets of identity attributes may be specified as an identifier depending on program or service requirements and legislation. For example, one program may specify *name* and *date of birth* as the identifier set of identity attributes. Another program may specify *name*, *date of birth*, and *sex* as the identifier set of identity attributes. Yet another program may use an *assigned identifier* (such as a health insurance number) as the identifier set of identity attributes. The Standard provides flexibility on what can be specified as the identifier set of identity attributes.

When determining the set of identity attributes to be used as an identifier, the following factors should be considered:

- **Universality** – Every person within the program/service population must possess the identifier set of identity attributes. For example, including a cell phone number as part of the identifier set may result in many null values for the identity attribute because ownership of a cell phone may not be sufficiently universal enough within the population of interest. Even when an identity attribute is universal, widespread missing or incomplete values for the identity attribute may render it useless as part of an identifier set. For example, many dates of birth for persons born outside of Canada consist only of the year or the year and the month.

- **Uniqueness** – The values associated with the identity attributes must be sufficiently different for each person within the program/service population that the persons within the program/service population can be distinguished from one another. For example, date of birth information by itself is insufficient to distinguish between persons in a population because many people have the same birthdate.
- **Constancy** – The values associated with the identity attributes should vary minimally (if at all) over time. For example, having address information in the identifier set is problematic because a person's address is likely to change several times in their lifetime.
- **Collectability** – Obtaining a set of values for the identity attributes should be relatively easy. For example, human DNA sequences are universal, unique, and very stable over time, but they are difficult to obtain.

7.4.2 Assigned Identifier

It is generally agreed that *name* and *date of birth* comprise the minimum set of identity attributes required to constitute an identifier. Analyses[7] have shown that a combination of *name (surname + first given name*) and full *date of birth* will distinguish between upwards of 96% of the persons in any population. While adding other identity attributes (e.g. *sex*, *place of birth*) to the set provides some marginal improvement, no combination of identity attributes can guarantee absolute uniqueness for 100% of a given population. Consequently, due to the potential for identity overlap in whatever residual percentage of the population remains, government organizations employ the use of an *assigned identifier*. An assigned identifier is an artificial identity attribute that is used solely for the purpose of providing identity uniqueness. It consists of a numeric or alphanumeric string that is generated automatically and is assigned to the person at the time of identity establishment or enrolment. However, before an assigned identifier can be associated with a person, the uniqueness of the person's identity within the relevant population must first be established (i.e. identity resolution must be achieved (see next section)) through the use of other identity attributes (e.g. *name*, *date of birth*, etc.). Therefore, the use of an assigned identifier does not eliminate the need for traditional identity resolution techniques, but it does reduce the need to a one-time only occurrence for each person within a population.

Once associated with a person, an assigned identifier uniquely distinguishes that person from all other persons in a population without the use of any other identity attributes. Examples of assigned identifiers include birth registration numbers, driver's license numbers, and social insurance numbers. The following considerations apply to the use of assigned identifiers:

- Assigned identifiers may be kept internal to the program that maintains them. Examples of internal assigned identifiers are database unique keys and globally

[7] NASPO IDPV Project, Report of the IDPV Identity Resolution Project, February 17, 2014

unique identifiers.

- Assigned identifiers maintained by one program may be provided to other programs so that those programs can also use the assigned identifier to distinguish between different persons within their program/service population; however, there may be restrictions on this practice due to privacy considerations or legislation.
- Certain assigned identifiers may be subject to legal and policy restrictions. For example, the Government of Canada imposes restrictions on the collection, use, retention, disclosure, and disposal of the social insurance number.

7.5 Identity Resolution

Identity resolution is defined as the establishment of the uniqueness of a person within a program/service population through the use of identity information. A program or service defines its identity resolution requirements in terms of identity attributes; that is, it specifies the set of identity attributes that is required to achieve identity resolution within its population. Since the identifier is the set of identity attributes that is used to uniquely distinguish a unique and particular person within a program/service population, the identifier is the means by which identity resolution is achieved.

Identity resolution requirements may differ from one program or service to another. The Standard provides a set of specifications for dealing with differing identity resolution requirements.

The responsibilities of authoritative parties and relying parties in respect to identity resolution are the following:

- Both authoritative parties and relying parties must establish the identity resolution requirements of their program/service populations.
- An authoritative party must publish the identity resolution requirements of its program/service population.
- When preparing a validation or retrieval request, a relying party must fulfill the authoritative party’s identity resolution requirements.
- Based on the identity information provided by a relying party in a validation or retrieval request, the authoritative party must achieve identity resolution as the first step to preparing the validation or retrieval response.
- Based on the identity information provided by the authoritative party in a notification, the relying party must achieve identity resolution as the first step to processing the notification.

7.6 Ensuring the Accuracy of Identity Information

Identity information must be accurate, complete, and up to date[8]. Accuracy ensures the quality of identity information. It ensures that the information represents what is true about a person, and that it is as complete and up to date as necessary.

For identity information to be considered accurate, three requirements must be met:

- **The identity information is correct and up to date.** Identity information, due to certain life events (e.g. marriage), may change over time. Ongoing updates to identity information may be required; otherwise, it becomes incorrect.
- **The identity information relates to a real person**. Identity information must be associated with a person who actually exists. In most cases, the person is still alive, but cases of deceased persons also apply.
- **The identity information relates to the correct individual.** In large populations, persons may have the same or similar identity information as other persons. While the requirement for identity uniqueness addresses this issue, the possibility of relating identity information to the wrong person still remains.

It is the responsibility of government organizations to ensure the accuracy of the identity information that is used within their programs and services. The accuracy of identity information can be ensured by using an authoritative source. There are three methods by which this can be achieved:

- On an as needed basis, request confirmation from an authoritative source that the identity information is accurate. This process is referred to as *identity information validation*. For example, a person's sex might be electronically validated using a provincial vital statistics registry[9].
- On an as needed basis, request the identity information from an authoritative source. This process is referred to as *identity information retrieval*. For example, a person's place of birth might be electronically retrieved from the federal registry of persons born abroad.
- Subscribe to a notification service provided by an authoritative source. This

[8] This is one of the requirements for establishing an identity assurance level. See Appendix C of the *Standard on Identity and Credential Assurance*.

[9] Factors such as spelling and phonetic variations, name changes, and different character sets can make the validation of some identity data elements problematic. Such factors may make it difficult to demand exact matching. Government organizations may need to use approximate or statistical matching methods to determine if identity information acceptably matches an authoritative record. However, it should be noted that **an *identifier* is always subject to an exact match**. In cases where the integrity of an identifier can be determined using a mathematical algorithm (e.g. a checksum calculation for an assigned identifier), these methods should be applied.

process is referred to as *identity information notification*. For example, death notifications might be received from a provincial vital statistics registry.

These methods can be used independently or in combination, and an effective strategy usually requires the use of all three.

If ensuring the accuracy of identity information by means of an authoritative source is not feasible, other methods may be employed, such as corroborating identity information using one or more instances of evidence of identity.

Determining the accuracy of identity information includes confirming that the person currently exists or previously existed (i.e. is now deceased). This means that the identity information relates to a real person (living or dead), and not to a false or incorrect person. The accuracy of identity information is independent of whether a person is living or deceased. A person's identity information does not become invalid after death.

8 VALIDATION REQUEST/RESPONSE PROCESS OVERVIEW

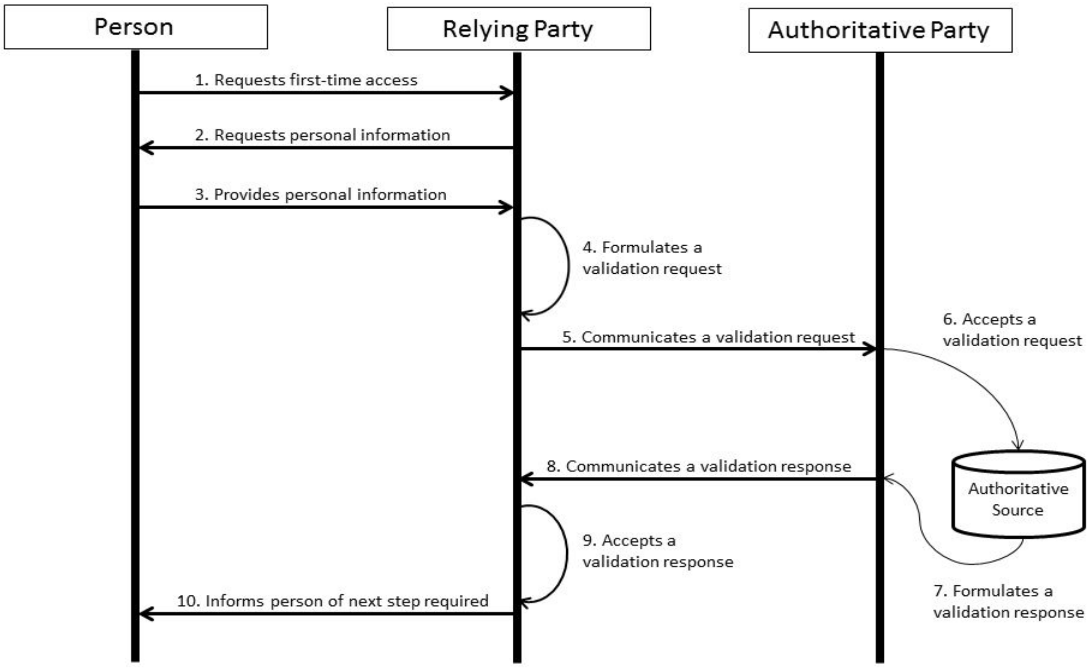
8.1 Validation Request and Response Flow Sequence

A generic validation use case is illustrated in the flow sequence diagram below. This use case involves an individual as a client, a relying party as a service provider to the client, and an authoritative party providing the validation service.

For simplicity, this use case flow diagram assumes the following:

- All interactions are conducted within a secure context and comply with privacy legislation
- Privacy and consent notices are provided as appropriate
- The relying party and the authoritative party have the necessary authorities to collect, use, and disclose personal information
- The relying party has a process in place to ensure that the claimed identity legitimately matches the individual making the claim (i.e. an *identity verification* process). This identity verification process is separate from the validation process.

Figure 1: Validation Request and Response Flow Sequence Diagram


Person
Relying Party
Authoritative Party
1. Requests first-time access
2. Requests personal information
3. Provides personal information
4. Formulates a validation request
5. Communicates a validation request
6. Accepts a validation request
Authoritative Source
7. Formulates a validation response
8. Communicates a validation response
9. Accepts a validation response
10. Informs person of next step required

8.2 Validation Request and Response Process Description

The process of validation is described in Steps 4 through 9. The shaded steps (Steps 4, 6, 7, and 9) represent what is in the current scope of the Standard.

Process	Standards
Step 1: A person requests first-time access to a service provided by a relying party. **Step 2:** The relying party requests personal information from the person. **Step 3:** The person provides the requested personal information to the relying party.	The relying party must determine its authority to collect personal information before formulating a validation request.
Step 4: The relying party formulates a validation request using the personal information provided by the person.	Standardization of how a relying party formulates a validation request
Step 5: The relying party communicates the	Standardization of how a relying party communicates a validation request to an

validation request to an authoritative party.	authoritative party
Step 6: The authoritative party receives the validation request from the relying party.	Standardization of how an authoritative party receives and accepts a validation request
Step 7: The authoritative party formulates a validation response using an authoritative source**.**	Standardization of how an authoritative party formulates a validation response using an authoritative source
Step 8: The authoritative party communicates the validation response to the relying party.	Standardization of how an authoritative party communicates a validation response to a relying party
Step 9: The relying party receives the validation response from the authoritative party and uses the result to prepare for the next step in the first-time access request**.**	Standardization of how a relying party receives and accepts a validation response
Step 10: The relying party informs the person of the next step required.	The relying party must determine how to integrate the validation response into its business processes.

Steps 4 through 9 may be integrated into many different business process scenarios, including:

- **Validation as part of a credential or document issuance process** where personal information is validated prior to the issuance of a credential or document
- **Validation as part of a user-based consent process** where an individual consents to share their validated personal information with another relying party
- **Validation as part of a program integrity process** where a program may periodically validate personal information to ensure ongoing accuracy

9 Validation Request/Response Process Details

9.1 Types of Validation

9.1.1 Identity Information Validation

Identity information validation is the confirmation of the accuracy of identity information about a person as established by an authoritative party. If identity resolution is achieved based on the identity information of a person as supplied by the relying party in an identity information validation request, the authoritative party will confirm (via an identity information validation response) the accuracy of the relying party's identity information about the person.

9.1.2 Personal Information Validation

Personal information validation is the confirmation of the accuracy of personal information about a person as established by an authoritative party. If identity resolution is achieved based on the identity information of a person as supplied by the relying party in a personal information validation request, the authoritative party will confirm (via a personal information validation response) the accuracy of the relying party's personal information about the person.

9.2 Types of Information

9.2.1 Personal Information

Personal information is defined generally in legislation *as information about an identifiable person*[10] and this can include a wide range of information "about" a person, including metadata. Personal information includes the stricter subset of personal attributes known as identity information (see next section).

Personal information that is collected and used for the specific purpose of administering a program or delivering a service may be referred to as *program-specific* personal information. Program-specific personal information is usually restricted to the program and constrained by privacy legislation to ensure consistent use for which it was collected (e.g. to determine program eligibility).

Although the legislative definition of personal information may be very broad, the Standard supports the validation of only a limited set of personal information (see Section 9.3). Categories of personal information that are not listed in Section 9.3 fall outside the scope of the Standard.

[10] This is the generic definition that is generally found in the different legislation.

9.2.2 Identity Information

Identity information is the set of identity attributes that is sufficient to distinguish one person from all other persons within a program/service population and that is sufficient to describe the person as required by a program or service. Identity information is a subset of personal information.

Identity information often varies between different programs and services. Factors that determine what constitutes identity information for a given program or service include mandate, target population (i.e. clients), and other responsibilities prescribed by legislation or agreements.

An important subset of identity information is the set of identity attributes that is required to achieve *identity resolution* within a program/service population. Identity resolution is defined as the establishment of the uniqueness of a person within a program/service population through the use of identity information. Identity resolution requirements may differ from one program or service to another and the Standard provides a set of specifications for dealing with differing identity resolution requirements.

It is important to note that overlap between identity information and program-specific personal information can occur. For example, *date of birth* is used to help achieve identity resolution (i.e. it is used as identity information) and it can also be used as an age eligibility requirement (i.e. it is used as program-specific personal information).

9.2.2.1 Additional Identity Information Required for Identity Resolution

Additional identity information is personal information that may be supplied by the relying party to assist the authoritative party in achieving identity resolution. The need to supply additional identity information in a validation request is normally the result of a misalignment between the relying party's identity resolution requirements and the authoritative party's identity resolution requirements. Additional identity information, although not required by the relying party to distinguish one person from all other persons within the relying party's program/service population, may be required by the authoritative party to assist the authoritative party in achieving identity resolution, especially in the case where the authoritative party maintains a large population.

It is the responsibility of the relying party to supply sufficient identity information in a validation request to allow the authoritative party to achieve identity resolution. While this is normally achieved by providing the identity information that the relying party uses for identity resolution (e.g. *name*, *date of birth*, and *assigned identifier*), additional identity information may need to be provided to further assist in the authoritative party's identity resolution process. This is important in cases where an *assigned identifier* is not available and *name* and *date of birth* as identity information are insufficient to resolve to a unique person. To achieve identity resolution, the authoritative party might require additional identity information, such as *sex, place of birth,* etc.

Privacy legislation may restrict what can be used as additional identity information in a validation request. The relying party may require additional authority to use other personal information as additional identity information in a validation request.

Depending on what is provided as additional identity information, the authoritative party may decide to use only a subset of the additional identity information to assist in the identity resolution process. For example, if a health insurance number and a driver's license number are supplied in the validation request, the authoritative party may determine that the driver license number is sufficient to resolve to the right person (and therefore not use the health insurance number).

9.3 Personal Information Categories

The Standard specifies the eight personal information categories that may be or must be included as part of a validation request:

1. **PERSON NAME** indicates the name by which a person is known or referred to. A person's name is usually a combination of a *surname* and one or more *given names*. A person may have several known names (due to name change, name variations, marriage, etc.).
2. **DATE OF EVENT** indicates the date on which an event in a person's life occurred. Examples of date of event are: date of birth, date of death, and date of stillbirth. The completeness and accuracy of date of event information are dependent on where and when the event occurred.
3. **PLACE OF EVENT** indicates the place where an event in a person's life occurred. Examples of place of event are: place of birth, place of death, and place of stillbirth. The completeness, accuracy, and currency of place of event information are dependent on where and when the event occurred.
4. **SEX, GENDER, DOCUMENTED SEX** indicates the sex, gender, or documented sex of a person. Depending on the program or service delivery requirement, a person may have one or several indications.
5. **ASSIGNED IDENTIFIER** indicates an artificial identifier (typically a numeric or alphanumeric string) that has been assigned to a unique person. An assigned identifier may be associated with an event (e.g. a birth registration), a program (e.g. a provincial health insurance program), or a document issued to a person (e.g. a passport). A person may have several assigned identifiers – for example, a person may have a birth registration number, a provincial health insurance number, and a passport number.
6. **PERSON STATUS** indicates an officially recognized standing of a person. Depending on the program or service delivery requirement, a person may have one or several indications.
7. **ADDRESS** indicates where a person lives or can be communicated with. A person may have several addresses, including primary and secondary residences,

mailing addresses, and previous residences.

8. **ASSOCIATED PERSON** indicates another person who has an affiliation with or a legal authority to act on behalf of a person (e.g. spouse, parent, guardian, power of attorney, etc.). A person may have several associated persons.

For each personal information category, the Standard specifies the associated data elements that may be or must be used.

9.4 Validation Request/Response Parameters

The Standard defines validation request and response parameters that will be used to limit the disclosure of personal information and to leverage trust frameworks.

Specification and use of validation request and response parameters are governed by the applicable authorities (MOUs, legislation, privacy, etc.) and trust frameworks.

9.4.1 Disclosure Level Parameters

Disclosure level parameters are used to limit the level of disclosure of personal information. Disclosure levels range from requesting an indicator of the result of the comparison of two data element values, to requesting the correct information on record. Disclosure levels are specified in Table 10.

9.4.2 Assurance Level Parameters

Assurance level parameters are used to indicate the level of assurance required and/or supplied in a validation response. Levels of assurance are defined in a trust framework. Assurance levels are specified in Table 11.

10 Validation Request Specifications

The Standard defines the validation request specifications for each personal information category and its associated data elements. The specifications for a personal information category are categorized by function (i.e. identity resolution or validation) and by information type (i.e. identity information, additional identity information, or personal information). In the case of the data elements associated with a personal information category, the specifications are categorized by function only.

10.1 Specification Syntax

Certain terms used in the specifications have the following meanings:

- The terms *must* and *mandatory* mean that the specified object or behaviour is an absolute requirement of the Standard.
- The terms *must not* and *not permitted* mean that the specified object or behaviour is an absolute prohibition of the Standard.
- The terms *may, permitted,* and *optional* mean that the specified object or behaviour is discretionary.

An item in bold, all caps (e.g. **ASSIGNED IDENTIFIER**) refers to the standard label of a personal information category. An Item in bold (e.g. **Assigned Identifier Type Code**) refers to the standard label of a data element (i.e. a data element name).

Additional constraints or restrictions are specified within the square brackets (**[ ]**) that may appear after a personal information category label or a data element name. The meanings of these values are:

- MIN(n_1), MAX(n_2) – the personal information category can be present from n_1 to n_2 times.
- CSV – the value provided for the data element must adhere to a defined *codeset* [11]

[11] These codesets are enumerated in the *Pan-Canadian Identity Management Information Exchange Specification* document.

10.2 Usage of Personal Information Categories in Validation Requests

Table 1 presents the validation request usage specifications for the eight personal information categories. For each personal information category, the table indicates whether it is PERMITTED, NOT PERMITTED, or MANDATORY in relation to function (identity resolution or validation) and information type (identity information, additional identity information, or personal information).

Table 1 is the primary decision point when formulating a validation request. Once it has been determined which personal information categories will comprise a validation request, the data element validation request specifications tables (see next section) are used to determine which data elements may be or must be used in terms of function.

Note: Since validation cannot occur unless identity resolution is achieved by the authoritative party, a personal information category (or categories) must be provided for the identity resolution function.

Table 1: Usage of Personal Information Categories in Validation Requests

Personal Information Category	Function			
	Identity Resolution		Validation	
	Identity Information	Additional Identity Information	Identity Information	Personal Information
PERSON NAME [MIN(1), MAX(5)]	PERMITTED	PERMITTED	MANDATORY	NOT PERMITTED
DATE OF EVENT [MIN(1), MAX(2)]	PERMITTED	PERMITTED	MANDATORY	NOT PERMITTED
PLACE OF EVENT [MIN(0), MAX(2)]	PERMITTED	PERMITTED	PERMITTED	PERMITTED
SEX, GENDER, DOCUMENTED SEX	PERMITTED	PERMITTED	PERMITTED	PERMITTED
ASSIGNED IDENTIFIER [MIN(0), MAX(5)]	PERMITTED	PERMITTED	PERMITTED	PERMITTED
PERSON STATUS	NOT PERMITTED	NOT PERMITTED	NOT PERMITTED	PERMITTED
ADDRESS [MIN(0), MAX(3)]	NOT PERMITTED	NOT PERMITTED	NOT PERMITTED	PERMITTED

ASSOCIATED PERSON [MIN(0), MAX(5)]	PERMITTED	PERMITTED	PERMITTED	PERMITTED

10.3 Data Element Validation Request Specifications

In the sections that follow, the validation request specifications for the associated data elements of each personal information category are detailed. Each section contains an overview of the personal information category, followed by a list of restrictions and a table showing the validation request specifications for the data elements associated with the personal information category. The data element validation request specifications tables indicate the provision requirements for each data element within the personal information category in relation to function.

Note: When a specification statement or table entry references a data element, it is referring to both the data element name and the data element value. For example, a specification statement such as “the **Event Date** data element must be provided” means that both the data element name (i.e. **Event Date**) and a value for the data element (e.g. 2001-12-16) must be provided[12].

[12] This assumes an XML or XML-like (e.g. JSON, YAML) implementation where the concept of a data element consists of a data element *tag* **plus** a data element *value* (XML example: <EventDate>2001-12-16</EventDate>).

10.3.1 PERSON NAME Data Element Validation Request Specifications

PERSON NAME indicates the name by which a person is known or referred to. A person's name is usually a combination of a *surname* and one or more *given names*. A person may have several known names (due to name change, name variations, marriage, etc.).

The Standard supports the use of three types of names: Foundation Name, Primary Name, and Previous Primary Name. The Standard does not support the use of Preferred Name which is a name provided by the person by which he or she prefers to be informally addressed (e.g. a nickname).

The Standard supports the provision of up to a maximum of five instances of **PERSON NAME** in a validation request. The provision of several instances of **PERSON NAME** may be required in those cases in which a person provides documentation having different names, such as a birth certificate, marriage license, legal name change document, etc.

The Standard recognizes two different given name formats.

Restrictions:

1. The **Person Name Type Code** data element must be provided.
2. The **Surname** data element must be provided.

Table 2: PERSON NAME Data Element Validation Request Specifications

Data Elements Associated with PERSON NAME	Function	
	Identity Resolution	Validation
Person Name Type Code [CSV]	MANDATORY	MANDATORY
Surname	MANDATORY	MANDATORY
Given Names Listed	OPTIONAL	OPTIONAL
First Given Name Listed	OPTIONAL	OPTIONAL
Second Given Name Listed	OPTIONAL	OPTIONAL
Third and Additional Given Names Listed	OPTIONAL	OPTIONAL

10.3.2 DATE OF EVENT Data Element Validation Request Specifications

DATE OF EVENT indicates the date on which an event in a person's life occurred. Examples of date of event are: date of birth, date of death, and date of stillbirth. The completeness and accuracy of date of event information are dependent on where and when the event occurred.

The Standard supports the use of three types of events: Birth, Death, and Stillbirth.

The Standard supports the provision of up to a maximum of two instances of **DATE OF EVENT** in a validation request.

Restrictions:

1. The **Date of Event Type Code** data element must be provided.
2. The **Event Date** or **Event Year** data element must be provided.
3. If provided, the **Event Date** data element must contain the full date (year, month, and day).

Table 3: DATE OF EVENT Data Element Validation Request Specifications

Data Elements Associated with DATE OF EVENT	Function	
	Identity Resolution	Validation
Date of Event Type Code [CSV]	MANDATORY	MANDATORY
Event Date	Provision of at least one of these data elements is MANDATORY	Provision of at least one of these data elements is MANDATORY
Event Year		
Event Month	OPTIONAL	OPTIONAL
Event Day	OPTIONAL	OPTIONAL

10.3.3 PLACE OF EVENT Data Element Validation Request Specifications

PLACE OF EVENT indicates the place where an event in a person's life occurred. Examples of place of event are: place of birth, place of death, and place of stillbirth. The completeness, accuracy, and currency of place of event information are dependent on where and when the event occurred.

The Standard supports the use of three types of events: Birth, Death, and Stillbirth.

The Standard supports the provision of up to a maximum of two instances of **PLACE OF EVENT** in a validation request.

The Standard recognizes different methods of representing geographic information.

Restrictions:

1. The **Place of Event Type Code** data element must be provided.
2. At least one additional **PLACE OF EVENT** data element must be provided.

Table 4: PLACE OF EVENT Data Element Validation Request Specifications

Data Elements Associated with PLACE OF EVENT	Function	
	Identity Resolution	Validation
Place of Event Type Code [CSV]	MANDATORY	MANDATORY
Municipality Name	Provision of at least one of these data elements is MANDATORY	Provision of at least one of these data elements is MANDATORY
Province/Territory Code [CSV]		
Province/Territory/State Abbreviation Code [CSV]		
Province/Territory/State Name		
Country Code [CSV]		
Country Name		
Census Division and Census Subdivision Code [CSV]		

10.3.4 SEX, GENDER, DOCUMENTED SEX Data Element Validation Request Specifications

SEX, GENDER, DOCUMENTED SEX indicates the sex, gender, or documented sex of a person. Depending on the program or service delivery requirement, a person may have one or several indications.

Restrictions:

1. At least one of the **SEX, GENDER, DOCUMENTED SEX** data elements must be provided.

Table 5: SEX, GENDER, DOCUMENTED SEX Data Element Validation Request Specifications

Data Elements Associated with SEX, GENDER, DOCUMENTED SEX	**Function**	
	Identity Resolution	**Validation**
Sex Code [CSV]	Provision of at least one of these data elements is MANDATORY	Provision of at least one of these data elements is MANDATORY
Gender Code [CSV]		
Documented Sex Code [CSV]		

10.3.5 ASSIGNED IDENTIFIER Data Element Validation Request Specifications

ASSIGNED IDENTIFIER indicates an artificial identifier (typically a numeric or alphanumeric string) that has been assigned to a unique person. An assigned identifier may be associated with an event (e.g. a birth registration), a program (e.g. a provincial health insurance program), or a document issued to a person (e.g. a passport). A person may have several assigned identifiers – for example, a person may have a birth registration number, a provincial health insurance number, and a passport number.

Note: The status of a document (e.g. lost, stolen, expired, etc.) is specified by means of the **Person Identifier Status Code** and the **Person Identifier Status Reason Code** data elements in the validation request.

The Standard supports the provision of up to a maximum of five instances of **ASSIGNED IDENTIFIER** in a validation request.

<u>Restrictions:</u>

1. The **Assigned Identifier Type Code** data element must be provided.
2. The **Person Identifier** data element must be provided.

Table 6: ASSIGNED IDENTIFIER Data Element Validation Request Specifications

Data Elements Associated with ASSIGNED IDENTIFIER	Function	
	Identity Resolution	Validation
Assigned Identifier Type Code [CSV]	MANDATORY	MANDATORY
Person Identifier	MANDATORY	MANDATORY
Registration Date	OPTIONAL	OPTIONAL
Effective Date	OPTIONAL	OPTIONAL
Expiry Date	OPTIONAL	OPTIONAL
Issue Date	OPTIONAL	OPTIONAL
Person Identifier Status Code [CSV]	OPTIONAL	OPTIONAL
Person Identifier Status Reason Code [CSV]	OPTIONAL	OPTIONAL

10.3.6 PERSON STATUS Data Element Validation Request Specifications

PERSON STATUS indicates an officially recognized standing of a person. Depending on the program or service delivery requirement, a person may have one or several indications.

The Standard supports the provision of **PERSON STATUS** in a validation request for the purpose of personal information validation only.

Restrictions:

1. At least one of the **PERSON STATUS** data elements must be provided.

Table 7: PERSON STATUS Data Element Validation Request Specifications

Data Elements Associated with PERSON STATUS	**Function**	
	Identity Resolution	**Validation**
Death Status Code [CSV]	NOT APPLICABLE	Provision of at least one of these data elements is MANDATORY
Marital Status Code [CSV]		
Change of Legal Name Status Code [CSV]		
Canadian Citizenship Status Code [CSV]		
Legal Presence in Canada Status Code [CSV]		

10.3.7 ADDRESS Data Element Validation Request Specifications

ADDRESS indicates where a person lives or can be communicated with. A person may have several addresses, including primary and secondary residences, mailing addresses, and previous residences.

The Standard supports the provision of up to a maximum of three instances of **ADDRESS** in a validation request for the purpose of personal information validation only.

The Standard recognizes three different street address formats and also recognizes different methods of representing geographic information.

Restrictions:

1. The **Address Type Code** data element must be provided.
2. At least one additional **ADDRESS** data element must be provided.

Table 8: ADDRESS Data Element Validation Request Specifications

Data Elements Associated with ADDRESS	**Function**	
	Identity Resolution	**Validation**
Address Type Code [CSV]	NOT APPLICABLE	MANDATORY
Street Address	NOT APPLICABLE	Provision of at least one of these data elements is MANDATORY
Street Address Line 1		
Street Address Line 2		
Unit Specification		
Civic Number		
Civic Number Suffix		
Street Name		
Street Type		
Street Direction		

Postal Box		
Rural Route		
Postal Station		
Additional Delivery Specifications		
Municipality Name		
Province/Territory Code [CSV]		
Province/Territory/State Abbreviation Code [CSV]		
Province/Territory/State Name		
Country Code [CSV]		
Country Name		
Postal Code		
Census Division and Census Subdivision Code [CSV]		

10.3.8 ASSOCIATED PERSON Data Element Validation Request Specifications

ASSOCIATED PERSON indicates another person who has an affiliation with or a legal authority to act on behalf of a person (e.g. spouse, parent, guardian, power of attorney, etc.). A person may have several associated persons.

The Standard supports the provision of up to a maximum of five instances of **ASSOCIATED PERSON** in a validation request.

ASSOCIATED PERSON is comprised of the **Associated Person Type Code** data element and five of the personal information categories defined earlier in the Standard: **PERSON NAME**; **DATE OF EVENT**; **PLACE OF EVENT**; **SEX, GENDER, DOCUMENTED SEX**; and **ASSIGNED IDENTIFER**. For these five personal information categories, the table below references the respective table that lists the data element specifications for the personal information category.

Restrictions:

1. The **Associated Person Type Code** data element must be provided.
2. In the case of the identity resolution function, at least one personal information category must be provided, and in the case of the validation function, the **PERSON NAME** personal information category must be provided.

Table 9: ASSOCIATED PERSON Data Element Validation Request Specifications

Data Elements Associated with ASSOCIATED PERSON	**Function**	
	Identity Resolution	**Validation**
Associated Person Type Code [CSV]	MANDATORY	MANDATORY
PERSON NAME [MIN(1), MAX(2)]	OPTIONAL See Table 2 for data element specifications	MANDATORY See Table 2 for data element specifications
DATE OF EVENT [MIN(0), MAX(2)]	OPTIONAL See Table 3 for data element specifications	OPTIONAL See Table 3 for data element specifications
PLACE OF EVENT [MIN(0), MAX(2)]	OPTIONAL See Table 4 for data element specifications	OPTIONAL See Table 4 for data element specifications
SEX, GENDER, DOCUMENTED SEX	OPTIONAL See Table 5 for data element specifications	OPTIONAL See Table 5 for data element specifications
ASSIGNED IDENTIFIER [MIN(0), MAX(2)]	OPTIONAL See Table 6 for data element specifications	OPTIONAL See Table 6 for data element specifications

10.4 Validation Request/Response Parameter Specifications

10.4.1 Disclosure Level Parameters

A relying party must specify within a validation request a disclosure level to limit the degree of disclosure.

An authoritative party must provide a disclosure level within a validation response. The authoritative party may return a disclosure level that is different from the disclosure level requested by the relying party.

Standardized disclosure levels range between:

- **No disclosure** – where no personal information is disclosed (This may be the case when an authoritative party does not have the authority to provide a response to a request from a relying party.)
- **Partial disclosure** – where the result of the comparison of two data element values is disclosed
- **Full disclosure** – where the correct value on record is disclosed

Published service profiles will specify which request and response disclosure level types are supported. These service profiles will form part of the trust framework.

Table 10 lists the disclosure level types that may be requested in a validation request and the disclosure levels that may be provided in a validation response.

Table 10: Disclosure Levels

Requested Disclosure Level Type	Description of Requested Disclosure Level Type	Possible Response Disclosure Level Types
VALIDATION DISCLOSURE LEVEL TYPE 1	● a VALIDATION INDICATOR for each data element (Validation Indicator codeset: “**Same**”, “**Similar**”, “**Different**”, “**Not available**”, “**No disclosure**”)	● VALIDATION DISCLOSURE LEVEL TYPE 1

VALIDATION DISCLOSURE LEVEL TYPE 2	● a VALIDATION INDICATOR for each data element (Validation Indicator codeset: “**Same**”, “**Similar**”, “**Different**”, “**Not available**”, “**No disclosure**”) ● a VALIDATION SCORE for each data element (if applicable)	● VALIDATION DISCLOSURE LEVEL TYPE 2 **OR** ● VALIDATION DISCLOSURE LEVEL TYPE 1
VALIDATION DISCLOSURE LEVEL TYPE 3	● a VALIDATION INDICATOR for each data element (Validation Indicator codeset: “**Same**”, “**Similar**”, “**Different**”, “**Not available**”, “**No disclosure**”) ● a VALIDATION SCORE for each data element (if applicable) ● the VALUE ON RECORD for each data element (if available)	● VALIDATION DISCLOSURE LEVEL TYPE 3 **OR** ● VALIDATION DISCLOSURE LEVEL TYPE 2 **OR** ● VALIDATION DISCLOSURE LEVEL TYPE 1

Notes:

- VALIDATION SCORE refers to a value calculated by the authoritative party that indicates the probability that the value that the relying party has supplied and the value that the authoritative party has on record are equivalent.
- VALUE ON RECORD refers to the identity information or personal information that the authoritative party has on record. It can be assumed that this identity information or personal information is accurate subject to an integrity or assurance standard.

10.4.2 Assurance Level Parameters

The Standard supports the specification of an assurance level which may be provided in a validation request or a validation response. The incorporation of assurance levels enables the Standard to be used in conjunction with trust frameworks that have been recognized or adopted by the participating parties.

Currently, the existing trust frameworks have predominantly agreed on the four assurance levels[13] listed in Table 11.

Table 11: Assurance Levels

Assurance Level	Description
Level 1	Little or no (low) degree of confidence required.
Level 2	Some (substantial) degree of confidence required.
Level 3	High (high) degree of confidence required.
Level 4	Very high degree of confidence required.

In conjunction with an agreed on trust framework, a relying party may specify an assurance level to indicate requirements relative to the degree of accuracy, quality, and integrity of the information being validated. Similarly, an authoritative party may specify an assurance level to indicate the level of requirements that have been met.

For example, **Level 1** may be used by a relying party to indicate that little to no confidence is required, while **Level 4** would indicated that very high confidence is required. The authoritative party, in providing a validation response, would indicate the assurance level it is providing in the validation response (in accordance with the requirements of a trust framework).

<u>Assurance Level Specifications:</u>

1. As part of a validation request, a relying party may provide an assurance level to indicate the level of confidence that is required.
2. As part of a validation response, an authoritative party may provide an assurance level to indicate the level of confidence that they are capable of providing to the relying party.
3. The specific interpretation of the assurance levels are defined using an applicable

[13] For more detailed information, see the *Standard on Identity and Credential Assurance*.

agreement or trust framework.

11 Appendix A: Terms and Definitions

The definitions that follow include authoritative definitions from the *Standard on Identity and Credential Assurance*, definitions found in related guidelines and industry references, and definitions developed by the working group for the purposes of this document.

Term	Definition
anonymous credential	Refers to a credential that, while still making an assertion about some property, status, or right of the person, does not reveal the person's identity. A credential may contain identity attributes but still be treated as anonymous if the identity attributes are not recognized or used for identity validation purposes. Anonymous credentials provide persons with a means by which to prove statements about themselves and their relationships with public and private organizations anonymously.
assigned identifier	A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between persons without the use of any other identity attributes.
assurance	A measure of certainty that a statement or fact is true.
assurance level	A level of confidence that may be relied on by others.
assurance of credential	Concerns the binding of a credential to a person (without regard to their identity).
assurance of identity	Concerns the claim that the person is really who they say they are.
attribute	A property or characteristic associated with an entity. See also “identity attribute”.
authentication	The process of establishing truth or genuineness to generate an assurance of credential or identity.
authoritative party	A federation member that provides assurances of credential or identity to other federation members (i.e. “relying parties”).
authoritative source	A collection or registry of records maintained by an authority that meets established criteria.
biological or behavioural	A process that compares biological (anatomical and

characteristic confirmation	physiological) characteristics in order to establish a link to a person (e.g. facial photo comparison).
biometrics	A general term used alternatively to describe a characteristic or a process. It can refer to a measurable biological (anatomical and physiological) or behavioural characteristic that can be used for automated recognition. It can also refer to automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioural characteristics.
business event	A business event is a significant discrete episode that occurs in the life span of a business. By law a business event must be recorded with a government entity and is subject to legislation and regulation. Examples of business events are registration of charter, merger, amalgamation, surrender of charter, and dissolution.
client	The intended recipient for a service output. External clients are generally persons (Canadian citizens, permanent residents, etc.) and businesses (public and private sector organizations). Internal clients are generally public service employees and contractors.
context	A set of circumstances, a situation, or a scenario in which a person interacts with other persons or with an organization.
credential	A unique physical or electronic object (or identifier) issued to, or associated with, a person, organization, or device (e.g. key, token, document, program identifier).
credential assurance	The assurance that a person, organization, or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).
credential assurance level	The level of confidence that a person, organization, or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).
credential federation	A federation established for the purpose of credential

	management.
credential risk	The risk that a person, organization, or device has lost control over the credential with which they have been entrusted.
document authentication	The process of confirming the authenticity of a document: genuine, counterfeit, forged, etc. Document authentication is achieved by checking the security features of a document, such as secure laminate, holographic images, etc.
documentary evidence	Any physical record of information that can be used as evidence. This is widely understood to mean information written on paper, but the more general definition is preferable.
documented sex	An attribute copied from the “sex” or “gender” indicator on a credential.
electronic or digital evidence	Any data that is recorded or preserved on any medium in, or by, a computer system or other similar device. Examples include database records, audit logs, and electronic word processing documents.
evidence of identity	A record from an authoritative source that supports the integrity and accuracy of the claims made by a person. There are two categories of evidence of identity: foundational and supporting. See “foundational evidence of identity” and “supporting evidence of identity”.
federated credential management	The sharing of assurances of credentials with trusted members of a federation.
federated identity management	The sharing of assurances of identity with trusted members of a federation.
federating credentials	The process of establishing a federation in which members share assurances of credentials with trusted members of the federation.
federating identity	The process of establishing a federation in which members share assurances of identity with trusted members of the federation.
federation	A cooperative agreement between autonomous entities that have agreed to relinquish some of their autonomy in order to work together effectively to support a

	collaborative effort. The federation is supported by trust relationships and standards to support interoperability.
foundation name	The name of a person as indicated on an official record identifying the person (e.g. vital statistics record, immigration record).
foundation registry	A registry that maintains permanent records about persons who were born in Canada, persons who are Canadian but who were born abroad, or persons who are foreign nationals who have applied to enter Canada.
foundational evidence of identity	Evidence of identity that establishes core identity information such as surname, given name(s), date of birth, sex, and place of birth. Examples include records of birth, death, immigration, or citizenship originating from a jurisdictional authority.
gender	The socially constructed roles, behaviours, activities, and attributes that a given society considers appropriate for a male or a female.
identifier	The set of identity attributes used to uniquely distinguish a unique and particular person, organization, or device.
identity	A reference or designation used to distinguish a unique and particular person, organization, or device.
identity assurance	A measure of certainty that a person, organization, or device is who or what it claims to be.
identity assurance level	The level of confidence that a person, organization, or device is who or what it claims to be.
identity attribute	A property or characteristic associated with an identifiable person, organization, or device (also known as “identity data element”).
identity claim	An assertion of the truth of something that pertains to a person's identity.
identity data element	See “identity attribute”.
identity establishment	The creation of an authoritative record of identity that is relied on by others for subsequent government activities, programs, and services.
identity federation	A federation established for the purpose of identity management.

identity fraud	The deceptive use of personal information in connection with frauds such as the misuse of debit/credit cards or applying for loans using stolen personal information.
identity information	The set of identity attributes that is sufficient to distinguish one person from all other persons within a program/service population and that is sufficient to describe the person as required by the program or service. Identity information is a subset of personal information.
identity information notification	The disclosure of identity information about a person by an authoritative party to a relying party that is triggered by the establishment of the person’s identity, a change in their identity information, or an indication that their identity information has been exposed to a risk factor (e.g. the death of the person, use of expired documents, a privacy breach, fraudulent use of the identity information).
identity information retrieval	The disclosure of identity information about a person by an authoritative party to a relying party that is triggered by a request from the relying party.
identity information validation	The confirmation of the accuracy of identity information about a person as established by an authoritative party. Note: Identity information validation does not ensure that the person is using their own identity information, only that the identity information the person is using is accurate and up to date.
identity management	The set of principles, practices, processes, and procedures used to realize an organization's mandate and its objectives related to identity.
identity resolution	The establishment of the uniqueness of a person within a program/service population through the use of identity information.
identity risk	The risk that a person, organization, or device is not who or what it claims to be.
identity theft	The preparatory stage of acquiring and collecting someone else's personal information for criminal purposes.
identity verification	The confirmation that the identity information being presented relates to the person who is making the

	claim.
interoperability	The ability of organizations to operate synergistically through consistent security and identity management practices.
jurisdictional hub	A system that all entities within a jurisdiction connect to in order for them to electronically interact with all other jurisdictions via one external facing common gateway.
knowledge-based confirmation	A process that compares personal or private information (i.e. shared secrets) to establish a person's identity. Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information, and credit or financial information.
legal name	See “primary name”.
legal presence	Lawful entitlement to be or reside in Canada.
person	A human being including “minors” and others who might not be deemed to be persons under the law.
personal information	Information about an identifiable person.
personal information notification	The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by the establishment of the person’s identity or a change in their personal information.
personal information retrieval	The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by a request from the relying party.
personal information validation	The confirmation of the accuracy of personal information about a person as established by an authoritative party.
physical possession confirmation	A process that requires physical possession or presentation of evidence to establish a person's identity.
preferred name	The name by which a person prefers to be informally addressed.
primary name	The name that a person uses for formal and legal purposes (also known as “legal name”).
relying party	A federation member who relies on assurances of credential or identity from other federation members

	(i.e. "authoritative parties").
risk	The uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.
sex	The biological characteristics that define a human being as female or male. These sets of biological characteristics are not mutually exclusive as there are persons who possess both female and male characteristics.
supporting evidence of identity	Evidence of identity that corroborates the foundational evidence of identity and assists in linking the identity information to a person. It may also provide additional information such as a photo, signature, or address. Examples include social insurance records; records of entitlement to travel, drive, or obtain health insurance; and records of marriage, name change, or death originating from a jurisdictional authority.
trust	A firm belief in the reliability or truth of a person or thing.
trust framework	A formalized scheme that ensures that federation members have continued confidence in one another. A trust framework formally underpins trust relationships by stipulating adherence to standards, formalizing assessment processes, and defining roles and responsibilities of multi-party arrangements.
trust relationship	A defined arrangement or agreement that ensures confidence.
trusted referee confirmation	A process that relies on a trusted referee to establish a link to a person. The trusted referee is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries, and certified agents.
vital event	A vital event is a significant discrete episode that occurs in the life span of a person. By law a vital event must be recorded with a government entity and is subject to legislation and regulation. Examples of vital events are live birth, foetal death (i.e. stillbirth), adoption, legitimation, recognition of parenthood, marriage, annulment of marriage, legal separation, divorce, and

	death.

12 Appendix B: Related Documents

Identity Management Sub-Committee (IMSC)

- Pan-Canadian Assurance Model
- Pan-Canadian Paper on Trusting Identities

Treasury Board of Canada Secretariat (TBS)

- Standard on Identity and Credential Assurance
- Guideline on Identity Assurance
- Guideline on Defining Authentication Requirements