BRITISH COLUMBIA
Office of the Chief Information Officer

EVIDENCE OF IDENTITY STANDARD

Version 1.0
April 2010

Office of the Chief Information Officer,
Architecture, Standards and Planning Branch

-- This page left intentionally blank --

Revision History

Version	Date	Changed By	Description of Change
1.0	April 23, 2010	Charmaine Lowe	

Document Purpose

This document is part of the Identity Information Management Standards Package and is a supporting standard to the *Identity Assurance Standard*.

It re-introduces the Identification Levels set out in the *Identity Assurance Standard* and sets evidence of identity, registration and operational diligence standards for establishing an individual's identity to four increasing levels of identification strength. It also sets standards for the subsequent confirmation or verification of an individual's identity over-the-counter (i.e., in-person) and over the telephone.

Unless otherwise noted, the standards set out in this document apply to all service delivery channels (i.e., they apply to both online and off-line identity management transactions.)

Intended Audience

The intended audience for this Standard is registration agents and individuals who perform identity-proofing services. The standard will also assist business and technical analysts, data architects, and developers in developing detailed specifications for identity information management systems.

Accessing Advice on this Standard

Advice on this Standard can be obtained from the:

Architecture and Standards Branch
Office of the Chief Information Officer
Ministry of Citizens' Services

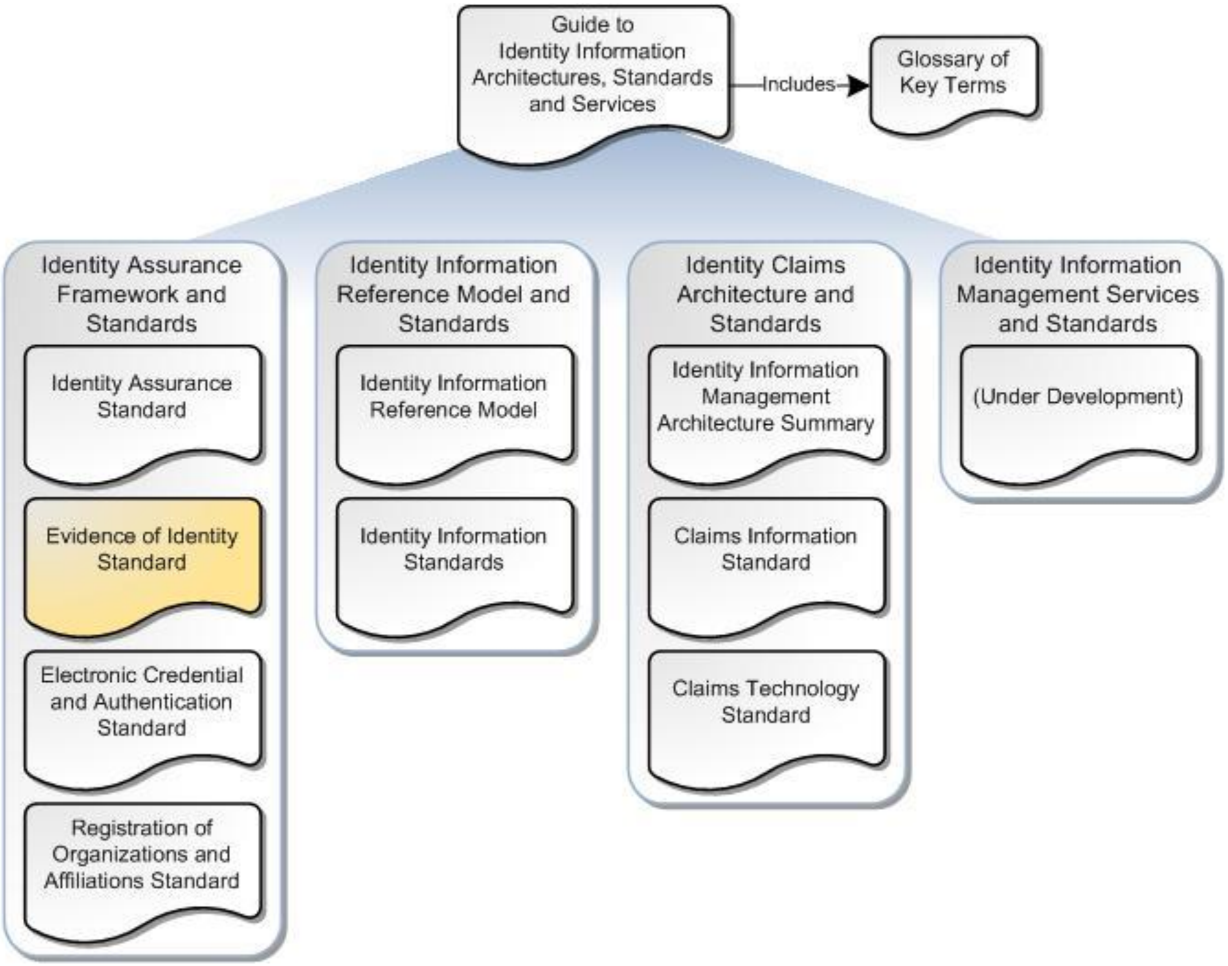
Postal Address:	PO Box 9412 Stn Prov Govt
Telephone:	(250) 387-8053
Facsimile:	(250) 953-3555
Email:	asb.cio@gov.bc.ca
Web:	http://www.cio.gov.bc.ca/cio/standards/index.page

Identity Information Management Standards Package

This document is one of a set of standards and related documents included in the *Identity Information Management Standards Package.* The Package includes a set of architectures, frameworks, models, standards and supporting documents which, when implemented together, will result in a common, secure and trusted approach to identifying and authenticating users and subjects of government services and protected resources.

The Package can be divided into four main topic areas: Identity Assurance Framework and Standards; Identity Information Reference Model and Standards; Identity Claims Architecture and Standards; and Identity Information Management Services and Standards. The Package also contains a high-level Overview and Glossary which assist in the understanding of, and act as a navigational guide to, the other documents in the Package.

Figure 1 - The Identity Information Management Standards Package


Guide to Identity Information Architectures, Standards and Services
Includes
Glossary of Key Terms
Identity Assurance Framework and Standards
Identity Assurance Standard
Evidence of Identity Standard
Electronic Credential and Authentication Standard
Registration of Organizations and Affiliations Standard
Identity Information Reference Model and Standards
Identity Information Reference Model
Identity Information Standards
Identity Claims Architecture and Standards
Identity Information Management Architecture Summary
Claims Information Standard
Claims Technology Standard
Identity Information Management Services and Standards
(Under Development)

Readers wishing to find more information on a related topic should refer to one or more of the other documents available within the package.

Table 1, below, describes the purpose of each of the Identity Information Management Standards and Documents, with the document you are currently reading highlighted. Please refer to the *Guide to Identity Information Architectures, Standards and Services* for a more comprehensive description of the documents in the Package.

Table 1 - Identity Information Management Standards and Documents

Standard/Document Name	**Purpose**
Guide to Identity Information Architectures, Standards and Services • *Includes Glossary of Key Terms* *(Under Development)*	Provides a high-level overview of the Province of British Columbia's Identity Information Management solution and acts as a navigational guide to the supporting identity information management architectures, standards and services set out in the following four topic areas.
1. Identity Assurance Framework and Standards	
Identity Assurance Standard	Introduces the Identity Assurance Framework and sets standards for achieving increasing levels of identity assurance over multiple service delivery channels. Provides a framework for supporting standards, listed below.
Evidence of Identity Standard	Supports the *Identity Assurance Standard* by setting evidence of identity and operational diligence standards for registering and identity-proofing individuals to increasing levels of identification strength. Applies to both online and off-line (i.e., real world) identity management transactions.
Electronic Credential and Authentication Standard	Supports the *Identity Assurance Standard* by setting standards for issuing, managing and authenticating electronic credentials to increasing levels of strength.
Registration of Organizations and Affiliations Standard *(Under Development)*	Sets information and process standards for identifying and registering organizations and establishing affiliations between individuals and organizations.
2. Identity Information Reference Model and Standards	
Identity Information Reference Model *(Under Development)*	Establishes an Identity Information Reference Model that sets out how individuals represent themselves in different identity contexts (i.e., as an employee, a professional, a student, a business representative, etc.). Provides a framework for the *Identity Information Standards.*
Identity Information Standards *(Under Development)*	Sets semantic and syntactic standards for core identity and supporting information such as names, identifiers, dates and locators, as set out in the *Identity Information Reference Model*. These standards support both the *Evidence of Identity Standard* and the *Claims Information Standard*.
3. Identity Claims Architecture and Standards	
Identity Information Management Architecture Summary	Establishes a base architecture to support the exchange of identity claims between authoritative and relying parties. Introduces concepts such as user-centric claims-based architecture, authoritative parties, relying parties, identity agents, and federation, and relates these to identity assurance.

Claims Information Standard	Supports the *Identity Information Management Architecture Summary* by setting standards for the definition and use of claims. Provides definitions for the core set of claims related to the *Identity Information Standards.*
Claims Technology Standard	Supports the *Identity Information Management Architecture Summary* by setting standards and profiles related to industry open standard protocol specifications. Also sets standards for security controls and logon user experience to promote secure and usable implementations.
4. Identity Information Management Services and Standards	
(Under development)	Describes the Province's Identity Information Management Services and sets standards for their use and applicability, including: identity services, authentication services and federation services.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 Introduction

The *Evidence of Identity Standard* supports the *Identity Assurance Standard* by setting requirements for registering and identity-proofing individuals to four increasing levels of identification strength. Evidence of Identity refers to the information, types of evidence and verification processes that, when combined, provide sufficient confidence that individuals are who they say they are.

Use of this standard will give organizations greater assurance in an individual's identity, prior to the delivery of a service to that individual. It will also help to:

- provide a consistent customer experience to individuals seeking services of a similar nature from different government organizations and across different service delivery channels;
- provide confidence to the public that the evidence of identity they are asked to provide is appropriate and proportionate to the particular service they wish to access;
- reduce the risk of identity fraud occurring and any downstream criminal activity that this facilitates;
- protect individuals from others stealing and using their identities to access government services; and
- provide confidence that privacy concerns are addressed for evidence of identity processes used by government.

All government services and resources that require a level of identity assurance before permitting access will require an evidence of identity process. The comprehensiveness of that process will depend on the level of identity assurance needed to access the particular service or resource. Services and resources that have low identity assurance needs will require minimal evidence of identity processes. Conversely, services and resources with higher identity assurance requirements will require more robust evidence of identity processes. For more information on the relationship between identity assurance and identification levels, readers should refer to the *Identity Assurance Standard*.

1.1 Scope

The *Evidence of Identity Standard* sets information and process requirements for establishing and verifying the identity of individuals seeking access to government services or resources.

Standards for establishing and verifying the identity of organizations and an individual's relationship (or affiliation) with an organization are set out in the *Registration of Organizations and Affiliations Standard.*

In Scope

This *Evidence of Identity Standard* sets the minimum information, evidence and verification requirements that all organizations must adopt for:

- the initial establishment of an individual's identity;
- subsequent authentication of an individual's identity over the counter and over the telephone;
- updating an individual's identity information; and
- ensuring operational diligence.

Out of Scope but covered in Related Standards

The following are outside the scope of the *Evidence of Identity Standard* but, as noted below, are covered by other related standards:

- Standards for determining identity assurance requirements and assessing risk and other factors (covered in the *Identity Assurance Standard*).

- Definitions, rules and data formats for identity-related and supporting data attributes (covered in the *Identity Information Standards*).

- Standards for issuing, managing and authenticating electronic credentials used to prove identity (covered in the *Electronic Credential and Authentication Standard)*. Organizations that provide both identity proofing and electronic credential issuing services MUST comply with both the *Evidence of Identity Standard* and the *Electronic Credential and Authentication Standard.*

- Standards for registering and identity-proofing organizations and an individual's affiliation (or relationship) to an organization (covered in the *Registration of Organizations and Affiliations Standard).*

Out of Scope – Not covered in other standards

The following are outside the scope of the *Evidence of Identity Standard* and currently outside the scope of related standards and documents:

- Criteria for establishing program eligibility or entitlement and guidance for managing eligibility or entitlement fraud.
- Collection and verification of program specific information that organizations may wish to collect to enable or enhance their own specific internal processes and services including program-specific identity and entitlement information.
- Guidance on reducing or managing identity-related fraud. While use of this standard will assist with identity-related fraud and the consequences that arise from those activities, it will not completely mitigate these risks nor will it prevent cases of administrative error in

relation to the establishment and confirmation of an individual's identity. Organizations SHOULD, therefore, apply this standard alongside other good practices that assist in the reduction of identity-related fraud and administrative error.

1.2 Applicability

Applicability of this Standard

This standard applies to British Columbia Government Ministries and Central Agencies (hereafter referred to as government organizations). Other organizations may choose to adopt these standards or may agree to adopt these standards for the purpose of fulfilling contractual, federation or other legal agreements.

This standard applies to organizations that perform their own registration and identity-proofing services and to organizations that provide registration and identity-proofing services for other organizations. Government organizations that require third parties to follow this standard can include a requirement to comply with this standard in their contract for service.

This standard MUST be applied to all government services and resources that require identity assurance, regardless of the service delivery channel (i.e., this standard applies to both online and offline identity management transactions). This standard applies to both the initial establishment of identity and to the subsequent confirmation or verification of identity. This standard also applies to the identification and authentication of individuals in an employment context (i.e., to the recruitment of, and the use of government services and resources by, government employees).

In some cases complete application of this standard will not be possible due to the nature of a service's client base. For example, some services have a client base made up largely of individuals without required documentation such as children, homeless individuals or individuals residing outside of Canada. Complete application of this standard may also not be suitable for some law-enforcement related services or services where the identities of certain individuals are protected. In these cases, agencies SHOULD apply for, and use, exception processes that are aligned as closely as possible to the content of this standard.

Interpretation of this Standard

The following keywords, when used in this standard, have the following meaning:

MUST, REQUIRES, REQUIRED or SHALL means that the definition is an absolute requirement of the standard.

MUST NOT or SHALL NOT means that the definition is an absolute prohibition of the standard.

SHOULD or RECOMMENDED means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT or NOT RECOMMENDED means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY or OPTIONAL means that an item is truly optional. (Often there is a practice to do something, however it is not a requirement.)

The definitions of these keywords are taken from the IETF RFC 2119. When these words are not capitalized, they are meant in their natural-language sense.

1.3 References

Key References

The following documents and standards should be read to set the context for, and assist in the understanding of, this standard:

- *Identity Assurance Standard*
- *Identity Information Reference Model*

For a full overview of the Identity Information Management solution and a complete list of related documents and standards see:

- *Guide to Identity Information Architectures, Standards and Services*

Other References and Acknowledgements

Many of the concepts and processes set out in this standard are based on the following identity assurance and evidence of identity standards and frameworks:

- Pan-Canadian Strategy for Identity Management and Authentication available at: http://www.cio.gov.bc.ca/cio/idim/idmatf.page
- New Zealand's Department of Internal Affairs' Evidence of Identity Standard, Version 2.0 available at http://www.e.govt.nz/standards/e-gif/authentication/
- U.S. National Institute of Standards and Technology's Electronic Authentications Guide available at: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- Kantara Initiative's Identity Assurance Framework: Service Assessment Criteria (formerly Liberty Alliance Identity Assurance Framework) available at http://kantarainitiative.org/confluence/display/certification/Identity+Assurance+Certification+Program

In particular, the authors of this standard wish to acknowledge the authors of New Zealand's *Evidence of Identity Standard* whose work greatly influenced this standard.

1.4 Terms and Definitions

Key terms and definitions related to the *Evidence of Identity Standard* are set out in Appendix A. For a listing of all Identity Information Management Terms and Definitions, see the *Glossary of Key Terms* in the *Guide to Identity Information Architectures, Standards and Services*.

1.5 Document Structure

This document has seven main sections:

Section 1: The document introduction section which includes the document's purpose, scope, and applicability.

Section 2: This section sets context for the *Evidence of Identity Standard* and explores core concepts and challenges associated with establishing and verifying identity.

Section 3: This section sets out Evidence of Identity Requirements for establishing and verifying identity. It sets criteria for core identity information like names and specifies what credentials are acceptable as evidence for different components of identity.

Section 4: This section sets out the minimum registration, evidence of identity and verification processes that an organization must follow to establish an individual's identity to four increasing levels of identification strength.

Section 5: This section sets out operational diligence and service standards for organizations that register and identity-proof individuals, including identity lifecycle processes and legal, security and service requirements.

Section 6: This section describes how credentials can be used to confirm or verify identity and sets out credential strength levels for different types of physical credentials.

Section 7: This section sets out standards that an organization must follow to confirm or verify an individual's identity over-the-counter (i.e., in-person) or over the telephone.

2 Context, Core Concepts and Challenges of Establishing and Verifying Identity

This section sets the context for the *Evidence of Identity Standard* by explaining how this standard relates to, and supports, the *Identity Assurance Standard*.

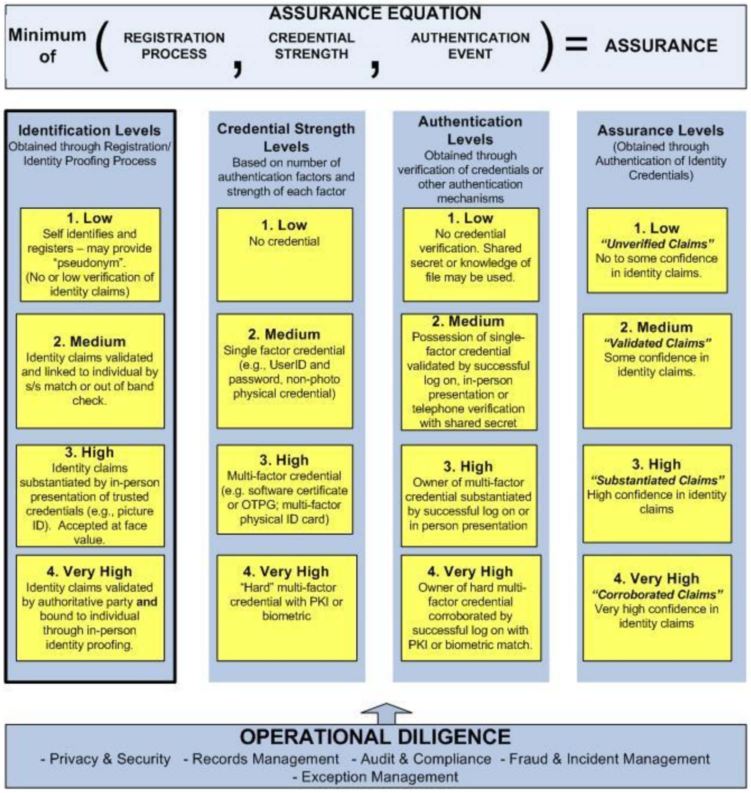
This section also explores core concepts and challenges associated with the establishment and verification of identity.

2.1 Context - the Identity Assurance Equation

The initial establishment of identity is the first component in the Identity Assurance Equation as illustrated below (for further information on the Identity Assurance Equation and the process for establishing increasing levels of Identity Assurance, refer to the *Identity Assurance Standard*).

Identification is the process of associating identity-related attributes with a particular person. When the identification process is accompanied by a registration process, a record of the identity is established which can later be used for confirmation or verification purposes in order to control access to a service or resource. In some cases, a registering organization will issue a credential, such as a User ID and password, which can be used for subsequent authentication against the record of identity.

Figure 2 – The Identity Assurance Equation



ASSURANCE EQUATION

Minimum of (REGISTRATION PROCESS , CREDENTIAL STRENGTH , AUTHENTICATION EVENT) = ASSURANCE

Identification Levels Obtained through Registration/ Identity Proofing Process	**Credential Strength Levels** Based on number of authentication factors and strength of each factor	**Authentication Levels** Obtained through verification of credentials or other authentication mechanisms	**Assurance Levels** (Obtained through Authentication of Identity Credentials)
1. Low Self identifies and registers – may provide "pseudonym". (No or low verification of identity claims)	**1. Low** No credential	**1. Low** No credential verification. Shared secret or knowledge of file may be used.	**1. Low** ***"Unverified Claims"*** No to some confidence in identity claims.
2. Medium Identity claims validated and linked to individual by s/s match or out of band check.	**2. Medium** Single factor credential (e.g., UserID and password, non-photo physical credential)	**2. Medium** Possession of single-factor credential validated by successful log on, in-person presentation or telephone verification with shared secret	**2. Medium** ***"Validated Claims"*** Some confidence in identity claims.
3. High Identity claims substantiated by in-person presentation of trusted credentials (e.g., picture ID). Accepted at face value.	**3. High** Multi-factor credential (e.g. software certificate or OTPG; multi-factor physical ID card)	**3. High** Owner of multi-factor credential substantiated by successful log on or in person presentation	**3. High** ***"Substantiated Claims"*** High confidence in identity claims
4. Very High Identity claims validated by authoritative party **and** bound to individual through in-person identity proofing.	**4. Very High** "Hard" multi-factor credential with PKI or biometric	**4. Very High** Owner of hard multi-factor credential corroborated by successful log on with PKI or biometric match.	**4. Very High** ***"Corroborated Claims"*** Very high confidence in identity claims

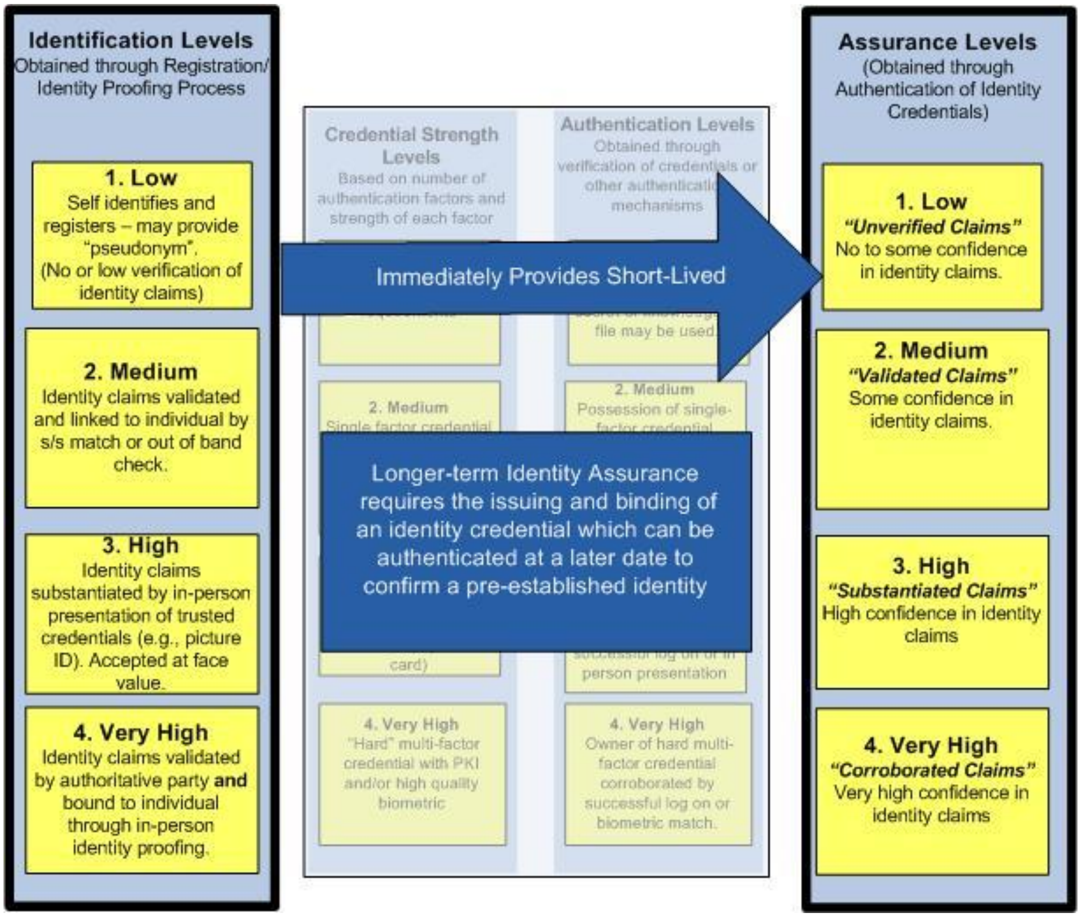
OPERATIONAL DILIGENCE
- Privacy & Security - Records Management - Audit & Compliance - Fraud & Incident Management - Exception Management

2.2 Relationship of Identification Levels to Identity Assurance Levels

It is important to note that the completion of a registration process that establishes an identity to a given identification level immediately produces the equivalent identity assurance level (see figure 3, below). However, that assurance is short lived, lasting only as long as the current transaction. Once the individual walks away from, or otherwise ends, the transaction, the identity assurance is lost unless the individual was issued and/or bound to a credential or shared secret which can be used for future confirmation (or authentication) of identity.

If a credential is issued and bound to the individual that is the same strength as the initial identification process (e.g., Level 3 credential bound to a Level 3 identification process), the individual will be able to present that credential in the future to access appropriate Level 3 services and resources. If no credential is issued, or if a credential of a lower strength than the initial identification process is issued, the service will need to repeat or strengthen the initial identification process at a later date to recreate the identity assurance initially established at the time of registration.

Figure 3: Relationship of Identification Levels to Identity Assurance Levels


Identification Levels
Obtained through Registration/ Identity Proofing Process
1. Low
Self identifies and registers – may provide "pseudonym". (No or low verification of identity claims)
2. Medium
Identity claims validated and linked to individual by s/s match or out of band check.
3. High
Identity claims substantiated by in-person presentation of trusted credentials (e.g., picture ID). Accepted at face value.
4. Very High
Identity claims validated by authoritative party and bound to individual through in-person identity proofing.
Credential Strength Levels
Based on number of authentication factors and strength of each factor
2. Medium
Single factor credential
card)
4. Very High
"Hard" multi-factor credential with PKI and/or high quality biometric
Authentication Levels
Obtained through verification of credentials or other authenticatio mechanisms
file may be used.
2. Medium
Possession of single-factor credential
person presentation
4. Very High
Owner of hard multi-factor credential corroborated by successful log on or biometric match.
Immediately Provides Short-Lived
Longer-term Identity Assurance requires the issuing and binding of an identity credential which can be authenticated at a later date to confirm a pre-established identity
Assurance Levels
(Obtained through Authentication of Identity Credentials)
1. Low
"Unverified Claims"
No to some confidence in identity claims.
2. Medium
"Validated Claims"
Some confidence in identity claims.
3. High
"Substantiated Claims"
High confidence in identity claims
4. Very High
"Corroborated Claims"
Very high confidence in identity claims

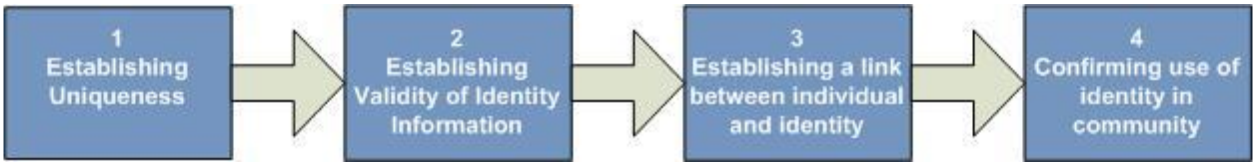
2.3 Core Concepts for Establishing Identity

Identification is the process of associating identity-related attributes with a particular person. For many services it will be necessary for the organization providing the service to uniquely identify the individuals who are seeking access to the service. An appropriate evidence of identity process is a necessary first step in managing identity-related risks associated with these services. The organization MUST either perform this identification process itself or rely on another organization to provide the identification service (i.e., utilize corporate identity services).

It is not feasible to prove with absolute certainty the identity of individuals seeking access to government services. This would require an evidence of identity process so cumbersome and intrusive that the costs would greatly outweigh any benefits. This Standard follows a risk-based approach to establishing identity to a level of assurance appropriate to the service being delivered.

The evidence of identity processes outlined in this Standard are based on four distinct but related components to establishing identity. Each component proves a different aspect of identity and not all components are required for all identification levels (lower levels require fewer components while higher levels may require all components). Applying these components in a consistent way will provide an appropriate level of assurance that an individual is actually who he or she claims to be.

Figure 4: Steps to Establishing Identity


1
Establishing Uniqueness
2
Establishing Validity of Identity Information
3
Establishing a link between individual and identity
4
Confirming use of identity in community

As set out above, the four components involved in establishing identity include:

1. Establishing Uniqueness

This component is about establishing that an individual is the only claimant of an identity. This step is necessary for all Identification Levels (including Level 1). Even a pseudonymous or unverified identity should be unique within the service's community of subjects where it is necessary to ensure that the same person (identified or not) is accessing a service that he or she accessed before.

At lower levels, establishing uniqueness can be accomplished by a simple database search to ensure that another identity with the same attributes does not already exist. At higher levels, collection and verification of other names may be required to ensure that the individual has not already registered under another name and at the very highest level, facial recognition or other biometric technology may be required. Establishing and ensuring persistent uniqueness can be enhanced by the assignment of a unique identifier.

2. Establishing Validity of Identity Information

This component is about establishing that the claimed identity information is valid (i.e., that a person with this identity information was actually born and, secondly, is still alive). Validating identity information is necessary for Identification Level 2 and above, but the evidence required and the rigour applied to validate the identity information increases with each level. For example, validating identity information at Identification Level 2 may be accomplished either directly by confirming it with an Authoritative Party or indirectly by the provision of government-issued photo identification. Identification Level 3 requires additional evidence in the form of a birth certificate or other foundation identity credential; and Level 4 requires the same evidence as Level 3 plus validation of the identity information with an Authoritative Party.

The most rigorous way to ensure that a claimed identity belongs to a person that is still alive is to verify the claimed identity against a death registry. This is not always practical or available at lower identification levels and even at Level 4, where it is required, the search may be limited to deaths registered in a particular jurisdiction. A death registry search will not necessarily reveal that a person with the claimed identity died in another jurisdiction.

3. Establishing a Link between the Individual and the Identity

This component is about establishing a link between a valid identity and a person claiming that identity (i.e., verifying that the person is really who he or she claims to be). Establishing this link is necessary for Identification Level 2 and above, but the evidence required and the rigour applied to establish the link varies depending on the identification level.

At lower identification levels, this link may be established through a successful shared secret match, knowledge of file history or a mail out of an activation code to an address on record. At higher identification levels, this link must be established through an in-person identity-proofing process or a high-quality biometric match.

4. Confirming that the individual uses the identity in the community

This component is about confirming that a person claiming an identity actually uses that identity in the community. Confirmation of the use of an identity is necessary for Level 2 and above. and is generally verified through the provision of photo identification.

This step is particularly important where an individual is legally entitled to use more than one name. For example, British Columbia's *Name Act* states that an individual may legally use both the surname he or she was born with and the surname of a spouse. While this provision applies to both spouses, it is less usual for a man to assume his wife's surname (even though he is legally entitled to). For this reason, production of a marriage certificate may not be sufficient evidence to confirm that an individual actually uses a spouse's surname. The registering organization may require the production of other evidence to confirm that the individual actually uses their spouse's surname in the community.

This Standard prescribes evidence and verification processes that assess individuals against the above components to increasing levels of assurance. In some cases, different evidence and processes will be required to satisfy all components; in other cases, a single piece of evidence or process may satisfy multiple identification components.

2.4 Challenges Associated with Establishing Identity

Establishing an individual's identity to a high degree of certainty through business processes that are repeatable, trusted and convenient for citizens is challenging. This is particularly so given that:

- The individual whose identity is to be established will generally not be known to the person(s) administering the identification process.
- Identity information associated with an individual can change over time and individuals may represent themselves differently (i.e., use different names) in different contexts.
- Not everyone will have the same credentials or records available to assist in establishing their identity (e.g., individuals born outside of Canada, children, the homeless).
- Recognizing authentic identity documents – especially documents issued in other countries – is difficult. At the same time, technologies for creating fraudulent documents are becoming more sophisticated.
- Increasing the certainty about an individual's identity can involve increasing cost, time and effort for both the individual and the registering organization.
- Verifying identity information at the source (i.e., with authoritative parties) is not always possible or practical, particularly when the authority is located outside of Canada.
- Some people may have criminal intent to misrepresent themselves.

2.4.1 Residual Risk Mitigation

While implementation of this Standard will go a long way to mitigating identity-related risk associated with the delivery of a service, it will not mitigate all risk. There are a number of residual risks inherent in the minimum evidence of identity requirements, even at the highest identification levels. Some services, due to the nature of the delivered service or their client base, will have more residual risk than others. To manage residual risk, registering organizations:

- MUST assess and pay attention to the residual risk that is inherent within the minimum evidence of identity requirements;
- MUST decide if additional processes will be required to cover off the residual risk; and,
- SHOULD use the results of their initial risk assessment (see section 3 of the *Identity Assurance Standard*) as a guide for how they should manage residual risk.

If discrepancies are found in the identity information provided by an individual, an organization might have cause to suspect that the claims of identity made by an individual are not genuine. In these situations, the organization may require additional supporting information (e.g. an additional document or an additional process such as an interview) or may wish to apply some

of the requirements for a higher identification level to the individual case to resolve those discrepancies. Standards for dealing with evidence discrepancies are set out in section 4 – the Identification and Registration of Individuals Standard.
In such cases, organizations MUST be confident that the additional requirements are consistent with the privacy principle that organizations SHOULD only require the amount of information necessary for the purpose it is being collected. Additional information or processes SHOULD only be required to the extent necessary to mitigate the level of risk involved.

As well, organizations SHOULD only use alternative credentials or processes as a proxy for required credentials or processes where they are confident that the process for issuing the alternative credential is equivalent or higher to the required credential. This may not always be feasible for credentials issued in other countries. Where an alternative credential or process is used on a regular basis, approval of the Chief Information Officer for the Province of British Columbia MUST be obtained.

2.4.2 Exception Processes

In some cases it will not be possible to meet the minimum evidence of identity and process standards set out in this document. For example, in some instances an individual may not have the required credentials set out in the Evidence of Identity Requirements. Examples of individuals who may not have required evidence of identity credentials include children, homeless individuals and individuals born or residing outside of Canada. In other cases, an individual may have the required evidence of identity credentials but may not have reasonable access to in-person identity proofing services (either because they live too far away or because they have disabilities or other barriers preventing their access).

In such cases, the registering organization SHOULD consider whether:

- the minimum evidence of identity standards from a lower identification level will be acceptable;
- other processes can be adopted to ensure the required level of assurance in an individual’s identity; and/or,
- other processes should be put in place to mitigate any residual risk.

Complete application of this standard may also not be suitable for some law-enforcement related services or for services where the identities of certain clients are protected.

In all of these cases, registering organizations SHOULD apply for and use exception processes that are aligned as closely as possible to the content of this Standard.

2.4.3 Establishing the Identity of Children

Establishing the identity of children can be particularly challenging where the provision of credentials and photo identification is an evidence of identity requirement. Children are less able to provide this type of evidence and do not have well-established and authoritatively documented social footprints. Children, particularly babies, do not usually possess photographic identification, and the value of photographic identification at very young ages is more limited as children can change appearance relatively quickly.

Registering organizations SHOULD therefore consider the following approaches where the establishment of a child's identity is required:

1. Establishing a documentary link between the child and their parent(s) or guardian(s). This is particularly relevant where the child is very young.

2. Using a range of evidence to indicate the child's use of the identity in the community (e.g. documentation produced through the child's engagement with the health and education sectors, or social service, religious, and cultural institutions).

3 Evidence of Identity Requirements

This section supports the Identification and Registration of Individuals Standard (set out in section 4) and the In-Person and Telephone Authentication Standard (set out in section 7) by listing specific credentials that are acceptable for meeting evidence of identity requirements. This section also sets criteria for core identity information (such as names) that must be collected and verified. As such, this section MUST be read in conjunction with the standards set out in sections 4 and 7.

3.1 Criteria for Names

The Identification and Registration of Individuals Standard requires the collection and verification of an individual's name or names to support the establishment of a unique identity. Because an individual's name can change during their lifetime and because an individual can simultaneously use different names in different contexts, the collection of more than one name may be required, particularly at higher identification levels.

The different types of names that MUST or MAY be collected for different identification levels are described below:

3.1.1 Legal Name

When these standards refer to a "legal name", it means a name that an individual uses for official or legal purposes. In British Columbia, the criteria for "legal name" is set out in the *Name Act.*

According to the *Name Act*, an individual is legally entitled to use:

- the given names and surname the individual had at birth or adoption, unless the individual has had them legally changed;
- the surname of a spouse by marriage;
- the surname the individual used immediately before marriage (which may include the surname of a former spouse); and,
- any name – given or surname – that the individual has had legally changed.

Based on the above definition, an individual may be legally entitled to use up to three surnames at once: their surname at birth, the surname of their former spouse, and the surname of their current spouse. No legal change of name is required to assume the name of a spouse by marriage.

An individual may have perfectly valid identity credentials with different legal names. For this reason, it is important at higher registration and identity proofing levels, to ensure that a foundation identity credential (see below) is always presented or referenced to ensure a linkage between different legal names that an individual may use or have used.

3.1.2 Full Legal Name

When these standards refer to a "full legal name", it means all the given names (first and middle names) that an individual was given at birth or adoption (unless they have been legally changed) plus the surname (last name or family name). The given names of the full legal name MUST be set out in the order that they appear on the foundation identity credential or name change certificate.

3.1.3 Primary (Full) Legal Name

When these standards refer to a "primary legal name", it means the full legal name that the individual is currently or primarily using. As set out above, the primary legal name may be an individual's registered birth name or it may include the surname of their spouse or former spouse. The primary legal name SHOULD be the name that appears on an individual's government-issued photo identification.

3.1.4 Other Names

1. Where an individual uses more than one legal name in the community (e.g., uses birth name and married name in different contexts), has previously used a different legal name in their transactions with government, or is commonly known by a variant of their primary legal name, the organization MAY or MUST (depending on the identification level) collect these "other names" to support a unique identification and to enable authorization decisions by other organizations that may rely on this information.

2. For the purposes of these standards, an acceptable "Other Name" is a name that is different than the name shown on the individual's government-issued photo identification and meets one of the criteria set out below:

    a. Is the individual's surname by birth or adoption as shown on the individual's birth certificate (i.e., the individual's previous legal name);

    b. Is the individual's surname on their Canadian Citizenship Certificate or Permanent Resident Card (i.e., the individual's previous legal name);

    c. Is the surname of the individual's spouse as shown on a Marriage Certificate or proof of marriage document;

    d. Varies the individual's given names in a way that meets the accepted Legal Name Discrepancy criteria set out in section 3.5.

3. Where an “other name” is the individual’s “previous legal name”, the registering organization MAY wish to distinguish it as such (and distinguish it from the individual’s current “primary legal name”) to aid data matching and authorization decisions by other organizations that may rely on this information.

3.1.5 Previous Legal Name

When these standards refer to a “previous legal name”, it means a legal name that the individual previously used. For example, the previous legal name of a married person, currently using their spouse’s surname, might be their registered birth name or might include a surname of a former spouse.

3.1.6 Preferred Name

When these standards refer to a “Preferred Name”, it means the name the individual prefers to use. Collecting and using the individual’s preferred name enables a more personalized service experience. The use of a “Preferred Name” is particularly relevant in the employment context where the individual may wish to use a more personal version of their name on a daily basis.

1. A Preferred Name may be the same name as the “Primary Legal Name”, one of the “Other Names”, or a variation of one of those names.
2. A “Preferred Name” may also include a nickname in place of a given name.

   a. The use of a nickname in place of a given name for a “preferred name” MAY only be acceptable where there is evidence that the individual uses that name in the community.

3. A Preferred Name that uses a surname that the individual is not legally entitled to use (see Legal Name Criteria set out in section 3.1.1) SHOULD NOT be accepted.

3.1.7 Pseudonym

When these standards refer to a “pseudonym”, it means a fictitious name that an individual uses to conceal or obscure his or her identity.

1. Pseudonyms are acceptable (and often preferred) for Level 1 identification processes where no real identity information is required or where there is a desire to provide a anonymized but repeatable service.
2. Where an individual chooses to provide their real name, instead of a pseudonym, for a Level 1 Identification process, the registering organization must treat the unverified name as if it were a pseudonym. For the purposes of these standards there is no difference in assurance between an unverified name and a pseudonym.

3.2 Foundation Identity Credentials

A foundation identity credential is a credential that establishes the foundation of an individual's identity in Canada. For individuals born in Canada, their foundation identity credential is a birth certificate. For individuals that immigrated, or are temporary visitors, to Canada, their foundation identity credential is a Permanent Resident Card, a Canadian Citizenship Card, a Student or Work Permit or similar document.

Foundation Identity Credentials are important as evidence of identity at higher identification levels because they establish a chain of identity, are the basis upon which other credentials are issued, and they contain a unique registration number which helps organizations ensure that they are registering an individual uniquely.

Where a Foundation Identity Credential is required as evidence of identity, one of the following credentials MUST be presented or referenced. Unless otherwise stated, all credentials/ documents used as evidence MUST be an original document (not a photocopy).

Table 2 – Acceptable Foundation Identity Credentials[1]

Foundation Identity Credential	Issuing or Authoritative Party	Requirements/Restrictions
Canadian Birth Certificate **see note on certificates that are not accepted*	Provincial or Territorial Government; Registrar of Vital Statistics	Not accepted: • baptismal certificates, • "live birth" certificates, • pre-1994 Quebec birth certificates, or • Manitoba birth certificates signed by a division registrar
Canadian Citizenship Card	Government of Canada; Citizenship and Immigration	
Permanent Resident Card	Government of Canada; Citizenship and Immigration	
Canadian Record of Landing/Canadian Immigration Record	Government of Canada; Citizenship and Immigration	
Certificate of Naturalization in Canada	Government of Canada; Citizenship and Immigration	

[1] Adapted from the Insurance Corporation of British Columbia's Identification Requirements

Foundation Identity Credential	Issuing or Authoritative Party	Requirements/Restrictions
Study, Work, Visitor or Temporary Resident Permit (formerly Minister's Permit) **see note on expiry dates*	Government of Canada; Citizenship and Immigration	If the identification/registration process results in the issuance of a credential or privileges, the credential and/or privileges MUST not have an expiry date that exceeds the expiry date of the permit.
Identity Card *(Issued to foreign representatives accredited to Canada and eligible members of their family)*	Department of Foreign Affairs and International Trade	
Any other credential or evidence approved by the Chief Information Officer for the Province of British Columbia		Where an individual is ineligible for one of the required credentials, additional credentials or evidence may be accepted where approved by the Chief Information for the Province of British Columbia as providing equivalent assurance.

3.3 Government-Issued Photo Identification

Government-issued photo Identification is used to visually associate a legal name and associated identity information to an individual.

Where government-issued photo identification is required, one of the following credentials MUST be presented or referenced. Unless otherwise stated, all documents/credentials used as evidence MUST be an original document (not a photocopy).

Table 3 – Acceptable Government-Issued Photo Identification[2]

Government-Issued Photo Identification	Issuing or Authoritative Party	Requirements/Restrictions
Canadian or U.S. Driver's Licence, Learner's Licence or Enhanced Driver's Licence	• Insurance Corporation of British Columbia; • Canadian Province or Territory's Driver Licensing Agency; or • U.S. State's Department of Motor Vehicles or equivalent	• MUST display a recent (within 5 years) photo • MUST be valid (not expired)

[2] Adapted from the Insurance Corporation of British Columbia's Identification Requirements

Government-Issued Photo Identification	Issuing or Authoritative Party	Requirements/Restrictions
BC Identification (BCID) card or Enhanced Identification Card	Insurance Corporation of British Columbia	• MUST be valid (not expired) • Older cards without an expiry date are not accepted
Passport (Canadian or foreign)	• Passport Canada; or • Foreign Government Passport Issuing Agency	• MUST be valid (not expired)
U.S. Passport Card	U.S. Department of State	• MUST be valid (not expired)
Canadian Citizenship Card	Government of Canada; Citizenship and Immigration	• MUST display a recent (within 5 years) photo
Canadian Permanent Resident Card	Government of Canada; Citizenship and Immigration	• MUST be valid (not expired) • MUST display a recent (within 5 years) photo
Canadian Forces Identification	Government of Canada; Department of National Defence and the Canadian Forces	• MUST be valid (not expired) • MUST display a recent (within 5 years) photo
Secure Certificate of Indian Status Card (new secure version issued after 2009, only)	Government of Canada; Department of Indian and Northern Affairs Canada	• MUST display a recent (within 5 years) photo • Certificate of Indian Status cards issued prior to 2009 are not accepted
Any other credential or evidence approved by the Chief Information Officer for the Province of British Columbia		Where an individual is ineligible for one of the required credentials, additional credentials or evidence may be accepted where approved by the Chief Information for the Province of British Columbia as providing equivalent assurance.

3.4 Required Name Linking Documentation

Where the legal name on an individual's foundation identity credential doesn't match the legal name on their government-issued photo identification, due to marriage or a legal change of name, additional documentation MUST be presented at higher identification levels to establish a link between the two names.

An individual may have legally changed their name that appears on their foundation identity credential, in which case a Change of Name Certificate would be issued. In addition, an individual that marries is legally allowed to assume the surname of their spouse. Married or formerly married individuals are legally allowed to use both their surname by birth and the surname of their spouse or former spouse.

One of the following approved linking documents MUST be presented at the time of registration. Unless otherwise stated, all documents used as evidence MUST be an original document (not a photocopy).

Table 4 – Required Name Linking Documentation

Name Linking Document	Issuing or Authoritative Party	Requirements/Restrictions
Change of Name Certificate	Canadian Province or Territory's Registrar of Vital Statistics	
Marriage Certificate, Certified Statement of Marriage, or Record of Marriage Form	• Canadian Province or Territory's Registrar of Vital Statistics; or • Clergy member, judge or justice of the peace that performed the marriage	Record of Marriage Form MUST: • be the original issued; • signed by the clergy member, judge or justice of the peace who performed the marriage; • contain the name of both spouses, the date of the marriage and licence number.
Any other credential or evidence approved by the Chief Information Officer for the Province of British Columbia Passport (Canadian or foreign)		Where an individual cannot produce one of the required credentials, additional credentials or evidence may be accepted where approved by the Chief Information for the Province of British Columbia as providing equivalent assurance.

3.5 Legal Name Discrepancy

In some cases, the legal name on the foundation identity credential, the government-issued photo identification and supporting documents will not match exactly. This discrepancy is acceptable where:

1. The individual has legally changed their name or has assumed the surname of a spouse or former spouse by marriage.

   a. In this case, the individual MUST produce linking documentation that meets the requirements set out in section 3.4, above.

2. The given names do not match exactly but are common variants, such as Robert to Bob or Susannah to Sue.

3. One or more given names are transposed (i.e., middle name is used as first name), absent (i.e., no middle names) or replaced by initials.

3.6 Evidence of Current Residential Address

Where evidence of an individual's current residential address is required, it may be met by the aforementioned presentation of acceptable government-issued photo identification (see Table 3, section 3.3) where that identification displays the individual's current residential address.

Some government-issued photo identification does not display an individual's residential address (such as a passport). In these cases, or where the presented government-issued photo identification doesn't contain the current address, the following documents or evidence may be accepted as proof of current residential address.

All documents used as evidence:

- MUST, unless otherwise stated, be an original document (not a photocopy).
- MUST contain a name that matches the individual's government-issued photo identification.
- MUST contain the individual's current address (as confirmed by the individual).

Table 5 – Acceptable Evidence of Residential Address[3]

Evidence of Residential Address	Issuing or Authoritative Party	Requirements/Restrictions
An Accepted Government-Issued Photo Identification Credential listed in section 3.3, Table 3.	As set out in Table 3 (see section 3.3)	
Major credit card statement along with the related valid credit card	Issuing Credit Card Company	• Statement MUST be dated within 3 months
Bank statement	Issuing Bank	• Statement MUST be dated within 3 months
School, College or University report card or transcript	Issuing School, College or University	• Document MUST be dated within 1 year

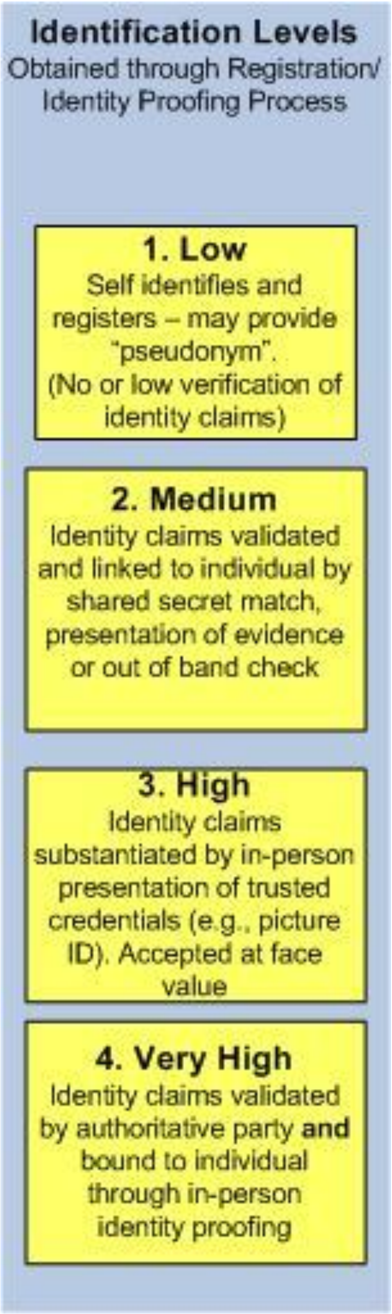
[3] Adapted from Canada Post's Customer Identification Requirements

Evidence of Residential Address	Issuing or Authoritative Party	Requirements/Restrictions
Residential Lease or Residential Mortgage statement or agreement	Issuing Mortgage or Lease Company	• Document MUST be dated within 1 year
Insurance Policy	Issuing Insurance Company	• Document MUST be dated within 1 year
Vehicle Ownership or Insurance document	Issuing Motor Vehicle or Insurance Company	• Document MUST be dated within 1 year
Municipal tax notice	Issuing Municipal Government	• Document MUST be dated within 1 year
Recent utility bill (residential telephone, cable TV, public utilities commission, hydro, gas or water)	Issuing Utility Company	• Document MUST be dated within 3 months
Canada Child Tax Benefit statement	Government of Canada	• Statement MUST be dated within 1 year
Income tax assessment - most recent	Revenue Canada and Customs Agency	• Statement MUST be dated within 1 year
Government Cheque or Government Cheque Stub with elector name and address	Issuing Government Agency	• Cheque or cheque stub MUST be dated within 3 months
Statement of Employment Insurance Benefits Paid (T4E)	Issuing Agency	• Statement MUST be dated within 1 year
Canada Pension Plan Statement of Contributions/Quebec Pension Plan Statement of Participation	Government of Canada or Quebec Government	• Statement MUST be dated within 1 year

Evidence of Residential Address	Issuing or Authoritative Party	Requirements/Restrictions
Statement of Old Age Security (T4A) or Statement of Canada Pension Plan Benefits (T4AP)	Government of Canada	• Statement MUST be dated within 1 year
Statement of Benefits from Provincial Workplace Safety or Insurance Board	Issuing Agency	• Statement MUST be dated within 1 year
Statement of Direct Deposit for Provincial Works or Provincial Disability Support Program	Issuing Provincial Government	• Statement MUST be dated within 1 year
Attestation of Residence issued by the responsible authorities (shelters, soup kitchens, student/senior residence, long-term care facilities, Aboriginal reserves, work camps)	Issuing Authority	• Document MUST be dated within 3 months

4 Identification and Registration of Individuals Standard

This standard supports and sets requirements for four increasing levels of identification strength. These four levels of identification strength apply to the identification of individuals regardless of the identity context (i.e., it applies to identifying individuals in a personal context, an employment context, a business context and a professional context). Additional information and evidence standards for establishing an affiliation between an identified individual and an organization are set out in the *Registration of Organizations and Affiliations Standard.*


Identification Levels
Obtained through Registration/ Identity Proofing Process
1. Low
Self identifies and registers – may provide "pseudonym".
(No or low verification of identity claims)
2. Medium
Identity claims validated and linked to individual by shared secret match, presentation of evidence or out of band check
3. High
Identity claims substantiated by in-person presentation of trusted credentials (e.g., picture ID). Accepted at face value
4. Very High
Identity claims validated by authoritative party and bound to individual through in-person identity proofing

Identification Strength Level Descriptions

A high level description of each Identification Level is set out below.

1. Low Identification Level (“Pseudonymous ”)

- At this level, the individual self-identifies and may self-register.
- There is no requirement for verified information at this level. The individual may provide their real name and information or they may provide a pseudonym. Either way the result is the same: no to little confidence can be placed in the information because it is not verified.
- An example of a low level identification process is registering for a hotmail account or for a Basic BC*e*ID.

2. Medium Identification Level (“Validated”)

- This level requires a managed registration process and the provision of specific identity information and evidence to uniquely identify the individual to a medium level of certainty and to enable verification of the information provided.
- Identity information provided must be either validated by an Authoritative Party and linked to the individual through a shared secret match or similar check; or substantiated through the in-person provision of a government-issued credential.
- An example of a medium level identification process is registering for the Fair PharmaCare Plan or registering for a Level 2 Business BCeID.

3. High Identification Level (“Substantiated”)

- This level requires an in-person identity proofing process and the provision of sufficient identity information to establish a unique identity within a given identity context to a high level of certainty.

- Identity claims are substantiated and linked to the individual through the in-person presentation of specific trusted credentials. A combination of trusted credentials is required at this level to establish a unique identity to a high level of certainty including a foundation identity credential (such as a birth certificate, citizenship or immigration document).

- An example of a high level registration process is registering for a Personal BCeID, or any other registration process which requires an individual to produce, for in-person verification, both a foundation identity credential (e.g., birth certificate, citizenship certificate, permanent resident card) and a government-issued photo ID.

4. Very High-Identification Level (“Corroborated”)

- This level has the same requirements as Level 3 and additionally requires:
  - The corroboration of each identity claim and supporting credential by a designated Authoritative Party (e.g., name, date of birth and registration number on birth certification must be corroborated by Vital Statistics).
  - The collection of a digital image of the individual that can be verified as unique against existing images in the registering organization’s system.
- An example of a very high level registration process is registering for a British Columbia Driver’s Licence.

Summary of Requirements

Many of the requirements in this section apply to all Identification Levels. Where a requirement applies to a particular Level or Levels, it is specifically noted. Otherwise, the requirements should be read as applying to all Identification Levels.

The requirements for achieving increasing levels of identification strength include:

1. Unique Identity Requirements: These include requirements to ensure unique subject and service identities.

2. Identity Information Requirements: These include identity attributes such name, date of birth, and current residential address.

3. Contact Information Requirements: These include information such as email address, telephone number and mailing address, captured for contact purposes and for the delivery of credentials and notifications.

4. <u>Collection of Information Requirements:</u> These include requirements related to the collection of information, including permitted service delivery channels.

5. <u>Evidence of Identity Requirements</u>: These include what credentials are trusted as evidence of the information provided and/or what Authoritative Parties are trusted to validate the information provided.

6. <u>Verification Requirements</u>: These include what verification processes and channels are acceptable to validate or substantiate required identity information.

7. <u>Evidence and Verification Discrepancy Requirements</u>: These include requirements for dealing with discrepancies identified in the presented evidence or arising out of the verification process.

8. <u>Record of Registration Requirements</u>: These include information that MUST be recorded to support the registration and verification process such as identity information, credential reference numbers, names of issuing authorities, date and time of verification events and identity of registrar.

Where a requirement in this standard requires that an individual match a photographic image, a "match" means a reasonable resemblance as judged by a human being or recognition software.

Requirements for ensuring operational diligence in the identification and registration process follow in section 5.0.

4.1 Unique Identity Requirements (All Levels)

These requirements apply to all Identification Levels.

4.1.1 Unique Subject Identity

1. The registering organization MUST ensure that each registered identity (whether pseudonymous or not) is unique within its service's community of subjects.
2. Where a credential is issued by the registering organization's service, it MUST be uniquely linked to the registered identity.

4.1.2 Unique Service Identity

A service that issues a credential MUST ensure that a unique identity is attributed to the service, such that credentials issued by the service can be distinguished from those issued by other services, including services operated by the same organization.

4.2 Identity Information Requirements

To achieve the specified Identification Level, the following identity information MUST be collected from the individual. Definitions, criteria and required evidence for Primary Legal

Name, Other Names and Preferred Name are set out in section 3 – Evidence of Identity Requirements.

4.2.1 Identification Level 1 (Low)

1. **Required Identity Information**

   No real identity information is required at this level. An individual MAY register with a pseudonym.

4.2.2 Identification Level 2 (Medium)

1. **Required Identity Information**

   The registering organization MUST collect the following identity information from the individual:

   a. primary (full) legal name, exactly as shown on government-issued photo ID (see list of acceptable credentials in Evidence of Identity Requirements, section 3.3)

   b. date of birth

   c. current residential address

2. **Optional Identity Information**

   The registering organization MAY also collect the following identity information from the individual:

   a. other names used by, or previously used by, the individual. Collection of other names supports the identification process by establishing a complete picture, or chain, of an individual's identity and may aid authorization decisions for services where the individual previously used another name.

   b. preferred name (this may be the same name as the primary legal name, one of the other names, or a variation of one of those names). Collecting and using the individual's preferred name enables a more personalized service experience.

4.2.3 Identification Level 3 (High)

1. **Required Identity Information**

   The registering organization MUST collect the following identity information from the individual:

   a. all information required for Identification Level 2 (Medium);

   b. all other names used by or previously used by the individual (if applicable), exactly as shown on the foundation identity credential; and,

c. place of birth, exactly as stated on the foundation identity credential (where no place of birth is listed on the foundation identity credential[4], the registering organization may leave this blank or refer to it as unknown).

2. **Optional Identity Information**

The registering organization MAY also collect the following identity information from the individual:

a. preferred name

4.2.4 Identification Level 4 (Very High)

1. **Required Identity Information**

The registering organization MUST:

a. collect all information required for Identification Level 3 (High)

b. collect and store a digital image of the individual that can be verified as unique against existing images in the registering organization's system.

2. **Optional Identity Information**

The registering organization MAY collect the same optional identity information as permitted by Identification Level 3 (High).

4.3 Contact Information Requirements (All Levels)

The following requirements apply to all Identification Levels unless otherwise noted.

4.3.1 General Contact Information Requirements

For contact purposes and/or the delivery of credentials and notifications, the registering organization MAY require the individual to provide:

1. an email address if the individual is registering using the online channel or is registering for an electronic credential which will be used to access services online;

2. a telephone number, if the individual is registering using the telephone channel or is registering specifically to use a service that uses telephone authentication; and/or,

3. an email address, telephone number or mailing address if the individual is registering using the in-person or postal mail channel.

[4] For some citizenship and immigration credentials, the recording of a place of birth is optional

4.3.2 Exception for Anonymity Purposes

1. For Level 1 (Low) Identification Level, a requirement for contact information MUST be waived where anonymity is preferred or a requirement of the service.

4.4 Collection of Information Requirements (All Levels)

The following requirements apply to the collection of identity and contact information for all Identification Levels.

4.4.1 Service Delivery Channels

1. The registering organization MAY, subject to (a), below, collect identity and contact information over any service delivery channel as long as appropriate security measures are applied.

   a. Requiring individuals to provide identity information by electronic mail is NOT RECOMMENDED unless appropriate security mechanisms such as encryption are utilized.

   Note: Specific service delivery channels may be required for verification of identity information, particularly at higher Identification Levels (see verification requirements below) but a registering organization may initially collect the identity information over a different channel than the channel it uses to verify the information.

4.5 Evidence Requirements

To achieve the specified Identification Level, the following evidence requirements MUST be met. Approved evidence of identity credentials and supporting documentation is set out in section 3 – Evidence of Identity Requirements.

4.5.1 Identification Level 1 (Low)

1. There are no evidence of identity requirements at this level. A self-attestation is acceptable at this level.

4.5.2 Identification Level 2 (Medium)

At this level, evidence of an individual's primary legal name and date of birth is REQUIRED. Evidence of current residential address MAY be required, depending on the business requirements of, and the verification process used by, the registering organization.

1. **Evidence of primary legal name, date of birth, and use of identity in community**

   The following credentials are REQUIRED as evidence of an individual's primary legal name, date of birth and use of identity in the community:

a. an accepted government-issued credential that bears a photographic image of the individual (see list of accepted government-issued photo identification credentials in, section 3.3) that:

   i. is valid (i.e., has not expired); and,

   ii. contains the individual’s primary (full) legal name and date of birth.

2. **Evidence of Current Residential Address**

Where evidence of current residential address is required, it may be met by either:

a. the accepted government-issued photo identification; or,

b. other accepted evidence (see list of accepted credentials and documents for verifying current residential address in Evidence of Identity Requirements, section 3.6).

3. **Other Evidence**

Additional credentials or documents MAY be required to substantiate the required identity information (see specific verification requirements below).

4.5.3 Identification Level 3 (High)

At this level, evidence of an individual’s primary legal name, other names, date of birth and current residential address is REQUIRED.

1. **Evidence of primary legal name, date of birth, and use of identity in community**

The same government-issued photo identification credential required as evidence for Identification Level 2 (Medium) is REQUIRED for this level.

2. **Foundation Identity Credential**

At this level, a foundation identity credential issued in Canada (see list of accepted foundation identity credentials in Evidence of Identity Requirements, section 3.2 is REQUIRED. The credential MUST:

a. be valid (i.e., has not expired); and,

b. contain the individual’s date of birth and legal name as it was at the time the credential was issued (i.e., may or may not be the legal name the individual is currently known by).

3. **Name Linking Documentation**

Where the legal name on the foundation identity credential and the government-issued photo identification are different, linking documentation (see Evidence of Identity requirements, section 3.4) MUST be presented to link the names on the two credentials. Acceptable linking credentials include:

a. a Change of Name Certificate issued by a Canadian province or territory; or,

b. a Marriage Certificate(s) or other proof of marriage.

4. **Evidence of Current Residential Address**

   The same credentials accepted as evidence of current residential address for Identification Level 2 (Medium) is REQUIRED for this level.

   Note: While evidence of current residential address is optional at Identification Level 2 (Medium), it is required for Identification Level 3 (High)

5. **Other Evidence**

   Additional credentials or documents MAY be required to substantiate required identity information (see verification requirements below).

4.5.4 Identification Level 4 (Very High)

The Evidence Requirements for Level 4 (Very High) are the same as for Level 3 (High). See section 4.5.3, above.

4.6 Verification Requirements

To achieve the specified Identification Level, the following verification requirements MUST be met:

4.6.1 Identification Level 1 (Low)

There are no verification requirements at this level.

4.6.2 Identification Level 2 (Medium)

Different service delivery channels (i.e., in-person, online, telephone, postal mail) MAY be used for verification of identity information at this level. However, different channels may require different verification processes.

The specific verification requirements that are REQUIRED by registration channel are as follows:

4.6.2.1 Over-the-Counter (In-Person) Channel

Summary of Verification Process:

Primary Legal Name and Date of Birth are substantiated through the in-person presentation of required evidence. Current Residential Address MAY be substantiated if required for identification purposes; otherwise, the registering organization MAY accept a self-attested residential address.

The registering organization MUST:

1. Ensure that the presented government-issued photo identification credential:

   a. appears to be genuine and unaltered;

b. appears to be valid (i.e., has not expired); and,

c. bears a photographic image that matches the individual.

2. Where the identity information was previously provided or provided over a different service delivery channel, verify that the primary legal name and date of birth on the presented credential match the identity information previously provided by, or on file about, the individual.

3. If required for identification purposes, verify that the individual's current residential address, as provided by the individual, matches the address on the presented government-issued photo identification credential.

   a. Where the address on the presented credential does not match the current residential address provided by the individual, or where the presented credential does not contain an address, the registering organization MAY:

      i. require the individual to present another accepted document that contains the individual's name and current address (see list of accepted evidence in Evidence of Identity Requirements, section 3.6); or,

      ii. accept a self-attestation and verify the address by a mail-out confirmation.

4. Ensure that any additional presented evidence, where required:

   a. appears to be genuine and unaltered;

   b. appears to be valid (i.e., has not expired)

   c. contains a name that matches or can be linked to the name on the presented government-issued photo identification credential.

4.6.2.2 Online or Telephone Channel

Summary of Verification Process:

Primary Legal Name and Date of Birth are validated by an Authoritative Party and linked to the individual through an accepted verification method. Current Residential Address MAY be validated by an Authoritative Party if required for identification or mail-out confirmation purposes; otherwise, the registering organization MAY accept a self-attested residential address.

The registering organization MUST:

1. Ensure that the individual submits the references of, and attests to the current possession of, the required government-issued photo identification credential. Specifically, the individual MUST provide:

   a. the document, registration or identification number;

   b. the name and jurisdiction of the issuing authority; and

   c. the issue and expiry dates, if applicable.

2. Ensure that the individual provides the following identity information:
   a. primary (full) legal name, exactly as shown on the referenced government-issued photo identification credential;
   b. date of birth; and
   c. current residential address (and whether or not the referenced government-issued photo identification credential contains the individual's current address).

3. Validate the provided identity and credential information with the Authoritative Party that issued the credential, specifically:
   a. the existence and validity of the credential with matching name and reference/identification number;
   b. the date of birth; and,
   c. if applicable, the current residential address.

4. Link the information to the individual by one of the following methods:
   a. Where the current residential address provided by the individual matches the Authoritative Party's address of record, the registering organization may:
      i. send notice to the address of record and receive a mailed, e-mailed or telephone reply from the individual; or,
      ii. issue or activate credentials in a manner that confirms the currency of the residential address such as by requiring the individual to provide online, or over the telephone, some information from a notice sent to the individual.
   b. Through a shared secret match of information previously provided by the individual or likely to be known only to the individual. Shared secret matches may be verified:
      i. by the registering organization itself, if it has a pre-existing relationship with the individual; or,
      ii. with the consent of the individual, by another organization that has a pre-existing relationship with the individual.

4.6.2.3 Postal Mail Channel

Summary of Requirements:

Primary Legal Name and Date of Birth are substantiated by the mail-in of a notarized photocopy of required evidence. Current Residential Address MAY be substantiated if required for identification purposes; otherwise, the registering organization MAY accept a self-attested residential address.

The registering organization MUST:

1. Ensure that the individual mails a notarized photocopy of the required government-issued photo identification credential and attests:
   a. to being the holder of the credential; and,
   b. that the following information contained on it is current and correct:
      - primary (full) legal name;
      - date of birth;
      - current residential address, if applicable.
2. Ensure that all information, dates and reference numbers on the photocopy are readable and unaltered.
3. Ensure that the photocopy contains an unaltered notary signature, seal and statement that certifies that the photocopy is a true copy of the original government-issued identification and that the photographic image of the holder matches that of the individual.
4. Where the identity information was previously provided, or provided over a different service delivery channel, verify that the primary legal name and date of birth on the notarized photocopy match the identity information previously provided by, or on file about, the individual.
5. If required for identification purposes, verify that the individual's current residential address, as provided by the individual, matches the address on the notarized photocopy.
   a. Where the address on the notarized photocopy does not match the current residential address provided by the individual, or where the notarized photocopy of the government-issued photo identification does not contain an address, the registering organization MAY:
      i. require the individual to present another document (the original or a notarized photocopy) that contains the individual's name and current address (see list of accepted evidence in Evidence of Identity Requirements, section 3.6); or,
      ii. accept a self-attestation and verify the address by a mail-out confirmation.

6. Ensure that any additional evidence, where required:
    a. contains a name that matches or can be linked to the name on the notarized photocopy of the government-issued photo identification;
    b. appears to be unaltered; and,
    c. if a notarized photocopy, bears an unaltered notary signature, seal and statement that certifies that the photocopy is a true copy.

4.6.3 Identification Level 3 (High)

Summary of Requirements:

Verification of required identity information MUST be done through the in-person presentation of evidence at this level.

The registering organization MUST:

1. Ensure that the presented government-issued photo identification:
    a. appears to be genuine and unaltered;
    b. appears to be valid (i.e., has not expired);
    c. bears a photographic image that matches the individual; and,
    d. contains a legal name and date of birth that matches identity information that may have been previously provided or provided over a different service delivery channel by the individual.

2. Ensure that the presented foundation identity credential:
    a. appears to be genuine and unaltered;
    b. appears to be valid (i.e., has not expired);
    c. contains a registration number; and,
    d. contains a date of birth that exactly matches the date of birth on the presented government-issued photo identification.

3. Ensure that the legal names on the foundation identity credential and the government-issued photo identification either:
    a. match exactly;
    b. meet the requirements of an acceptable Legal Name Discrepancy (see criteria in Evidence of Identity Requirements, section 3.5); or,
    c. can be linked together by a Marriage Certificate(s), Change of Name Certificate or other approved evidence (see required name linking documentation in Evidence of Identity Requirements, section 3.4).

4. Ensure that any Marriage Certificate, Change of Name Certificate or other name linking documentation presented by the individual:
   a. appears to be genuine and unaltered;
   b. contains a registration number; and,
   c. contains legal names that link the individual's other evidence of identity credentials together. For example, the surname of a spouse on a marriage certificate may be legally used by an individual while a maiden name on a marriage certificate should match a birth certificate.

5. Verify the current residential address provided by the individual:
   a. by ensuring that the address on the government-issued photo identification credential matches the address information that may have been previously provided or provided over a different service delivery channel by the individual; or,
   b. where the address on the presented credential does not match, does not appear, or is not current, by requiring the individual to present another accepted document that contains the individual's name and current address (see list of acceptable evidence of residential address in Evidence of Identity Requirements, section 3.6).

6. Ensure that any additional presented evidence:
   a. appears to be genuine and unaltered;
   b. contains a name that matches or can be linked to the name on the government issued photo identification.

4.6.4 Identification Level 4 (Very High)

Summary of Requirements:

Required identity information is verified through the in-person presentation of evidence and corroborated by a party trusted to be authoritative on the information.

The registering organization MUST:

1. Perform all of the in-person verification steps required by Identification Level 3 (High) (See section 4.6.3).
2. Corroborate the provided information with the Authoritative Parties that issued the credentials used as evidence, specifically:
   a. the existence and validity of the presented credentials with matching names and reference numbers;
   b. date of birth; and,
   c. if applicable, current residential address.

3. Verify that the collected digital image of the individual is unique (i.e., does not already exist) in the registering organization's system.

4. Confirm current residential address, by:

   a. sending notice to the verified address and receiving a mailed, e-mailed or telephone reply from the individual; or,

   b. issuing or activating credentials in a manner that confirms the verified address such as by requiring the individual to enter online or over the telephone some information from a notice sent to the individual.

4.7 Evidence or Verification Discrepancy (All Levels)

As set out in section 4.6, corroboration of the identity information and evidence of identity with Authoritative Parties is only required for Identification Level 4. At lower identification levels, evidence may be accepted at "face value".

However where the registering organization identifies a discrepancy in the identity information provided that cannot be resolved through the presentation of name linking documentation (see section 3.4); has reason to believe that a presented credential is altered or fraudulent; or, observes that the individual being identified is behaving suspiciously; the registering organization MUST undertake one or more of the following additional verification measures:

1. verify the provided information with the Authoritative Party that issued the credential;
2. request the provision of additional evidence of identity;
3. apply some of the requirements for a higher Identification Level; or
4. interview the individual.

4.8 Record of Registration Requirements

To achieve the specified Identification Level, the following record of registration requirements MUST be met:

4.8.1 Identification Level 1 (Low)

There are NO record requirements at this level.

4.8.2 Identification Level 2 (Medium)

1. The registering organization MUST retain records of the registration and identity proofing (verification) that it undertakes. At a minimum, records MUST include:

   a. the individual's primary (full) legal name, exactly as shown on the presented government-issued photo identification credential;

   b. the individual's date of birth;

c. the current address provided by the individual and whether or not it was verified;

d. the type, issuing authority, and reference number(s) of all credentials checked or referenced in the identity proofing process;

e. contact information for related contact purposes and/or the delivery of credentials and notifications;

f. any other names collected by the registering organization;

g. the date and time of verification;

h. the identity of the registrar; and,

i. the identity of the Authoritative Party that provided the validation service or the location at which the (in-person) verification was performed.

2. The registering organization MUST either retain, securely, the records of the registration and verification process for the duration of the individual's account plus 7.5 years, or submit the records to a Credential Service Provider that has undertaken to retain the record for the requisite period.

3. Electronic records of the registration and verification process MUST NOT be stored in plaintext form and all records (whether electronic or not) MUST be subject to security controls that restrict access to only those roles or applications that require access.

4.8.3 Identification Level 3 (High)

The registering organization MUST:

1. Comply with all record of registration requirements that are required for Identification Level 2 (Medium); and,

2. Retain the following additional records associated with the Identification Level 3 (High) registration and identity-proofing (verification) process:

   a. the individual's full legal name, exactly as shown on the foundation identity credential.

4.8.4 Identification Level 4 (Very High)

The registering organization MUST:

1. Comply with all of the record of registration requirements that are required for Identification Level 3 (High); and,

2. Retain the following additional records associated with the Identification Level 4 (Very High) registration and identity-proofing (verification) process:

a. the identity of the Authoritative Parties providing the verification service as well as the date and time of verification.

5 Operational Diligence and Service Standard

This standard sets operational diligence requirements for organizations that register and identity proof individuals and, as such, MUST be read in conjunction with the Identification and Registration of Individuals Standard set out in section 4.

This standard supports four increasing levels of identification strength – low, medium, high and very high. Many of the requirements in this section apply to all Identification Levels. Where a requirement applies to a particular level or levels, it is specifically noted. Otherwise, the requirements should be read as applying to all Identification Levels.

The operational diligence requirements for registering individuals to increasing levels of identification strength include:

1. Legal Compliance Requirements: These include requirements for complying with applicable laws.

2. Service Requirements: These include good practice requirements for registration and identity proofing services.

3. Notification Requirements: These include requirements for notifying individuals about the purpose for collecting, using and disclosing identity information; terms of use that may apply to the use of a credential; and, who in the organization may answer questions.

4. Identity Lifecycle Processes: These include requirements for correction or change to identity information, reconfirmation of identity, credential issuance and management, and flagging and deleting accounts and records.

5. Personnel and Contractor Requirements: These include requirements for personnel training and contractor compliance with policies, procedures and practices.

5. Security Requirements: These include requirements for security policies and procedures, security methodologies and controls, information security management, organizational controls and secure communications.

5.1 Legal Compliance

The registering organization MUST:

1. Comply with relevant British Columbian and Canadian law, including the *Freedom of Information and Protection of Privacy Act*, the *Electronic Transaction Act,* Human Rights legislation and any authorizing legislation for the particular service.

5.2 Service Design Requirements

The registering organization SHOULD implement evidence of identity processes that not only meet requirements for establishing increasing levels of identification strength (see section 4) but also incorporate good practice requirements in each of the following operational aspects:

5.2.1 Acceptability

The registration and identity proofing process or service SHOULD be generally acceptable to customers. It SHOULD take into account the different needs of individuals and avoid the creation of unnecessary barriers. The process SHOULD be convenient, easy to use and as non-intrusive as possible.

5.2.2 Security and privacy

1. Information MUST be suitably protected, whether it is owned by government or by individuals.
2. An individual's right to privacy MUST be appropriately protected in accordance with relevant privacy law.
3. Processes MUST be implemented for the retention of private (personal and business) information, its secure storage and protection against loss and/or destruction, and the protection of private information against unlawful or unauthorized access.
4. Appropriate security policies should be in place and followed.

5.2.3 Affordability, reliability and timeliness

The registration and identity proofing process or service SHOULD be affordable and reliable and SHOULD NOT create unnecessary delays for either individuals or government organizations.

5.2.4 Complaints handling

The registration and identity proofing process or service MUST include a process for handling questions, concerns and complaints related to the collection, verification and use of identity information.

5.2.5 Fraud and Incident Management

The registration and identity proofing process or service MUST include fraud and incident management processes that are appropriate to the level of identification strength established. Level 1 identification processes will require minimal fraud and incident management while Level 4 processes will require more rigorous management.

1. The processes for managing fraud MUST:
   a. address all service delivery channels and partners; and,
   b. include both proactive and reactive elements
      i. Proactive activities would include risk assessment, mitigation and fraud detection.
      ii. Reactive activities would address investigation of, and response to, actual cases of fraud.

5.3 Notification Requirements

1. The registering organization MUST inform individuals of:
   a. the legal authority and purpose for collecting their identity and contact information;
   b. how their information will be used; and,
   c. the circumstances under which their information will be disclosed, if any.

2. Where a credential is issued as part of the registration process, the registering organization MUST inform individuals of any Terms of Use that apply to the credential.

3. The registering organization MUST inform individuals of who within the organization can answer questions about the collection and use of their identity and contact information and, if applicable, terms of use associated with their credential.

5.4 Identity Lifecycle Processes

Organizations that conduct registration and identity proofing processes for their own or other organizations' services MUST include the following lifecycle processes into their service:

5.4.1 Registration and Identity Proofing

The registering organization MUST have registration, identity proofing and records management processes in place that comply with the Identification and Registration of Individuals Standard set out in section 4.

5.4.2 Correction or Change to Identity Information

1. The registering organization MUST have a process in place for individuals to correct or change their identity and contact information.

    a. Changes to identity information MUST be verified using evidence of identity and verification processes appropriate to the Identification Level associated with the identity information (i.e., must be verified using a verification process equivalent or higher to the process used to initially establish the identity during the registration process).

    b. Changes to contact information MAY be verified but is NOT REQUIRED as long as the registering organization has assurance that the individual associated with the contact information has initiated or approved the change request.

2. A record of changes to identity and contact information SHOULD be maintained for Identification Level 2 (Medium) and MUST be maintained for Identification Level 3 (High) and Identification Level 4 (Very High).

    a. For Identification Level 3 (High) and Identification Level 4 (Very High):

        i. the record of changes to identity information MUST include all changes that occur over the life of the individual's involvement with the service.

        ii. the record of changes to contact information MUST include at least the last change (i.e., the service will store current and last previous contact information) and MAY include more or all changes.

    b. A record of the date on which the change occurred SHOULD be included for Identification Level 2 (Medium) and MUST be included for Identification Level 3 (High) and Identification Level 4 (Very High).

    c. The records of changes MUST be retained securely, in accordance with risk management requirements and applicable legislation, and MUST be maintained for the duration of the individual's involvement with the service plus 7.5 years.

        i. Electronic records of changes to identity information MUST NOT be stored in plaintext form and all records (whether electronic or not) MUST be subject to security controls that restrict access to only those roles or applications that require access.

5.4.3 Reconfirmation of Identity

1. For Identification Level 2 (Medium), the registering organization SHOULD have a process in place to regularly reconfirm an individual's identity information and MUST reconfirm an individual's identity information if a credential is being renewed or replaced (see requirements for credential issuance and management under section 5.4.4).
2. For Identification Level 3 (High) and Identification Level 4 (Very High), the registering organization MUST reconfirm an individual's identity information at least every five years.
3. For all Identification Levels, the registering organization MUST reconfirm an individual's identity if discrepancies arise or the service increases its evidence of identity requirements.
4. For all Identification Levels, the reconfirmation process MUST use evidence of identity and a verification process equivalent or higher to the process used to initially establish the individual's identity during the registration process.

5.4.4 Credential Issuance and Management

This section only applies to registering organizations that issue a credential to the individual as part of the registration process.

1. The registering organization MUST have a process in place for renewing credentials and replacing lost or damaged credentials, subject to reconfirmation of the individual's identity information as set out in section 5.4.3, above.
2. The registering organization MUST have a process in place for suspending or deactivating credentials where there is suspicion of misuse or where the individual has failed to comply with one or more of the terms of use.
3. If the registering organization issues an electronic credential, it MUST comply with the requirements set out in the *Electronic Credential and Authentication Standard.*

5.4.5 Flagging and Deletion

The registering organization MUST have processes in place for flagging and deleting an account or record containing an individual's identity information.

1. Where there is an unresolved discrepancy or incident of suspected fraud associated with an individual's identity information, the associated records MUST be flagged as under review until the discrepancy or incident is resolved.
    a. An unresolved discrepancy would include receipt of a notification that an individual is deceased that has not yet been confirmed.
    b. Where a record is flagged as under review, it SHOULD not be relied upon for access and eligibility decisions and information from the record SHOULD not be shared with other parties who may rely on it to make access or eligibility decisions.

2. Where an individual is no longer a client of a service or involved with the service, records of identity information associated with the individual SHOULD be deleted, subject to legal and records management requirements.
   a. Where a registering organization has evidence that an individual is deceased, it SHOULD delete records of identity information associated with the individual, subject to legal and records management requirements.

5.5 Personnel and Contractor Requirements

The registering organization MUST comply with the following requirements for recruiting, training and contracting personnel:

5.5.1 Personnel Training

The registering organization MUST:

1. Ensure that employees and contracted personnel are sufficiently trained, qualified, experienced, and current for the roles they fulfill.
   a. Such measures MUST be accomplished either by recruitment practices or through a specific training program.
   b. Where employees are undergoing on-the-job training, they MUST do so under the guidance of a mentor with established leadership skills.
2. Ensure that employees and contracted personnel that perform registration and identity-proofing functions:
   a. have training in identity-proofing and in document recognition;
   b. have the tools and resources they need to conduct the specified evidence of identity process; and,
   c. have training in how to handle discrepancies and suspicious behavior during the registration and identity-proofing process
3. Have sufficient staff to operate the service according to its policies and procedures**.**

5.5.2 External Service Providers

Where the registering organization uses external service providers for the delivery of parts of its service or for resources that are integrated with its own operations and under its control, the registering organization MUST:

1. Ensure that the external service providers are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures, and practices that the contractor is required to fulfill.

2. Ensure that contractors' compliance with contractually stipulated policies and procedures can be proven and subsequently monitored.

5.6 Security Requirements

The registering organization MUST comply with the following security requirements:

5.6.1 Security Policies and Procedures

1. If the registering organization is a British Columbia government organization, it MUST comply with the B.C. Government's Information Security Policy.

2. If the registering organization is not a British Columbia government organization, it SHOULD do one of the following:

   a. Comply with the B.C. Government's Information Security Policy, or,

   b. Have security-relevant administrative, management, and technical policies and procedures in place that are:

      i. based upon recognized standards or published references;

      ii. adequate for the specified service;

      iii. applied in the manner intended;

      iv. managed, controlled and promulgated by a senior-level manager, and,

      v. properly maintained so as to be effective at all times.

5.6.2 Security Methodologies and Controls

The registering organization MUST:

1. Use a risk management methodology that adequately identifies and mitigates identity-related risks related to the specified service and its client base.

2. Use a quality management system that is appropriate for the specified service.

3. Apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications.

5.6.3 Information Security Management

The registering organization MUST have in place a clear plan for:

1. the protection of individuals' personal information which MUST ensure the ongoing secure preservation and protection of required records; and,

2. the secure destruction and disposal of any such information whose retention is not required.

5.6.4 Organizational (Internal) Controls

The registering organization MUST:

1. Employ technical controls that provide the level of security required by its risk assessment plan and information security management system, or other IT security management methodology.

   a. These controls MUST be effectively integrated with the appropriate procedural and physical security measures.

2. Apply physical access control mechanisms to ensure that access to sensitive areas is restricted to authorized personnel.

3. Employ logical access control mechanisms to ensure that access to sensitive system functions and controls is restricted to authorized personnel.

5.6.5 Secure Communications

1. The registering organization MUST ensure that electronic communications with other organizations that happen over a public or unsecured network use a secure communication protocol that authenticates both systems and uses encryption.

2. The registering organization MUST ensure that:

   a. access to shared secrets and passwords is subject to discretionary controls that permit access to those roles/applications requiring such access;

   b. stored shared secrets are not held in their plaintext form; and,

   c. shared secrets are revealed only to the individual and to registering organization’s direct agents (bearing in mind item (a) in this list).

6 Physical Credentials

Credentials may be issued to individuals to enable future authentication of their identity or privileges for a number of different purposes including accessing services and information.

Credentials may be physical cards or documents, such as a British Columbia CareCard or Driver's Licence, or they may be electronic such as a User ID and password or hardware token with public key infrastructure (PKI). Physical credentials are referenced in this document while electronic credentials are referenced in the *Electronic Credential and Authentication Standard.*

Physical credentials can be categorized by strength level, based on their features (e.g., a card with no photo is a single-factor credential; while a card with a biometric, like a photo, is a multi-factor credential) and the processes followed to issue them. Credential strength is based on the extent to which the credential can be trusted to be a proxy for the individual it represents and not someone else (known as identity binding). This factor is directly related to:

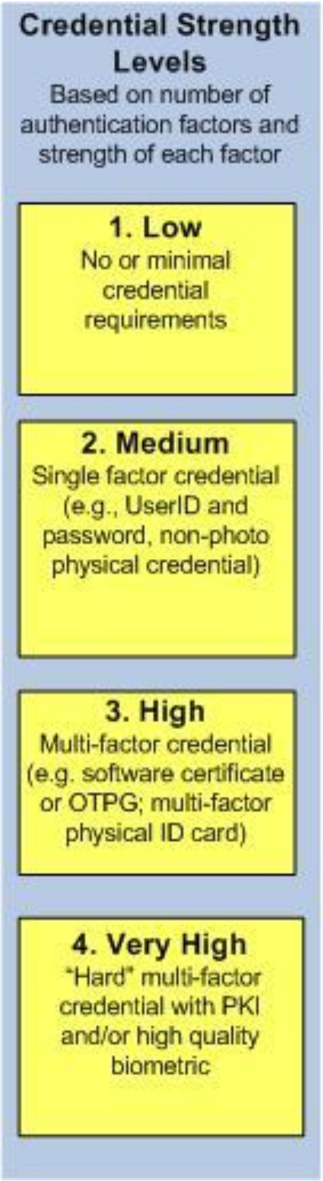
- the integrity and reliability of the technology and/or security features associated with the credential itself;
- the processes by which the credential and its verification token are issued, managed and verified; and,
- the system and security measures followed by the Credential Service Provider responsible for issuing, managing and verifying the credential.

This document sets no standards for technology and security features associated with a physical credential. It is also sets no process standards for issuing physical credentials, including the system and security measures a physical credential issuer should follow in issuing a credential.

This document does, however, categorize physical credentials commonly used to verify identity for the purpose of supporting the In-Person and Telephone Authentication Standard set out in section 7. Physical credentials can be presented to support in-person or over-the-counter identity authentication and some physical credentials provide greater authentication assurance than others. As well, information on physical credentials (such as identification numbers) can be referenced to support telephone authentication. Standards for achieving different levels of authentication strength for in-person and telephone authentication are set out in section 7.

Credential Strength Level Descriptions

This section sets requirements for four increasing levels of credential strength associated with physical credentials. A high level description of each level is set out below.



Credential Strength Levels
Based on number of authentication factors and strength of each factor

1. Low
No or minimal credential requirements

2. Medium
Single factor credential (e.g., UserID and password, non-photo physical credential)

3. High
Multi-factor credential (e.g. software certificate or OTPG; multi-factor physical ID card)

4. Very High
"Hard" multi-factor credential with PKI and/or high quality biometric

1. **Low Credential Strength Level** (No Credential Required)
   - At this level, no credential is required.
   - Where a credential is issued that does not meet the requirements of Level 2 Credential Strength, the credential strength, by default, will be considered to have Level 1 (Low) Strength.
2. **Medium Credential Strength Level** (Single-factor Credential)
   - This level requires a single-factor credential.
   - An example of a physical credential with medium level strength is a non-photo credential like a B.C. CareCard or Social Insurance Card.
3. **High Credential Strength** (Multi-factor Credential)
   - This level requires a multi-factor credential.
   - An example of a physical credential with high level strength is a government-issued multi-factor (i.e., with photo) credential like a driver's licence or passport.
4. **Very High-Credential Strength** (Multi-factor "Plus" Credential)
   - This level requires a multi-factor credential that stores, or securely links to, a high-quality biometric such as a digital image or fingerprint scan.
   - An example of a physical credential with very high level strength would be a smart card that stores a fingerprint scan or an e-passport that contains a digitized photo of the holder.
   - A physical credential with very high strength can only be authenticated to very high strength when the biometric associated with the credential can be accessed. If the authenticating organization is not able to access the biometric associated with the credential, it must reconsider the strength of the credential based on its visible features.

7 In-Person and Telephone Authentication Standard

This standard sets requirements for verifying (or authenticating) a registered individual's identity over the counter (i.e., in person) or over the telephone for the purpose of permitting access to information or a service.

Authentication is the act of establishing or confirming something or someone as authentic – that is, that claims made by, or about, the thing or person are true. Authenticating a person often consists of verifying their identity.

The requirements set out in this standard MUST NOT be used to register an individual for a service. Standards for registering an individual's identity for a service are much more comprehensive and are set out in section 4. This standard MUST only be used to verify (or authenticate) the identity of an individual that has already registered for the service for the purpose of subsequent access or service delivery.

This standard MAY also be used to establish that an unregistered individual is generally entitled to access a resource or service based on age, residency or other eligibility factor.

This standard does not apply to the authentication of electronic credentials (e.g., User IDs and passwords, smart cards, etc.). Authentication of electronic credentials by Credential Service Providers is dealt with in the *Electronic Credential and Authentication Standard*.

In the physical world, where an individual presents a physical credential (e.g., Driver's Licence, B.C. CareCard, etc.) over the counter or references a credential over the telephone, an organization is responsible for determining the authenticity of that credential and linking it to the individual making a claim for information or a service. Where no credential is presented or referenced, the organization may need to rely on other verification mechanisms like shared secrets or knowledge of file history.

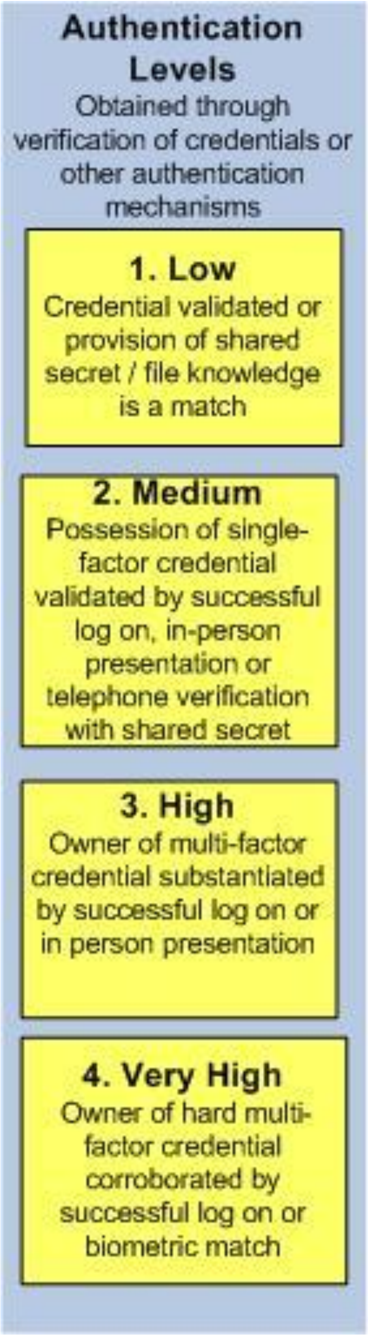
This standard sets out the requirements for authenticating a physical (i.e., non-electronic) credential to different levels of strength over the telephone or over the counter (i.e., in person) The strength of the authentication event is based on:

- the strength of the credential authenticated (see section 6.0); and
- the processes and protocols used to conduct the authentication.

This standard relies on, and refers to, the Evidence of Identity Requirements, set out in section 3, with respect to what credentials are accepted as evidence for the purpose of verifying (or authenticating) an individual's identity to different authentication strength levels. As such this standard should be read in conjunction with the Evidence of Identity Requirements set out in section 3.

Authentication Strength Level Descriptions

This standard supports and sets requirements for four increasing levels of authentication strength. A high-level description of how each level is applied to in-person or telephone authentication is set out below:



Authentication Levels
Obtained through verification of credentials or other authentication mechanisms

1. Low
Credential validated or provision of shared secret / file knowledge is a match

2. Medium
Possession of single-factor credential validated by successful log on, in-person presentation or telephone verification with shared secret

3. High
Owner of multi-factor credential substantiated by successful log on or in person presentation

4. Very High
Owner of hard multi-factor credential corroborated by successful log on or biometric match

1. Low Authentication Level

- No credential must be verified at this level.
- Shared secrets or knowledge of file history may be used as an authentication mechanism at this level.

2. Medium Authentication Level

- A real world identity must be authenticated:
  - by the in-person presentation of a single factor physical credential (e.g., a card with no photo); or,
  - over the telephone by the provision of the credential's identification or registration number plus a shared secret match.

3. High Authentication Level

- A real world identity must be authenticated by the in-person verification of a multi-factor physical credential (e.g., a card with a photo) such as a Driver's Licence or Passport.
- There is currently no method of telephone authentication that is strong enough to meet the requirements of Authentication Level 3 (although technological advancements may change this in the near future).

4. Very High Authentication Level

- A real world identity must be authenticated by:
  - the in-person verification of a multi-factor physical credential that stores, or securely links to, a high-quality biometric such as a digital image or fingerprint scan that can be read and matches the presenting individual; or,
  - a high-quality biometric match utilizing biometric technologies such as facial recognition, fingerprint recognition, iris recognition or similarly strong biometric technology.

Authentication Requirements

The requirements or specifications for achieving increasing levels of authentication strength over the counter or over the telephone include:

1. Acceptable Credentials: These include specified credentials that are acceptable for in-person and telephone authentication.

2. Acceptable Authentication Methods: These include the methods or steps that must be followed to authenticate an individual's identity.

Where a requirement in this standard requires that an individual match a photograph or other biometric, a "match" means a reasonable resemblance as judged by a human being or recognition software.

7.1 Authentication Level 1 (Low)

To achieve Authentication Level 1 (Low), the following requirements must be met:

7.1.1 Acceptable Credentials

No credential must be presented at this level.

7.1.2 Acceptable Authentication Methods

If applicable (i.e., a previous relationship exists), the authenticating organization MAY rely on shared secrets or knowledge of file history.

7.2 Authentication Level 2 (Medium)

To achieve Authentication Level 2 (Medium), the following requirements must be met:

7.2.1 Acceptable Credentials

The following credentials are acceptable at this level:

1. a government-issued photo identification credential (see list of accepted credentials in Evidence of Identity Requirements, section 3.3); or

2. any other government-issued identification or eligibility credential that meets the following criteria:
   a. was issued to an individual using at least a Level 2 Identification process;
   b. displays the individual's name and a signature or photo;
   c. is being used to access information or a service that is related to the purpose of the credential.

7.2.2 Acceptable Authentication Methods

The authenticating organization MUST confirm that the individual is the holder of one of the credentials specified in section 7.2.1, and that the name on the credential matches the name of a registered individual of the service.

Confirmation can be achieved by one of the following methods:

1. In-person presentation of the credential where the following requirements are met:
   a. the credential MUST be inspected to ensure that it appears to be genuine, unaltered and valid (i.e., has not expired, if applicable);
   b. the name on the credential MUST match the name of a registered individual; and,
   c. where the credential contains a photographic image, it MUST match the presenting individual.

2. Over the telephone or online, where the authenticating organization has a pre-existing relationship with the individual and has access to a verified source of the credential's particulars either because:
   - the organization is also the credential issuer;
   - the organization can verify the information on the credential with the credential issuer; or,
   - the organization already has a verified record of the information on the credential.

   a. In this case, the individual MUST provide:
      i. his or her name and the credential's registration or identification number which MUST match the verified information the organization has access to; and,
      ii. a shared secret or knowledge of file history that the organization can verify.

7.3 Authentication Level 3 (High)

To achieve Authentication Level 3 (High), the following requirements MUST be met:

7.3.1 Acceptable Credentials

The following credentials are acceptable at this level:

1. a government-issued photo identification credential (see list of accepted credentials in *Evidence of identity requirements*, section 3.3).

7.3.2 Acceptable Authentication Methods

In-person verification of the government-issued photo identification credential is REQUIRED at this level.

1. The authenticating organization MUST inspect the credential to ensure that it:
   a. appears to be genuine and unaltered;

b. appears to be valid (i.e., has not expired);

c. Bears a photographic image that matches the individual; and,

d. Contains identity information (i.e., name and date of birth) that matches the identity information of a registered individual of the service.

7.4 Authentication Level 4 (Very High)

To achieve Authentication Level 4 (Very High), the following requirements MUST be met:

7.4.1 Acceptable Credentials

The following credentials are acceptable at this level:

1. a multi-factor credential that stores, or securely links to, a high-quality biometric (such as a digital image or fingerprint scan) and identity information (e.g., name and date of birth).
   a. The authenticating organization MUST have the necessary technology to read or access the biometric associated with the credential.
   b. This standard prescribes no list of acceptable credentials that meet this requirement.

7.4.2 Acceptable Authentication Methods

In-person verification of the multi-factor credential using technology that can access the biometric associated with the credential is REQUIRED at this level.

1. The authenticating organization MUST:
   a. ensure that the biometric associated with the credential matches the individual presenting the credential;
   b. confirm that the stored identity information (e.g., name and date of birth) matches the identity information of a registered individual of the service; and,
   c. confirm that the credential is still valid (i.e., has not expired).
2. If the authenticating organization does not have the necessary technology to access the biometric associated with the credential, or for any other reason is unable to access the biometric, it MUST reconsider the strength of the presented credential based on its visible features.

APPENDIX A – TERMS AND DEFINITIONS

This appendix contains definitions for the key terms used in this document.

For a listing of the key terms used in all the standards and documents contained in the Identity Information Standards Package, see the *Glossary of Key Terms* set out in the *Guide to Identity Information Architectures, Standards and Services*.

Term	Definition
Affiliation	A relationship between two parties (usually an individual and an organization) that can be verified by an authoritative source
Assurance	see **Identity Assurance**
Assurance Level	see **Identity Assurance Level** and **Transaction Assurance Level**
Authentication	The act of establishing or confirming something (or someone) as authentic, that is that claims made by, or about. the thing or person are true. Authenticating a person often consists of verifying their identity
Authentication Level	Relative measure (i.e., low, medium, high, very high) of the strength of an authentication event
Authoritative Party	An organization or individual that is trusted to be an authority on the identity related attributes or roles associated with users and subjects of services. Authoritative Parties may issue credentials (in which case, they may be referred to as Credential Service Providers) and are often, but not always, government organizations that have specific legislative authority and accountabilities (e.g., Vital Statistics Agencies)
Biometric	Physiological or behavioral aspects of an individual that can be measured and used to identify or verify that individual
Claim	An assertion that something is true (see **Identity Claim)**
Contact information	Information used to contact an individual or organization
Context	see **Identity Context**
Credential	A physical or electronic object (or identifier) that is issued to, or associated with, one party by another party and attests to the truth of certain stated facts and/or confers a qualification, competence, status, clearance or privilege. Identity credentials can be cards, like a driver's license or smart card; documents like a passport; or, in the context of digital identities, a User ID and password or digital certificate
Credential Service Provider	A party that issues and manages a credential that asserts identity attributes or privileges associated with an individual

Term	Definition
Credential Strength	A measure of the ability of the credential to withstand attack or compromise
Credential Strength Level	Relative measure (i.e., low, medium, high, very high) of the strength that can be placed in a credential
Electronic Credential	A digital object or document that contains a token, such as a password or cryptographic key, used for authentication to bind to a digital identity
Evidence of Identity	The information, types of evidence and verification processes that, when combined, provide sufficient confidence that individuals are who they say they are
Foundation Identity Credential	A credential that establishes the foundation of an individual's identity in Canada (e.g. Birth Certificate, Citizenship Card, etc.)
Given name	A name other than a surname (includes first and middle names)
Identification	The process of associating identity-related attributes with a particular person
Identification Level	Relative measure (i.e., low, medium, high, very high) of the strength associated with an identification process
Identity	A set of characteristics by which a person or thing is definitively recognized or known
Identity Assurance	A measure of confidence that an identity claim or set of claims is true
Identity Assurance Level	Relative measure (i.e., low, medium, high, very high) of the strength of assurance that can be placed in an identity claim or set of claims
Identity Assurance Model	A four level model that illustrates several key concepts about Identity Assurance Levels, their relationship to Transaction Assurance Levels and their dependency on registration processes, credential strength, authentication events and the underlying operational infrastructure and processes
Identity Claim	An assertion of the truth of something which pertains to a person's identity An identity claim could convey a single attribute such as an identifier (e.g. a student number) or it could convey that a person is part of a certain group or has certain entitlements (e.g. I am over 18, I am a company employee) A set of identity claims could provide sufficient identity attributes (e.g. name, date of birth address) to permit the identification of a person
Identity Context	The environment or circumstances in which identity information is communicated and perceived. Individuals operate in multiple identity contexts (e.g., legal, social, employment, business, pseudonymous) and identify themselves differently based on the context

Term	Definition
Identity Information	A set of attributes used to describe a person and may be used to distinguish a unique and particular individual or organization
Identity Information Management	A set of principles, practices, policies, processes and procedures that are used within an organization to manage identity information and realize desired outcomes concerning identity
IDIM	See **Identity Information Management**
Legal Name	A name that a person uses for official or legal purposes
Multi-factor Credential	A credential that utilizes multiple factors of different types (e.g., something you know, something you have, or something you are) for authentication
Name	Given name or surname (or both) of an individual
Personal Information	Recorded information about an identifiable individual other than business contact information
Pseudonym	A fictitious name used by an individual to conceal or obscure his or her identity
Registering Organization	A organization that collects and verifies identity claims a person makes during a registration process
Registration	A process by which a name or other fact becomes formally recorded (usually in a registry). Registration may result in the issuing of a credential for future authentication
Relying Party	A party that controls access to a resource or service and relies on an Authoritative Party to provide identity assurance and identity related attributes about a user or subject
Surname	The last name of a person (includes a family name and patronymic such as ‘Mac’ or ‘-son’)