Office of the Chief Information Officer

# IDENTITY ASSURANCE 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.

It provides a framework for establishing trust and confidence between parties issuing and receiving identity claims in both the real and online worlds.

Adoption of the Identity Assurance Standard by government and broader public sector organizations will:

- Provide a common understanding of what identity assurance is, and what combination of information, processes and technology is involved in creating and maintaining identity assurance over time;
- Ensure, to the greatest extent possible, consistency and equivalency of identity information, technology and processes used over different service delivery channels (e.g., in-person, over the telephone, online);
- Provide a secure, trusted and privacy-enhancing environment in which to exchange identity claims; and,
- Ensure alignment or equivalency with national and international identity assurance frameworks and standards in order to maximize the potential for the Government of British Columbia to connect to, and be trusted by identity management systems in other jurisdictions.

## Intended Audience

The intended audience for this Standard is service owners who must determine what level of Identity assurance is necessary for their service. This standard will also assist business and technical analysts developing detailed specifications for identity information management systems.

## Accessing Advice on this Standard

Advice on this Standard can be obtained from the:

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

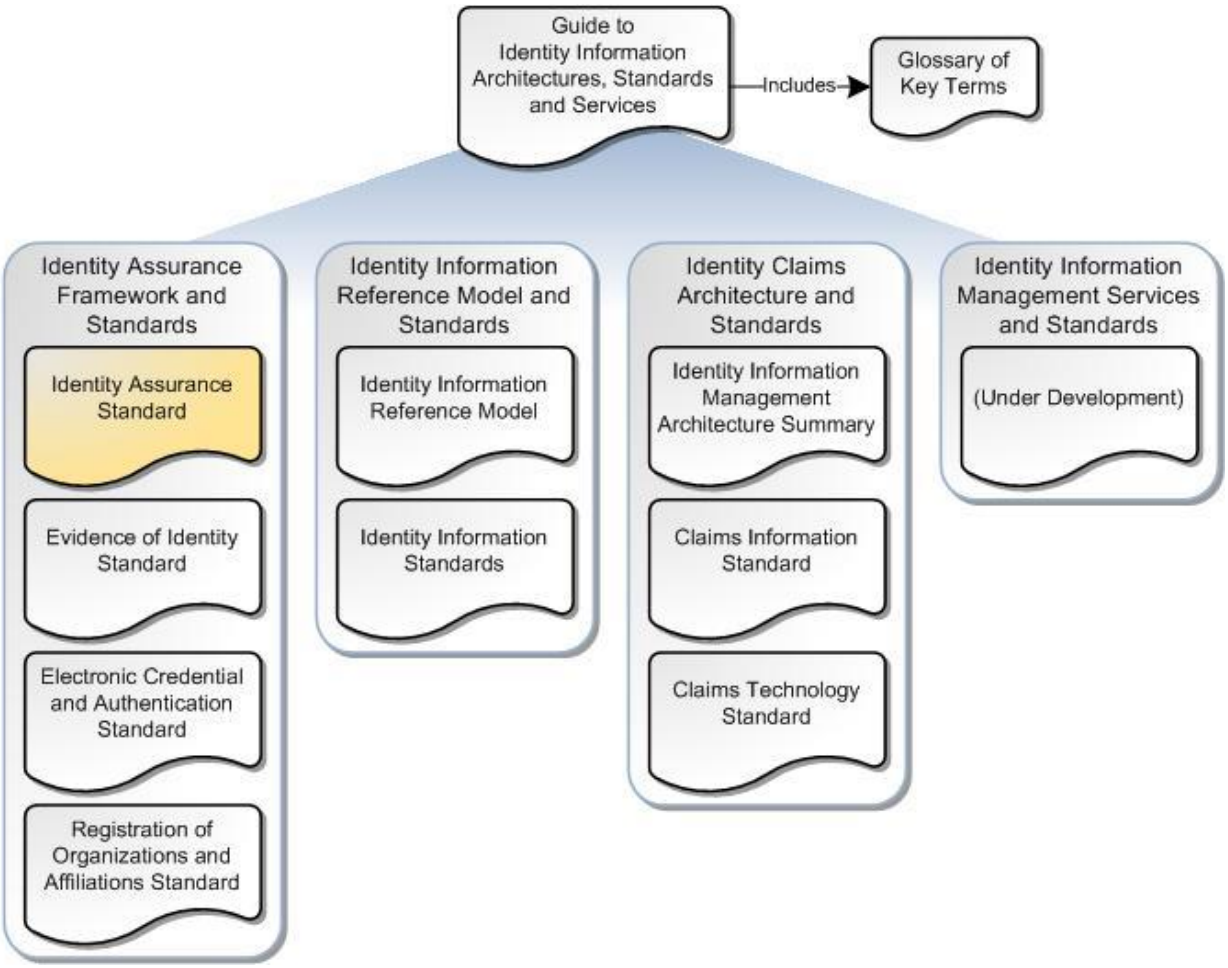
Postal Address: PO Box 9412 Stn Prov Govt
Telephone: (250) 387-8053
Facsimile: (250) 953-3555
Email: asb.cio@gov.bc.ca
Web: http://www.cio.gov.bc.ca/cio/standards/index.page

# 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**




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*<br>- *Includes Glossary of Key Terms*<br>*(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*<br>*(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*<br>*(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*<br>*(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 Standards* | 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 Standards* | 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

# 1 Introduction

Identity assurance is at the core of most government and business transactions. It is also a critical underpinning of a number of strategic government and broader public sector initiatives such as online or multi-channel service delivery, integrated case management and improving outcomes for citizens through better information sharing and citizen-centric services. All of these initiatives are dependent on knowing, with a high degree of certainty:

- who is attempting to access government information and services (including what organizations they work for and what roles and privileges they have); and,
- who the information or service, at issue, is about.

In other words, government needs identity assurance about both users of information and services and subjects of information and services.

***Identity Assurance is a measure of the confidence that an identity claim or assertion is true***

Moving towards online service delivery and information sharing across previously "siloed" information systems has highlighted the current weaknesses and limitations in our mostly paper-based identification and authentication systems. It has also raised concerns about increased opportunities for identity fraud, serving the wrong client, and privacy and security breaches. If there is to be trust among parties sharing information and issuing and receiving identity claims[1] about individuals, professionals, and business representatives, there must be:

- a common understanding of what identity assurance is;
- secure and privacy-enhancing processes for establishing and communicating identity assurance;
- transparency and clear accountability for all parties involved in an identity assurance transaction; and
- standards for the information, processes and technology involved in establishing and communicating identity assurance.

[1] An identity claim is an assertion of the truth of something which pertains to a person's "identity". An identity claim could convey a single attribute such as a student number or personal health 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 licensed physician", "I am a company employee" ). A set of identity claims could provide verification of sufficient identity attributes (e.g., name, date of birth, address) to permit the identification of a unique "identity" or person.

## 1.1 Scope

The *Identity Assurance Standard* sets a framework for assessing identity assurance needs and establishing increasing levels of identity assurance. It sets the minimum information, process and technology requirements for achieving four increasing levels of identity assurance.

It also provides guidance for conducting identity-related risk assessments and sets an overall framework for the supporting standards and guidelines that are necessary for achieving identity assurance including: the *Evidence of Identity Standard*; the *Electronic Credential and Authentication Standard*; and, the *Registration of Organizations and Affiliation Standard*.

### *Out of Scope but covered in Related Standards*

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

- Information, evidence and process requirements for establishing and verifying the identity of individuals seeking access to government services or resources (covered in the *Evidence of Identity 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)*.
- 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 *Identity Assurance 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. Government organizations that require third parties to follow this standard can include a requirement to comply with this standard in its 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 service delivery). This standard also applies to the identification and authentication of individuals in an employment context (i.e., to the use of government services and resources by government employees).

### *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*

This document sets the context and an overall framework for the following supporting standards:

- *Evidence of Identity Standard*
- *Electronic Credential and Authentication Standard*
- *Registration of Organizations and Affiliations Standard*

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*

To ensure future interoperability and trust with identity management systems in other jurisdictions, this Standard was designed to align with the following national and international Identity Assurance Frameworks and Standards:

- Pan-Canadian Strategy for Identity Management and Authentication available at: http://www.cio.gov.bc.ca/cio/idim/idmatf.page
- 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

This Standard also benefited from the concepts set out in New Zealand's e-GIF Authentication Standards (see link, below) particularly with respect to the guidance provided for conducting identity-related risk assessments.

- New Zealand's e-GIF Authentication Standards available at http://www.e.govt.nz/standards/e-gif/authentication/key-strengths/chapter4.html

## 1.4 Terms and Definitions

Key terms and definitions related to the *Identity Assurance 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 three main sections:

**Section 1.0** is the Introduction section which sets out the document's purpose, scope, applicability, and related standards and documents.

**Section 2.0** introduces core concepts related to identity assurance and sets out the Province's Identity Assurance Framework. The framework describes, at a business level, the combination of information, processes and technology involved in creating increasing levels of identity assurance.

**Section 3.0** contains the *Identity Assurance Standard* and guidance for conducting identity-related risk assessments. The *Identity Assurance Standard* sets requirements for pre-determining needed identity assurance as well as requirements for attaining increasing levels of identity assurance. The standard also sets the context for the supporting standards contained in the *Evidence of Identity Standard* and the *Electronic Credential and Authentication Standard.*

# 2 The Identity Assurance Framework

This section provides a business level overview of the Province's Identity Assurance Framework which illustrates and describes the combination of information, processes, and technology involved in creating four increasing levels of identity assurance.

***An Identity Assurance Level is a relative measure (e.g., low, medium, high, very high) of the strength of assurance that can be placed in an identity claim. A lower level of assurance means less certainty in an identity claim, while a higher level of assurance indicates a higher degree of certainty.***

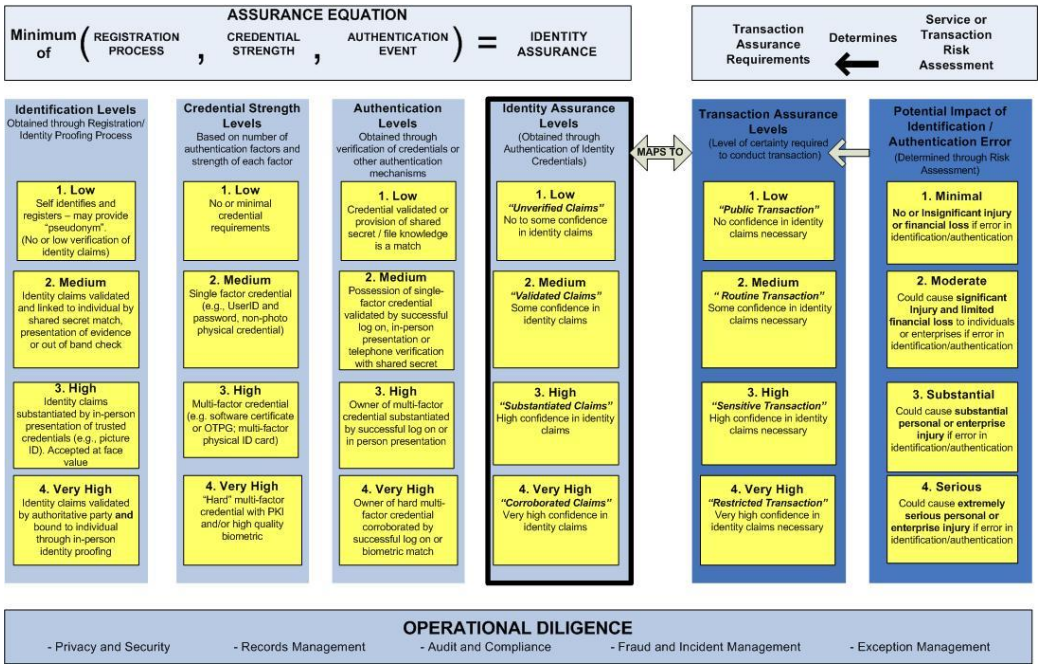
It describes the steps an organization responsible for a service or resource must take to pre-determine its identity assurance requirements. It also describes the processes an organization must follow to establish identity assurance. An organization may establish identity assurance for its own purposes or it may act as an authority (i.e., Authoritative Party[2]) for other organizations (i.e., Relying Parties[3]).

The Identity Assurance Framework, set out below, 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 (i.e., operational diligence):

**Figure 2: Identity Assurance Framework**

[2] An Authoritative Party is a party whose authority to make identity claims about individuals or organizations is recognized by one or more other parties. An authoritative party verifies claims made by individuals in order to provide assurance to Relying Parties. Authoritative Parties may issue credentials (in which case, they may be referred to as Credential Service Providers).

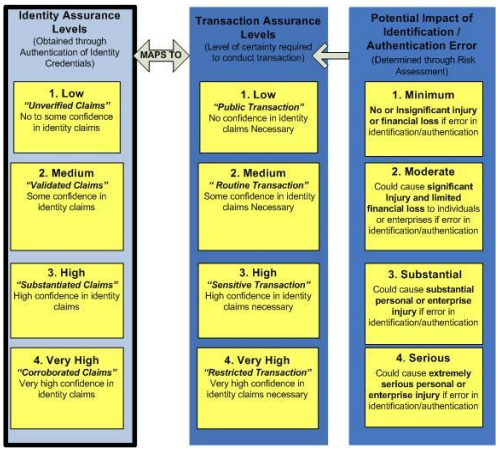
[3] A Relying Party controls access to information or a service and relies on another party (e.g., an Authoritative Party) to provide identity assurance. Relying parties can be any type of organization (e.g., a government, commercial or not-for profit organization).




## 2.1 Application of the Identity Assurance Framework

1. As a first step, an organization responsible for a service or resource must conduct a risk assessment to determine an appropriate Transaction Assurance Level for a transaction or service it is responsible for.

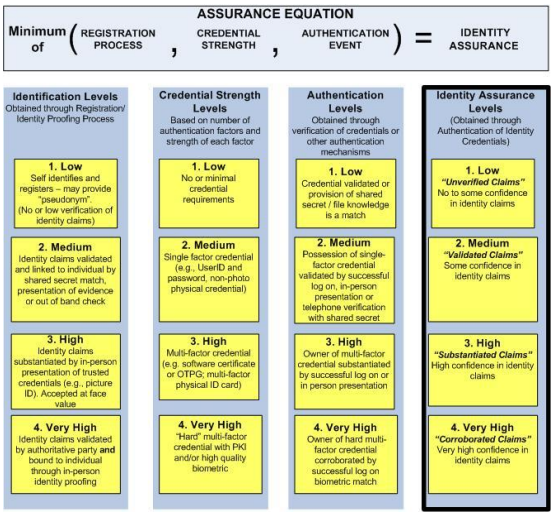
> ***A transaction assurance level is pre-established and applies to a transaction or service. It pre-sets the level of certainty in an identity claim that is needed to access information or conduct a transaction.***




The risk assessment should consider the sensitivity or security classification of the information involved and the impact of an identification or authentication error to an individual or organization.

2. Once a Transaction Assurance Level is assigned, it dictates the Level of Assurance in an identity claim that is required before permitting access to the transaction or service. The right hand side of the model illustrates how an assessment of risk pre-determines the Transaction Assurance Level which, in turn, determines the Level of Identity Assurance required.

3. Identity Assurance Levels, unlike Transaction Assurance Levels, cannot be pre-established. Rather, they are dynamically created through an authentication event (e.g., individual successfully logs-on) and are dependent on the combination of information, processes and technology standing behind the identity claim the individual is making.




The left hand side of the model, referred to as the "Assurance Equation", illustrates how assurance in a given identity claim is built and maintained over a connected set of processes and technology, including: the registration and identity proofing process; the strength of the issued credential; and, the authentication event, itself.

Different levels of identity assurance are created using different combinations of registration processes, credential strength and authentication steps which are, in turn, appropriate for different types of transactions and services.

4. And the entire chain of processes and technology is supported by the underlying infrastructure or environment within which these events occur (i.e., operational diligence).


## 2.2 Identity Assurance Levels

An Identity Assurance Level is a relative measure of the strength of assurance that can be placed in an identity claim. A lower level of assurance means less certainty in an identity claim, while a higher level indicates a higher degree of certainty.

The Province of British Columbia, in alignment with national and international standards, supports four increasing levels of Identity Assurance. A range of identity assurance levels is necessary to ensure proportionate identification and authentication processes. While it is important that there are consistent processes in place for creating and maintaining a high level of identity assurance for those organizations that need it in order to permit access to sensitive information and transactions, it is equally important to ensure, for privacy and cost reasons, that individuals are not over-identified and over-authenticated for routine transactions.

### *2.2.1 Identity Assurance Level Descriptions*


A high-level description of each level is provided below:

**1. Low Identity Assurance** ("Unverified Claims")

Description:

- Identity claims are unverified at this level and, as such, provide no to little confidence in the truth of the claim.
- This level of assurance may be appropriate for public transactions or for transactions where no specific link to a real-world person is necessary (i.e., a pseudonym is sufficient) but the ability to contact the individual or the ability for the individual to resume a transaction is a requirement (e.g., participating in an on-line learning course, signing up for an e-mail newsletter, or paying a bill or parking ticket where no specific identity is required, only an authorized payment).

**2. Medium Identity Assurance** ("Validated Claims")

Description:

- Identity claims are validated by an Authoritative Party and require the individual to use a credential for future transactions. This combination provides some confidence in the truth of the claim.
- This level of assurance may be appropriate for routine transactions where some assurance of identity is required such as access to appointment information or obtaining a business or fishing license.

**3. High Identity Assurance** ("Substantiated Claims")

Description:

- Identity claims are substantiated through the in-person presentation of evidence and require the individual to use a multi-factor credential for future transactions. This combination provides high confidence in the truth of the claim.
- This level of assurance may be appropriate for transactions that involve sensitive personal information or confidential business information such as an individual's health and financial information or a business's trade secrets, intellectual property or financial and commercial information.

**4. Very High Identity Assurance** ("Corroborated Claims")

Description:

- Identity claims are substantiated through an in-person identity-proofing process and corroborated by an Authoritative Party. They also require the use of a very high strength credential or authentication mechanism for future transactions such as the use of a “hard” multi-factor credential based on Public Key Infrastructure (PKI) or a high-quality biometric match. This combination results in very high assurance in the truth of the claim.

- This level of assurance may be appropriate for extremely sensitive transactions where a very high-degree of certainty is required such as access to witness protection lists, security plans or online drug prescribing.

### *2.2.2 Identity Assurance Standards*

Standards for achieving increasing levels of identity assurance are set out in section 3 of this document.

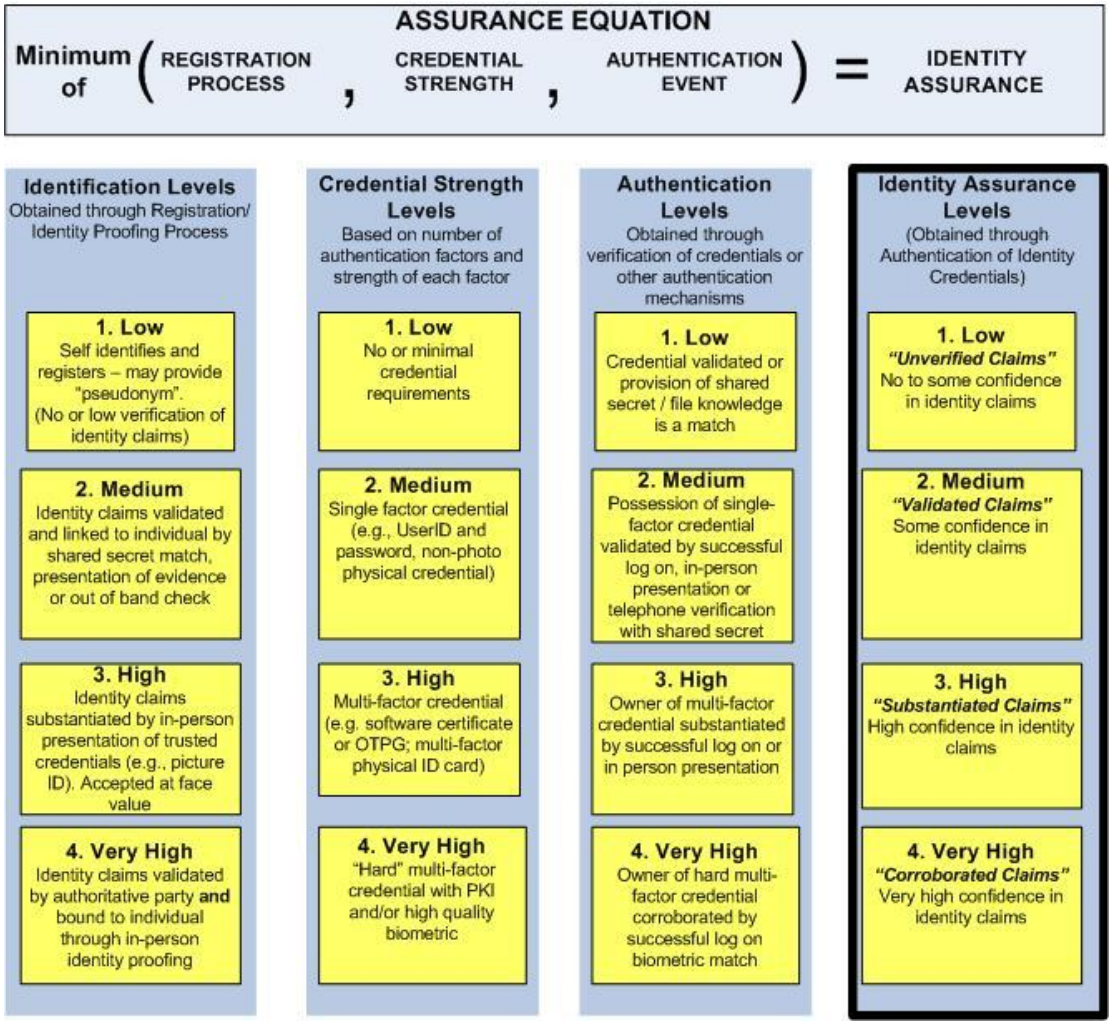
## 2.3 The Identity Assurance Equation

Assurance levels are dynamically created through an authentication event (whether through a successful log-on or a successful in-person or telephone verification) and are dependent on the original identification or registration process and the strength of the credential used to authenticate the identity claim.

Figure 3, below, illustrates this relationship as an equation. Essentially, the levels of assurance created are a minimum function of this equation which consists of:

1. the rigour of the original registration and evidence of identity process;
2. the strength of the credential used for authentication; and,
3. the authentication event, itself.

**Figure 3 – The Identity Assurance Equation**

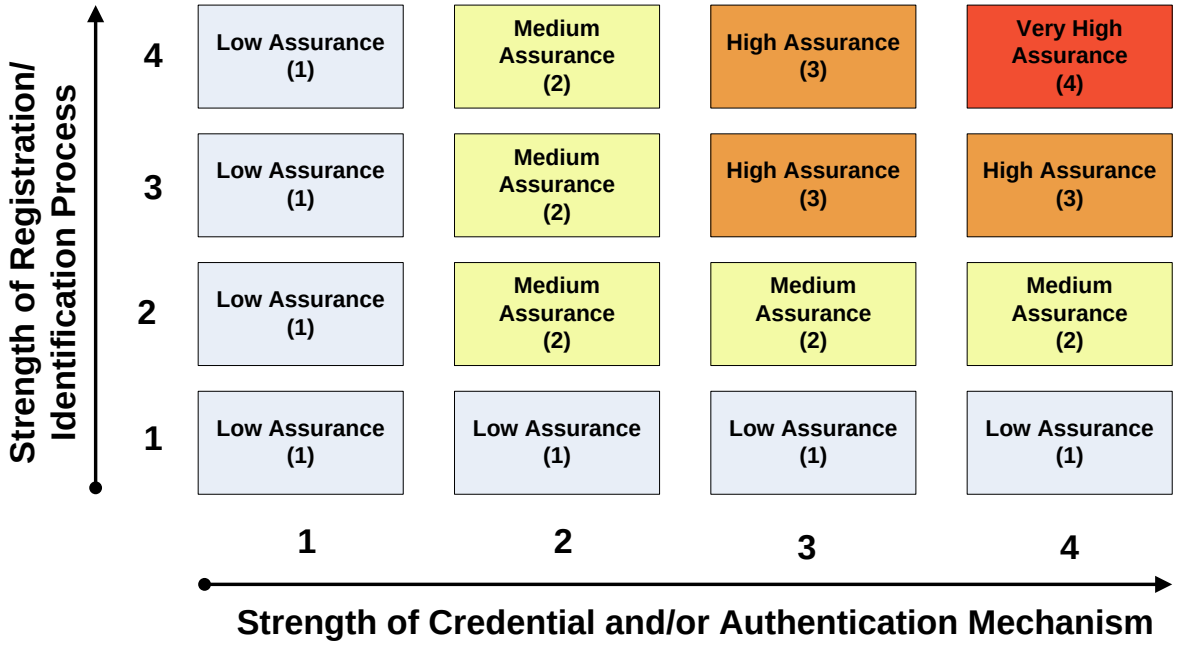


The level of assurance that can be placed in an identity claim is only as strong as the weakest component in the Identity Assurance Equation.

As illustrated below, an authenticated identity claim that is based on a Level 4 identification process, (e.g., a combination of in-person identity proofing with corroboration by an Authoritative Party), but on a Level 1 authentication credential (such as a weak password), would only result in Level 1 (or Low) identity assurance. Similarly, strong or Level 4 authentication credentials (e.g., smart card based on PKI) combined with weak Level 1 identification processes also result in Low identity assurance. It is only by combining equivalently high identification and authentication mechanisms that higher identity assurance can be obtained.

Figure 4, below, illustrates this key principle:

**Figure 4 – Impact of Registration Process and Credential / Authentication Strength on Identity Assurance**



## 2.4 Identification Levels

The first component in the Identity Assurance Equation is the Registration and Identification Process. This is the process by which an organization registers an individual and, in some cases, issues an identity credential, such as a User ID and password, for subsequent authentication.

Different registration and evidence of identity processes result in different levels of identification strength and are appropriate for different types of transactions. Establishing registration and evidence of identity standards for each level will bring consistency to how people are identified across programs and contexts and classify different registration and verification processes so that there is common understanding of their relative strength. This will help to engender trust among organizations responsible for registering and identifying people and those organizations that rely on that information.


### *2.4.1. Identification Strength Level Descriptions*

The Identity Assurance Framework supports four increasing levels of identification strength (low, medium, high and very high). A high-level business description of each 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 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.

### *2.4.2 Identification and Registration Standards*

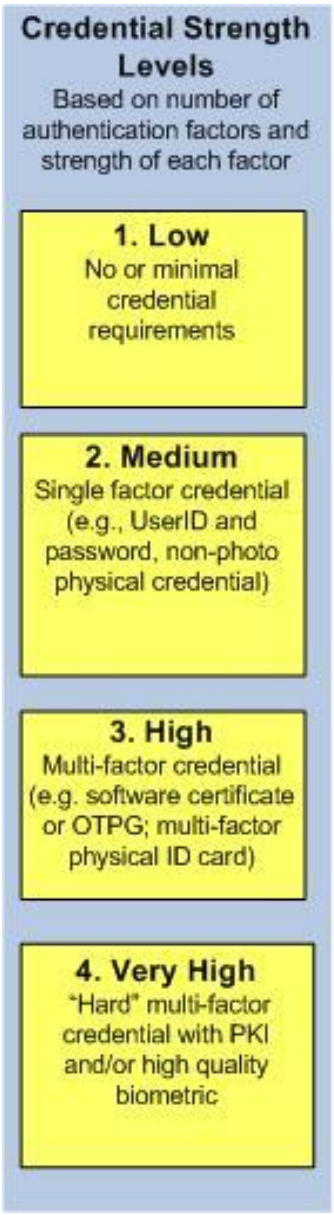
Standards for establishing increasing identification strength levels are set out in the *Evidence of Identity Standard*. This standard sets information, evidence and process requirements for establishing and verifying the identity of individuals seeking access to government services or resources. It also includes operational diligence and service standards that support the identification and registration process.

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.*

## 2.5 Credential Strength Levels

Credentials are issued to individuals (including professionals and employees of organizations) 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 B.C. CareCard or Driver's Licence, or they may be electronic such as a User ID and password or hardware token based on Public Key Infrastructure (PKI). 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.

### *2.5.1 Credential Strength Level Descriptions*

The Identity Assurance Framework supports and sets requirements for four increasing levels of credential strength. A high level business description of each level is set out below.

**1. Low Credential Strength Level** (Minimal Credential Requirements)

- At this level, there are no or minimal technology requirements. Where a credential is issued that does not meet the requirements of Level 2 Credential Strength (e.g., a PIN or password that does not meet requirements), the credential strength, by default, will be considered to have Level 1 (Low) Strength.
- There are no or minimal processes for issuing, managing and verifying credentials and minimal system and security requirements.

**2. Medium Credential Strength Level** (Single-factor Credential)

- This level requires a single-factor credential.
- There are required processes for issuing, managing and verifying electronic credentials with medium level strength.
- There are system and security requirements at this level.
- An example of a credential with medium level strength in the online world is a User ID and strong password. An example of a credential with medium level strength in the physical world 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.
- For electronic credentials, both soft (e.g., software certificates, one-time password generators, etc.) and hard multi-factor credentials are acceptable.
- There are required processes for issuing, managing and verifying credentials with high level strength.
- There are high system and security requirements at this level.
- An example of a credential with high level strength in the online world is a User ID and password plus a software certificate. An example of a credential with high level strength in the physical world is a government-issued credential with a recent photo like a driver's licence or passport.

**4. Very High-Credential Strength** (Multi-factor "Plus" Credential)

- For electronic credentials, this level requires a "hard" multi-factor credential based on public key infrastructure (PKI). Biometrics like digital imaging or fingerprint scans may also be included
- There are required processes for issuing, managing and verifying credentials with very high level strength.
- System and security requirements are very rigorous at this level.
- An example of a credential with very high level strength in the online world is a smart card based on public key infrastructure (PKI). An example of a credential with very high level strength in the physical world is a multi-factor credential that utlizes digital imaging and/or fingerprint scan biometrics.

### *2.5.2 Standards for Electronic and Physical Credentials*

Standards for attaining and maintaining increasing strength levels for electronic credentials are set out in the *Electronic Credential and Authentication Standard*. This standard includes technology, issuance and management standards for different types of electronic credential such as passwords, software certificates and smart cards. The standard also includes supporting operational diligence and security standards for the issuance and management of electronic credentials.

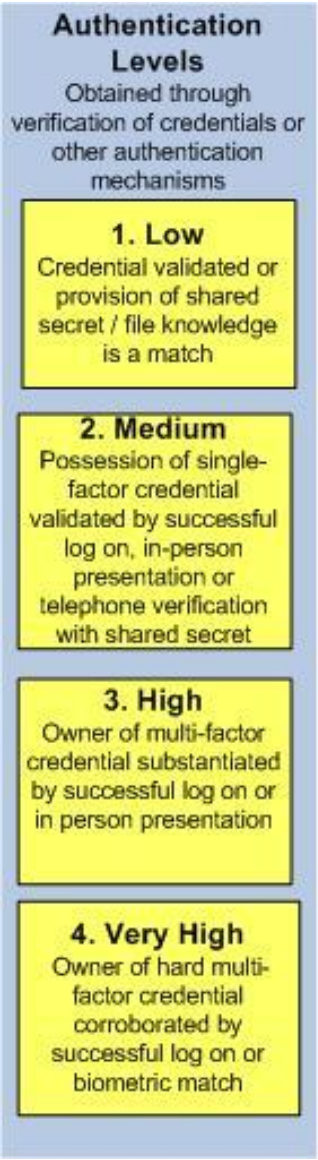
Strength levels associated with different types of physical credentials like driver's licences and passports are set out in the *Evidence of Identity Standard*. While the *Evidence of Identity Standard* categorizes physical credentials based on key characteristics for the purposes of setting minimum authentication requirements, it sets no specific technology standards and does not prescribe issuance and management standards for physical credentials.

## 2.6 Authentication Levels

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.

In the physical world, an organization verifies (or authenticates) the identity of an individual in-person by inspecting physical credentials (such as a Driver's Licence or Passport). An organization may also verify the identity of an individual remotely (such as over the telephone), using shared secrets or knowledge of file history.

In the digital world, an individual uses an electronic credential to send a communication, such as a request to log on, to a Credential Service Provider (i.e., Authoritative Party). The Authoritative Party authenticates the digital identity of the individual, and then passes a verified claim to a Relying Party.




The strength of the authentication event is based on:

- the strength of the credential authenticated (see section 2.6); and
- the processes and protocols used to conduct the authentication.

### *2.6.1 Authentication Strength Level Descriptions*

The Identity Assurance Framework standard supports and sets requirements for four increasing levels of authentication strength. A high-level business description of each level is set out below.

#### 1. Low Authentication Level

- In the digital world, the digital identity must be authenticated by a successful log on. There are minimal authentication requirements at this level.
- In the physical world, authentication of a credential is not required at this level. Shared secrets or knowledge of file history may be used as an authentication mechanism at this level.

#### 2. Medium Authentication Level

- In the digital world, the digital identity must be authenticated by a successful log on with a single factor electronic credential such as a User ID and Password.
- In the physical world, 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 number plus a shared secret match.

### 3. High Authentication Level

- In the digital world, the digital identity must be authenticated by a successful log on with a multi-factor electronic credential (e.g., software certificate plus a User ID and password).
    - At this level both "soft" (e.g., one-time password generators, software certificates) and "hard" (e.g., smart cards) electronic credentials are acceptable.
- In the physical world, 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

- In the digital world, the digital identity must be authenticated by a successful log on with a "hard" multi-factor electronic credential based on public key infrastructure (PKI).
    - At this level, only credentials that employ technology that requires hardware tokens protected by password are permitted.
- In the physical world, a real world identity must be authenticated by a high-quality biometric match utilizing facial recognition, fingerprint recognition, iris recognition or similarly strong biometric technology.
    - There are currently no government-wide requirements or approved technologies for biometric authentication. As such there are currently no standards governing the use of biometric authentication.

## *2.6.2 Authentication Standards*

Standards for authenticating electronic credentials to increasing authentication strength levels are set out in the *Electronic Credential and Authentication Standard*.

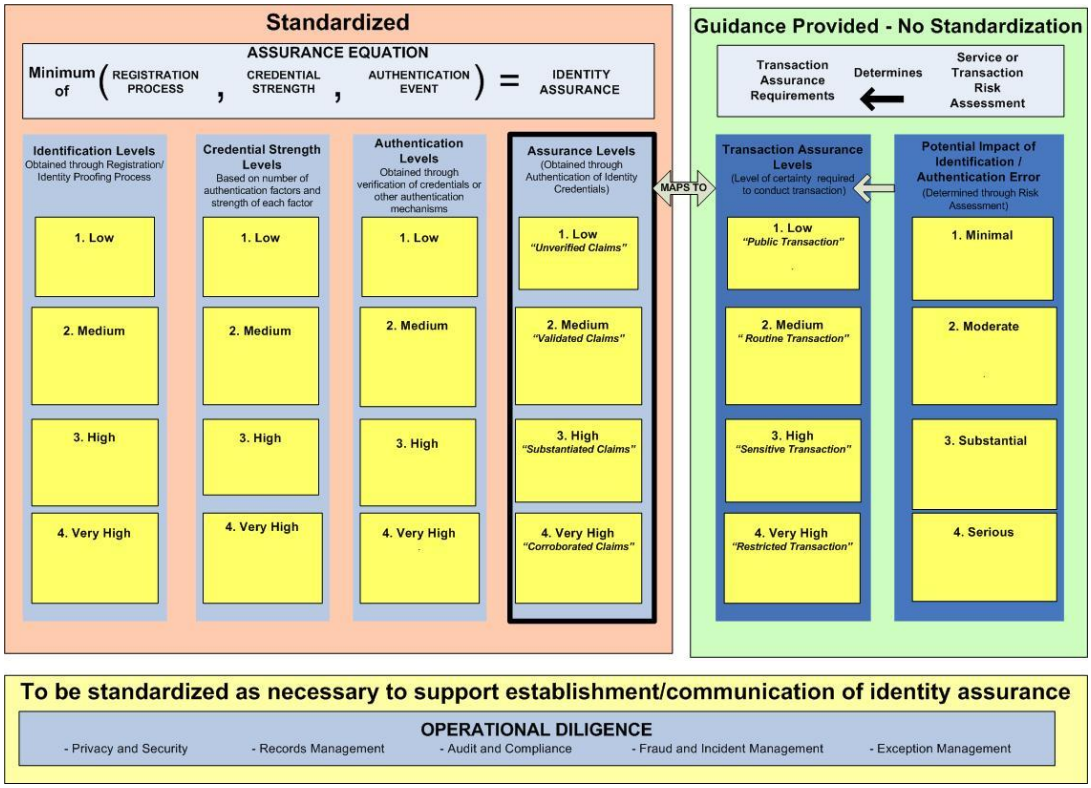
Standards for authenticating physical credentials over the counter and over the telephone are set out in the *Evidence of Identity Standard*.

# 3 Standardizing the Identity Assurance Framework

This section sets the base standard for establishing, and maintaining over time, increasing levels of identity assurance (i.e., standardizes the left-hand side of the Identity Assurance Framework model).

Standards are required in this area to enable trust, system interoperability, and information sharing. Setting standards on what is required to achieve and maintain a given level of identity assurance (e.g., low, medium, high, very high) will enable organizations to understand, and therefore better trust, the identity claims they receive from other organizations. This will, in turn, enable the sharing of information between parties involved in an identity management transaction.

**Figure 5: Standardizing the Identity Assurance Framework**




Where necessary to support the establishment and communication of identity assurance claims, standards in the area of operational diligence (e.g., security, privacy, lifecycle management) will also be set. Those standards are not set out in this document, but are contained in supporting standards documents.

Finally, this document provides general guidance but does not set detailed standards for conducting identity-related risk-assessments or for how an organization determines what level of assurance in an identity claim is required for a given service or resource (i.e., it does not set

standards for the right-hand side of the Identity Assurance Framework model). While undertaking this assessment is a REQUIRED first step, it is up to each organization to determine for itself what level of risk it can tolerant and what additional strategies might be deployed to mitigate or manage identity-related risk.

## 3.1 Identity Assurance Standard

This standard sets requirements for pre-determining an information resource or service's Identity Assurance requirements. There are four increasing levels of identity assurance (low, medium, high and very high) and this standard sets the requirements for attaining each level.

### *3.1.1 Pre-determining Identity Assurance Requirements*

1. All organizations that control access to a service or resource MUST pre-determine what minimum level of identity assurance is required to permit access to that service or resource (i.e., MUST pre-determine a Transaction Assurance Level).

2. This pre-determination MUST be based on a risk assessment of the sensitivity or security classification of the information involved and the impact of an identification or authentication error to an individual or organization. Guidance for conducting a identity-related risk assessment is set out in section 3.2.

3. This pre-determination MUST result in a minimum requirement for one of the four identity assurance levels set out in section 2.2.1. The requirements for attaining each Identity Assurance Level are set out below in section 3.1.2.

4. Organizations SHOULD require an Identity Assurance level that is equivalent to the Transaction Assurance Level necessary for the service or resource. If an organization chooses to accept a lower level of Identity Assurance than is required, it MUST mitigate the risk of doing so by additional security or authentication controls or by other factors acceptable to the organization.

### *3.1.2 Identity Assurance Level Requirements*

Increasing levels of Identity Assurance have increasing levels of identification strength. Where a credential is issued for the purpose of permitting ongoing access to a service or resource, increasing levels of Identity Assurance also have increasing credential and authentication strength requirements. Requirements for attaining increasing levels of identification, credential and authentication strength are set out in separate standards which are referenced below.

The requirements listed here are the minimum requirements. Higher levels of identification, credential and authentication strength will meet the requirements of lower levels and SHOULD be accepted by organizations.

**Assurance Level 1 (Low)**

1. There are NO requirements for attaining a Level 1 (Low) Assurance Level.

2. Where the combination of evidence of identity and registration processes, credential strength and authentication processes does not meet the requirements for Level 2 (Medium) Assurance, the identity claim MUST, by default, be considered to have Level 1 (Low) Assurance.

**Assurance Level 2 (Medium)**

1. For one-time only access to a service or resource, this level REQUIRES:

    a. Access immediately following a Level 2 or higher evidence of identity and registration process (see *Evidence of Identity Standard* for detailed requirements).

2. For ongoing access, this level REQUIRES the maintenance of identity assurance through the following combination of processes and technology:

    a. A Level 2 or higher evidence of identity and registration process (see *Evidence of Identity Standard* for detailed requirements);

    b. A Level 2 or higher strength credential (see *Evidence of Identity Standard* or *Electronic Credential and Authentication Standard* for detailed requirements); and,

    c. A Level 2 or higher authentication process (see *Evidence of Identity Standard* or *Electronic Credential and Authentication Standard* for detailed requirements).

**Assurance Level 3 (High)**

1. For one-time only access to a service or resource, this level REQUIRES:

    a. Access immediately following a Level 3 or higher evidence of identity and registration process (see *Evidence of Identity Standard* for detailed requirements).

2. For ongoing access, this level REQUIRES the maintenance of identity assurance through the following combination of processes and technology:

    a. A Level 3 or higher evidence of identity and registration process (see *Evidence of Identity Standard* for detailed requirements);

    b. A Level 3 or higher strength credential (see *Evidence of Identity Standard* or *Electronic Credential and Authentication Standard* for detailed requirements); and,

    c. A Level 3 or higher authentication process (see *Evidence of Identity Standard* or *Electronic Credential and Authentication Standard* for detailed requirements).

**Assurance Level 4 (Very High)**

1. For one-time only access to a service or resource, this level REQUIRES:

    a. Access immediately following a Level 4 evidence of identity and registration process (see *Evidence of Identity Standard* for detailed requirements).

2. For ongoing access, this level REQUIRES the maintenance of identity assurance through the following combination of processes and technology:

    a. A Level 4 evidence of identity and registration process (see *Evidence of Identity Standard* for detailed requirements);

    b. A Level 4 credential (see *Evidence of Identity Standard* or *Electronic Credential and Authentication Standard* for detailed requirements); and,

    c. A Level 4 authentication process (see *Evidence of Identity Standard* or *Electronic Credential and Authentication Standard* for detailed requirements).

## 3.2 Conducting Identity-Related Risk Assessments

The following guidance applies to an organization that is conducting an identity-related risk assessment in order to pre-determine the level of identity assurance required for its information resource or service.

***Identity-related risk is the risk related to the incorrect attribution of an individual's identity.***

1. Prior to delivering a new or existing service, an organization MUST conduct an identity-related risk assessment of the possible consequences to an individual or organization of an identification or authentication error.

2. Possible consequences SHOULD be considered from multiple perspectives, including a government, individual, non-government organization and general public perspective.

   For example, in the case of an identity-related error resulting in a non-eligible person receiving a service or benefit, there are possible consequences to a number of different parties, including:

   a. **Individuals** (e.g. an entitled person may be deemed ineligible for a service because their identity has been used previously by others to claim the same service).

   b. **Non-government organizations** (e.g. if identity-related documents are mistakenly issued to people with false identities, they may be used to commit fraud against other organizations).

   c. **The Public** (e.g. identification and authentication errors may result in significant losses for an organization which may have a downstream impact on the public if the organization increases the cost for providing the service).

   d. **The Organization itself**: (e.g. an organization's reputation may suffer as a result of negative publicity that the organization has been defrauded by a large number of people claiming false identities).

   Where risk to government as a whole is identified, the organization MUST consult with the Chief Information Officer for the Province of British Columbia to determine overall impact.

3. At a minimum, the risk assessment SHOULD consider the following possible consequences of an identification or authentication error in relation to the particular service:

| Risk Consequence | Examples |
|---|---|
| **Inconvenience, distress, or damage to standing or reputation** | Theft and subsequent use of an identity may have a significant impact on the true owner of that identity. The true owner's ability to participate effectively in the community, and to receive the services he or she is entitled to receive is diminished. Likewise, if an organization provides services on numerous occasions to people claiming false identities, this can negatively affect that organization's reputation for being able to carry out its functions effectively. |

| Risk Consequence | Examples |
|---|---|
| **Financial loss or liability** | Payment of a financial benefit to a person using a stolen or fictitious identity, who is not entitled to receive that benefit, creates a direct financial loss to the government. |
| **Harm to an organization's programs or the public interest** | Public or political perception that non-eligible people operating under fraudulent identities are receiving services from an organization leads to a loss of the organization's credibility with the public. |
| **Unauthorised release of sensitive information** | An individual's privacy rights are violated if their personal information is released to an unauthorised person. As well, release of a business's trade secrets or sensitive financial or commercial information to an unauthorized person could significantly impact the business's competitive position. |
| **Personal safety** | Theft of an identity enables access to information required to locate and harm a person whose location details are secret. |
| **Downstream effects external to the organization** | An identity-related document issued to a person on the basis of a fictitious identity by one organization is then used to verify their identity for services with other organizations. |

4. After determining whether any of the above consequences apply to the particular service, an evaluation of the impact level (e.g., "none", "low", "moderate" "high") and likelihood of each consequence occurring (e.g., "unlikely", "possible", "likely") SHOULD be made.

5. The organization SHOULD also consider any specific vulnerabilities it has that would increase the impact or likelihood for any of the possible consequences.

6. The Transaction Assurance Level for a particular service or resource SHOULD be determined based on the overall composite risk level achieved from an evaluation of the impact and likelihood of all possible consequences.

7. Completion of an identity-related risk assessment does not address all risks associated with a service and DOES NOT relieve an organization of any responsibility it might have to conduct related risk assessments such as a Security Threat and Risk Assessment (STRA) or a Privacy Impact Assessment (PIA).

### *3.2.1 Additional Guidance*

Organizations looking for additional guidance in conducting identity-related risk assessments and translating that into a Transaction Assurance Level may wish to refer to the following documents:

- 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. Government's E-Authentication Guidance for Federal Agencies available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

# 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 |
| **Biometric Authentication** | The automated use of biometric attributes to establish or verify an individual's identity (biometric recognition) |
| **Claim** | An assertion that something is true (see **Identity Claim**) |
| **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 |
| **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.<br>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)<br>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 |
| **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 |

| Term | Definition |
|---|---|
| **IDIM** | See **Identity Information Management** |
| **Multi-factor Authentication** | Authentication that utilizes one or more credentials that incorporate multiple factors (e.g., something you know, something you have, or something you are) |
| **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 |
| **Pseudonym** | A fictitious name used by an individual to conceal or obscure his or her identity |
| **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 |
| **Smart Card** | A high strength credential with an embedded chip that can be used for authentication |
| **Transaction Assurance Level** | A pre-established assurance level (i.e., low, medium, high, very high) that applies to a transaction or service. It pre-sets the level of certainty in an identity claim that is needed to access information or conduct a transaction |