Office of the Chief
Information Officer

ELECTRONIC CREDENTIAL AND AUTHENTICATION STANDARD

-- This page left intentionally blank --

Revision History

Version	Date	Changed By	Description of Change
1.0	April 23, 2010	Patricia Wiebe	

Document Purpose

This document supports the *Identity Assurance Standard* that describes the Province's assurance framework and requirements for identification, credential and authentication processes to support identity information management. This document sets the standards for issuing, managing and authenticating electronic credentials to increasing levels of strength.

Audience

The intended audience for this document is technical architects, infrastructure solution designers and application developers. Readers are assumed to have knowledge of electronic credentials and authentication, application development and integration, cryptography and internet-based transport and security protocols.

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

Exemptions to the standards or parts of any standard may be requested.

Office of the Chief Information Officer
BRITISH COLUMBIA

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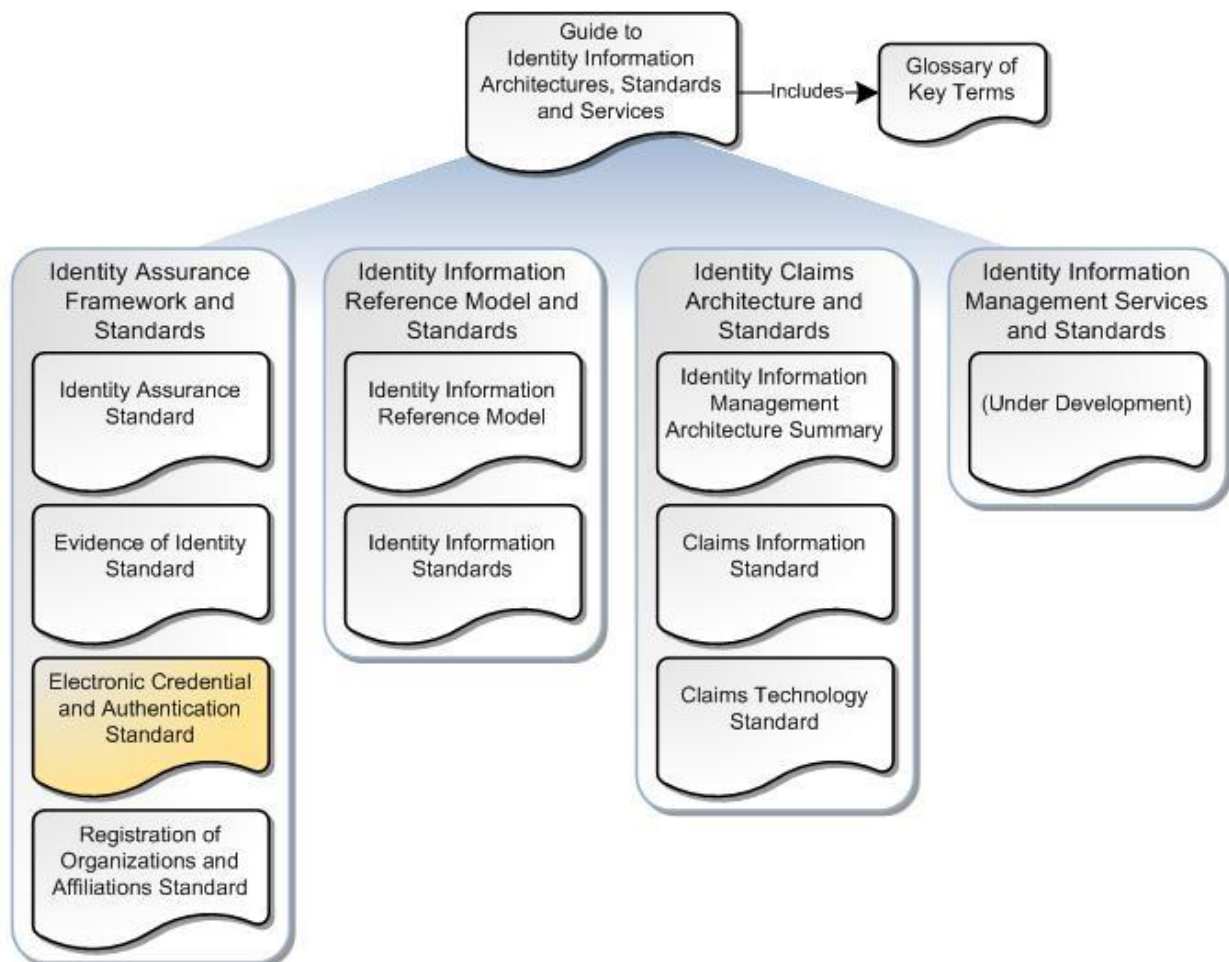
Readers wishing to find more information on a related topic should refer to one or more of the other documents available within the package.

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 - *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.
Evidence of Identity Standard	Supports the *Identity Assurance Standard* by setting evidence of identity standards for registering and identity-proofing individuals to increasing levels of identification strength. Applies to both online and off-line identity management transactions and to the registration of individuals acting in multiple identity contexts (i.e., in a personal, professional or employment context).
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 registering organizations and 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 Standard.*
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 Standard.*
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

1 Introduction

The *Electronic Credential and Authentication Standard* consists of a set of standards that when implemented by government organizations will enable a secure system that provides identity assurance for the benefit of information systems or applications. These standards support the *Identity Assurance Standard* by specifying the combination of technology, security and management controls that must be in place to achieve the different levels of credential and authentication strength, specifically in the area of electronic credentials and electronic authentication. This standard supports the online channel of government service delivery by focusing on individuals who are users of information systems. These standards do not describe the in-person, telephone or postal service channels that may also used by the government services.

The set of standards includes the following:

- The *Electronic Credential Technology Standard* sets out the technology requirements for the types of electronic credentials that are acceptable at each of the Credential Strength Levels described in the *Identity Assurance Standard*.

- For those electronic credentials that use passwords (or PINs), the *Password Standard* sets the requirements for appropriate password values and how to store and manage password and related data.

- The *Electronic Authentication Standard* sets out the technology requirements for the authentication mechanisms and protocols that are acceptable at each of the Authentication Levels described in the *Identity Assurance Standard*.

- The *Electronic Assertion Standard* then sets out the technology requirements for the assertion mechanisms that are acceptable to communicate the results of the authentication to an information system or application.

- The *Electronic Credential Lifecycle Management Standard* sets out the requirements for the lifecycle management of electronic credentials, including how a credential is uniquely linked to an identity, how credentials are created, delivered to the user and maintained over time.

- Finally, the *Organizational Diligence and Service Standard* sets out additional service management and information security policy requirements for organizations that provide electronic credential and authentication services.

These standards have been adapted from the US National Institute of Standards and Technology (NIST) Special Publication 800-63, titled *Electronic Authentication Guideline*, dated April 2006. The Liberty Alliance Project also developed its Identity Assurance Framework based on this document, thus they are comparable.

1.1 Scope

These standards specify the technology and security controls and management processes required to implement credential and authentication services for electronic information systems and applications.

In Scope

The *Electronic Credential Standard* sets specific usage of acceptable credential technology that an individual can use to authenticate to identify themselves for logical access to information systems. The general types of credential technology are:

- user-selected passwords,
- one time password generators,
- digital certificates and private keys within software-based and hardware-based tokens,
- assertions from other authentication services.

The *Electronic Authentication Standard* sets specific usage of acceptable authentication mechanisms from the perspective of which security threats the authentication protocol must protect against. It covers the topics of:

- proving that the user has control or possession of the credential,
- using secure communication channels, and
- validating that the credential is valid and has not been revoked.

The *Electronic Assertion Standard* sets requirements for how to communicate the results of the authentication to an information system or application. It covers the topics of:

- using secure communication channels,
- protecting the assertion, and
- expiring the assertion after a certain amount of time.

The *Electronic Credential Lifecycle Management Standard* sets requirements for how to manage and issue credentials. Organizations that provide credential services or authentication services also need to follow the *Operational Diligence and Service Standard* that specifies additional requirements on the operational environment in which these services are managed.

Out of Scope but covered in other Standards

The following are outside the scope of this Standard but, as noted, are covered by other related standards:

- explanation of identity assurance and the information, processes and technology involved in creating and maintaining identity assurance over time (covered in the *Identity Assurance Standard*);

- information, evidence and process requirements for establishing and verifying the identity of individuals to whom credentials are issued (covered in the *Identity Assurance Standard*);

- specification about how to securely interact between a Relying Party and an Authoritative Party (covered in the *Claims Technology Standard*);

- specification of claims about identity assurance or other identity information that can be used in an assertion from an Authoritative Party to a Relying Party (covered in the *Claims Information Standard*); and,

- specification of encryption algorithms and secure communication protocols (covered in the Cryptographic Standards for Information Protection).

Out of Scope - Not covered in other Standards

The following are outside the scope of this Standard and currently outside the scope of related standards and documents:

- specification of business rules for how electronic assertions are applied to processing within Information Systems;

- specification of biometric technology and controls;

- specification of how systems are issued credentials and are authenticated to each other (also called machine to machine authentication);

- specification on how to establish a technical configuration between an information system and an authentication service;

- specification of session management controls used in an information system;

- comprehensive implementation guidance.

1.2 Applicability

Applicability of this Standard

This standard applies to any BC government ministry or central agency that issues and manages electronic credentials, authenticates electronic credentials or has an information system that relies on the use of electronic credentials and authentication. Government organizations that require third parties to follow this standard can include a requirement to comply with this standard in its contract for service.

Organizations are responsible for ensuring that the Information Systems solutions that they build or buy are able to meet these standards. In addition, identity management shared services will be designed to comply with these standards. Where an organization uses the identity management shared services, the responsibility for complying with the relevant parts of the standards will be devolved to the shared service.

Interpretation of this Standard

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

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

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

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 (See the References section). When these words are not capitalized, they are meant in their natural-language sense.

1.3 References

1.3.1 Normative References

The following documents are required to be read in order to understand this document.

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

Other documents are significant to this document/standard and should be read. They are required to be understood and adhered to for the implementation of the standards.

- *Evidence of Identity Standard*

1.3.2 Informational References

Additional documents are related and provided for informational purposes. Content within these references are generally described within this document such that it is not required to read the reference material for a general understanding.

- IETF RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels
  - http://www.ietf.org/rfc/rfc2119.txt
- *Cryptographic Standards for Information Protection*

- o http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf
- US National Institute of Standards and Technology (NIST) Special Publication 800-63, *Electronic Authentication Guideline*, version 1.0.2, April 2006
  - o http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- Liberty Alliance *Identity Assurance Framework*, version 1.1, 2008 (specifically section 3.5 – *Common Organizational Service Assessment Criteria* and section 3.7 – *Credential Management Service Assessment Criteria*).
  - o http://www.projectliberty.org/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf
- US National Institute of Standards and Technology (NIST) Federal Information Processing Standardization (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, December 2006
  - o http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

1.4 Terms and Definitions

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

1.5 Document Structure

This document has eight main sections:

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

Section 2: This section sets context and explains the concepts for the standards, including describing the Credential Strength Levels and Authentication Levels from the *Identity Assurance Standard*.

Section 3: This section sets the requirements for electronic credential technology for each level.

Section 4: This section sets the requirements for password strength and the management of password data for each level.

Section 5: This section sets the requirements for electronic authentication for each level.

Section 6: This section sets the requirements for communicating the results of the electronic authentication for each level in the form of an assertion to an information system or application.

Section 7: This section sets the requirements for managing the lifecycle of credentials – linking to an identity, issuing and managing a credential throughout its lifecycle.

Section 8: This section sets the requirements for organizational diligence for those organizations that have credential and authentication services.

Office of the Chief
Information Officer
BRITISH COLUMBIA

2   Core Concepts of Electronic Authentication

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. Once an individual has been successfully authenticated, the individual may be enabled to access services and information. Authenticating a person often consists of verifying their identity through the presentation of credentials.

Electronic credential and authentication services are used to verify and link a user to an individual's identity for use within an information system to support the online channel of government service delivery.

2.1   Electronic Authentication Model

This section describes the general steps and services involved in an electronic credential and authentication system.

Identity Registration

Before an individual can authenticate to an electronic service, the individual must be registered and issued an electronic credential.

As described in the *Identity Assurance Standard*, an individual may be registered and identified to increasing levels of identification strength to provide higher assurance in their identity. The identification of an individual may involve a verification process called identity proofing. This is described in the *Evidence of Identity Standard*. In this document, the service that manages registration and identity proofing process is referred to as the identity registration service.

The following diagram shows the conceptual process of identity registration.

Figure 2 - Identity Registration Flow
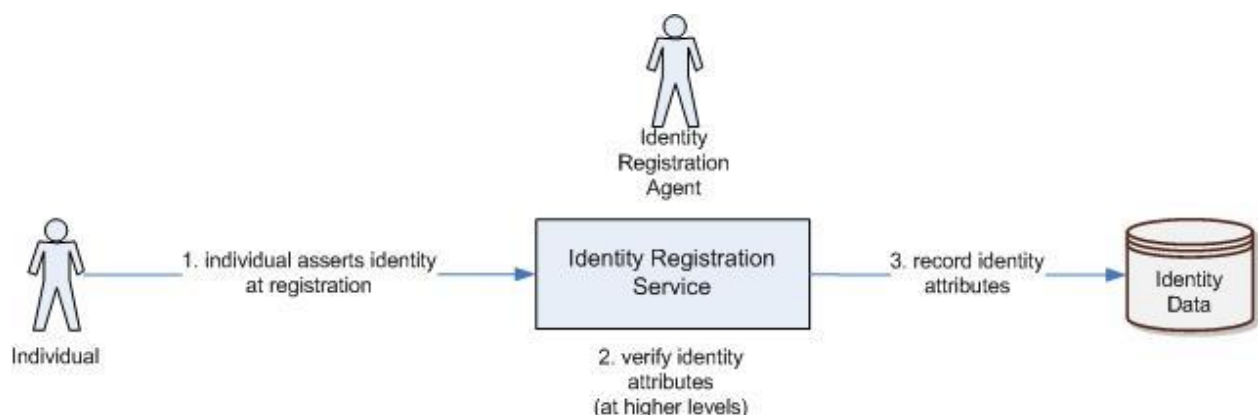
Authentication Factors

Authentication is often categorized by the number of factors that they incorporate. This is directly related to the types of credentials issued. The three foundational factors of authentication are:

- Something you know (for example, a password or PIN);
- Something you have (for example, a token like a smart card);
- Something you are (for example, a biometric like a fingerprint).

Authentication strength is based on the number of factors and the strength of each factor. Systems that incorporate multiple factors are generally considered stronger than those that use only one, however it is important to recognize that not all factors are considered equal.

Biometrics are unique personal attributes that can be used to identify a person, however are more challenging to implement. Multi-factor (or two-factor) authentication approaches are usually based on a user ID and password plus a digital certificate or one-time password.

Contextual information, such as the location of the user authenticating, or the time of day, may also be considered significant to the authentication. Network security controls may further restrict authentication to certain locations. Observations of how users authenticate may be developed into a behavioural pattern that may be used to detect abnormalities which may represent an attacker. Risk-based approaches such as these may be used in authentication systems to increase the confidence in the authentication event, and may in some cases be considered mitigation when used with a lower strength credential. Further discussion of this topic is out of scope for this document.

Credential Issuance

An individual must be issued an electronic credential so that they can use it to enable future authentication of their identity.

As described in the *Identity Assurance Standard*, different forms of credential technology may be used to provide higher assurance when the credential is used to prove a user's identity. In this document, the service that issues and manages the electronic credentials is referred to as the credential service.

The following diagram shows the conceptual flow of credential issuance.

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● Collaboration ● Innovation

Office of the Chief
BRITISH COLUMBIA | Information Officer

Figure 3 - Credential Issuance Flow
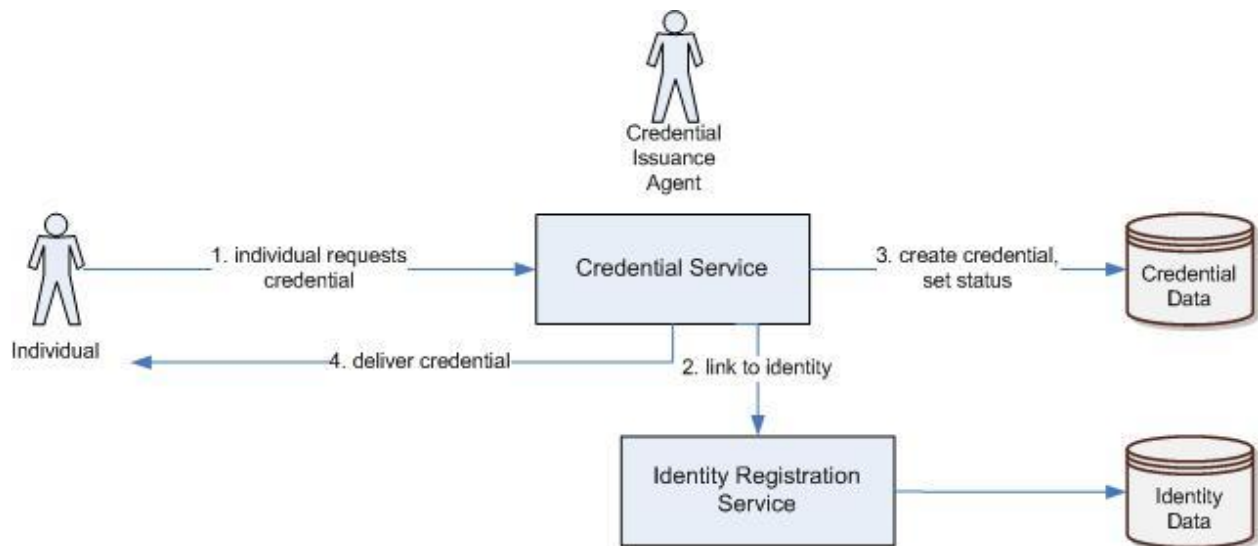
Authentication Event

When a user requests access an information system or application (also referred to as a relying party), the user is required to present their electronic credential in order to authenticate themselves. Once an individual has been successfully authenticated, the individual may be enabled to access services and information. Commonly individuals are also required to be authorized to access services and information; authorization is out of scope for this discussion.

As described in the *Identity Assurance Standard*, credentials may be authenticated with different processes that result in providing higher assurance. The authentication mechanism or protocol involves getting the user to demonstrate or prove that they are in control or have possession of the credential. This may be in the form of entering a user ID and password that they know, or inserting a smart card into a device and activating it with a password. In this document, the service that authenticates a user (or verifies a credential) is referred to as the authentication service.

Assertions

After an authentication event, the result of the authentication needs to be communicated to the information system or application (relying party) that the user was attempting to access. This is communicated in the form of an assertion, which states who the user claims to be, possibly with some identity attributes about the user. The assertion mechanism or protocol involves securely communicating this assertion and setting it to expire after a period of time.

The following diagram shows the conceptual flow of authenticating with an electronic credential and sending an assertion to a relying party.

Figure 4 - Authentication and Assertion Flow
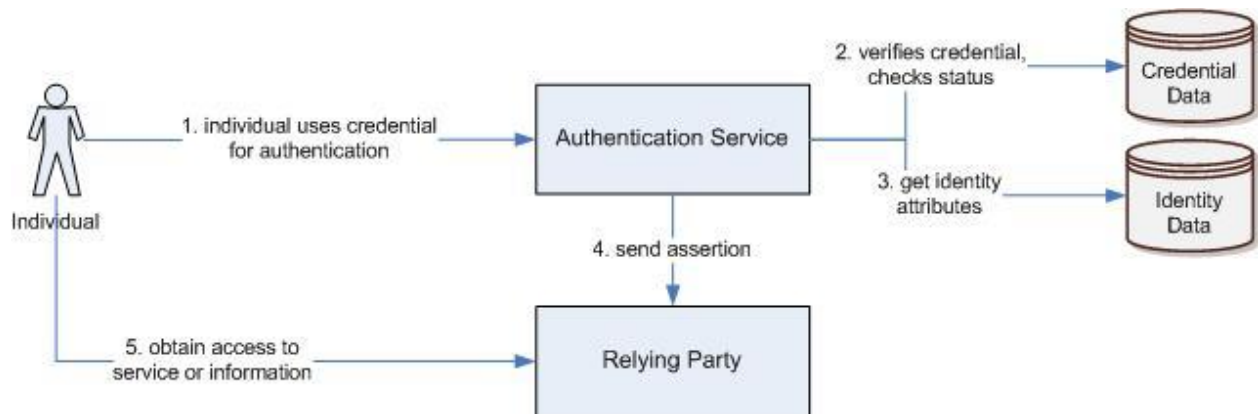
Service Dependencies

One organization may provide all three services (identity registration service, credential service, authentication service) in one system. It is also common for the services to be distributed across multiple organizations or systems. The credential service relies on an identity registration service in order to properly associate and link a credential to a recorded identity (except for Identity Assurance Level 1). A credential service relies on authentication services to gather the credential data (such as passwords) and verify it, however an authentication service must be authorized to do so.

2.2 Electronic Credential Threats

Authentication systems are commonly threatened by the compromise of the electronic credential. If an attacker can gain control of someone else's credential, they can act as that individual and inappropriately access services or information. Threats to electronic credentials can be categorized into attacks on each of the three factors described above:

- Something you know may be disclosed to or guessed by an attacker;
- Something you have may be stolen or cloned by the attacker;
- Something you are may be replicated by an attacker.

Several strategies are used to mitigate these threats.

- Multiple factors of authentication make it harder for an attacker to gain control of credentials;
- Hardware-based tokens have mechanisms to prevent or detect tampering to make it harder for an attacker to duplicate them;
- Complex passwords and one-time passwords make it harder for an attacker to guess a password;
- Security controls, such as encryption, make it harder for an attacker to decipher data and communication.

These strategies are expressed in the *Electronic Credential Technology Standard* in section 3 and *Password Standard* in section 4.

2.3 Electronic Authentication Threats

Authentication systems are also threatened by attacks against the authentication protocol. If an attacker can observe the communication occurring during an authentication and access the sensitive information, such as someone else's password, they may be able to use that knowledge to act as that individual and inappropriately access services or information. Threats to the authentication protocol include:

- Eavesdropping to observe the communication of an authentication event;
- Pretending to be the user and testing guessed passwords;
- Pretending to be the authentication service to gather user-submitted passwords (phishing);
- Hijacking an already authenticated session, possibly to change a password for later use.

Several strategies are used to mitigate these threats.

- Eavesdropping resistance to make it impractical for an attacker to learn passwords or encryption keys by observing the communication of an authentication event;
- Password guessing resistance to make it impractical for an attacker to guess a password;
- Replay resistance to make it impractical for an attacker to record a successful authentication and replay it to obtain access;
- Impersonation resistance to prevent an attacker from learning passwords or encryption keys when it attempts to impersonate an authentication service;
- Man-in-the-middle resistance to prevent an attacker from intercepting and replaying messages by requiring authentication of the services so that a third party would be detected;
- Hijacking resistance to prevent an attacker from inserting, deleting or re-routing messages without being detected.

These strategies are expressed in the *Electronic Authentication Standard* in section 5.

There are other attacks relevant to electronic authentication that are not part of the authentication protocol. These include:

- Malicious code, intrusion or hacking into authentication systems;
- Social engineering that allows an attacker to learn or observe a user's password;
- Confusing a user into using an insecure authentication protocol.

Specific mitigation is not expressed in this document, however these threats are generally covered by requirements in the *Operational Diligence and Service Standard* in section 8.

2.4 Credential Strength Levels

Credentials are 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 the BC CareCard or Driver's Licence, or they may be electronic such as a user ID and password or a smart card.

This document focuses on electronic credentials only; physical credentials are described in the *Identity Assurance Standard* and *Evidence of Identity Standard*.

Electronic credential strength is based on the extent to which the credential can be trusted to be a proxy for the individual it represents (known as identity binding). The strength of the credential directly relates to:

- the integrity and reliability of the technology and security features associated with the credential itself;
- the processes by which the credential is issued, managed and authenticated; and,
- the system and security measures followed by the service provider responsible for issuing, managing and authenticating the credential.

The standards in this document support and set requirements for the four levels of credential strength. A high level description of each level is provided on the next page, along with the relevant section of the Identity Assurance Framework Model.

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

Credential Strength Level 1 – Low

This level requires a single-factor electronic credential with low security requirements. An example is a user ID and password with simple password requirements.

There are minimal required processes for issuing and managing credentials with low level strength, and system and security requirements for credential services.

Where an electronic credential is issued that does not meet the medium level strength requirements (Level 2), for example, a password that does not meet the password strength requirements, then it is considered to meet the low level strength requirements (Level 1).

Credential Strength Level 2 – Medium

This level also requires a single-factor electronic credential, but at this level the requirements are stronger than for Level 1. An example is a user ID and password with strong password requirements.

There are required processes for issuing and managing credentials with medium level strength, and system and security requirements for credential services.

Where a multi-factor credential is issued that does not meet the high level strength requirements (Level 3), for example, a device that does not meet the cryptographic module validation requirements, then it is considered to meet the medium level strength requirements (Level 2).

Credential Strength Level 3 – High

This level requires a multi-factor electronic credential. Software-based and hardware-based cryptographic tokens and one-time password generators are acceptable. An example is a digital certificate combined with a password.

There are strong processes for issuing and managing credentials with high level strength, and system and security requirements for credential services.

Credential Strength Level 4 – Very High

This level also requires a multi-factor electronic credential, but at Level 4 it must use a hardware-based cryptographic token. An example is a smart card that uses public key infrastructure (PKI). Biometrics like digital imaging or fingerprint scans may also be included.

There are very strong processes for issuing and managing credentials with very high level strength, and more rigorous system and security requirements for credential services.

2.5 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. Once an individual has been successfully authenticated, the individual may be enabled to access services and information. Authenticating a person often consists of verifying their identity through the presentation of credentials.

This document focuses on electronic authentication only (i.e. the verification of electronic credentials); the authentication of an individual using physical credentials, shared secrets or knowledge of file history is described in the *Evidence of Identity Standard*.

Electronic authentication strength is based on the extent to which the authentication protocol can securely communicate with the user and allow the user to demonstrate proof of possession of the electronic credential. A successful authentication results in the binding of the user to a previously registered identity or set of identity attributes. The strength of the authentication directly relates to:

- the strength of the credential authenticated; and,
- the processes and protocols used to conduct the authentication.

The standards in this document support and set requirements for the four levels of authentication. A high level description of each level is provided on the next page, along with the relevant section of the Identity Assurance Framework Model.

**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

Authentication Level 1 – Low

This level requires authentication of a single-factor credential with low security requirements. An example is authenticating a user ID and password through a challenge and response protocol.

There are minimal processes and protocols for verifying credentials with low level strength, and system and security requirements for authentication services.

Authentication Level 2 – Medium

This level requires authentication of a single-factor credential with medium level security requirements. An example is authenticating a user ID and password through an encrypted communication session using Transport Layer Security (TLS).

There are required processes and protocols for verifying credentials with medium level strength, and system and security requirements for authentication services.

Authentication Level 3 – High

This level requires authentication of a multi-factor credential. An example is authenticating a digital certificate with a user ID and password through an encrypted communication session using Transport Layer Security (TLS).

There are strong processes and protocols for verifying credentials with high level strength, and system and security requirements for authentication services.

Authentication Level 4 – Very High

This level requires authentication of a multi-factor credential that uses a hardware-based cryptographic token. An example is authenticating a smart card and PIN through an encrypted communication session using Transport Layer Security (TLS). This level includes authentication of high-quality biometrics, however there are currently no standards governing the use of biometric authentication.

There are very strong processes and protocols for verifying credentials with very high level strength, and more rigorous system and security requirements for authentication services.

3 Electronic Credential Technology Standard

This standard sets out the technology requirements for the types of electronic credentials that are acceptable at each of the Credential Strength Levels described in section 2.4, and the security and technical features associated with them.

3.1 Credential Technology Requirements for Level 1 – Low

When implementing an electronic credential to achieve a low credential strength level, the following standard describes the technology and/or security features that MUST be met.

1. The electronic credential MUST use either
   a. a password (that may or may not comply with the *Password Standard* set out in section 4); or,

   b. an assertion from another authentication service that used any credential strength and authentication method, and that is deemed by the Relying Party to be an authoritative and trusted service.

3.2 Credential Technology Requirements for Level 2 – Medium

When implementing an electronic credential to achieve a medium credential strength level, the following standard describes the technology and/or security features that MUST be met.

1. The electronic credential MUST use either
   a. a password that conforms to the Password Standard, as set out in section 4; or,

   b. an assertion from another authentication service that used a medium (or higher) credential strength and authentication method (Level 2 to 4), and follows the *Electronic Assertion Standard*, as set out in section 6; or,

   c. a multi-factor credential that may or may not conform to the higher credential strength (Level 3 or 4) standards (for example, a one-time password device that does not meet the cryptographic module validation requirements).

3.3 Credential Technology Requirements for Level 3 – High

When implementing an electronic credential to achieve a high credential strength level, the following standard describes the technology and/or security features that MUST be met.

1. The electronic credential MUST use either
    a. a software-based cryptographic token that meets the following requirements:
        i. uses a key and cryptographic mechanism validated at FIPS 140-2 Level 2 or higher;
        ii. requires the use of a password or biometric by the individual to activate the cryptographic mechanism; or a password in combination with the cryptographic mechanism in the same authentication protocol; and,
        iii. follows the *Password Standard*, as set out in section 4, for any passwords used.

    b. a hardware-based cryptographic token that meets the following requirements:
        i. uses a key and cryptographic mechanism stored on a special hardware device validated at FIPS 140-2 Level 1 or higher;
        ii. requires the use of a password or biometric by the individual to activate the cryptographic mechanism; or a password in combination with the cryptographic mechanism in the same authentication protocol; and,
        iii. follows the *Password Standard*, as set out in section 4, for any passwords used.

    c. a one-time password device token that meets the following requirements:
        i. depends on a symmetric key stored on a personal hardware device that is a cryptographic module validated at FIPS 140-2 Level 1 or higher;
        ii. permits at least 10^6 possible password values; and,
        iii. requires the use of a password or biometric by the individual to activate the retrieval or generation of the one-time password.

    d. an assertion from another authentication service that used a high (or very high) credential strength and authentication method (Level 3 to 4), and follows the *Electronic Assertion Standard*, as set out in section 6.

3.4 Credential Technology Requirements for Level 4 – Very High

When implementing an electronic credential to achieve a high credential strength level, the following standard describes the technology and/or security features that MUST be met.

1. The electronic credential MUST use
    a. a hardware-based cryptographic token that meets the following requirements:
        i. uses a key and cryptographic mechanism stored on a special hardware device validated at FIPS 140-2 Level 2 or higher with at least FIPS 140-2 Level 3 physical security (i.e. tamper proof device);

ii.   requires the user of a password or biometric by the individual to activate the cryptographic mechanism; or a password in combination with the cryptographic mechanism in the same authentication protocol; and,

iii.   follows the *Password Standard*, as set out in section 4, for any passwords used.

4 Password Standard

This standard sets out the requirements for appropriate password values and how to store and manage password and related data. They are directly related to the types and levels of electronic credentials described in the *Electronic Credential Technology Standard* in section 3. The term password is meant to include PINs (Personal Identification Numbers) which implies numeric values, and passphrase, which implies multiple words in succession.

4.1 Password Strength Requirements for Level 1 – Low

When implementing an electronic credential with a password to achieve a low credential strength level, there are no minimum standards for the strength of the password.

1. The password strength MAY be the same or weaker than the requirement for level 2 or higher.

4.2 Password Strength Requirements for Level 2 to 4 – Medium to Very High

When implementing an electronic credential with a password to achieve a medium or higher credential strength level, the following standard describes the password strength requirements that MUST be met.

1. Where passwords are implemented by BC government ministries and central agencies, the password MUST be composed as follows:
   a. contain a minimum of 8 characters;
   b. contain characters from at least three of the following categories:
      i. English upper case characters (A to Z)
      ii. English lower case characters (a to z)
      iii. Numerals (0 to 9)
      iv. Non-alphanumeric keyboard symbols (e.g., ! $ # %); and,
   c. not contain the user name or any given or surnames of the user.

2. Where passwords are implemented by other organizations and resulting electronic assertions are used for interaction with the BC government, the password SHOULD be composed according to the above requirements. Where the password is not composed according to the above requirements, at a minimum, the password MUST be composed as follows:
   a. contain a minimum of 8 characters; and,
   b. require some form of strong or complex password rule, similar to the above.

4.3 Password Data Management Requirements for Level 1 - Low

When implementing a credential service that stores and manages passwords at the low credential strength level (Level 1), the following standard describes security controls about storing and managing the password data.

1. Password data and management functions MUST be protected by access controls that limit access to administrators and only those applications that require access.

2. Password data MUST NOT be stored in plaintext. It can use either of the storage methods described in higher levels, or a reasonably similar approach.

4.4 Password Data Management Requirements for Level 2 – Medium

When implementing a credential service that stores and manages passwords or use at medium credential strength level (Level 2), the following standard describes security controls about storing and managing the password data.

1. Encryption keys, password data and management functions MUST be protected by access controls that limit access to administrators and only those applications that require access.

2. Password data submitted by the user MUST only be revealed to authentication services or through authentication protocols that are authorized by the credential service. Relying party applications MUST NOT prompt the user to enter their password there.

3. Password data MUST NOT be stored in plaintext; each password MUST be protected individually with either of the following methods:
    a. concatenate the password to a salt or nonce and/or username, then hash with a BC government-approved hash algorithm. The hashed password is then stored.
    b. encrypt the password with a BC government-approved keyed encryption algorithm. The encrypted password is then stored.

    Refer to the government's *Cryptographic Standards for Information Protection* for detailed guidance on approved techniques and algorithms for cryptography. That standard states that:
    o   the encryption algorithm MUST be Advanced Encryption Standard (AES) with a key length of 256 bits.

4.5 Password Data Management Requirements for Level 3 to 4 – High to Very High

When implementing a credential service that stores and manages passwords for use at high or very high credential strength levels (Levels 3 and 4), the following standard describes security controls about storing and managing the password data and encryption keys.

1. Encryption keys, password data and management functions MUST be protected by access controls that limit access to administrators and only those applications that require access.

2. Password data submitted by the user MUST only be revealed to authentication services or through authentication protocols that are authorized by the credential service. Relying party applications MUST NOT prompt the user to provide their password to it.

3. Where password data is stored, it MUST NOT be stored in plaintext; it MUST be encrypted with a BC government-approved keyed encryption algorithm, as described in the previous section.

4. The encryption key for storing password data MUST be encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module.

5. Passwords used to access private keys in hardware-based cryptographic tokens MUST be held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module. Passwords MUST NOT be exportable in plaintext from the module.

5 Electronic Authentication Standard

This standard sets out the technology requirements for the authentication mechanisms and protocols that are acceptable at each of the Authentication Levels described in section 2.5, and the security and technical features associated with them. The authentication mechanisms and protocols are used to verify the presented electronic credentials, and so their strength is directly related to the types of electronic credentials described in the *Electronic Credential Technology Standard* in section 3.

5.1 Electronic Authentication Requirements for Level 1 – Low

When implementing an authentication mechanism to verify a low strength credential, the following standard describes the authentication protocol and/or security features that MUST be met. The purpose of the authentication is to provide some assurance that the same user is accessing the protected resource each time.

1. The authentication protocol MUST prove that the user controls (has possession of) the credential.

2. The authentication protocol MUST NOT send passwords across a network in plaintext. The protocol is not required to use cryptographic controls, and the protocol is not required to prevent against eavesdropper attacks.

5.2 Electronic Authentication Requirements for Level 2 – Medium

When implementing an authentication mechanism to verify a medium strength credential, the following standard describes the authentication protocol and/or security features that MUST be met. The purpose of the authentication is to bind to the identity of the individual that the credential was issued to.

1. The authentication protocol MUST prove that the user controls (has possession of) the credential. As described in the *Electronic Credential Technology Standard* in section 3, the electronic credential uses one of the following:
    a. a password, or
    b. an assertion from another authentication service.

2. The authentication protocol MUST be capable of protecting against compromise from the following types of attacks:
    a. eavesdropper attacks, through the use of cryptographic controls, for example through an encrypted communication session using Transport Layer Security (TLS);
    b. replay attacks; and,

c. online guessing attacks, through limiting the number of unsuccessful authentication attempts and/or controlling the rate at which attempts can be carried out. This MAY include locking or suspending a credential for a period of time after a number of unsuccessful attempts.

Note that online guessing attacks are also reduced by requiring strong passwords.

3. The authentication service MUST check to ensure that the presented electronic credentials are valid, and have not been revoked. This SHOULD be done by checking the status of a user's account or using a validation mechanism listed in Level 3 (High).

4. If the authentication service is not able to authenticate the user, it MUST reject the request and SHOULD communicate this to the Relying Party.

5. When authenticating with a password, the password MUST NOT be revealed to any party except the authentication service, authorized by the credential service.

5.3 Electronic Authentication Requirements for Level 3 – High

When implementing an authentication mechanism to verify a high strength credential, the following standard describes the authentication protocol and/or security features that MUST be met. The purpose of the authentication is to bind to the identity of the individual that the credential was issued to.

1. The authentication protocol MUST prove that the user controls (has possession of) the credential. As described in the *Electronic Credential Technology Standard* in section 3, the electronic credential uses one of the following:
   a. a software-based cryptographic token;
   b. a hardware-based cryptographic token;
   c. a one-time password device token; or,
   d. an assertion from another authentication service.

2. The authentication protocol MUST be capable of protecting against compromise in the same manner as described above for medium strength credentials (Level 2), plus:
   d. verifier impersonation attacks, by requiring the authentication service to be authenticated by the client; and,
   e. man-in-the-middle attacks, by requiring the authentication service and client to be authenticated to each other such that it prevents a third party from being undetected; and,

f.   hijacking attacks, by requiring the authentication to be bound to the transfer of messages such that it prevents a third party that alters the contents of messages from being undetected.

3.   The authentication service MUST check to ensure that the presented electronic credentials are valid, and have not been revoked. This SHOULD be done by checking the status of a credential against a revocation list or using a validation service, or using credentials with known short lifetimes (for example, one-time password tokens).

4.   If the authentication service is not able to authenticate the user, it MUST reject the request and SHOULD communicate this to the Relying Party.

5.   When authenticating with a password, the password MUST NOT be revealed to any party except the authentication service, authorized by the credential service.

5.4 Electronic Authentication Requirements for Level 4 – Very High

When implementing an authentication mechanism to verify a very high strength credential, the following standard describes the authentication protocol and/or security features that MUST be met. The purpose of the authentication is to bind to the identity of the individual that the credential was issued to.

1.   The authentication protocol MUST prove that the user controls (has possession of) the credential. As described in the *Electronic Credential Technology Standard* in section 3, the electronic credential MUST use a hardware-based cryptographic token.

2.   The authentication protocol MUST be capable of protecting against compromise in the same manner as described for high strength credentials (Level 3).

3.   The authentication service MUST check to ensure that the presented electronic credentials are valid, and have not been revoked. This SHOULD be done by checking the status of a credential against a revocation list or using a validation service.

4.   If the authentication service is not able to authenticate the user, it MUST reject the request and SHOULD communicate this to the Relying Party.

6 Electronic Assertion Standard

This standard sets out the technology requirements for the assertion mechanisms and protocols that are acceptable at each of the Authentication Levels describe in section 2.5, and the security and technical features associated with them. The assertion mechanisms and protocols are used to communicate the results of an authentication event to a information system or application (relying party). An example of an assertion is a security token, such as a SAML token.

6.1 Electronic Assertion Requirements for Level 1 – Low

When implementing an assertion mechanism to communicate the results of an authentication event, the following standard describes the assertion mechanism and/or security features that MUST be met.

1. The assertion mechanism MAY be the same or weaker than the requirement for level 2 or higher.

6.2 Electronic Assertion Requirements for Level 2 to 4 – Medium to Very High

When implementing an assertion mechanism to communicate the results of an authentication event, the following standard describes the assertion mechanism and/or security features that MUST be met.

1. The authentication service MUST produce assertions that are either
   a. digitally signed by the authentication service; or,
   b. obtained by the relying party directly from the authentication service using a secure communication protocol (for example, Transport Layer Security (TLS)) that authenticates the service to the relying party and protects the assertion.

2. Where an assertion relates to a medium strength authentication event (Level 2), the authentication service MUST set the assertion to expire after 12 hours.

3. Where an assertion relates to a high or very high strength authentication event (Level 3 or 4), the authentication service MUST set the assertion to expire after 2 hours.

4. Where an assertion relates to a very high strength authentication event (Level 4), the authentication service MUST ensure that sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

7 Electronic Credential Lifecycle Management Standard

This standard sets the process requirements for the lifecycle management of electronic credentials that are acceptable at each of the Credential Strength Levels described in section 2.4.

The credential lifecycle management requirements include:

1. Unique Identity Requirements: These include requirements linking credentials uniquely to individuals who have been through registration and identity proofing processes.

2. Credential Creation Requirements: These include requirements for creating unique credentials.

3. Cryptographic Key Generation Requirements: These include requirements for generating cryptographic keys for those electronic credentials that use them.

4. Credential Delivery Requirements: These include requirements for how to deliver credentials to the individual.

5. Credential Renewal and Replacement Requirements: These include requirements for how credentials can be changed, such as password resets.

6. Credential Revocation Requirements: These include requirements for how credentials can be revoked, and when revocations need to take effect.

7. Credential Deactivation Requirements: These include requirements for how credentials can be deactivated, and when unused credentials need to be deactivated.

8. Credential Status Requirements: These include requirements for how the status of credentials are maintained.

9. Credential Policy and Practice Statement Requirements: These include requirements for how a credential service describes its service to its users.

10. Credential Records Management Requirements: These include requirements for the records about credential issuance, changes and revocation.

7.1 Unique Identity Requirements (All Levels)

When issuing and managing credentials at any level, the following standard describes the requirements for uniquely linking to the individual's identity.

1. Before a credential service creates a credential, it MUST ensure that the individual being issued the credential was registered and identity proofed to the specific Identification Level by using the evidence of identity processes described in the *Evidence of Identity Standard*.

    When the required Identification Level is Level 1 (Low), there is no requirement for identity proofing.

2. Before a credential service creates a credential, it MUST ensure that the identity (whether pseudonymous or not) of the individual being issued the credential is unique within the service's community of subjects, including identities previously issued and that are now deactivated.

    This is intended to prevent a new identity from inadvertently inheriting a previously assigned identity's access at a relying party.

3. A credential service MUST include identifying information in the electronic credential that permits the recovery of records of the registered identity of the individual that was issued the credential.

4. Given the issuer and the identifying information in the credential, an identity registration service and credential service MUST be able and prepared to recover the records of the registration and identity proofing process.

5. A credential service 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.

7.2 Credential Creation Requirements (All Levels)

When issuing credentials at any level, the following standard describes the requirements for creating credentials for individuals.

1. The credential service MUST have a process in place for creating credentials, subject to the identification and linking to an identity (whether pseudonymous or not).

2. The credential service MUST ensure that the credential is uniquely assigned to an identity.

3. The credential service MUST ensure that the credential is unique, including credentials previously issued and that are now deactivated.

   This is intended to prevent a new credential from inadvertently inheriting a previously assigned identity's access at a relying party.

4. Requests for creating credentials MUST be verified to have come from authorized personnel.

7.3 Cryptographic Key Generation (Levels 3 or 4)

When issuing credentials at Level 3 or 4 that involve cryptographic keys, the following standard describes the requirements for generating those keys.

1. Where a credential service uses cryptographic keys within the electronic credentials (Level 3 or 4) or for the encryption of password data, the cryptographic keys MUST be generated using a BC government-approved key generation algorithm with an approved key length.

   Refer to the government's *Cryptographic Standards for Information Protection* for detailed guidance on approved techniques and algorithms for cryptography. This standard states that:
   - X.509 certificates MUST use public keys based on the RSA algorithm; and,
   - The minimum RSA key length MUST be 1024 bits.

2. Where a certificate service generates the cryptographic key pair, it MUST use a key generation process that binds the keys to the certificate generation, and maintains the secrecy of the private key.

3. Where a certificate service generates the cryptographic private key on behalf of the user, it MUST store the private key in a secure manner until delivery and acceptance by the user.

7.4 Credential Delivery Requirements (All Levels)

When issuing credentials at any level, the following standard describes the requirements for delivering a credential to the individual that was identified to be the user.

1. For contact purposes and/or the delivery of electronic credentials and notifications, the organization MAY require the individual to provide an email address.

2. Where a credential needs to be delivered (e.g. an initial password, one-time password device or cryptographic token device), a credential service MUST have a process in place for delivering credentials in a secure manner to the individual that was identified to be the user of the credential. This includes ensuring the secrecy of passwords and private keys that accompany the credential.

3. A credential service MUST notify the individual that a credential was issued to them, and do so separately from the delivery of the credential.

4. When a credential service issues a credential at Level 2 (Medium) or higher, it SHOULD notify the individual in such a way as to confirm the individual's contact information by:
   a. Sending notice to the individual using their provided contact information confirmed during identity proofing, or
   b. Issuing the credential in a manner that confirms the supplied contact information.

2. When a credential service issues a credential at Level 3 or 4 (High or Very High), it MUST receive acknowledgement from the individual that the credential was received before it is activated and its status is published.

7.5 Credential Renewal and Replacement (All Levels)

When managing credentials at any level, the following standard describes the requirements for allowing changes to a credential.

1. The credential service MUST have a process in place for renewing credentials and replacing lost or damaged credentials, subject to reconfirmation of the individual's identity information.

2. Requests for renewing credentials or replacing lost or damaged credentials MUST be verified to have come from the individual linked to the credential at the same identification level as the original credential issuance.

3. A credential service MUST permit individuals to change their passwords, including those used at Level 3 (High) or higher to activate their credential (such as software or hardware-based cryptographic token).

4. When an individual requests to change their password associated with Credential Strength Level 1 or 2 (Low or Medium), the credential service MAY leverage knowledge-based authentication (predetermined questions/answers or knowledge of past file history) or comparable approaches to link the identity of the individual to the credential.

7.6 Credential Revocation Requirements (All Levels)

When managing credentials at any level, the following standard describes the requirements for revoking a credential.

1. The credential service MUST have a process in place for revoking credentials.

2. A credential service MUST revoke credentials and tokens, such that they can no longer be used to authenticate successfully, after:

a. receiving a valid request to revoke,

b. being notified that a credential is no longer valid, or

c. being notified that a credential is compromised.

3. Requests and notifications for revoking credentials MUST be verified to have come from authenticated and authorized personnel.

4. When a credential service needs to revoke a credential at Level 2 (Medium), it MUST revoke the credential within 72 hours of receiving the request or notification.

5. When a credential service needs to revoke a credential at Level 3 or 4 (High or Very High), it MUST revoke credentials within 24 hours of receiving the request or notification.

6. Where a credential service uses passwords as electronic credentials, it MUST revoke the credential by deactivating the use of the password.

7.7 Credential Deactivation (All Levels)

When managing credentials at any level, the following standard describes the requirements for deactivating a credential.

1. The credential service MUST have a process in place for suspending or deactivating credentials where there is suspicion of misuse, where the individual has failed to comply with one or more of the Terms of Use, or when the credential has been unused for authentication after a period of time.

2. Requests for deactivating credentials MUST be verified to have come from authorized personnel.

3. When a credential at Level 2 (Medium) has not been successfully used for authentication during a period of 18 months, the credential service MUST deactivate a credential.

4. When a credential at Level 3 or 4 (High or Very High) has not been successfully used for authentication during a period of 6 months, the credential service MUST deactivate a credential.

7.8 Credential Status Requirements (All Levels)

When issuing and managing credentials at any level, the following standard describes the requirements for maintaining the status of a credential (e.g. active, deactivated, revoked).

1. The credential service MUST have a process in place for maintaining the status of all credentials issued.

2. Where a credential service issues electronic credentials that use a software-based and hardware-based cryptographic token, it MUST provide a secure mechanism, such as a digitally signed revocation list or a validation service provided with a secure communication protocol, to allow an authentication service to check that the credentials are still valid at the time of the authentication event.

7.9 Credential Policy and Practice Statement (All Levels)

When issuing and managing credentials at any level, the following standard describes the requirements for a credential service to describe its service to its users.

1. A credential service MUST publish its policies and practices for issuing and managing its credentials. At a minimum, the policies and practices MUST specify:
   a. how individuals subscribe to the service and apply for credentials;
   b. how an individual's identity is linked to the credential and how it may need to be re-proven;
   c. how credentials are delivered to individuals, and how individuals acknowledge receipt of them, and what obligations they accept in doing so;
   d. how credentials are renewed, replaced, revoked, suspended, and deactivated including how requests are authenticated and authorized;
   e. the response time for a revocation request and approach to publication of the status of credentials; and,
   f. how an individual terminates their subscription and credential.

2. Where the credential service issues and manages electronic credentials at Level 4 (Very High), it MUST publish its certificate policies and practices in reasonable alignment with IETF RFC 3647 in content and scope.

7.10 Credential Management Record Requirements (All Levels)

When issuing and managing credentials at any level, the following standard describes the requirements for records about credential issuance, changes and revocation.

1. A credential service and authentication service MUST produce auditable records (logs) of all events that are pertinent to the correct and secure operation of the service.

2. The credential service MUST retain records of the issuance, changes, and revocation of credentials that it manages. At a minimum, records MUST include:
   a. the individual's identity information and identity context (i.e. individual, employee or representative of an organization, professional), or a reference to it through an identity registration service;
   b. the individual's acceptance of Terms of Use agreements;
   c. contact information for related contact purposes and/or the delivery of credentials and notifications;

     d.   the date and time of the issuance, change or revocation;

     e.   where applicable, the name of the individual performing the action on behalf of the credential service;

     f.   where the records are about revocation, the authority of the individual to revoke and the reason for the revocation.

3.   Where the credential service manages credentials at Level 3 or 4 (High or Very High), records MUST also include:

     a.   evidence of generation of the individual's keys and certificate;

     b.   evidence of dissemination of the individual's certificate; and,

     c.   any revocation or suspension associated with the individual's certificate, including the information about the identity of the individual requesting it and their authorization to do so.

4.   The credential service MUST retain, securely, the records of the credential management processes for the duration of the individual's account plus 7.5 years.

5.   Electronic records of the credential management processes 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.

8 Operational Diligence and Service Standard

This standard applies to organizations that provide either a credential service that issues and manages electronic credentials, or an authentication service that verifies electronic credentials.

This standard sets the requirements for the overall operating environment in which the credential lifecycle management and authentication processes are conducted. This standard refers to other documents where policies and standards are documented.

The operational diligence requirements include:

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

2. Service Design Requirements: These include good practice requirements for credential and authentication services.

3. User Agreements and 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.

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

8.1 Legal Compliance

1. The organization MUST 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.

8.2 Service Design Requirements

The organization SHOULD implement credential technology, management processes and services that not only meet relevant Identity Assurance Levels but also incorporate good practice requirements in each of the following operational aspects:

8.2.1 Acceptability

1. The credential technology, management processes and services 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.

8.2.2 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. (See section 8.6)

8.2.3 Affordability, reliability and timeliness

1. The credential technology, management processes and services SHOULD be affordable and reliable and should not create unnecessary delays for either individuals or government organizations.

2. Credential and authentication services that are relied on by other organizations or services (relying parties) MUST be available at least 99%, including the credential validation service.

3. The credential and authentication services that are relied on by other organizations or services (relying parties) MUST have a help desk that is available for inquiries and incident management.

8.2.4 Complaints handling

1. The credential management processes and services MUST include a process for handling questions, concerns and complaints related to the collection, verification and use of identity information.

8.2.5 Fraud and Incident Management

1. The credential management processes and services MUST include fraud and incident management processes.
2. 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 focus toward risk assessment, mitigation and fraud detection.
        ii. Reactive activities would address investigation of, and response to, actual cases of fraud.

8.3 User Agreements and Notification Requirements

8.3.1 User Agreements

1. The organization MUST have a Terms of Use agreement with those that subscribe to the credential service. It MUST include any conditions that apply to the use of the credential.

2. The organization MUST inform and require the user to accept the Terms of Use agreement before issuing the credential. They MUST also inform and require acceptance of any changes to the Terms of Use.

3. The organization MUST keep a record of the individual's acceptance of the Terms of Use agreement.

8.3.2 Notifications

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

2. The organization MUST inform individuals of who within the organization can answer their questions about their identity, contact information, and use of their credential.

8.4 Identity Lifecycle Processes

1. Organizations that conduct registration and identity proofing processes in support of their credential management processes and services MUST follow standards set out in the *Evidence of Identity Standard*.

2. Organizations that rely on other organizations for conducting registration and identity proofing processes MUST include the following lifecycle processes into their service:

8.4.1 Correction or Change to Identity Information

1. The 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 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 during 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.

8.4.2   Reconfirmation of Identity

1. For Identification Level 2 (Medium), the 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.
2. For Identification Level 3 (High) and Identification Level 4 (Very High), the organization MUST reconfirm an individual's identity information at least every five years.

   a. 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.

3. For all Identification Levels, the organization MUST reconfirm an individual's identity if discrepancies arise or the service increases its evidence of identity requirements.

8.4.3   Flagging and Deletion

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

2. Where there is an unresolved discrepancy or incident of suspected fraud associated with an individual's identity information, their 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.

3.   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 an 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.

8.5 Personnel and Contractor Requirements

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

8.5.1 Personnel Training

1.   The organization MUST 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.   The organization MUST ensure that employees and contracted personnel that perform functions to support credential management processes and services:

    a.   have training in managing credentials;

    b.   have the tools and resources they need to securely manage credentials; and,

    c.   have training in how to handle discrepancies and suspicious behavior during the credential management processes.

3.   The organization MUST have sufficient staff to operate the service according to its policies and procedures**.**

8.5.2 External Service Providers

1. Where the 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 organization MUST:

   a. 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.

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

8.6 Security Requirements

The organization MUST comply with the following security requirements:

8.6.1 Security Policies and Procedures

1. If the organization is a BC government ministry or central agency, it MUST comply with the government's Information Security Policy.

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

   a. Comply with the BC 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.

8.6.2 Security Methodologies and Controls

The 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.

8.6.3 Information Security Management

The 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.

8.6.4 Organizational (Internal) Controls

The 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.

8.6.5 Secure Communications

1. The organization MUST ensure that electronic communications with other organizations that happen over a public or unsecured network use a secure communication protocol that authenticated both systems and uses encryption. In particular, this applies to identity registration services, credential services and authentication services that are operated across separate organizations or networks.

2. The organization MUST ensure that:

a. access to shared secrets and passwords shall be subject to 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 authorized agents of an organization.

APPENDIX A – TERMS AND DEFINITIONS

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

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

Term	Definition
AES	Advanced Encryption Standard. A specific encryption algorithm that is currently adopted as the industry and government standard. Refer to FIPS 197 for more information.
Assertion	A message from an authentication service sent to a relying party that communicates the result of an authentication and typically contains identity related attributes about the user.
Authentication	The process by which an individual or system's identity is determined by another by verifying the presented credentials.
Authentication Level	Relative measure (i.e. low, medium, high, very high) of the strength of an authentication event.
Authoritative Party	An organization (or person) 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.
Biometric	Physiological or behavioural 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).
Certificate Revocation List (CRL)	A list of revoked digital certificates that is used by an authentication service to check that a credential is still valid.
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 (over its lifecycle) that asserts identity attributes or privileges associated with an individual.
Credential Strength	A measure of the ability of the credential to withstand attack or

Term	Definition
	compromise.
Credential Strength Level	Relative measure (i.e. low, medium, high, very high) of the strength that can be placed in a credential.
Cryptographic Module	A software, firmware or hardware component that performs the cryptographic (e.g. encryption, key generation) functions.
Cryptographic Token	A software component or hardware-based device that the user possesses or controls for which the secret is a cryptographic key.
Digital Certificate	An electronic credential that binds the identity of a user, organization or computer to their public key.
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.
FIPS	Federal Information Processing Standards. A set of standards developed by the US federal government for use by their agencies, and adopted by the industry.
Hash	A computation performed on a piece of data to encode it for security purposes.
Identification Level	Relative measure (i.e. low, medium, high, very high) of the strength associated with an identification process.
Identity Assurance	A measure of confidence that an identity claims 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.
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
Nonce	A number used only once and never re-used with the same key, typically used in a security-related algorithm.
Password Authentication	The use of a password (a character string) known only by the user to verify an individual's identity.
PIN	Personal Identification Number. A numeric password.
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

Term	Definition
Public Key	The public part of an asymmetric key pair that is typically used to verify digital signatures or encrypt data.
Public Key Infrastructure (PKI)	A set of technology and processes used to manage public keys embedded in digital certificates.
Relying Party	A service that requests claims about users from one or more Authoritative Parties so that it can apply its own security or access control policies to determine whether to allow the user access to a resource or service.
Revocation List	A list of revoked credentials that is used by an authentication service to check that a credential is still valid. See Certificate Revocation List.
Revoke	To cancel or deactivate a credential and invalidate its use.
Salt	A value that is used in a security-related algorithm to ensure that the result for one instance cannot be re-used by an attacker.
SAML	Security Assertion Markup Language. An XML-based standard for exchanging authentication and authorization data between security domains.
SAML Token	A package of data that contains claims (or assertions) that follows the SAML XML format.
Security Token	A package of data that contains claims that is typically digitally signed and encrypted to ensure security. It is used to prove identity to obtain access to information or a service.
Smart Card	A high strength credential with an embedded chip that can be used for authentication.
SSL	Secure Sockets Layer. A communications protocol that uses digital certificates to provide security for messages sent over the internet. SSL is the predecessor of TLS.
TLS	Transport Layer Security. A communications protocol that uses digital certificates to provide security for messages sent over the internet. TLS is the successor of SSL.
X.509 Certificate	A structure and format standard for digital certificate documents based on public key infrastructure. The digital certificate binds a public key with a set of attributes about the certificate and identity of the subject of the certificate.