Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Better government: with partners, for Canadians

Guideline on Identity Assurance
FINAL DRAFT FOR CONSULTATION

Chief Information Officer Branch
Security and Identity Management Division

October 1, 2013

GCDOCS# 4549339

Canada

Document Revision History

Version	Description of Change	Author(s)	Date
Consultation Draft April 25, 2013	Applied new template – minor pagination edits; no content change	Tim Bouma, TBS-CIOB	22 May 2013
Working Group Final Draft	Incorporated comments and feedback	Tim Bouma, TBS-CIOB	15 July 2013
Working Group Final Draft	Feedback from Working Group meeting on July 18, 2013	Tim Bouma, TBS-CIOB	30 July 2013
English Edit	English Editing – filed under new GCDOCS # 4549339	Tim Bouma, TBS-CIOB	25 Sept 2013
Final Consultation Draft	Incorporated feedback from working group meeting on Sept 26, 2013	Tim Bouma, TBS-CIOB	1 Oct 2013

Table of Contents

List of Tables

List of Figures

1. Purpose

The purpose of the Guideline on Identity Assurance is to support implementation of the minimum requirements for establishing an identity assurance level for an individual, as specified in subsection 6.1.4 and Appendix C of the *Standard on Identity and Credential Assurance*. This standard is issued under the *Policy on Government Security* and the *Directive on Identity Management*.

This guideline is intended to be used in conjunction with the *Guideline on Defining Authentication Requirements*, which provides government organizations with an assessment framework for determining their identity assurance level requirements. It may also be used to support security checks related to identity, specified in the Standard on Security Screening of Individuals (currently in draft). This standard defines the requirements for Government of Canada security screening practices.

For requirements related to security and IT design, organizations may wish to consult two publications from Communications Security Establishment Canada: ITSC-31, *User Authentication Guidance for IT Systems* and ITGS-33, *IT Security Risk Management: A Lifecycle Approach*.

1.1 Audience

This guideline is intended for the following users:

- **Program and service delivery managers**, who are responsible for identifying Government of Canada clients (individuals and businesses), employees and contractors as a critical part of their program or service delivery requirements; and

- **Security practitioners,** who recommend, design, build or provide solutions for meeting program requirements.

1.2 Application

In accordance with the *Directive on Identity Management*, the Guideline on Identity Assurance is intended to apply when there is a requirement to uniquely identify individuals, organizations or devices for the purposes of carrying out a program activity, service or transaction. This includes internal services for employees and external services for Government of Canada clients.

The focus of the guideline is on establishing the identity assurance level required for individuals. However, the principles and guidance discussed here can be applied to devices and organizations. Guidelines specific to devices and organizations will be provided in a later revision of this document or in a separate guideline.

This guideline assists in standardizing how the identities of individuals are established in relation to government programs and services. It is intended to promote consistent identity assurance practices, while enabling government organizations to remain flexible for innovation and appropriate risk management. The guideline is also intended to assist in the transition toward a federated approach to identity.

*Management of the relationships between individuals, organizations and devices is outside the sc*ope of this guideline. It is acknowledged that relationships exist between individuals, organizations and devices for the purposes of granting authority or permission to act on behalf of others, and examples of these relationships are provided. However, these examples are not to be construed as guidance.

This guideline does not apply to decisions about access, authorization or entitlement. It is not applicable when there is no requirement to uniquely identify individuals for the purposes of administering a federal program or service.

This guideline does not recommend specific technologies, architectures or solutions, nor does it recommend the use of specific documents or document authentication techniques. It does not confer authority beyond what is prescribed in the Standard on Identity and Credential Assurance.

2. Context and Background

2.1 Introduction

Identity is at the core of most government business processes involving valuable resources and sensitive personal information. Once identity is established, all subsequent government activities, ranging from providing services to granting benefits and status, rely on the accuracy and rightful use of identity. For many service encounters or client transactions, government organizations must ensure that they correctly establish identity—that they are dealing with the right person, organization or device—to be able to meet and fulfill their program objectives.

In Canada, unlike many other nations, there exists no single document that has as its sole purpose that of identifying an individual. Instead, many documents are used. These documents, along with their authoritative sources enabled by federal, provincial and territorial Acts and regulations, are recognized across different jurisdictions and include vital events, benefits administration, taxation, legal status and entitlements that relate to the individual bearing the document. The Canadian system has a number of benefits, especially from a privacy perspective; however, it presents challenges in providing seamless services across jurisdictions and in combatting fraudulent activity.

In this context, the Government of Canada has taken a whole-of-government, federating approach to managing identity assurance, which respects the autonomy and the laws of the different jurisdictions in Canada and internationally. This approach enables departments and agencies to fulfill program and service requirements by relying on identity assurance processes that have been carried out by other organizations.

The Government of Canada's approach is not about prescribing a solution; rather, it is founded on defining a few appropriate instruments that enable government organizations to respond to the changing technology landscape and take advantage of innovation. Because of the complexity of the environment, an important aspect of this approach is that it is phased and incremental. This means that it is gradual enough to allow for application of lessons learned and changes in the environment when necessary.

Today, physical documents are still the predominant method of presenting evidence of identity. However, as digital delivery methods become more trustworthy and secure, electronic evidence of identity will also be required. More and more clients are demanding electronic authentication, and governments recognize its potential cost savings. As government services become electronically interconnected, identity and identity risk must be managed across organizational and jurisdictional boundaries. This can only be achieved through standardization and identity federation.

As organizations begin the implementation of the *Standard on Identity and Credential Assurance*, they are encouraged to think beyond document-based processes and specific technology implementations. They are also encouraged to standardize their practices and processes so that these can be extended beyond their own organization to enable participation in a broader identity federation.

For further description of the Government of Canada's approach to federating identity, please refer to *Federating Identity Management in the Government of Canada: A Backgrounder*.

2.2 Federation and Trust Frameworks

There is a business need to provide online services seamlessly across departmental and jurisdictional boundaries in a way that encompasses both public and private service providers. Fulfilling this need requires a level of trust between many organizations that have diverse mandates and act under different authorities. Well-defined arrangements, often referred to as "trust relationships," are needed between organizations to ensure confidence in each other's services and in the underlying business and technical processes.

A federation is a cooperative agreement between autonomous entities that have agreed to work together. The federation is supported by trust relationships and standards to support interoperability. A federation can consist of public and private sector organizations, different jurisdictions or different countries. Many federations today are informal in nature and are based upon shared practices and shared objectives that have been developed over time. However, as federations become more formalized, the informal arrangements are replaced by assessment processes, contractual agreements, service agreements, legal obligations and dispute resolution mechanisms.

Recently, these individual trust relationships are being organized into more encompassing schemes called "trust frameworks." Trust frameworks formally underpin trust relationships by stipulating adherence to standards, formalizing assessment processes and defining roles and responsibilities of multi-party arrangements. By adopting a trust framework (instead of each trust relationship individually), a federation ensures that its member participants have confidence in all other participants in the federation. A trust framework is usually governed as a whole by the members of a federation.

Presently, there are several formalized frameworks available and in use by industry (e.g., Kantara Initiative, Open Identity Exchange (OIX)).

Governments are beginning to formalize the adoption of trust frameworks. The US Federal Identity, Credential and Access Management Program (FICAM) has formalized a Trust Framework Provider Adoption Process (TFPAP). This process enables industry trust frameworks such as Kantara and OIX to be approved for government use.

The Government of Canada is currently formalizing a trust framework adoption process that will approve industry and public sector trust frameworks. It is important to understand that under this process, the *Standard on Identity and Credential Assurance* as well as this guideline will be an integral part of a trust framework and the associated adoption processes. Government organizations can be assured that the standard and its implementation are designed to support existing and emerging trust frameworks.

2.3 Identity and Credential Assurance

The *Standard on Identity and Credential Assurance* makes a distinction between identity assurance and credential assurance. This distinction or separation of two areas of assurance is necessary to enable government organizations to integrate into a federation using a phased incremental approach and to comply with privacy and program legislation requirements.

2.3.1 Credential Risk and Credential Assurance

"Credential assurance," as defined in the *Standard on Identity and Credential Assurance*, is a measure of certainty that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, modified). "Credential risk" is the risk that an individual, organization or device has lost control over the credential that has been issued to him or her, or that the credential itself has been otherwise compromised.[1]

Credential assurance answers the question "How sure are you that you have the **same** individual, organization or device?" before a service is delivered or a transaction is carried out. Credential assurance requirements are specified separately from identity assurance requirements so that it is possible to have the assurance of dealing with same individual without necessarily knowing their identity (e.g., online surveys completed over several days).

[1] *Standard on Identity and Credential Assurance*, subsection 3.5

Credential assurance can have different “credential assurance levels.” The use of standardized credential assurance levels has allowed for the implementation of commercially offered authentication services, currently available to government organizations:

- **Commercial broker service (CBS):** A commercial service provided by contract to the Government of Canada that enables clients to use external credentials they already have from other organizations (e.g., financial institutions) to access government services.

- **GCKey:** A Government of Canada–issued credential for use by clients who do not have a credential issued through the CBS, or who prefer to use a Government of Canada credential.

2.3.2 Identity Risk and Identity Assurance

“Identity assurance,” as defined in the *Standard on Identity and Credential Assurance*, is a measure of certainty (or level of confidence[2]) that an individual, organization or device is who or what it claims to be. “Identity risk” is the risk that an individual, organization or device is not who or what it claims to be.[3]

Before a service is delivered or a transaction is carried out, identity assurance answers the question “How sure are you that you have the **right** individual, organization or device?” As discussed in the previous section, it is useful to define or specify identity assurance requirements independently from credential assurance requirements.

Like credential assurance, identity assurance can have different “identity assurance levels.” The objective of a standardized identity assurance level is to manage identity risk to an acceptable level and to provide a standardized identity assurance service to other organizations that are relying parties within a federation.

Currently, there are no standardized identity assurance services in use by the Government of Canada. Over time, standardized identity assurance services will be developed and made available through federation.

Due to policy and legal requirements, the development of these services will be a complex undertaking, with services being implemented incrementally. Taking this into account, the requirements in Appendix C of the *Standard on Identity and Credential Assurance* have been stated in a manner that allows them to be implemented independently, before becoming part of a larger Government of Canada–wide service offering.

2.4 Managing Identity Risk

The objective of the *Standard on Identity and Credential Assurance* is to ensure that identity risk and credential risk are “managed consistently and collaboratively within the Government of Canada and with other jurisdictions and other industry sectors.”[4] Managing identity risk is an important step toward “federating identity,” that is, toward supporting the Government of Canada’s vision of enabling a federation of organizations that trust each other’s assurances of identity.

[2] The terms “measure of certainty,” “level of confidence” and “level of assurance” are used interchangeably throughout the *Standard on Identity and Credential Assurance* and this guideline. The reader should consider these terms as being equivalent.

[3] *Standard on Identity and Credential Assurance*, subsection 3.4

[4] *Standard on Identity and Credential Assurance*, subsection 5.1

This guideline focuses on managing identity risk for individuals. Managing identity risk is similar to managing other corporate or departmental risks; however, there are special considerations for identity risk that apply:

- **Identity risk is difficult to manage by one organization alone**. The factors for managing identity risk may be outside the organization's direct control. For example, a department may rely on documents to identify individuals, but it may not be able to discern if these documents are fraudulent or stolen.

- **Impacts of identity risk go beyond a single organization**. An error or fraudulent activity having a low impact in one organization may result in a higher impact in another organization. For example, a fraudulently issued document in one department may be used to gain significant benefits in another department.

There are many interrelated risk factors regarding the identity of individuals, including the following:

- **An individual is associated with the wrong identity information.** Two individuals may have identical names and dates of birth. The result is a possible confusion of services and entitlements.

- **Identity information is inaccurate or out of date.** Life events, such as marriage, may result in name changes. Data entry errors may result in transpositions of dates and names.

- **Identity information is asserted by parties that are not considered to be authoritative.** An individual, such as newcomer or visitor to Canada, may present identity information that may be accurate, but is impossible to validate against an authoritative source.

- **Identity information may be used by someone other than its rightful owner or authorized representative.** An individual is using the identity information of another individual. If this is intentional, it may be considered as identity fraud under the *Criminal Code*, section 403(1).

- **False documents may be used to substantiate identity.** An individual may use or modify a copy of a birth certificate that was originally issued to another person and claim the identity.

- **Documentation may be lacking.** An individual may not have documents that can be determined as being genuine or that can be validated against an authoritative source.

2.4.1 Credential Risk in Relation to Identity Risk

Credential risk has been separated from identity risk. While not the focus of this guideline, credential risk is discussed to assist the reader in understanding how it is different from and related to identity risk.

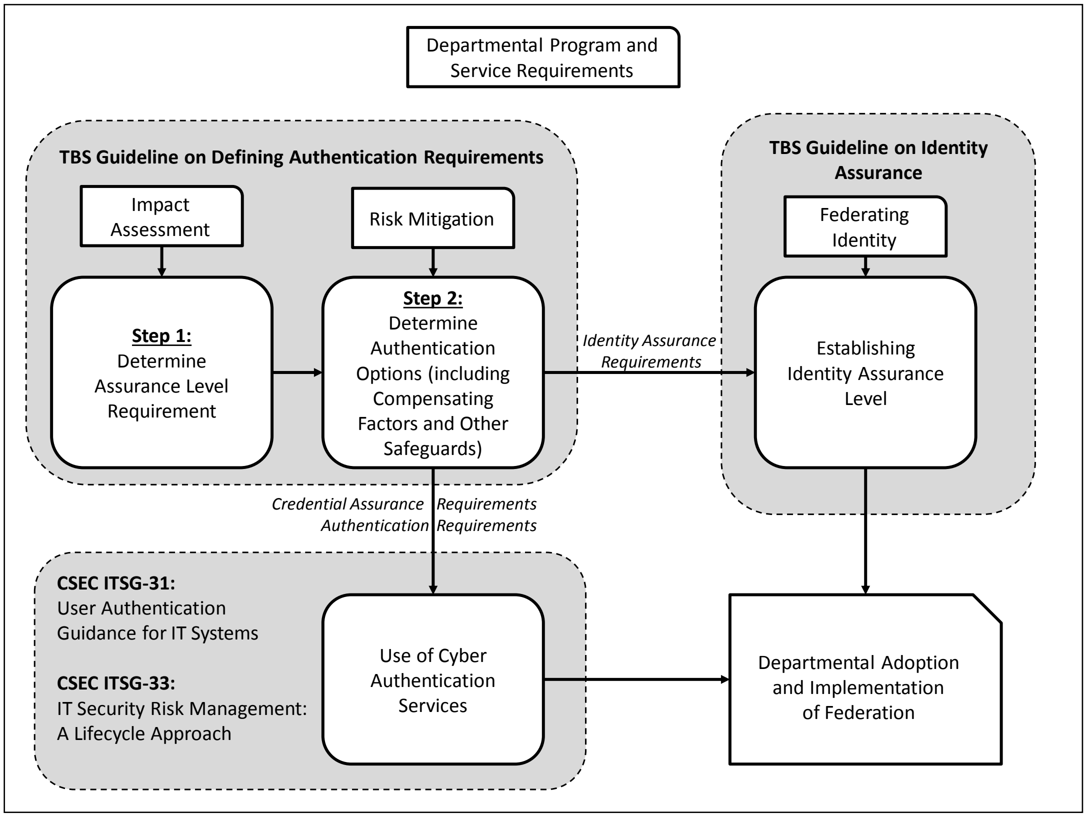
Credential risk is the risk that an individual, organization or device has lost control over the credential that has been issued. When a service or program does not require the identity of a client or party (i.e., the service is anonymous or pseudonymous), credential risk may be limited to the direct impact on the program or service relying on the credential.

When the identity of a client or party is required (i.e. identity information), government organizations are advised to consider identity risk as the predominant risk. Credential risk should be viewed as a sub-component of identity risk, because the potential theft or misuse of a credential (i.e., credential risk) is often a direct contributing factor to identity risk.

2.5 Assurance Level Assessment

Figure 1 illustrates the related use of the Treasury Board guidelines and the Communications Security Establishment Canada (CSEC) IT Security Guidance (ITSG) guidelines in the assurance level assessment and the IT design process.

Figure 1. Related Government of Canada Guidelines


Departmental Program and Service Requirements
TBS Guideline on Defining Authentication Requirements
Impact Assessment
Risk Mitigation
Step 1: Determine Assurance Level Requirement
Step 2: Determine Authentication Options (including Compensating Factors and Other Safeguards)
Identity Assurance Requirements
TBS Guideline on Identity Assurance
Federating Identity
Establishing Identity Assurance Level
Credential Assurance Requirements
Authentication Requirements
CSEC ITSG-31: User Authentication Guidance for IT Systems
CSEC ITSG-33: IT Security Risk Management: A Lifecycle Approach
Use of Cyber Authentication Services
Departmental Adoption and Implementation of Federation

The Treasury Board's *Guideline on Defining Authentication Requirements* defines a two-step process that determines the following:

Step 1

- **Assurance level requirement:** The overall level of confidence required to carry out a program activity, service or transaction. The assurance level assessment is conducted using the worksheet in Appendix A of the *Guideline on Defining Authentication Requirements*.

Step 2

- **Identity assurance requirements**: The minimum requirements to establish the identity of an individual to a given level of assurance. The guidelines on implementing these requirements are set out in Section 3 of this document.

- **Credential assurance requirements:** The minimum requirements to ensure that an individual has maintained control over a credential that has been issued to him or her and that the credential has not been compromised. The guidelines on the implementation of these requirements are set out in CSEC's ITSG-31, *User Authentication Guidance for IT Systems*.

- **Authentication requirements:** The minimum technical design and/or business process requirements that are necessary to carry out an electronic or manual authentication process. The guidelines on the implementation of these requirements are set out in CSEC's ITSG-31and ITSG-33, *IT Security Risk Management: A Lifecycle Approach*.

The *Guideline on Defining Authentication Requirements* also provides recommendations on other mechanisms for mitigating risk:

- **Compensating factors:** Additional (i.e., non-standard) measures that can be used during the authentication process to reduce a risk. A compensating factor is intended to mitigate the residual risks or to counter new threat possibilities, whether anticipated or unanticipated. An example of a compensating factor is challenging an individual to answer additional questions when his or her credential is authenticated from a previously unknown device or location.

- **Other safeguards:** Other controls that exist within the larger system downstream from the authentication process. Other safeguards may be security control mechanisms used in a downstream process or "flags" that are raised to initiate exceptions or interventions.

It is recommended that government organizations be familiar with these related guidelines. Organizations are expected to complete the assurance level assessment process prior to implementing requirements set out in Section 3.

3. Implementing Standard Requirements for Identity Assurance

3.1 Overview of Assurance Level Requirements

Appendix C of the *Standard on Identity and Credential Assurance* specifies the four major categories of requirements that are used to establish an identity assurance level. The four categories are listed below with a control objective statement and a description:

1. **Uniqueness**. *An identity must be unique.*

   Uniqueness ensures that individuals can be distinguished from one another and, when required, uniquely identified.

2. **Evidence of identity.** *Evidence of identity must support the claims made by an individual.*

   Evidence of identity supports the integrity and accuracy of the claims made by an individual. The amount of evidence that is sufficient to confirm the accuracy of the identity information and its linkage to the individual depends on the assurance level requirement. The standard defines two categories of evidence of identity—foundational evidence of identity and supporting evidence of identity (see subsection 3.3.1 of this document).

3. **Accuracy of identity information**. *Identity information about an individual must be accurate, complete and up-to-date.*

   Accuracy ensures the quality of identity information. It ensures that the information represents what is true about the individual, and that it is as complete and up-to-date as necessary. Accuracy can be confirmed by using an authoritative source or by corroborating different sources of information (when no authoritative source is available).

4. **Linkage of identity information to the individual.** *Identity information must relate to the individual making the claim.*

   Linkage ensures that identity information relates to the individual making the claim, that it does not relate to another individual and that it reflects how the individual is known within a community or legally recognized within a jurisdiction.

Table 1, reproduced from Appendix C of the *Standard on Identity and Credential Assurance*, specifies the minimum requirements to establish each level of assurance for each category. Prior to implementing any requirements, government organizations are expected to complete an assurance level assessment to determine their overall assurance level requirement (see subsection 2.5 for details).

As federal organizations begin to implement the requirements, it is recommended that they take the following into consideration:

- The requirements are independent of the delivery channel and the technology used. This is to support the Government of Canada’s commitment to multi-channel access and service delivery.

- In implementing these requirements, it is a good practice to consider channel and service delivery alternatives that best suit the needs of clients, enable accessibility to a wide range of people with disabilities, and encourage adoption through trust and confidence.

- The requirements may be implemented in collaboration with other government organizations to support being “federation-ready” (as described in subsection 4.2, Federation Considerations).

Table 1. Minimum Requirements to Establish an Identity Assurance Level[5]

Requirement	Level 1	Level 2	Level 3	Level 4
Uniqueness	Define identity information Define context	Define identity information Define context	Define identity information Define context	Define identity information Define context
Evidence of Identity	No restriction on what is provided as evidence	**One** instance of evidence of identity	**Two** instances of evidence of identity (At least one must be foundational evidence of identity)	**Three** instances of evidence of identity (At least one must be foundational evidence of identity)
Accuracy of Identity Information	Acceptance of self-assertion of identity information by an individual	Identity information acceptably matches assertion by an individual and evidence of identity[6] **and** Confirmation that evidence of identity originates from appropriate authority	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **and** Confirmation of the foundational evidence of identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source **or** inspection by trained examiner	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **and** Confirmation of the foundational evidence of identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source **or** inspection by trained examiner
Linkage of Identity Information to Individual	No requirement	No requirement	At least **one** of the following: i. Knowledge-based confirmation ii. Biological or behavioural characteristic confirmation iii. Trusted referee confirmation iv. Physical possession confirmation	At least **three** of the following: i. Knowledge-based confirmation ii. Biological or behavioural characteristic confirmation iii. Trusted referee confirmation iv. Physical possession confirmation
Note 1: When the authoritative source is outside Canadian jurisdiction, the accuracy of identity information will be determined through a risk-managed approach.				

For further information on determining the overall assurance level requirement, please refer to the *Guideline on Defining Authentication Requirements*.

[5] This table is a replica of Appendix C in the Standard on Identity and Credential Assurance.

[6] Subsection 3.4 in this guideline provides guidance on determining the accuracy of identity information and on what is considered to be an acceptable match.

3.2 Uniqueness

3.2.1 Uniqueness

The uniqueness requirement is to ensure that individuals can be distinguished from one another and that the right service is delivered to the right individual. Uniqueness reduces the possibility of the wrong individual receiving a service or benefit (i.e., the service or benefit is intended for someone else).

Uniqueness does not determine eligibility or entitlement for a service or benefit. Information that is collected to determine uniqueness may be used for the purposes of eligibility or entitlement, but it is best to treat the collection purposes as separate.

Uniqueness is required when a service must deliver an output or benefit to a specific individual (e.g., the **same** individual as from a previous registration process). The identity of the individual may or may not be required or desired.

Services that do not require the identity of the individual are usually referred to as “anonymous” or “pseudonymous services,” such as the following:

- Confidential online surveys, where a specified population of individuals (e.g., employees) are asked to complete a survey only once. The identities of individuals are not known and cannot be linked to the completed surveys.

- An online discussion forum or a social media site where a user may choose a “handle” (i.e., a user ID) and engage in discussions without disclosing his or her identity. While the identity of the user may not be required, terms and conditions may stipulate the disclosure of certain identity information, which is not validated.

- An issuance of an electronic fare card that indicates the bearer of the card (or user of an electronic number) has paid for and is entitled to a specified number of trips. The identity of the user is not required.

In practice, the terms “anonymous” and “pseudonymous” are used interchangeably. An anonymous service does not name, identify or distinguish between its users. A pseudonymous service distinguishes between its users by employing a pseudonym or identifier. However, many pseudonymous services are considered to be anonymous because they maintain the anonymity of the user, either by not collecting identity information or by protecting identity information that has been collected.

The uniqueness requirement is fulfilled by defining or specifying the identity information needed to deliver a program or service and by defining the context of this program or service.

3.2.2 Identity Information

As per the *Directive on Identity Management*, government organizations are responsible for ensuring the legitimacy of identity under the following circumstances:

- Unique identification of an individual, organization or device is required for the purposes of administering a federal program or service enabled by legislation; and

- Disclosure of identity information by the individual, organization or device is required for receiving a government service, participating in a government program or becoming a member of a government organization.[7]

[7] *Directive on Identity Management*, subsection 3.5

“Identity” is defined in the *Standard on Identity and Credential Assurance* as “a reference or designation used to distinguish a unique and particular individual, organization or device.”[8]

A property or characteristic associated with an identifiable individual is typically referred to as an “identity attribute” or an “identity data element.” “Identity information” is understood to be the set of identity attributes that is:

- Sufficient to distinguish between different individuals; and
- Sufficient to recognize the individual, as required by the service or program.

The attribute or set of attributes that is used to uniquely distinguish a unique and particular individual, organization or device is called an “identifier.” It is best that identity attributes used as identifiers be constant over time. Since in many cases this is not possible, government organizations may choose instead to create or use an “assigned identifier.” This is typically a numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between individuals without the use of any other identity characteristics.

Other identity attributes, over and above those that are sufficient to establish identity information, may be used to assist in the recognition of an individual. These attributes may not necessarily be unique to the individual (e.g., hair colour) and may change over time.

Protecting Identity Information

Information about an identifiable individual is considered to be personal information; therefore, it is subject to the *Privacy Act.* Collecting, using, disclosing or disposing of identity information must be in accordance with the *Privacy Act* and departmental legislation. All identity information should be considered a subset of “personal information” as defined by the *Privacy Act*. Government organizations are advised to consult with legal counsel to ensure that their management of identity information is consistent with their enabling legislation.

The Treasury Board *Policy on Privacy Protection* applies to identity information. This includes the applicability of all related privacy directives, standards and guidelines. As such, government organizations are expected to identify, assess, monitor and mitigate any privacy risks involved in the creation, collection, use, retention, disclosure and disposal of identity information.

Identity information may be collected, used, retained, disclosed and disposed of as part of a larger business process, such as registration, enrolment or determination of entitlement. If the identity information is to be derived from existing program-specific information, government organizations need to ensure compliance with the *Policy on Privacy Protection*. This includes ensuring that the use of identity information is consistent with the original purpose(s) for which the information was obtained or compiled.

There are various means of protecting identity information, such as by separating records into different data repositories, encrypting data and substituting or mapping identifiers. Regardless of the mechanisms used, the resulting information should be considered as personal information.

Government organizations need to be familiar with and understand the potential applicability of the following sections in the *Criminal Code*, including its definitions of “identity documents” and “identity information” as they apply in the context of the Code:

- **Subsections 56.1(1)** and **(2)** regarding the use of identity documents relating to another person;
- **Subsection 56.1(3)** regarding the definition of identity document, as related to subsections 56.1(1) and (2);
- **Subsections 57(1)** to **(6)** regarding the use of the Canadian passport;

[8] *Standard on Identity and Credential Assurance*, Appendix A

- **Section 402.1** regarding the definition of identity information. Note that this is a narrower definition of identity information for the purposes of sections 402.2 and 403 in relation to identity theft and identity fraud only;
- **Section 402.2** regarding the wrongful possession of identity information (i.e., identity theft); and
- **Section 403** regarding fraudulent personation of another person.

Defining Identity Information

When defining or determining the sufficiency of the identity information for a given service delivery context or program administration requirement, government organizations need to distinguish between identity information and program-specific information, which can overlap. This is to ensure that the use of identity information is consistent with the original purpose for which the information was obtained and that it can be managed separately or additionally protected with security and privacy controls, such as stronger encryption.

Government organizations are advised to define identity information narrowly and to reduce the overlap between identity information and program-specific information as much as possible. When overlap occurs, it is a good practice to describe both purposes. For example, date of birth can be used for uniqueness (as identity information) and for age eligibility (as program-specific information).

The following considerations apply when defining identity information:

- An identifier may be a unique attribute assigned and managed by the program or service.
- Assigned identifiers may be kept internal to the program or service. Examples of internal identifiers are database unique keys and universally unique identifiers.
- Assigned identifiers may be provided to other programs; however, there may be restrictions due to privacy considerations or legislation.
- Existing or previously assigned identifiers may be used that meet uniqueness requirements. Government organizations need to be aware that these identifiers may have privacy or legal implications associated with this use.
- Certain identifiers may be subject to legal and policy restrictions. For example, the *Directive on Social Insurance Number* outlines specific restrictions on the collection, use, retention, disclosure and disposal of the social insurance number.
- Identity information that is intended to distinguish or recognize a real person is subject to accuracy of identity information requirements (see subsection 3.4).
- Examples of identity information include name, date of birth and sex for individuals; business registration numbers for organizations; and serial numbers and network identifiers for telecommunications and computing devices.
- For privacy and security reasons, such as protecting the identities of individuals, certain identity attributes may be pseudonymous or anonymous. Examples of pseudonymous or anonymous identity attributes are the persistent anonymous identifier (PAI) used in GCKey and CBS, screen names, handles and user IDs.
- To reduce the sensitivity of identity information, government organizations may decide to collect only portions of certain identity attributes, such as birth month plus last digit of birth year (instead of date of birth) or city of residence (instead of complete mailing address).

Table 2 provides options for the combination of identity attributes that can be used to distinguish a unique individual within a large population.[9] This table can be used as baseline in defining identity information requirements.

Table 2. Identity Attribute Combinations

Option	Identity Attribute Combinations
1)	• **Name:** Given name and surname • **Partial Current Address:** Postal code or city and province/territory • **Partial Date of Birth:** Month and day or year only
2)	• **Name:** Given name and surname • **Full Date of Birth**: Month, day, and year
3)	• **Name:** Given name and surname • **Place of Birth:** City or municipality • **Partial Date of Birth:** Month and day or year only

3.2.3 Context

Identity information is considered to be valid within a defined context. A context can be regarded as a set of circumstances, a situation or a scenario in which an individual interacts with other individuals or with an organization. For example, a context can be a public service delivery jurisdiction within which an individual accesses a range of services provided by one or several government organizations.

Within a given context, it is crucial to ensure that individuals can be distinguished from one another, or uniquely identified, so that services can be delivered to the right individuals.

Conversely, it is also important to understand the context in which an identity exists when relying upon an identity assurance. An identity assurance provided from a social networking context, for example, may not be appropriate in a public service delivery context.

In delivering their programs and services, government organizations operate within a certain environment or set of circumstances, which can be considered as the context of the identity. Context is additionally determined by factors including mandate, target population (i.e., clients) and other responsibilities prescribed by legislation or agreements.

Context may be considered from the perspective of the individual, the federal organization or the Government of Canada. A context may be specified or defined as the set of external services to citizens, for example, or the set of internal services to employees. A defined context should be distinct, but it may overlap with other contexts.

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

It is recommended that government organizations keep the following in mind when defining the context of a given program or service:

[9] This table is a subset of a table from the draft American National Standard for Proof and Verification of Personal Identity being developed by the North America Security Products Organization (NASPO). The terminology in the table has been adjusted for the Canadian context; therefore, the table may not apply to different populations.

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

3.3 Evidence of Identity

“Evidence of identity” is a record from an authoritative source that supports the integrity and accuracy of the claims made by an individual. What constitutes sufficient evidence to support the claims depends on the level of assurance required, as illustrated in Table 1.

3.3.1 Foundational and Supporting Evidence of Identity

There are two categories of evidence of identity, as defined in the *Standard on Identity and Credential Assurance*:

- **Foundational evidence of identity:** Evidence of identity that establishes core identity information such as given name(s), surname, date of birth, sex and place of birth. Examples of such evidence include records of birth, immigration and citizenship from an authority with the necessary jurisdiction.

- **Supporting evidence of identity:** Evidence of identity that corroborates the foundational evidence of identity and assists in linking the identity information to an individual. It may also provide additional information such as a photo, signature or address. Examples include social insurance records; records of entitlement to travel, drive or obtain health insurance; and records of marriage, death or name change originating from a jurisdictional authority.[10]

It is a good practice to refer to documents specifically in keeping with their original purpose (e.g., passport, driver’s licence), rather than generally as “identity documents.”

3.3.2 Use of Evidence of Identity

It is recommended that government organizations use evidence of identity only for the following purposes:

- **To collect sufficient identity information about the individual** to ensure delivery of a program or service;

- **To determine the accuracy of identity information**, including that it is up-to-date.

- **To determine linkage**, which ensures that the identity information relates to the individual making the claim. Note that linkage requirements do not apply to Level 1 or Level 2 assurance levels.

In certain cases, identity information collected through evidence of identity (e.g., age, residency and citizenship status) can also be used to determine program entitlement or eligibility. Government organizations need to ensure that any additional use of information collected through evidence of identity is supported by legislation.

Evidence of identity may be presented or accepted in different forms:

- **Documentary evidence.** Documentary evidence is widely understood to mean information written on paper. More generally, documentary evidence is any physical record of information that can be used as evidence.

[10] *Standard on Identity and Credential Assurance*, Appendix A

- **Electronic or digital evidence.** Electronic evidence is any data that is recorded or preserved on any medium in, or by, a computer system or other similar device. Examples are database records, audit logs and electronic word processing documents.

Evidence of identity requirements specified in Table 1 are independent of the form in which the evidence is presented (documentary or electronic). One "instance" of evidence of identity is distinguished from another instance by originating from or being issued by a different authoritative source.

3.3.3 Acceptability Criteria for Evidence of Identity

Table 3 sets out the acceptability criteria for foundational and supporting evidence of identity. Like the requirements, the criteria are also independent of the form in which the evidence is presented (documentary or electronic). Government organizations are expected to adapt acceptability criteria to their particular program or service delivery context.

Table 3. Acceptability Criteria for Evidence of Identity

Evidence of Identity	Acceptability Criteria and Examples
Foundational Evidence of Identity	**Acceptability Criteria:** • Evidence originates from an authoritative source that is: - Under the control of a federal or provincial/territorial government, or the local equivalent abroad (see Note 1 below); and - Used to maintain registration of specific vital events or determine legal status. • If identity information is incomplete or inconsistent with information provided by the individual (e.g., name change), additional supporting evidence may be required. • If the authoritative record or evidence is flagged for any reason (e.g., fraud, expiry) appropriate identity notification is expected (refer subsection 4.1.3). **Acceptable Authoritative Sources, Records and Documents:** • Vital statistics records used in the issuance of birth certificates; • Legal status records used in the issuance of citizenship and naturalization certificates and permanent resident cards; and • Other authoritative records enabled by departmental legislation.
Supporting Evidence of Identity	**Acceptability Criteria:** • Evidence originates from an authoritative source that is under the control of an approved organization (see Note 2). • If the authoritative record or associated documentary evidence is flagged for any reason (e.g., fraud, expiry), appropriate identity notification is expected (refer to subsection 4.1.3). **If Accepted in Conjunction with Foundational Evidence of Identity (Level 3 and Level 4):** • Supporting evidence of identity is expected to be consistent with the information that is provided by the foundational evidence of identity. • In the case of incomplete or inconsistent identity information (e.g., name change), additional supporting evidence may be required. • An endorsement or certification may be required to verify that the supporting evidence is a true copy of an original. **Acceptable Authoritative Sources, Records and Documents:**

	• Licensing and registration records or documents used in the issuance of driver's licences; • Passport or Certificate of Indian Status; and • Professional qualifications used in the issuance of professional credentials.
Notes: 1. When the authoritative source is outside Canadian jurisdiction, the acceptability criteria will be determined through a risk managed approach defined by the government organization. 2. What an "approved organization" is depends on the context of the government program or service. For this reason, federal organizations are expected to formalize their own definitions and criteria for approved organizations. Such organizations may be Crown corporations, academic institutions, public agencies and commercial organizations that are subject to regulation and oversight.	

3.3.4 Considerations for Children, Minors and Other Vulnerable Individuals

Providing services to children, minors or other vulnerable individuals often involves special circumstances and additional risk factors:

- Children, minors and vulnerable individuals may not have sufficient evidence of identity to meet the requirements as specified in the standard.
- The applicant may not be the recipient or beneficiary of the service. A parent, custodial parent or legal guardian may be applying for a service or program in respect of a child, minor or other vulnerable individual.

For example, the affected or tampered passport of a child, minor or other vulnerable individual is much more likely being used for criminal purposes, such as smuggling or trafficking, than an adult's affected passport.

It is recommended that government organizations apply the following guidelines when providing services to children, minors and other vulnerable individuals:

- Have in place additional safeguards or compensating factors to reduce risk and initiate exceptions or interventions, as appropriate.
- Confirm that the applicant (e.g., a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor or other vulnerable individual.

A government program may decide to include evidence of identity requirements for a parent or guardian as part of the evidence of identity requirements for the child, minor or other vulnerable individual. For example, the passport of a parent could be used as supporting evidence of identity for the child.

Note: Confirming relationships between individuals is outside the scope of this guideline. The recommendations in this section are to be applied in order to establish the identity of a child, minor or other vulnerable individual, not to determine or confirm relationships between individuals.

3.3.5 Guidelines on Evidence of Identity Assurance Levels

Table 4 provides guidelines for the assurance levels related to evidence of identity presented in Table 1. Criteria are independent of documentary or electronic form.

Table 4. Assurance Level Guidelines for Evidence of Identity

Assurance Level	Appendix C Requirement	Guidelines*
Level 1	No restriction on what is	• Provide notice to individuals that any false or

	provided as evidence	misleading statements may result in violation of terms or conditions. • Record in an audit log that an individual has made an assertion.
Level 2	**One** instance of evidence of identity	• Only one instance of foundational **or** supporting evidence of identity is required. • Specify that foundational evidence of identity is preferable to supporting evidence of identity, if further stringency is desired.
Level 3	**Two** instances of evidence of identity (at least one must be foundational evidence of identity)	• The two instances of evidence may both be foundational evidence of identity **or** one instance may be foundational evidence of identity and the other supporting evidence of identity. • Instances of evidence of identity are expected to originate from different or independent authoritative sources (i.e., some authorities may issue more than one type of document). • It is recommended that the two instances of evidence not be the same type of record or document issued by different authorities. (This is an exceptional circumstance. For example, an authority may cease to exist and a new authority reissues the same document).
Level 4	**Three** instances of evidence of identity (at least one must be foundational evidence of identity)	• Further increase the stringency of this requirement, as needed, by requesting two instances of foundational evidence of identity. • Any increase in stringency is best stated as an additional program risk management requirement.
***Note:** It is understood that implementing the guidelines at a given level (e.g., Level 3) includes implementing all the guidelines for the preceding levels (e.g., the two guidelines in Level 2 and the two guidelines in Level 1).		

3.4 Accuracy of Identity Information

The requirement for accuracy is to ensure the quality of the identity information. It is expected that identity information represent what is true about an individual and that it is as complete and up-to-date as necessary. The following considerations apply to ensuring accuracy of identity information:

- **The identity information is correct.** Identity information, due to certain life events (e.g., marriage) may change over time. Ongoing updates to identity information may be required; otherwise, it becomes incorrect.

- **The identity information relates to a real individual**. Identity information relates to an individual who actually exists. In most cases, the individual is still alive, but cases of deceased individuals may apply.

- **The identity information relates to the correct individual.** In large populations, individuals may have the same or similar identity information as other individuals. While the requirement for uniqueness addresses this issue (see subsection 3.2), the possibility of relating identity information to the wrong individual remains.

Accuracy can be confirmed by using an authoritative source. For example, a date of birth may be electronically validated using a provincial vital statistics registry. If validation against an authoritative source is not feasible, other methods may be employed, such as verifying or corroborating identity information using one or more instances of evidence of identity. Government organizations are advised to keep in mind the fraud considerations described in subsection 4.3.

Depending upon the program or service requirements and the privacy considerations, government organizations may use various methods to validate identity information, such as providing a response that an attribute is “valid” or “invalid.”

Determining the accuracy of identity information includes confirming that the individual truly exists or existed. This means that the identity information relates to a real individual (living or dead), and not to a false or incorrect individual. Accuracy of identity information is independent of whether an individual is living or deceased. An individual’s identity information does not become invalid after death.

Factors such as spelling and phonetic variations, name changes and different character sets can make determining the accuracy of identity information problematic. Such factors may make it difficult to prescribe exact match criteria. Government organizations may need to use approximate or statistical matching methods to determine that identity information acceptably matches an authoritative record.

An identifier (refer to subsection 3.2.2) should be subject to an exact match. In cases where the integrity of an identifier can be determined using a mathematical algorithm (e.g., checksum) these methods should be applied as part of the validation process.

Table 5 provides guidelines for the assurance levels related to accuracy of identity information presented in Table 1. This guidance applies to establishing the accuracy of identity information only. It should not be used for program decision making (e.g., eligibility or entitlement decisions).

Table 5. Assurance Level Guidelines for Accuracy of Information

Level of Assurance	Appendix C Requirement	Guidelines*
Level 1	Acceptance of self-assertion of identity information by an individual	• Inform individuals in a notice that they are required to provide accurate information about who they are. • Inform individuals in a notice that any false or misleading statements may result in reduced quality of service or may be in violation of terms or conditions. • Record in an audit log when the self-assertion was made and when notices were provided.
Level 2	Identity information acceptably matches assertion by an individual and evidence of identity **And** Confirmation that evidence of identity originates from appropriate authority	• Have individuals acknowledge that their identity information is their own and that it is consistent with the evidence of identity provided. • Remind individuals that false or misleading statements may be grounds for criminal prosecution. • Confirm that evidence of identity (documentary or electronic) has been legitimately issued by an authority that is approved or recognized by the government organization. • Confirm the validity or integrity of the document

		including the information contained within it (e.g., inspect security features, checksums) and validate electronic certificates by checking certificate revocation lists. • It is not necessary to confirm accuracy using a remote electronic validation process (as there may be no facility for remote access or network connectivity). • Use matching methods to determine accuracy within acceptable limits (e.g., name variances). • Record in an audit log which evidence was used.
Level 3	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **And** Confirmation of the foundational evidence of identity using authoritative source **And** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source --- **or** inspection by trained examiner	• Have in place formal matching criteria that determine accuracy within specified tolerances (e.g., name variances). • Confirm identity information matches within specified tolerances across all presented instances of evidence of identity. • Validate identity information that is presented as foundational evidence of identity by using the most current authoritative record available from an authoritative source. If necessary, multiple authoritative sources may be used. • Determine the accuracy of identity information through a risk managed approach when the authoritative source is outside Canadian jurisdiction. • Have a trained examiner determine the accuracy of identity information in cases where the above guidelines cannot be applied. • Record in an audit log the results of the confirmation process.
Level 4	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **And** Confirmation of the foundational evidence of identity using authoritative source **And** Confirmation that supporting	• Use evidence of identity requirements equivalent to Level 3 requirements, but put in place more stringent matching criteria to determine accuracy within specified tolerances. • As in Level 3, have a trained examiner determine the accuracy of identity information in cases where the above guidelines cannot be applied. Document exceptional cases; it may be necessary to approve specific exceptions separately. • Record in an audit log the results of the matching process, including when matches fall outside specified tolerances.

	evidence of identity originates from appropriate authority, using authoritative source --- **or** inspection by trained examiner	
***Note:** It is understood that implementing the guidelines at a given level (e.g., Level 3) includes implementing all the guidelines for the preceding levels (e.g., the seven guidelines in Level 2 and the three guidelines in Level 1).		

3.5 Linkage to Individuals

The linkage requirement is to ensure that identity information relates to the individual making the claim. This includes ensuring that the identity information relates to a real person (born and still alive, in most cases).

3.5.1 Linkage Methods

The *Standard on Identity and Credential Assurance* describes four types of methods that can be used to determine linkage to an individual.[11]

- **Knowledge-based confirmation:** A process that compares personal or private information (i.e., shared secrets) to establish an individual's identity. Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information and credit or financial information.

- **Biological or behavioural characteristic confirmation:** A process that compares biological (anatomical and physiological) characteristics in order to establish a link to an individual. Example: Facial photo comparison.

- **Trusted referee confirmation:** A process that relies on a trusted referee to establish a link to an individual. The trusted referee is determined by program-specific criteria. Examples of trusted referee include guarantors, notaries and certified agents.

- **Physical possession confirmation**: A process that requires physical possession or presentation of evidence to establish an individual's identity.

Government organizations determine which linkage methods or combination of linkage methods they will use based on their program requirements. When selecting the appropriate methods, they need to assess all relevant cultural, privacy and legal considerations.

Table 6 lists possible ways to implement each linkage method.

Table 6. Linkage Methods

Method Types	Method Examples
Knowledge-based confirmation	• **Static knowledge-based confirmation:** Use of personal information previously collected or established at a specific point in time (e.g., during a registration process). • **Dynamic knowledge-based confirmation:** Use of personal

[11] *Standard on Identity and Credential Assurance*, Appendix A

	information collected or generated over period of time (i.e., as opposed to a specific point in time).
Biological or behavioural characteristic confirmation	• **Facial comparison:** Manual facial comparison between evidence of identity and the presenting individual, or the use of automated facial recognition. • **Iris comparison:** Comparison of iris patterns of an individual's eyes using previously collected templates. • **Fingerprint comparison:** Comparison of the physical structure of an individual's fingerprint for recognition purposes. • **Voice comparison:** Detection and comparison of spoken words with a previously collected voiceprint. • **Signature comparison:** Comparison of the signature provided by an individual with a signature associated with evidence of identity. • **Data analytics:** Use of previously collected information to identify characteristics, trends or behaviours that are attributable to the individual.
Trusted referee confirmation*	• **Guarantor:** An individual who has agreed to be responsible for confirming information provided by the individual. • **Notary:** A licensed person or organization that has the authority to administer oaths and attest to signatures in relation to legal documents. • **Individuals:** An individual that is in a position of trust.
Physical possession confirmation	• **Physical demonstration of control:** An individual physically demonstrates the exclusive possession or control of a secure document or physical object (i.e., token) that was issued previously to the individual: o In the case of a secure document, this may involve the submission for examination of security features or validation of the document; and o In the case of a secure physical object, this may involve a secure interaction with a physical or electronic validation process. • In either case, these processes may require the physical presence of the individual, but this requirement would not preclude the possibility of remotely enabled physical demonstration processes.
***Note:** It is recommended that government organizations develop formal criteria for trusted referees.	

Table 7 provides guidelines on linkage methods for the assurance levels related to linkage of identity information to individual presented in Table 1.

Table 7. Assurance Level Guidelines for Linkage Methods

Assurance Level	Appendix C Requirement	Guidelines*
Level 1	No requirement	• Employ methods to ensure that interaction is with a **real** individual (i.e., not an automated process).
Level 2	No requirement	• Employ methods to ensure that the initial and subsequent interactions can be linked to the **same** individual making the claims. This can be achieved by using a credential assurance (see

		subsection 2.3).
Level 3	At least **one** of the following linkage methods: i) Knowledge-based confirmation ii) Biological or behavioural characteristic confirmation iii) Trusted referee confirmation iv) Physical possession confirmation	• Employ out-of-band (OOB) methods for linkage processes. Out-of-band methods use communication channels or application services that are independent of, or separate from, the system used to carry out the transaction. Examples include short message services (SMS) or email. • Use OOB methods that are secure, private and exclusive to the individual. • Record in an audit log linkage and OOB transactions (delivery, receipt, used in confirmation).
Level 4	At least **three** of the following linkage methods: ii) Knowledge-based confirmation iii) Biological or behavioural characteristic confirmation iv) Trusted referee confirmation v) Physical possession confirmation	• Determine which linkage methods were used together to meet the linkage requirement by referring to the audit log.
*** Note:** It is understood that implementing the guidelines at a given level (e.g., Level 3) includes implementing all the guidelines for the preceding levels (e.g., the guideline in Level 2 and the guideline in Level 1).		

4. Integrating Identity Assurance into Business and System Processes

4.1 Introduction

The four categories of standard requirements for identity assurance presented in Section 3 are usually part of a more comprehensive set of program or service requirements. Implementing the standard requirements involves integrating them discretely into the broader business or system processes or creating a stand-alone identity assurance process that can be incorporated as a component.

For example, a department may decide to integrate the standard requirements for identity assurance into a client registration process to support a single program. Another department may decide to implement the standard requirements by creating an identity assurance process that can be incorporated into many programs and services. Regardless of the integration approach taken, government organizations need to be able to demonstrate how they meet all the requirements for their identity assurance level.

This section presents considerations and guidelines for government organizations when integrating the standard requirements into business or system processes

4.2 Business and System Process Considerations

4.1.1 Efficient and Transparent Procedures

When integrating the standard requirements for identity assurance into business or system processes, government organizations are advised to ensure that identity assurance procedures are as efficient and transparent to the client as possible. Procedures that are not clear or that are burdensome to the client may be a barrier to adoption of services.

4.1.1 Privacy Concerns

Government organizations must comply with the *Privacy Act.* When integrating identity assurance requirements into business and system processes, consideration needs to be given to individuals' right under the Act to access their personal information and, in certain circumstances, request the correction of their information.

It is important that government organizations distinguish between the information they collect to support identity assurance requirements and other personal information collected and used for a specific program or service. Failure to properly separate identity information from program or service–specific information may have privacy implications. This is a key consideration, for example, when identity information is collected and used to support several related services.

For discussion of defining identity information and complying with the *Policy on Privacy Protection*, please refer to subsection 3.2.2.

4.1.2 Linkage and Binding

Government organizations need to consider how linkage and binding procedures may impact the integration of identity assurance requirements into new or existing business processes.

Linkage of identity information is carried out when an individual has had no prior relationship with a program or service and is initiating a transaction for the very first time. For example, when an individual applies for a new benefit, the program or service, having had no prior interaction with the individual, must ensure that the individual is who he or she says they are. Linkage ensures that the identity information relates to the individual making the claim.

Binding of identity information occurs once linkage has taken place. Binding is the creation of a new relationship, usually to a credential the individual already possesses, which is then used to facilitate subsequent transactions. This type of binding is called "credential binding." Credential binding allows an individual to use his or her electronic credential for subsequent secure transactions.

Linkage and binding are important concepts in the context of federation. Presently, there are several authentication models in development that incorporate linkage and binding; however, discussion of these models is outside the scope of this guideline.

4.1.3 Using Identity Life Cycle Models

Government organizations may find it useful to define a formal identity life cycle model. An identity life cycle can be broken down into several major phases, including identity proofing; user provisioning; credential issuance, use and authentication; and attribute use.[12] Life cycle models may also include aspects of the information life cycle—creation, collection, use, retention, disclosure and disposal.

Table 8 lists the major phases that should be incorporated into any identity life cycle model, as a minimum.

Table 8: Identity Life Cycle Considerations

Life Cycle Phase	Description and Detail
Identity Establishment	• Carried out when an individual has no prior interaction with a program or service. • Results in a new authoritative record where none existed previously. • Usually reserved for organizations that intend to be authoritative providers within a federation. • Requires the implementation of all standard requirements for a given level of assurance.
Identity Validation	• Carried out when an individual has had a previous interaction with a program or service. • Uses a previously established authoritative record. • Does not create a new authoritative record (unless the validation process is part of the identity establishment process described above). • Ensures that identity information is accurate and up-to-date and is uniquely associated with the same individual. • **Does not** ensure that the individual is using his or her own identity information, only that the identity information is accurate and up-to-date. • May leverage an existing credential binding.
Identity Notification	• Provides notification that identity information may have changed or may have been exposed to risk factors (e.g., detection of fraudulent use or use of expired documents). • Can be provided when a life event occurs (e.g. birth, death, marriage). • Can be used to update an authoritative record resulting from the identity establishment process. • Can be provided to relying parties in conjunction with an identity validation or assurance service. • May be used by relying parties to put in place additional safeguards or

[12] These major phases are defined in Gartner's *Balancing the Identity and Risk Equation with Identity Assurance Frameworks*.

	compensating factors. • May be sent to authoritative parties, if relying parties detect fraud (or any other incident or risk factor). • Should not be used for entitlement or benefit decisions, which are separate from identity risk decisions.

4.2 Federation Considerations

A government organization may have implemented a federated model without necessarily being a formal member of a federation. Within a department, for example, a departmental sub-organization (e.g., a branch or sector) may assume the role of an authoritative party or a relying party. A departmental human resources (HR) system may be considered as an authoritative party for a departmental security system that is responsible for issuing ID badges. The owner of the security system in this model would be considered as the relying party.

Before a government organization becomes a member of a federation, it may be beneficial to implement the key elements of a federated model. Table 9 is intended to assist organizations in transitioning to a federated model by outlining key considerations for acting in the role of an authoritative party and a relying party.

Table 9. Considerations for Organizational Responsibilities

Organizational Role	Not a Member of a Federation	As a Member of a Federation
Acting in the role of an authoritative party	**Considerations for organization:** • May be an authoritative party for own organization. • May provide foundational or supporting evidence of identity that may be used by other organizations. • May provide identity assurance for own organization **only** (i.e., cannot provide identity assurance outside organization). • May provide identity information that supports an identity validation process in another organization. • Is responsible for managing own organizational identity risk. **Organizations should:** • Implement standard requirements at the required assurance level. Example: A departmental HR system that maintains an authoritative employee record.	**Considerations for organization:** • May be an authoritative party for participants in a federation (in addition to own organization). • May provide foundational or supporting evidence of identity that may be used by other organizations. • May provide identity assurances to relying party participants in a federation. • May apportion consequences of identity risk when providing identity assurances to relying party participants in a federation (to a level of assurance). **Organizations should:** • Implement standard requirements at the required assurance level. • Participate as authoritative party in a federation and comply with federation criteria and criteria established by the Government of Canada Chief Information Officer.
Acting in the role of a relying party	**Considerations for organizations:** • May use foundational and supporting evidence of identity provided by another organization. • May use identity information validated by	**Considerations for organizations:** • May rely upon identity assurances as provided by authoritative party participants in the federation (to a level of assurance).

	another organization. • Identity risk remains the responsibility of organization. • Program-specific risk remains the responsibility of organization. **Organizations should:** • Implement standard requirements at the required assurance level; **or** • Enter into an arrangement with another party to implement standard requirements on its behalf (e.g., MOU, bilateral agreement). Example: A departmental security system that relies on an authoritative employee record maintained by a departmental HR system.	• May share identity risk when relying on identity assurances (to a level of assurance). • Program-specific risk remains the responsibility of organization. **Organizations should:** • Participate in federation as a relying party; **and** • Comply with federation criteria established by Government of Canada Chief Information Officer.

4.3 Fraud Considerations

It is important for government organizations to be aware of the different methods of fraud, as these may be significant risk factors when implementing the standard requirements.

4.3.1 Document Fraud

Document fraud is the fraudulent acquisition, production or alteration of documents issued by an authority. The techniques of document fraud include:

- **Fabrication or counterfeiting of documents:** The unauthorized manufacture of documents using devices and processes available on the open market or acquired by unauthorized means. It involves the simulation or replication of security and/or personalization features of an authentic document.

- **Alteration of legitimately issued documents:** The unauthorized alteration of an existing legitimate document. This may involve altering date of birth to change entitlements or altering the photograph and/or biographical data to correspond to a fraudulent bearer.

4.3.2 Records Fraud

Records fraud is the unauthorized creation, insertion or deletion of authoritative records under the control of an institution. The creation of false records or the alteration of existing records may result in the issuance of documents and/or entitlements that are not legitimate. The techniques of record fraud include the following:

- **External Threat Agent:** Unauthorized creation, insertion or deletion of authoritative records as a result of external threat agents that have intruded into the record system.

- **Insider Fraud or Collusions:** The result of individuals in a position of trust (officers, employees, contractors) that use their knowledge and skills to carry out unauthorized creation, insertion or deletion of authoritative records.

4.3.3 Impostor Fraud

Impostor fraud is the fraudulent use of another person’s identity information, whether this person is real or fictitious. Impostor fraud may involve:

- **Use of another person’s evidence of identity, where the other person is a stranger**. To exploit the use of another person’s identity, the impostor may alter his or her own appearance or alter the evidence of identity. In these cases, the impostor usually does not have detailed knowledge of the victim, and fraudulent use can be detected using confirmation methods specified in the linkage requirements.

- **Use of another person’s evidence of identity, where the other person is known.** The fraudster may be acting as an impostor (as described above). The fraudster may also be attempting to act on behalf of another individual by means of an unauthorized role or relationship. Different methods should be used to ensure an individual is legitimately acting on behalf of another individual.

- **Use of another person’s credentials, where the other person is a fabricated or synthetic identity.** This is the most sophisticated form of fraud and may be carried out in conjunction with records fraud and document fraud. Due to its sophistication, this is usually carried out by highly motivated threat agents such as organized crime.

5. References

Legislation

- Criminal Code
- *Personal Information Protection and Electronic Documents Act*
- *Privacy Act*
- *Privacy Regulations*

Government of Canada Policy Instruments

- *Directive on Departmental Security Management*
- *Directive on Identity Management*
- *Directive on Information Management Roles and Responsibilities*
- *Directive on Privacy Impact Assessment*
- *Directive on Privacy Practices*
- *Directive on Privacy Requests and Correction of Personal Information*
- *Directive on Recordkeeping*
- *Guideline on Defining Authentication Requirements*
- *Information Technology Security Guideline 31 – User Authentication Guidance for IT Systems*
- *Information Technology Security Guideline 33 – IT Security Risk Management: A Lifecycle Approach*
- *Policy on Government Security*
- *Policy on Information Management*
- *Policy on Privacy Protection*
- *Standard on Identity and Credential Assurance*

Public Sector, Industry and International Resources

- *Cyber-Authentication Technology Solutions Interface Architecture and Specification Version 2.0*
- *E-Authentication Guidance for Federal Agencies*
- Electronic Authentication Guideline (draft)
- Entity Authentication Assurance Framework
- *Harmonized Threat and Risk Assessment (TRA) Methodology*
- Kantara Identity Assurance Framework
- Kantara Initiative
- North American Security Products Organization, *Identity Verification Standard IDP-V* (requires authorized access)
- *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*
- *Pan-Canadian Assurance Model*
- Requirements and Implementation Guidelines for Assertion, Evidence and Verification of Personal Identity (draft)

6. Additional Information

6.1 Next Review Date

This document will be reviewed and updated as required.

6.2 Enquiries and Comments

Please direct any enquiries or comments about this guideline to:

Chief Information Officer
Chief Information Officer Branch
Treasury Board of Canada Secretariat
2745 Iris Street
Ottawa, ON K1A 0R5

Telephone: 613-952-2400
Fax: 613-952-8536
Email: SEC@tbs-sct.gc.ca

Appendix A: Key Terms and Definitions

The key terms used in this guideline include authoritative definitions from the *Standard on Identity Credential Assurance*, terms defined in related guidelines and industry references, and definitions developed by the working group for the purposes of this guideline.

Assigned identifier: A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between individuals without the use of any other identity characteristics.

Assurance: A measure of certainty that a statement or fact is true. (Source: *Standard on Identity and Credential Assurance*)

Assurance level: A level of confidence that may be relied on by others. (Source: *Standard on Identity and Credential Assurance*)

Attribute: See "identity attribute."

Authentication: The process of establishing truth or genuineness to generate an assurance. (Source: *Guideline on Defining Authentication Requirements*).

Authoritative party: A federation member that provides assurances of credential or identity to other members (i.e., "relying parties"). (Source: *Standard on Identity and Credential Assurance*)

Authoritative source: A collection or registry of records maintained by an authority that meets established criteria. (Source: *Standard on Identity and Credential Assurance*)

Binding: A creation of a new relationship, usually to a credential the individual already possesses, which is then used to facilitate subsequent transactions

Biological or behavioural characteristic confirmation: A process that compares biological (anatomical and physiological) characteristics in order to establish a link to an individual (e.g., facial photo comparison). (Source: *Standard on Identity and Credential Assurance*)

Biometrics: A general term used alternatively to describe a characteristic or a process. It can refer to a measurable biological (anatomical and physiological) or behavioural characteristic that can be used for automated recognition. It can also refer to automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioural characteristics. (Source: Biometrics Consortium Glossary).

Context: A set of circumstances, a situation or a scenario in which an individual interacts with other individuals or with an organization.

Credential: A unique physical or electronic object (or identifier) issued to, or associated with, an individual, organization or device. (Source: *Standard on Identity and Credential Assurance*)

Credential assurance: The assurance that an individual, organization or device has maintained control over what has been entrusted (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, modified). (Source: *Standard on Identity and Credential Assurance*)

Credential assurance level: The level of confidence that an individual, organization or device has maintained control over what has been entrusted (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, corrupted, modified). (Source: *Standard on Identity and Credential Assurance*)

Credential risk: The risk that an individual, organization or device has lost control over the credential that has been issued. (Source: *Standard on Identity and Credential Assurance*)

Documentary evidence: Documentary evidence is widely understood to mean information written on paper. More generally, documentary evidence is any physical record of information that can be used as evidence.

Electronic or digital evidence: Electronic evidence is any data that is recorded or preserved on any medium in, or by, a computer system or other similar device. Examples are database records, audit logs and electronic word processing documents.

Evidence of identity: A record from an authoritative source that supports the integrity and accuracy of the claims made by an individual. There are two categories of evidence of identity:

- **Foundational evidence of identity –** Evidence of identity that establishes core identity information such as given name(s), surname, date of birth, sex and place of birth. Examples include records of birth, immigration or citizenship from an authority with the necessary jurisdiction; and

- **Supporting evidence of identity –** Evidence of identity that corroborates the foundational evidence of identity and assists in linking the identity information to an individual. It may also provide additional information such as a photo, signature or address. Examples include social insurance records; records of entitlement to travel, drive or obtain health insurance; and records of marriage, death or name change originating from a jurisdictional authority. (Source: *Standard on Identity and Credential Assurance*)

Federation: A cooperative agreement between autonomous entities that have agreed to work together. The federation is supported by trust relationships and standards to support interoperability. (Source: *Standard on Identity and Credential Assurance*)

Identifier: The set of attributes used to uniquely distinguish a unique and particular individual, organization or device.

Identity: A reference or designation used to distinguish a unique and particular individual, organization or device. (Source: *Standard on Identity and Credential Assurance*)

Identity assurance: A measure of certainty that an individual, organization or device is who or what it claims to be. (Source: *Standard on Identity and Credential Assurance*)

Identity assurance level: The level of confidence that an individual, organization or device is who or what it claims to be. (Source: *Standard on Identity and Credential Assurance*)

Identity attribute: A property or characteristic associated with an identifiable individual, which is also known as an identity data element.

Identity establishment: The creation of an authoritative record of identity that is relied on by others for subsequent government activities, programs and services.

.

Identity information: The set of identity attributes that is sufficient to distinguish between different individuals and sufficient to recognize the individual, as required by the service or program.

Identity management: The set of principles, practices, processes and procedures used to realize an organization’s mandate and its objectives related to identity. (Source: *Standard on Identity and Credential Assurance*)

Identity notification: Notification that identity information may have changed or may have been exposed to risk factors (e.g., detection of fraudulent use or use of expired documents).

Identity risk: The risk that an individual, organization or device is not who or what it claims to be. (Source: *Standard on Identity and Credential Assurance*)

Identity validation: Confirmation of the accuracy of identity information as established by an authoritative source.

Knowledge-based confirmation: A process that compares personal or private information (i.e., shared secrets) to establish an individual's identity. Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information and credit or financial information. (Source: *Standard on Identity and Credential Assurance*)

Linkage: Determining that identity information relates to the individual making the claim.

Physical possession confirmation: A process that requires physical possession or presentation of evidence to establish an individual's identity. (Source: *Standard on Identity and Credential Assurance*)

Relying party: A federation member that relies on assurances of credential or identity from other members (i.e., “authoritative parties”). (Source: *Standard on Identity and Credential Assurance*)

Trusted referee confirmation: A process that relies on a trusted referee to establish a link to an individual. The trusted referee is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries and certified agents. (Source: *Standard on Identity and Credential Assurance*)

Trust framework: A formalized scheme that ensures that federation members have continued confidence in one another. A trust framework formerly underpins trust relationships by stipulating adherence to standards, formalizing assessment processes and defining roles and responsibilities of multi-party arrangements.

Trust relationship: A defined arrangement or agreement that ensures confidence.

Appendix B: Annotated References

1. Treasury Board Policy Instruments

This section provides a summary of the policies, directives, standards and guidelines for the management area of information, IT security and privacy.

1.1 *Policy on Government Security*

The objective of the *Policy on Government Security* is to ensure that deputy heads effectively manage security activities within government organizations and contribute to effective government-wide security management. The policy is supported by two directives:

- *Directive on Departmental Security Management*. The objective of this directive is to achieve efficient, effective and accountable management of security within government organizations.
- *Directive on Identity Management*. The objective of this directive is to ensure effective identity management practices by outlining requirements to support government organizations in the establishment, use and validation of identity.

The *Directive on Identity Management* is supported by one standard and two guidelines:

- *Standard on Identity and Credential Assurance*. The objective of this standard is to ensure that identity risk is managed consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors.

- *Guideline on Defining Authentication Requirements*. This guideline provides guidance on conducting assurance level assessments and determining authentication options. Please refer to subsection 2.5.

- **Guideline on Identity Assurance**. This guideline provides guidance on the implementation of requirements specified in Appendix C of the *Standard on Identity and Credential Assurance*.

1.2 *Policy on Privacy Protection*

The objectives of the *Policy on Privacy Protection* are as follows:

- To facilitate statutory and regulatory compliance, and to enhance effective application of the *Privacy Act* and its regulations by government institutions.

- To ensure consistency in practices and procedures for administering the Act and its regulations so that applicants receive assistance in filing requests for access to personal information.

- To ensure effective protection and management of personal information by identifying, assessing, monitoring and mitigating privacy risks in government programs and activities involving the creation, collection, use, retention, disclosure and disposal of personal information.

The *Policy on Privacy Protection* is supported by the following directives:

- *Directive on Privacy Impact Assessment*. This directive requires that government organizations carry out a privacy impact assessment for new or substantially modified programs or activities that involve the creation, collection, use, retention, disclosure and disposal of personal information.

- *Directive on Privacy Practices*. This directive facilitates the implementation and public reporting of consistent and sound privacy management practices for the creation, collection, use, retention, disclosure and disposal of personal information under the control of government institutions.

- *Directive on Privacy Requests and Correction of Personal Information*. This directive establishes consistent practices and procedures for processing requests for access to, or correction of, personal information that is under the control of government institutions and has been used, is being used, or is available for use for administrative purposes.

Related guidelines and tools are available at the links provided above.

1.3 *Policy on Information Management*

The objective of the *Policy on Information Management* is to achieve efficient and effective information management to support program and service delivery; foster informed decision making; facilitate accountability, transparency and collaboration; and preserve and ensure access to information and records for the benefit of present and future generations.

The *Policy on Information Management* is supported by the following directives:

- *Directive on Information Management Roles and Responsibilities*. This directive identifies the roles and responsibilities of all departmental employees in supporting the deputy head in the effective management of information in their organization.

- *Directive on Recordkeeping*. This directive ensures effective recordkeeping practices that enable government organizations to create, acquire, capture, manage and protect the integrity of information resources of business value in the delivery of Government of Canada programs and services.

Related guidelines and tools are available at the links provided above.

2. Related Guidelines and Industry Standards

This section provides related guidelines and industry standards for the management area of information, IT security and privacy and for use in conjunction with the present guideline.

2.1 Threat and Risk Assessments

Government organizations may want to conduct more generalized security risk assessments using the *Harmonized Threat and Risk Assessment (TRA) Methodology*, which is jointly published by the Royal Canadian Mounted Police and Communications Security Establishment Canada (CSEC).

The Harmonized TRA Methodology is designed to address all employees, assets and services at risk. The assessment may be performed at any level of granularity, from broadly based departmental risk profiles to more tightly focused examinations of specific issues.

Organizations may want to use Harmonized TRA analysis as an additional consideration when implementing the minimum requirements in Appendix C of the *Standard on Identity and Credential Assurance*. For example, the Harmonized TRA may be useful in addressing the highly specialized threat agents associated with the rapidly evolving online environment and the potential vulnerabilities introduced by newer technologies (e.g., tablets, mobile phones).

2.2 IT Security Guidelines

For guidance on authentication related to IT systems and electronic service delivery, government organizations are advised to consult the following guidelines published by CSEC:

- ITSG-31, User Authentication Guidance for IT Systems. This guideline provides guidance on the design and selection of user authentication solutions.

- ITSG-33, IT Security Risk Management: A Lifecycle Approach. This guideline provides the framework for the IT security risk management activities that should be undertaken at both the departmental level and the information system level within government organizations.

2.3 Federation Standards and Protocols

Several documents have been developed to support the governance of, and contracting of services for, cyber authentication. Government organizations may wish to consult these documents, which can be provided by contacting the Chief Information Officer Branch (see Section 6).

- ***Cyber-Authentication Technology Solutions Interface Architecture and Specification Version 2.0*: *Deployment Profile*.** This document describes the deployment profile and messaging interface required for using Government of Canada credential authentication services. The deployment profile is based on the eGov Implementation Profile published by the Kantara Initiative and describes additional requirements and constraints specific to the Government of Canada.

- **Protocol for Federating Identity.** The Treasury Board of Canada Secretariat is currently developing the protocol for federating identity. This document will support the *Standard on Identity and Credential Assurance* and provide the detailed criteria for formally participating in the Government of Canada federation.

3. Use and Adoption of Other Frameworks, Standards and Guidelines

Government organizations are encouraged to use and adopt other frameworks, standards and guidelines, where appropriate. Industry and government have adopted the four-level assurance model (Level 1 through Level 4) in Appendix C of the *Standard on Identity and Credential Assurance*, which is illustrated in Table 1. However, there are a few differences between this model and the other frameworks, standards and guidelines. When applying related resources, government organizations are advised to consider the following:

- **Adherence to the four-level assurance model.** Although there are variations in descriptions and definitions, the four-level assurance model has been accepted by the global community and is considered normative across the standards and guidelines. Business requirements, technical standards and agreements need to adhere to this four-level model.

- **Separation of identity and credential assurance.** The pan-Canadian approach makes an explicit distinction between identity and credential assurance. Other standards do not make this distinction and, as result, there may be dependencies between different categories of requirements (e.g., between credential issuance and identity proofing). In applying other related standards, government organizations should pay particular attention to which requirements apply or do not apply within their particular context.

- **Formalize a standards adoption process.** Identity standards and related practices continue to evolve and change. Government organizations should formalize an adoption process, taking into account how these standards apply (or do not apply) within their context.

It should be noted that the Government of Canada is currently formalizing a trust framework adoption process that will approve industry and/or public sector trust frameworks. Following is a non-exhaustive list of frameworks, standards and guidelines that may be used:

- ***E-Authentication Guidance for Federal Agencies*** **(OMB M04-04).** This document requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication.

- **Electronic Authentication Guideline (NIST SP 800 63-2).** This document provides technical guidelines for U.S federal agencies implementing electronic authentication (e-authentication). This guideline supports the implementation of OMB M04-04.

- **Entity Authentication Assurance Framework (ISO 29115).** This document provides guidance concerning control technologies, processes and management activities. It also specifies assurance criteria that should be used to mitigate authentication threats,communicate the results of an authentication transaction, and protect personally identifiable information associated with the authentication process.

- **Kantara Identity Assurance Framework.** This framework comprises of a set of documents that includes assurance levels, an assessment scheme and certification requirements for identity-proofing services, credential strength and credential management services.

- **Requirements and Implementation Guidelines for Assertion, Evidence and Verification of Personal Identity (ANSI/NASPO-IDPV-2013).** This document is a draft American national standard that describes a process, specifies requirements and provides implementation guidelines for the assertion, resolution and verification of personal identity.

Table 10 uses the four-level assurance model to provide a high-level comparison of these frameworks, standards and guidelines.

Table 10. Comparison With Other Standards and Guidelines

	Standard on Identity and Credential Assurance		**OMB M04-04/ NIST SP 800 63-2**	**Kantara Identity Assurance Framework**	**ANSI/ NASPO-IDPV-2013**	**ISO 29115**
Level	**Identity Assurance Level**	**Credential Assurance Level**	**Assurance Level**	**Assurance Level**	**Identity Assurance Level**	**Level of Assurance**
Level 1	Little confidence required that an individual is who he or she claims to be	Little confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised	Little or no confidence exists in the asserted identity	Little or no confidence in the asserted identity's validity	Little or no confidence in the asserted identity's validity	Little or no confidence in the claimed or asserted identity
Level 2	Some confidence required that an individual is who he or she claims to be	Some confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised	On balance, confidence exists that the asserted identity is accurate	Some confidence in the asserted identity's validity	Some confidence in the asserted identity's validity	Some confidence in the claimed or asserted identity
Level 3	High confidence required that an individual is who he or she claims to be	High confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised	Appropriate for transactions needing high confidence in the asserted identity's accuracy	High confidence in the asserted identity's validity	High confidence in the asserted identity's validity	High confidence in the claimed or asserted identity
Level 4	Very high confidence required that an individual is who he or she claims to be	Very high confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised	Appropriate for transactions needing very high confidence in the asserted identity's accuracy	Very high confidence in the asserted identity's validity	Very high confidence in the asserted identity's validity	Very high confidence in the claimed or asserted identity