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

Guideline on Identity Assurance

Published: Mar 04, 2016

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-165/2016E-PDF
ISBN: 978-0-660-09759-6

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Ligne directrice sur l'assurance de l'identité

Guideline on Identity Assurance

1. Purpose

This guideline supports implementation of the minimum requirements for establishing the identity[Footnote 1] of an individual to a given level of assurance. Identity assurance levels are defined in Appendix B of the *Standard on Identity and Credential Assurance*, and the minimum requirements to establish an identity assurance level are set out in subsection 6.4.1 and Appendix C. This standard was issued to support the *Policy on Government Security* and the *Directive on Identity Management*.

Identity establishment is the creation of an authoritative record of identity that can be relied on by others for subsequent government activities, programs and services. This guideline assists in standardizing how the identity information of individuals is established in relation to government programs and services. This guideline is also intended to promote consistent identity assurance practices, while enabling government organizations to retain the flexibility to innovate and manage risk appropriately. It is also intended to assist in a phased approach toward federating identity that includes the use of standardized credential authentication services.

1.1 Audience

This guideline is intended for the following users:

- **Program and service delivery managers** who are responsible for ensuring consistency in 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 are responsible for recommending, designing, building or providing solutions for meeting program and service requirements.

1.2 Application and Use

This guideline

- applies when there is a requirement to uniquely identify individuals for the purpose of carrying out a service or a transaction, or for the purpose of administering a program;
- applies to both external and internal Government of Canada services;
- does not impose additional requirements beyond what is prescribed in the *Standard on Identity and Credential Assurance*;
- may apply to decisions about access, authorization or entitlement;
- may apply when determining relationships between individuals, organizations and devices. It is acknowledged that such relationships exist for the purpose of granting authority or permission to act on behalf of others. Examples of these relationships are provided; however, they are not to be construed as guidance;
- is to be used in conjunction with the *Guideline on Defining Authentication Requirements*, which provides government organizations with an assessment framework for determining their specific identity assurance level requirements;
- does not recommend specific technologies, architectures or solutions, nor does it recommend the use of specific documents or document authentication techniques;
- may be used to support security checks related to identity, as specified in the *Standard on Security Screening*; and
- may be used to support the implementation of the *Policy on Service*.

For an annotated list of policies, standards, guidelines and frameworks in support of, or related to, identity assurance, see Appendix B.

To meet the requirements of the standard, Government organizations are developing identity management practices and related tools that can be used to contribute to a coherent, consistent, standardized and interoperable approach across the Government of Canada. These identity practices and related tools will be shared via GCPedia and may be incorporated into future versions of this guideline.

2. Introduction

2.1 The Government of Canada's Approach to Identity Assurance

Identity is at the core of most government business processes and is the starting point of trust and confidence in interactions between the public and government. Once the identity information of an individual is established, all subsequent government activities, ranging from providing services to granting benefits and status, rely on the accuracy and rightful use of this information. For many service encounters or client transactions, government organizations must ensure that they are dealing with the right individual so that they can meet their program and service delivery objectives. For example, when an individual applies for a Canadian passport, certain documents are required to support the proof of his or her identity.

The management of identity information is a shared responsibility between the different orders of government within Canada. There are many authoritative sources, enabled by federal, provincial and territorial acts and regulations, that record information relating to an individual such as vital events, legal or professional status, and benefit entitlements. In most cases, a document or

certificate is issued to the individual, who uses to it prove his or her identity and related personal information.

In Canada, there is no single document whose sole purpose is to identify an individual. Instead, many documents issued by different jurisdictions are in use. This decentralized approach has been effective in serving Canadians. However, it can present challenges in providing a consistent service experience across jurisdictions and in combatting fraudulent activity.

Physical documents remain the predominant method of presenting evidence of identity for Government of Canada programs and services. As digital delivery methods become more prevalent, digital representations of identity may be accepted as alternatives to physical documents. Governments are recognizing the potential cost savings related to the use of digital alternatives and common infrastructure. As government programs and services become increasingly interconnected and interdependent, it becomes imperative to manage identity risk collaboratively across organizational and jurisdictional boundaries.

In 2011, in response to this changing environment, the Government of Canada published *Federating Identity Management in the Government of Canada: A Backgrounder*, which described an overall vision and approach that would permit trust, established by internal identity management business processes, to be extended across organizational boundaries within the Government of Canada and with other jurisdictions. As part of this document, several key concepts were formally defined, including "identity assurance" and "credential assurance," and then formalized in subsequent Treasury Board policy instruments.

2.2 Treasury Board Policy Instruments on Identity

The Treasury Board policy instruments on identity consist of one directive, one standard and two guidelines issued under the authority of the *Policy on Government Security*.

- The *Directive on Identity Management*, in effect since July 2009, supports effective identity management practices by outlining requirements to support departments in the establishment, use and validation of identity.
- The *Standard on Identity and Credential Assurance*, in effect since February 2013, ensures that identity risk is managed consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors. The standard is supported by two guidelines.
- The *Guideline on Defining Authentication Requirements*, issued in November 2012, supports the implementation of requirements 6.1.1, 6.1.2 and 6.1.3 of the *Standard on Identity and Credential Assurance*. For ease of reference, these requirements are as follows:
    - **6.1.1** Identifying and evaluating identity and credential risks using an assessment of harms related to a program, activity, service or transaction;
    - **6.1.2** Determining required identity and credential assurance levels using the standardized assurance levels specified in Appendix B [of the standard]; and
    - **6.1.3** Selecting identity and credential controls for achieving assurance level requirements using the standardized assurance levels specified in Appendix B [of the standard].
- The Guideline on Identity Assurance (this guideline) supports the implementation of requirement 6.1.4 of the standard:
    - **6.1.4** Ensuring that the minimum requirements for establishing an identity assurance level as specified in Appendix C [of the standard] are met.

Section 3 of this guideline provides detailed guidance on meeting these requirements.

2.3 Identity Assurance and Identity Assurance Levels

Most government programs and services need to know the individual they are dealing with. For external services, the individual is typically a client of a government program or service. For internal services, the individual is an employee, or a government worker acting on behalf of a government organization.

These different contexts may result in different risks that need to be managed. For example, not properly confirming the right individual as a client may result in a benefits payment to the wrong individual (a program integrity risk). Not confirming the right individual as an employee may result in the unauthorized disclosure of information (an information security risk or privacy breach, should personal information be disclosed). Regardless of the context, managing the risk of ensuring that a government organization is dealing with the right individual can be achieved consistently and coherently by means of identity assurance.

By definition, "identity assurance" is a measure of certainty (or a degree of confidence) that an individual, organization or device is who or what it claims to be. Identity assurance is used to answer the question, "How sure are you that you have the right individual, organization or device?[Footnote 2]

In addition to managing risk, a standardized approach to identity assurance allows people to interact with government programs or services that use, or rely on, identity establishment processes carried out elsewhere. For example, an individual may prove who he or she is once, according to standardized requirements, and the established identity for this individual can be relied on by many other programs and services. This is the essence of federation, which is discussed in subsection 3.9 of this document.

Different identity assurance levels allow government programs and services to carry out transactions commensurate with the level of risk. For some services, the level of risk is low; for others, it is higher. For example, the level of risk involved in providing personalized weather information to an individual is low, whereas the level of risk involved in accepting an application for a passport is higher.

The different identity assurance levels also allow government organizations to manage costs and to design optimal solutions using standardized services or capabilities developed for different (or lower) assurance levels while appropriately managing the residual risk.

Table 1 shows the identity assurance levels defined in the *Standard on Identity and Credential Assurance*.

Table 1: Identity Assurance Levels

Level	Description
4	**Very high confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause serious to catastrophic harm.
3	**High confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause moderate to serious harm.
2	**Some confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause minimal to moderate harm.
1	**Little confidence required that an individual is who he or she claims to be**. Compromise could reasonably be expected to cause nil to minimal harm.

The standardized levels range from one to four; each level describes a required degree of confidence that correlates to a range of expected harms should the level not be achieved and maintained. Subsection 3.2 of this document describes how a government organization determines which identity assurance level is required.

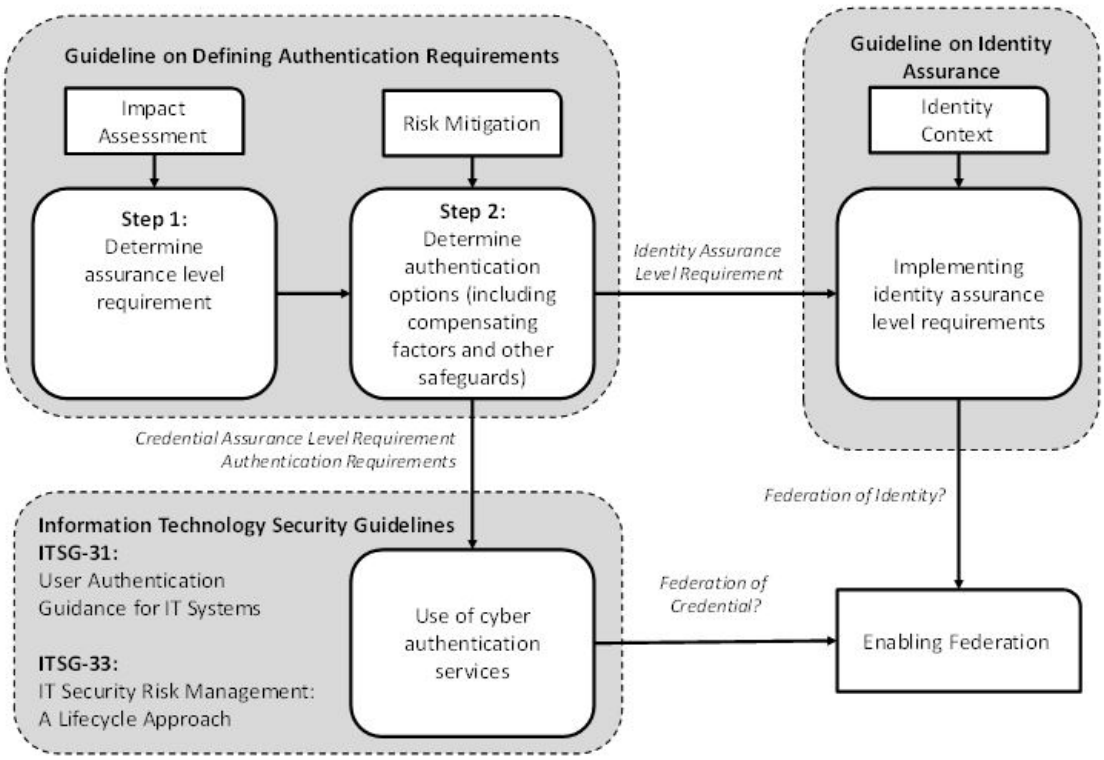
3. Guidelines for Implementing an Identity Assurance Level

3.1 Conducting an Assurance Level Assessment

An assurance level assessment should be conducted first to determine the assurance level requirement. The companion guidance document, *Guideline on Defining Authentication Requirements*, defines a two-step process that assists in determining this requirement.

Figure 1 presents an overview of the assurance level assessment and IT design processes in terms of the scope of the related Government of Canada guidelines.

Figure 1. Scope of Related Government of Canada Guidelines



[Text version: Figure 1. Scope of Related Government of Canada Guidelines]

The *Guideline on Defining Authentication Requirements* defines the following two-step process:

Step 1

- **Determine assurance level requirement**, which is 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

- **Determine authentication options** that will be used to achieve the assurance level requirement determined in Step 1. These authentication options are:
    1. **Identity assurance level requirement** specifies the minimum requirements to establish the identity of an individual for a given level of assurance. The identity assurance level requirement is the primary input into this guideline.
    2. **Credential assurance level requirement** specifies the minimum requirements to ensure that an individual has maintained control over a credential issued to him or her and that the credential has not been compromised. The guidelines for implementing these requirements are set out in CSE's ITSG (Information Technology Security Guideline)-31, *User Authentication Guidance for IT Systems*.
    3. **Authentication requirements** are the minimum technical design or business process requirements that are necessary to carry out an electronic or manual authentication process. The guidelines for implementing these requirements are set out in CSE'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** are additional 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. 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** are other controls put in place to manage risk or to ensure program integrity. Other safeguards may be security control mechanisms used in processes subsequent to authentication or indicators that are used to initiate exceptions or interventions.

3.2 Identity Assurance Level Requirements

This subsection provides detailed guidance on implementing the requirements specified in Appendix C of the *Standard on Identity and Credential Assurance*.

There are four categories of requirements to establish an identity assurance level. These four categories are listed below with a high-level control objective statement and a brief description.

Uniqueness. *An identity must be unique*.
Uniqueness ensures that individuals can be distinguished from one another and, when required, uniquely identified. Uniqueness is also used to determine identity information requirements.

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 needed to confirm the accuracy of the identity information and its linkage to the individual depends on the assurance level requirement determined by the program or service. The *Standard on Identity and Credential Assurance* defines two categories of evidence of identity: foundational evidence of identity and supporting evidence of identity (see subsection 3.4 of this document).

Accuracy of identity information. *Identity information about an individual must be accurate, complete and up to date.*
Accuracy ensures the quality of identity information - the information represents what is true about the individual and is complete and up to date. Accuracy can be confirmed by using an authoritative source or by corroborating different sources of information when no authoritative source is available.

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 is legally recognized within a jurisdiction.

For ease of reference, Table 2 is reproduced from Appendix C of the *Standard on Identity and Credential Assurance*. Table 2 specifies the minimum requirements by category associated with each level of assurance.

Table 2. Minimum Requirements to Establish an Identity Assurance Level

Requirement	Level 1	Level 2	Level 3	Level 4
Uniqueness	Define identity information	Define identity information	Define identity information Define context	Define identity information Define context

	Define context	Define context	Define context	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 **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

3.3 Requirements for Uniqueness

3.3.1 Uniqueness

The uniqueness requirement ensures that individuals can be distinguished from one another and that the right service is delivered to the right individual at the right time. Uniqueness reduces the possibility of an individual receiving a service or benefit intended for someone else.

Uniqueness is required when a service must deliver an output or benefit to a specific individual—for example, the **same** individual from a previous registration or enrolment process. In some cases the identity of the individual may not be required or desired, such as the identity of a survey respondent.

Uniqueness, on its own, does not determine eligibility or entitlement for a service or benefit. However, information that is collected to determine uniqueness may also be used for eligibility or entitlement purposes and may therefore be subject to other legislative and privacy requirements. In cases where a transaction has two or more purposes (for example, to determine identity and entitlement), the intended uses of the information need to be clear.

3.3.2 Defining Identity Context

In delivering programs and services, government organizations operate within a certain environment or set of circumstances known as the identity context. Identity context is further defined by factors such as mandate, target population (clients) and responsibilities prescribed by legislation or agreements.

Understanding and defining identity context assists government organizations in determining uniqueness requirements. Identity context helps establish what identity information is required, and what information is not required. It also helps determine commonalities with other government organizations or jurisdictions, and whether identity information or assurance processes can be used across contexts.

Identity context may be considered from the perspective of the individual, the federal organization or the Government of Canada. For example, an identity context may be the set of external services to citizens, or the set of internal services to employees.

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

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

3.3.3 Defining Identity Information

The term "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[Footnote 3].

Identity information is considered to be valid within a defined identity context (see subsection 3.3.2). Within an identity context, it is critical to be able to distinguish individuals from one another so that services can be delivered to the right individuals.

Under the *Directive on Identity Management*, government organizations are responsible for ensuring the legitimacy of identity when

- 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[Footnote 4].

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 both

- sufficient to distinguish between different individuals within an identity context; and
- sufficient to describe the individual as required by the service or program.

The identity attribute or the set of identity attributes used to distinguish a unique and particular individual, organization or device may also be referred to as an identifier. It is recommended that identity attributes used as identifiers be the same or continuous over time. In many cases continuity is not possible, and government organizations may choose instead to create or use an assigned identifier. This identifier is typically a numeric or alphanumeric string that is generated automatically, and that uniquely distinguishes between individuals and is independent of any other identity attributes.

Additional attributes may be used to further distinguish between similar individuals or to assist in the recognition of a particular individual. These attributes may not necessarily be unique to the individual (for example, hair colour, and height) or may change over time.

When defining or determining the sufficiency of identity information for a given service delivery context or program administration requirement, government organizations, for privacy reasons, should distinguish between identity information and program-specific personal information, which can overlap. This distinction ensures that the use of identity information is consistent with the original purpose for which the identity information was obtained and that it can be managed separately or protected by appropriate security and privacy controls[Footnote 5].

To minimize privacy risk, government organizations should reduce the overlap between identity information and program specific personal information as much as possible. However, when overlap is required, 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 personal information).

The following considerations apply when determining the sufficiency of identity information:

- Identity information that is intended to describe a real (existing) person or to distinguish one person from another is subject to accuracy of identity information requirements (see subsection 3.5).
- For privacy and security reasons, such as protecting the identities of individuals, some identity attributes may be randomly assigned identifiers, pseudonymous identifiers, user identifiers or usernames.
- Examples of identity information are name, date of birth, and sex, for individuals; business registration numbers, for organizations; and serial numbers and network identifiers, for telecommunications and computing devices.
- An identifier may be a unique identity 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 keys and universally unique identifiers.
- Assigned identifiers may be provided to other programs; however, there may be restrictions owing to privacy considerations or legislation.
- Existing or previously assigned identifiers that meet the uniqueness requirement may be used as identity information.

Government organizations need to be aware that the use of these identifiers may be subject to restrictions or have privacy implications.
- 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 Government of Canada Social Insurance Number.

3.4 Requirements for Evidence of Identity

Evidence of identity is an information record maintained by 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 2.

3.4.1 Foundational and Supporting Evidence of Identity

The *Standard on Identity and Credential Assurance* defines two categories of evidence of identity:

- **Foundational evidence of identity** establishes core identity information such as given name(s), surname, date of birth, sex and place of birth. Examples are records of birth, immigration and citizenship, from a vital statistics agency or immigration authority.
- **Supporting evidence of identity** 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 are 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[Footnote 6].

When defining operational requirements or procedures, it is a good practice to refer to documents specifically by name (for example, passport, driver's licence), in keeping with their original purpose, rather than generally as identity documents.

3.4.2 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 an individual to ensure delivery of a program or service to the individual;
- To determine that the identity information is accurate, complete and up to date; and
- To determine that the identity information is linked to the individual making the claim. Note that linkage requirements do not apply to Level 1 and Level 2 assurance levels.

It is recommended that government organizations have processes in place to ensure that the identity information about an individual

- is held only for the period needed; and
- is destroyed once it is no longer needed, e.g., upon the individual's death or voluntary withdrawal from a program or service.

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

Evidence of identity may be presented or accepted in the following forms:

Documentary evidence
: is any physical record of information that can be used as evidence (widely understood to mean information written on paper, but includes non-paper evidence more generally).

Electronic or digital evidence
: is any data 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.

The evidence of identity requirements specified in Table 3 are independent of the form in which the evidence is presented. Further, instances of evidence of identity should originate from, or be issued by, different authoritative sources.

3.4.3 Acceptability Criteria for Evidence of Identity

Table 3 sets out the acceptability criteria for foundational and supporting evidence of identity. 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 Category	Acceptability Criteria and Examples
	Acceptability criteria:

Foundational Evidence	• Evidence originates from an authoritative source that is
	  ◦ under the control of a federal, provincial or territorial government, or the local equivalent abroad;[Table 3 note i] and
	  ◦ used to maintain registration of specific vital events or to determine legal status.
	• Identity information that is incomplete or inconsistent with information provided by the individual (e.g., name change) may require additional confirmation by the authoritative source, or additional supporting evidence.
	
	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.
	
	Acceptability criteria:
	
	• Evidence originates from an authoritative source that is under the control of an approved organization.[Table 3 note ii]

Supporting Evidence	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. • Additional supporting evidence may be required in the case of incomplete or inconsistent identity information (e.g., name change). • 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 a driver's licence; • Passport or Certificate of Indian Status; and • Professional qualifications used in the issuance of professional credentials.

Table 3 Notes

Table 3 Note **i**

When the authoritative source is outside Canadian jurisdiction, the acceptability criteria will be determined through a risk-managed approach defined by the government organization.

Return to table 3 note i referrer

Table 3 Note **ii**

What constitutes an approved organization 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.

Return to table 3 note ii referrer

3.4.4 Considerations for Children, Minors and Other Vulnerable Individuals

Children, minors or other vulnerable individuals are more likely to be exploited for criminal purposes, and the tampering of their documents may result in more serious consequences. Providing services to these individuals often involves special circumstances and additional risk factors. For example,

- Children, minors and vulnerable individuals may not have sufficient evidence of identity to meet the requirements specified in the *Standard on Identity and Credential Assurance*.
- 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 on behalf of a child, minor or other vulnerable individual.

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 to initiate exceptions or interventions, as appropriate.
- Confirm that the applicant (for example, 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 that the recommendations in this subsection do not designate the authorized representatives who may act for other individuals—for example, parents acting for children, or lawyers acting for applicants.

3.4.5 Guidelines on Evidence of Identity Assurance Levels

Table 4 provides guidelines for the assurance levels related to evidence of identity presented in Table 3. The criteria are independent of the form (documentary or electronic) in which the evidence is presented.

Table 4. Assurance Level Guidelines for Evidence of Identity

Assurance Level	Requirements in Appendix C of the Standard	Guidelines[Table 4 note *]
Level 1	No restriction on what is provided as evidence	• Provide individuals with written notice that any false or 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. • Provide individuals with written notice that the unauthorized use of evidence of identity may result in the refusal of service or may be grounds for criminal prosecution.
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 (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. (Although rare, this situation could occur. For example, an authority may cease to exist and a new authority may reissue the same document.)
Level 4	**Three** instances of evidence of identity (at least one must be foundational evidence of identity)	• The stringency of this requirement may be increased, 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.

Table 4 Notes

Table 4 Note *****

It is understood that the guidelines specified at a given level (e.g., Level 3) are in addition to the guidelines specified for the lower levels (e.g., Level 1 and Level 2).

Return to table 4 note * referrer

3.5 Requirements for Accuracy of Identity

3.5.1 Confirming Accuracy of Identity Information

The requirement for accuracy ensures the quality of the identity information. Identity information is expected to represent what is true about an individual, and to be complete and up to date. To ensure the accuracy of identity information, the following considerations apply:

- **The identity information is correct.** Identity information for certain life events, such as marriage, may change over time. To maintain accuracy, identity information needs to be updated periodically.

- **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, since the individual's identity information does not cease to exist after death.
- **The identity information relates to the correct individual.** In large populations, some individuals may have the same or similar identity information—for example, name, sex and date of birth. Although the requirement for uniqueness addresses this issue, the possibility of relating identity information to the wrong individual remains.

Identity validation is the process of confirming the accuracy of identity information as established by an authoritative party[Footnote 7]. Depending on the program or service requirements and the privacy considerations, government organizations may validate identity information using different authoritative sources. For example, a date of birth may be electronically validated using a provincial vital statistics registry.

If validation using an authoritative source is not feasible, other methods may be used, such as 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 3.7.2.

Determining the accuracy of identity information involves confirming that the individual currently exists or previously existed (was alive but is now deceased). Identity information needs to relate to a real individual (living or dead) and not to a non-existent or incorrect individual.

When the authoritative source is outside Canadian jurisdiction, the accuracy of identity information may be determined through a risk-managed approach.

Accuracy of identity information is independent of whether an individual is living or deceased. An individual's identity information does not cease to exist after death. In cases of death, it becomes important that an individual's identity information is used properly by authorized individuals—for example, by the surviving spouse or executor.

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

An assigned identifier (see subsection 3.3.3) should be subject to an exact match. In cases where the integrity of an identifier can be determined using a mathematical algorithm (for example, checksum), these methods should be applied as part of the validation process.

Table 5 provides guidelines for requirements related to the accuracy of identity information presented in Table 1. This guidance applies only in establishing the accuracy of identity information.

Table 5. Assurance Level Guidelines for Accuracy of Information

Assurance Level	Requirements in Appendix C of the Standard	Guidelines[Table 5 note *]
Level 1	Acceptance of self-assertion of identity information by an individual	• Provide notice to individuals that they are required to provide accurate information about who they are. • Provide notice to individuals 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 an appropriate authority	• Request that individuals acknowledge that their identity information is their own and that it is consistent with the evidence of identity provided. • Provide notice to 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 validating the issuing authority and checking certificate revocation lists. • Provide a warning or caution when seeking validation from an authoritative source if the record or evidence is flagged for any reason (e.g., fraud, expiry). • If a remote electronic validation process is not available (as there may be no facility for remote access or network connectivity) a local or manual validation process may be used instead. • 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 an authoritative source **and** Confirmation that supporting evidence of identity originates from an appropriate authority, using an authoritative source **or** Inspection by a trained examiner	• Use formal matching methods to determine accuracy within specified tolerances (e.g., name variances). • Confirm that 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 an authoritative source **and** Confirmation that supporting evidence of identity originates from an appropriate authority, using an authoritative source **or** Inspection by a trained examiner	• Use the equivalent of Level 3 requirements for evidence of identity, but put in place more stringent matching criteria to determine accuracy within specified tolerances. If a match falls outside a specified tolerance, it should be treated as an exception and risk-managed accordingly. • 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 and have in place risk mitigation procedures. • Record in an audit log the results of the confirmation process, including when matches fall outside specified tolerances.

Table 5 Notes

Table 5 Note *****

It is understood that the guidelines specified at a given level (e.g., Level 3) are in addition to the guidelines specified for the lower levels (e.g., Level 1 and Level 2).

Return to table 5 note * referrer

3.6 Requirements for Linkage to an Individual

The linkage requirement ensures that identity information relates to the individual making the claim. Linkage ensures that the identity information relates to a real person who is using his or her own identity information—that is, the identity information is not being fraudulently used by an imposter.

The process of determining linkage to an individual is usually carried out when a person with no prior relationship or association with a program or service is initiating a transaction for the first time. For example, a first encounter with a program registration or a service enrolment process usually requires an individual to provide an indication of proof of identity.

Linkage to an individual may also be referred to as identity verification. Identity verification is not the same as identity validation. Identity verification is the process of confirming that the identity information relates to the person making the claim.

3.6.1 Methods for Determining Linkage to an Individual

The *Standard on Identity and Credential Assurance* describes four methods that can be used to determine linkage to an individual[Footnote 8].

- **Knowledge-based confirmation** compares personal or private information to establish an individual's identity. Examples of information that can be used for knowledge-based confirmation are passwords, personal identification numbers, hint questions, program-specific information, and credit or financial information.
- **Biological or behavioural characteristic confirmation** compares biological (anatomical and physiological) characteristics in order to establish a link to an individual. An example is a facial photo comparison.
- **Trusted referee confirmation** relies on a trusted referee to establish a link to an individual. The trusted referee is determined by program-specific criteria. Guarantors, notaries and certified agents are examples of trusted referees.
- **Physical possession confirmation** requires physical possession or presentation of evidence to establish an individual's identity.

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

Table 6. Examples of Methods for Determining Linkage to an Individual

Method Type	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 information collected or generated over a period of time (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 voice print. • **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 Table 6 note *	• **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. • **Certified agent:** An individual who has been approved to vouch for, or act on behalf of, an individual.

Physical possession confirmation	• **Physical demonstration of control:** An individual physically demonstrates the exclusive possession or control of a secure document or physical object (e.g., token) that was previously issued to the individual:
	  ◦ In the case of a secure document, confirmation may involve the submission for examination of security features or validation of the document; and
	  ◦ In the case of a secure physical object, confirmation 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.

Table 6 Notes

Table 6 Note *

It is understood that the guidelines specified at a given level (e.g., Level 3) are in addition to the guidelines specified for the lower levels (e.g., Level 1 and Level 2).

Return to table 6 note * referrer

3.6.2 Linkage Method Guidelines

Table 7 provides guidelines on selecting a method for confirming the linkage of identity information to an individual.

Table 7. Assurance Level Guidelines for Linkage Methods

Assurance Level	Requirement	Guidelines[Table 7 note *]
Level 1	No requirement	• Use methods to ensure that interaction is with a **real** individual (not an automated process).
Level 2	No requirement	• Use methods to ensure that the initial and subsequent interactions can be linked to the **same** individual making the claims. This can be achieved by relying on a credential assurance provided by an authentication service.
Level 3	At least **one** of the following linkage methods: • Knowledge-based confirmation • Biological or behavioural characteristic confirmation • Trusted referee confirmation • Physical possession confirmation	• These linkage methods should be used in addition to, or separately from, relying on a credential assurance provided by an authentication service. • The efficacy of linkage methods is dependent on factors such as the service delivery context, the threat environment, and the evidence that the individual is willing or capable of providing. Care should be taken to select and develop linkage methods that do not place undue burden on the individual or that can introduce unintentional vulnerabilities or risk (e.g., using sensitive personal information that may have an adverse effect if compromised). • Linkage methods may be enhanced by implementing a combination of techniques described in Table 6 (instead of only one technique per method). For example, a knowledge-based confirmation method may combine static and dynamic knowledge-based confirmation methods. • Similarly, for biological or behavioural characteristic confirmation, the method may include a combination of techniques. For example, biological or behavioural characteristic confirmation may include a combination of facial comparison and fingerprint comparison.
Level 4	At least **three** of the following linkage methods: • Knowledge-based confirmation • Biological or behavioural characteristic confirmation • Trusted referee confirmation • Physical possession confirmation	• Ensure that the linkage methods used are independent of each other (the use of one linkage method cannot compromise the use of another).

Table 7 Notes

Table 7 Note *****

It is understood that the guidelines specified at a given level (e.g., Level 3) are in addition to the guidelines specified for the lower levels (e.g., Level 1 and Level 2).

Return to table 7 note * referrer

3.7 Risk and Fraud Considerations

3.7.1 Risk Considerations

Managing identity risk is similar to managing other corporate risks; however, there are special considerations for identity:

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

stolen or fraudulent.
- 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.

The following are some of the specific risk factors related to the identity of individuals:

- An individual may be associated with incorrect identity information; for example, two individuals may have identical names and dates of birth. The result is a possible confusion of services and entitlements.
- Identity information may be inaccurate or out of date. Life events, such as marriage, may result in name changes. Data entry errors may result in the transposition of dates and names.
- Identity information may be asserted by parties that cannot be determined to be reliable or authoritative. An individual, such as a newcomer or visitor to Canada, may present identity information that is possibly accurate, but impossible to validate against an authoritative source.
- Identity information may be used by someone other than its rightful owner or authorized representative, such as in the case of an individual who uses the identity information of another individual. If this use is intentional, it may be considered to be identity fraud under subsection 403(1) of the *Criminal Code*.
- 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. This is considered identity fraud.
- Documentation may be lacking. An individual may have documents that cannot be determined to be genuine or cannot be validated against an authoritative source.

3.7.2 Fraud Considerations

Government organizations should be familiar with the different methods of fraud, as these may present risks when implementing the requirements of the *Standard on Identity and Credential Assurance*.

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

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

Records fraud is the unauthorized creation, insertion, alteration 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 or entitlements that are not legitimate. The following are the techniques of record fraud:

- **External threat agent:** Unauthorized creation, insertion, alteration or deletion of authoritative records as a result of external threat agents that have intruded into the record system.
- **Insider fraud or collusions:** Unauthorized creation, insertion, alteration or deletion of authoritative records by individuals in a position of trust or with access to sensitive or personal information.

Imposter fraud is the fraudulent use of another person's identity information, whether this person is real or fictitious. Imposter fraud may involve the following activities:

- **Use of another person's evidence of identity, where the other person is a stranger**. To use another person's identity, the imposter may alter his or her appearance or may alter the evidence of identity. In these cases, the imposter usually does not have detailed knowledge of the victim, and fraudulent use can be detected using the confirmation methods described in subsection 3.6.1.
- **Use of another person's evidence of identity, where the other person is known.** The fraudster may be acting as an imposter (as described above). The fraudster may also be attempting to act on behalf of another individual by means of an unauthorized role or relationship. Additional methods should be used to ensure that an individual is legitimately acting on behalf of another individual.
- **Use of another person's evidence of identity, where the other person is a fabricated or synthetic identity.** This is the most sophisticated type of fraud and may be carried out in conjunction with records fraud and document fraud. Owing to its sophistication, this type of fraud is usually carried out by highly motivated threat agents such as organized crime.

3.8 Integration Considerations

Identity assurance level requirements are typically part of a more comprehensive set of program or service requirements that are integrated into a broader business or system process. This subsection presents considerations for integrating identity assurance level requirements into business or system processes. For example, one department may decide to integrate these requirements into a client registration process to support a single program. Another department may decide to implement the 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 of the requirements for the identity assurance levels determined for their programs and services.

When implementing the requirements for identity assurance, it is recommended that government organizations consider the following:

- The requirements are independent of the delivery channel and the technology used. This independence supports the Government of Canada's commitment to multi-channel access and service delivery.
- It is a good practice to consider channel and service delivery alternatives that best suit the needs of clients, that enable accessibility to people with a wide range of disabilities, and that encourage adoption through trust and confidence.
- The requirements may be implemented in collaboration with other government organizations when considering federation (see subsection 3.9).
- When integrating the requirements of the *Standard on Identity and Credential Assurance* into business or system processes, government organizations should ensure that identity assurance procedures are as efficient, and transparent to the client as possible.

3.9 Federation Considerations

A federation is a cooperative agreement between autonomous entities that have agreed to work together. It can consist of public and private sector organizations, different jurisdictions or different countries. Many federations are informal in nature and are based on shared practices and objectives that have been developed over time. As these informal federations mature, the informal arrangements are replaced by agreed-on trust frameworks and assessment processes that can include contractual agreements, service agreements, legal obligations and dispute resolution mechanisms.

Federations become a compelling option when there is a business need to provide online services seamlessly across departmental and jurisdictional boundaries in a way that includes both public and private service providers. Fulfilling this need requires a level of trust between different kinds of organizations that have diverse mandates and act under different authorities. A trust framework stipulates adherence to agreed-on standards, formalizes assessment processes, and defines the roles and responsibilities within multi-party arrangements.

3.9.1 Enabling a Pan-Canadian Approach

The Government of Canada is committed to assisting federal, provincial, territorial and municipal partners in fulfilling their respective program and service requirements, using trusted common processes.

The Government of Canada is collaborating with jurisdictions to develop a pan-Canadian approach to federating identity that respects the autonomy and the laws of the different jurisdictions. In November 2014, the Federal, Provincial, Territorial Deputy Ministers' (FPT DM) Table on Service Delivery Collaboration approved the *Pan-Canadian Identity Validation Standard*[Footnote 9], which standardizes identity information and personal information validation requests and responses between federal, provincial, territorial and municipal organizations.

It is recommended that government organizations incorporate the *Pan-Canadian Identity Validation Standard* into the implementation planning of their programs and services.

3.9.2 Implementing a Federated Model

This guideline can be used as a framework to help a government organization transition to a federated model and rely on trusted services provided by other organizations. Instead of implementing the requirements for identity assurance on its own, a government organization may choose to adopt a federated model. Before becoming a member of a federation, however, a government organization should ensure that certain key elements of a federated model are implemented within its own organizational context, specifically, the roles of authoritative party and relying party.

An authoritative party is defined in the *Standard on Identity and Credential Assurance* as a federation member that provides assurance (of credential or identity) to other members (relying parties). A relying party is a federation member who relies on assurances (of credential or identity) from other members (authoritative parties). One unit of an organization may assume the role of an authoritative party while the other units take on the role of relying parties. For example, a departmental human resources (HR) system could play the part of the authoritative party regarding employee information, while the departmental security system responsible for issuing employee identification cards takes on the role of the relying party.

Table 8 outlines key considerations for taking on the roles of authoritative party and relying party.

Table 8. Considerations for Implementing a Federated Model

Organizational Role	Not a Member of a Federation	As a Member of a Federation
	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.	**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

Acting in the role of an authoritative party	• May provide identity assurance **only** for own organization (cannot provide identity assurance outside the organization). • May provide identity information that supports an identity validation process in another organization. • Is responsible for managing its own organizational identity risk. **Organizations should:** • Implement the requirements of the *Standard on Identity and Credential Assurance* (the standard) at the required assurance level. Example: A departmental HR system that maintains an authoritative employee record.	evidence of identity that may be used by other organizations. • May provide an identity assurance 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 requirements of the standard at the required assurance level. • Participate as an authoritative party in a federation and comply with federation criteria established by the Chief Information Officer of the Government of Canada.
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 another organization. • Identity risk remains the responsibility of organization. • Program-specific risk remains the responsibility of the organization. **Organizations should:** • Implement the requirements of the standard at the required assurance level; **or** • Enter into an arrangement with another party to implement the requirements of the standard on its behalf (e.g., memorandum of understanding, bilateral agreement). Example: A departmental security system that relies on an authoritative employee record maintained by a departmental HR system.	**Considerations for organizations:** • May rely upon identity assurances as provided by authoritative party participants in the federation (to a level of assurance). • May share identity risk when relying on identity assurances (to a level of assurance). • Program-specific risk remains the responsibility of the organization. **Organizations should:** • Participate in federation as a relying party; **and** • Comply with federation criteria established by the Chief Information Officer of the Government of Canada.

3.9.3 Adoption of Trust Frameworks

The Government of Canada is participating in the development of a Pan-Canadian Identity Trust Framework that will facilitate work with other jurisdictions and assess industry trust frameworks for use by the Government of Canada. The *Standard on Identity and Credential Assurance*, as well as this guideline, will be an integral part of this trust framework. Government organizations can be assured that the standard and its implementation are designed to support the adoption of existing and emerging trust frameworks.

3.10 Other Policy and Legislation Considerations

When implementing the requirements for identity assurance, government organizations should ensure compliance with other applicable policy instruments or legislation. For example, another policy may require a government organization to use a certain assigned identifier or may permit the collection of only a defined set of attributes that can be used as identity information.

3.10.1 *Privacy Act* and *Policy on Privacy Protection*

When implementing identity assurance requirements, government organizations must comply with the *Privacy Act* and the *Policy on Privacy Protection.* Consideration needs to be given to the right to the privacy of individuals, while ensuring access to their personal information and maintaining its accuracy.

Information about an identifiable individual is considered to be personal information and is therefore 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 to be 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 *Policy on Privacy Protection* and its related privacy directives, standards and guidelines apply to identity information. 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.

It is important that government organizations distinguish between the information they collect to support identity assurance requirements and other personal information that is collected, used, retained and disposed of 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.

Identity information may be collected, used, retained, disclosed and disposed of as part of a larger business process, such as processing registrations or determining 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*. Compliance 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 separating records into different data repositories, encrypting data, and substituting or mapping identifiers. Regardless of the mechanisms used, the resulting information should be considered to be personal information.

3.10.2 *Policy on Service*

Federal government organizations must comply with the *Policy on Service.* When implementing identity assurance requirements, government organizations should consider designing services that have a strong client orientation and that are integrated, simple, timely and convenient.

Government organizations, as they develop new services and transform existing services, are encouraged to think beyond document-based processes and technology-specific implementations. To enable participation in a broader identity management federation, government organizations are also encouraged to standardize practices, processes and technologies that can be extended beyond their own organizations in a manner that maintains trust and integrity.

For more information on complying with service delivery requirements, see the *Policy on Service*.

3.10.3 *Criminal Code* of Canada

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

- **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 56.1(2);
- **Subsections 57(1) to 57(6)** regarding the use of the Canadian passport;
- **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 (identity theft); and
- **Section 403** regarding fraudulent personation of another person.

3.10.4 Other Policies and Legislation

In addition to the policies and legislation discussed above, government organizations should determine whether other policy instruments or legislation may be applicable to their context.

4. 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*
- *Directive on Social Insurance Number*
- *Guideline on Defining Authentication Requirements*
- *ITSG-31: User Authentication Guidance for IT Systems*
- *ITSG-33: IT Security Risk Management: A Lifecycle Approach*
- *Policy on Government Security*
- *Policy on Information Management*
- *Policy on Privacy Protection*
- *Policy on Service*
- *Standard on Identity and Credential Assurance*
- *Standard on Security Screening*

For details on these instruments and other resources, including industry and international documents, refer to Appendix B.

5. Additional Information

5.1 Next Review Date

This guideline will be reviewed and updated as required.

5.2 Enquiries and Comments

For interpretation of any aspect of this Guideline, please contact Treasury Board of Canada Secretariat Public Enquiries.

Appendix A: Key Terms and Definitions

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

biological or behavioural characteristic confirmation:
A process that compares biological (anatomical and physiological) characteristics in order to establish a link to an individual (for example, 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).

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 (for example, key, token, document, identifier) and that the credential has not been compromised (for example, 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 (for example, 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:

Any physical record of information that can be used as evidence (widely understood to mean information written on paper, but includes non-paper evidence more generally).

electronic or digital evidence:

Any data that are 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, also known as an identity data element.

identity context:

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

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 individuals and sufficient to describe 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—for example, 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:

The process of confirming the accuracy of identity information as established by an authoritative party.

identity verification:

The process of confirming that the identity information relates to the person making the claim.

knowledge-based confirmation:

A process that compares personal or private information 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:

The process of 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 (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 guarantor, notary and certified agent. (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 formally underpins trust relationships by stipulating adherence to standards, formalizing assessment processes, and defining roles and responsibilities of multi-party arrangements.

trust relationship:
A defined arrangement or agreement that ensures confidence between the parties to the relationship.

Appendix B: Annotated References

Treasury Board Policy Instruments

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

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. Refer specifically to section 3.0, “Assurance Level Assessment Process.”
- *Guideline on Identity Assurance*. This guideline provides guidance on implementing the requirements specified in Appendix C of the *Standard on Identity and Credential Assurance*.

Policy on Privacy Protection

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

- 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 that has been used, is being used, or is available for use for administrative purposes.

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.

Policy on Service

The objective of the *Policy on Service* is to establish a strategic and coherent approach to the design and delivery of Government of Canada external and internal enterprise services that is client-centric, realizes operational efficiencies and promotes a culture of service management excellence.

The Policy on Service is supported by the following guidelines:

- *Guideline on Service Agreements: An Overview*. This guideline provides program and service managers and executives with an overview of the key concepts and steps in establishing service agreements.
- *Guideline on Service Agreements: Essential Elements.* This guideline provides advice, guidance, practical examples and templates for individuals charged with developing a service agreement or reviewing a service agreement drafted by the other party in an evolving service relationship.
- *Guideline on Service Standards.* This guideline provides general guidance on the use of service standards across the Government of Canada. Additional material on service standards from other Treasury Board of Canada Secretariat policy centres for specific types of services, such as grants and contributions, regulatory affairs and human resources, complement this guideline.

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

Other Related Guidelines and Standards

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

Threat and Risk Assessments

Government organizations may want to conduct a more generalized security risk assessment as an additional consideration when implementing the minimum requirements in Appendix C of the *Standard on Identity and Credential Assurance*. For example, a security risk assessment may be useful in addressing highly specialized threat agents associated with the rapidly evolving online environment and the potential vulnerabilities introduced by newer technologies—for example, tablets or mobile phones.

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 CSE:

- *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.

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 are available by contacting the Chief Information Officer Branch (see subsection 5.2 of this guideline).

- *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.
- *Federating Identity*. The Chief Information Officer Branch is currently developing criteria for formally participating in the Government of Canada federation. Further information can be obtained by contacting the Chief Information Officer Branch.

Pan-Canadian Standards Development

Government organizations are encouraged to become familiar with standards that enable a pan-Canadian approach. Pan-Canadian standards are currently being developed by the Identity Management Sub-Committee (IMSC), an inter-jurisdictional body that reports to the Public Sector Chief Information Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC) (also referred to as the Joint Councils). These councils are supported by the Institute for Citizen-Centred Service.

- *Pan-Canadian Identity Validation Standard*. This document standardizes identity information and personal information validation requests and responses between federal, provincial, territorial, and municipal organizations.

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 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 should 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; as result, there may be dependencies between different categories of requirements. In applying other related standards, government organizations should question whether requirements apply in 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) in their context.

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

- The US *Federal Identity and Credential Access Management* (FICAM) *Trust Framework Provider Adoption Process* (TFPAP). TFPAP is the mechanism used by the US government to leverage industry-based credentials that citizens already have, for use on government websites.
- *E-Authentication Guidance for Federal Agencies* (OMB M-04-04).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 US federal agencies implementing electronic authentication (e-authentication). This guideline supports the implementation of OMB M-04-04.
- *Information Technology – Security Techniques – Entity Authentication Assurance Framework* (ISO/IEC 29115:2013).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 a set of documents that includes assurance levels, an assessment scheme and certification requirements for identity-proofing services, and credential strength and credential management services.
- *Requirements and Implementation Guidelines for Assertion, Evidence and Verification of Personal Identity* (ANSI/NASPO-IDPV-2014). 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.

Footnotes

Footnote fn1

For a definition of identity and other terms used in this guideline, see Appendix A.

Return to footnote 1 referrer

Footnote fn2

This guideline applies only to individuals.

Return to footnote 2 referrer

Footnote fn3

Standard on Identity and Credential Assurance, Appendix A

Return to footnote 3 referrer

Footnote fn4

Directive on Identity Management, subsection 3.5.

Return to footnote 4 referrer

Footnote fn5

Additional controls as required by applicable legislation, such as *the Access to Information Act* and the *Privacy Act*.

Return to footnote 5 referrer

Footnote fn6

Standard on Identity and Credential Assurance, Appendix A.

Return to footnote 6 referrer

Footnote fn7

Identity validation is also known as identity information validation. The best reference on identity validation is the unpublished *Pan-Canadian Identity Validation Standard*, which is available by contacting the Security and Identity Management Division of the Chief Information Officer Branch.

Return to footnote 7 referrer

Footnote fn8

Standard on Identity and Credential Assurance, Appendix A.

Return to footnote 8 referrer

Footnote fn9

The *Pan-Canadian Identity Validation Standard* will be posted on the Institute for Citizen-Centred Service's website and GCPedia

Return to footnote 9 referrer