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

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

Guideline on Identity Assurance

Chief Information Officer Branch
Consultation Draft
April 25, 2013

Canada

Table of Contents

List of Tables

List of Figures

1.0 Purpose

The purpose of this guideline is to support the implementation of minimum requirements to establish an identity assurance level for an individual as specified in requirement 6.1.4 of the Standard on Identity and Credential Assurance and as listed in Appendix C. This standard is issued under the Policy on Government Security and the Directive on Identity Management.

This guideline is intended to be used in conjunction with the Guideline on Defining Authentication Requirements which provides departments with an assessment framework to determine their identity assurance level requirements.

This guideline may also be used to support security checks related to identity and specified in the Standard on Security Screening of Individuals (currently in draft). This standard defines requirements related to security screening practices for the Government of Canada.

For requirements related to security and IT design, departments may wish to consult CSEC ITSG-31 Information Technology Security Guideline - User Authentication Guidance for IT Systems which defines authentication requirements for IT systems and ITSG-33 IT Security Risk Management: A Lifecycle Approach

1.1 Audience

This guideline is intended for:

- **Program and Service Delivery Managers**[1], who are responsible for identifying Government of Canada clients (individuals and business), employees and contractors as a critical part of their program or service delivery requirements,

- **Security Practitioners,** who recommend, design, build or provide solutions to meet program requirements. The assurance level requirements determined by responsible managers may be used in the design and technical recommendation process.

1.2 Application

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

This guideline assists in the standardization of how the identities of individuals are established in relation to government programs and services. This guideline is also intended to assist in the transition towards a federated approach to identity.

This guideline focuses on establishing the identity assurance level of individuals. However, the principles and guidelines can be applied to devices and organizations. Guidelines specific to devices and organizations will be provided in a later revision of this document or in a separate guideline.

The management of relationships between individuals, organizations and devices is outside of the scope of this guideline. The guideline does acknowledge that relationships exist between individuals, organizations

[1] 'Program and Service Delivery Managers' are referred to in the remainder of the guideline as 'responsible managers'

and devices for the purposes of authority or granting permissions to act on behalf of others. Examples used and accompanying discussion concerning relationships should not be construed as guidance.

This guideline does not apply to access, authorization or entitlement decisions. The determination of access, authorization and entitlement decisions is outside of the scope of this guideline.

This guideline does not recommend specific technologies, architectures or solutions.

This guideline does not confer authority beyond what is prescribed in the standard.

1.3 Key Terms and Definitions

Key terms and definitions are provided below. These definitions may also be found in Appendix A of the Standard on Identity and Credential Assurance..

Assurance A measure of certainty that a statement or fact is true.

Assurance level A level of confidence that may be relied on by others.

Authoritative party A federation member that provides assurances (of credential or identity) to other members (relying parties).

Authoritative source A collection or registry of records maintained by an authority that meets established criteria.

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

Credential A unique physical or electronic object (or identifier) issued to, or associated with, an individual, organization or device.

Credential assurance The assurance that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, modified).

Credential assurance level The level of confidence that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, corrupted, modified).

Credential risk The risk that an individual, organization or device has lost control over the credential that has been issued to him or her.

Evidence of identity A record from an authoritative source indicating an individual's identity. There are two categories of evidence of identity: foundational and supporting.

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.

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.

Identity A reference or designation used to distinguish a unique and particular individual, organization or device.

Identity assurance A measure of certainty that an individual, organization or device is who or what it claims to be.

Identity assurance level The level of confidence that an individual, organization or device is who or what it claims to be.

Identity management The set of principles, practices, processes and procedures used to realize an organization's mandate and its objectives related to identity.

Identity risk The risk that an individual, organization or device is not who or what it claims to be.

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

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

Relying party A federation member that relies on assurances (of credential or identity) from other members (authoritative parties).

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.

Trusted referee confirmation A process that relies on a trusted referee to establish a link to an individual. The trusted referee is determined by program-specific criteria. Examples of trusted referee include guarantor, notary and certified agent.

2.0 Context and Background

2.1 Introduction

Identity is at the core of most government business processes involving valuable resources and sensitive personal information. Once the identity 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 identity. For many service encounters or client transactions, departments must ensure that they are dealing with the right person (or organization or device) so that they can meet and fulfil their program objectives.

Identity is also at the core of trusted relationships between individuals, organizations and devices. Federation is a network of trusted relationships that includes people, organizations, jurisdictions, or international bodies. For these trusted relationships to be valuable and effective, it's necessary to know with confidence who (or what) is standing behind a transaction. This is known as federating identity.

As part of its overall approach to federation, the Government of Canada is undertaking the next step of federating identity. Federating identity is a whole-of-government approach that enables departments and agencies to fulfill program and service requirements by relying on identity and credential assurance processes that have been carried out by another department or organization. The federated approach is part of a larger Pan-Canadian context that respects the autonomy and the laws of the different jurisdictions.

The underpinning of the Government of Canada's approach to federating identity is the principle that there is no single authoritative source of identity information within Canada. Instead, there are a number of authoritative sources enabled by federal, provincial and territorial acts and regulations. These authoritative sources are recognized across the different jurisdictions and include vital events, benefits administration taxation, legal status and entitlements, to name a few. As a result, no department, jurisdiction, or organization has a comprehensive picture of individuals as they carry on with their lives within the Canadian context. This is desirable from a privacy perspective but there are challenges related to providing seamless services across jurisdictions and effectively combatting fraudulent activity.

Another key principle is that there is also no single authoritative identity document within Canada. Instead, there are numerous official documents and records that are used as evidence to establish or verify identity (e.g. birth certificates, driver's licenses, etc.). No document or record is to be considered as the sole authoritative identity document or record for an individual. Instead, documents and records can be used as evidence of identity along with other options available to an individual in making themselves known to a program or service. As digital delivery methods become more trustworthy and secure, electronic validation and digital identity methods will become viable options in addition to the traditional document-based methods.

For a complete description of the Government Canada's approach, please refer to Federating Identity Management in the Government of Canada: A Backgrounder

Currently, federal departments are dependent on evidence of identity originating from other jurisdictions, other countries or other federal departments that have similar dependencies. Today, evidence is predominantly in the form of physical documents, such as birth certificates, driver's licenses or citizenship certificates. These documents are accepted with a pre-defined inspection or validation process. Identity risks due to document-based authentication practices have evolved over the decades. The practices have worked well in the past but they are difficult to translate to or make appropriate for the online context. It is difficult (indeed impossible) to physically present a document and manage the associated risk in an online process. Alternative methods are required.

Currently, electronic authentication practices in the online or digital environment are still evolving. As well, the different types of threats, vulnerabilities, and policy issues continue to evolve as well. Despite the uncertainties of these new practices, clients are demanding online services and they expect the same level of security, privacy and authentication rigour as currently exists in the physical world. It is now necessary to think beyond document-based approaches due to the demand by clients but also due to the potential cost savings for government.

As government systems become increasingly interconnected, identity has become an essential component that must be managed beyond a single system or organization. Furthermore, identity's counterpart, identity risk, must be managed across these systems and across organizational and jurisdictional boundaries. This can only be achieved through standardization - the first step towards consistency, interoperability, and, eventually, identity federation. The vision of an identity federation: once an identity is established it should be reliable for use by others throughout the federation.

As departments begin the implementation of the Standard on Identity and Credential Assurance, they are encouraged to think beyond document-based processes. They are also encouraged to think beyond their own organization and how they (and their clients) might benefit from participating in an identity federation.

Finally, departments are also encouraged to think beyond the specific technology implementation. Technology changes rapidly and what may be appropriate technology today, may not continue to be appropriate in the face of changing client expectations and a rapidly evolving environment.

2.2 Federation and Trust Frameworks

The first step towards participation in federation and the adoption of trust frameworks is standardization. Standardization is the basis for common practices and allows for portability and interoperability across different systems, services and organizations. The implementation of the Standard on Identity and Credential Assurance supported by this guideline will facilitate portability and interoperability within the Government of Canada, the adoption of standardized trust frameworks and participation within federations.

A federation is a cooperative agreement between autonomous entities that have agreed to work together. A federation comprises of multi-party trust relationships that are supported by standards to enable interoperability, to realize efficiencies and to reduce risk. Depending on the nature and formality of a federation, it may be supported by contractual agreements including service agreements, legal obligations, and dispute resolution mechanisms. Many federations are also informal in nature and governed by shared practices and common understanding that have evolved over time. At present, no formalized identity federation exists within Canada, but one is anticipated in the near future.

A trust framework is an agreement, within a relevant legislative context, that defines the set of standards, policy, business and technical requirements to which members of a federation have agreed to comply. Central to trust frameworks is the recognition that assurance, or more specifically, level of assurance is a critical ingredient to formalizing standards-based services, competitive business models, and appropriate client-centric models. Presently, there are several trust frameworks available and provided by industry. These include frameworks from the Kantara Initiative and the Open Identity Exchange (OIX). It is anticipated the Government of Canada will adopt one or several trust frameworks. The adoption process for the Government of Canada is currently being developed.

2.3 Identity Assurance and Credential Assurance

The standard makes a distinction between identity assurance and credential assurance. This distinction, or separation, is necessary to enable departments to integrate into a federation using a phased incremental approach and to comply with privacy and program legislation requirements.

Credential Risk and Credential Assurance

A *credential risk* is the risk that an individual, organization or device has lost control over the credential that has been issued to him or her or the credential has been otherwise compromised.

A *credential assurance* is a measure of certainty that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, modified).

A credential assurance is intended to answer the question “How sure are you that you have the same individual, organization or device, without having knowledge of their identity, before delivering a service or carrying out a transaction. A credential assurance is defined independently from identity assurance. A credential assurance can have different levels, known as *credential assurance levels*.

The use of standardized credential assurance levels has allowed for the implementation of commercially offered authentication services currently available to departments:

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

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

Identity Risk and Identity Assurance:

An *identity risk* is the risk that an individual, organization or device is not who or what it claims to be.

An *identity assurance* is a measure of certainty (or level of confidence[2]) that an individual, organization or device is who or what it claims to be. An identity assurance is intended to answer the question “How sure are you that you have the right individual, organization or device, before delivering a service or carrying out a transaction?” Identity assurance is defined independently from credential assurance. Identity assurance can have different levels, known as *identity assurance levels*.

The objective of a standardized identity assurance level is to manage identity risk to an acceptable level and to provide a standardized identity assurance service to other organizations that are relying parties within a federation.

Currently, there are no standardized identity assurance services in use by the Government of Canada. Over time, standardized identity assurance services will be developed and made available through federation. It is recognized that due to policy and legislative requirements, the development of these services will be a complex undertaking will be implemented as incremental components. Taking this into account, the requirements in Appendix C of the Standard on Identity and Credential Assurance are being designed in a manner such that they may be implemented as individual pilot projects prior to becoming components of a GC-wide service offering.

2.4 Managing Identity Risk

The objective of the Standard on Identity and Credential Assurance is to ensure that identity risk and credential risk is *managed consistently and collaboratively within the Government of Canada and with other jurisdictions and other industry sectors*. Managing identity risk is an important step towards supporting the Government of Canada’s vision to enable a federation of organizations that trust each other’s assurances of identity. This is also referred to as *federating identity*.

[2] The terms ‘measure of certainty’, ‘level of confidence’, and ‘level of assurance’ are used interchangeably in the Standard and Guideline. The reader should consider these as being equivalent.

This guideline focuses on management identity risk. Managing identity risk is not dissimilar to managing any other corporate or departmental risk. However there are special considerations for identity risk:

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

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

For individuals, identity risk can be caused by one or a combination of the following (with examples):

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

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

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

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

Credential Risk in Relation to Identity Risk

Credential risk is separate from but closely related to identity risk. While not the focus of this guideline, credential risk is discussed to assist the reader in understanding how it is differentiated from and related to identity risk.

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

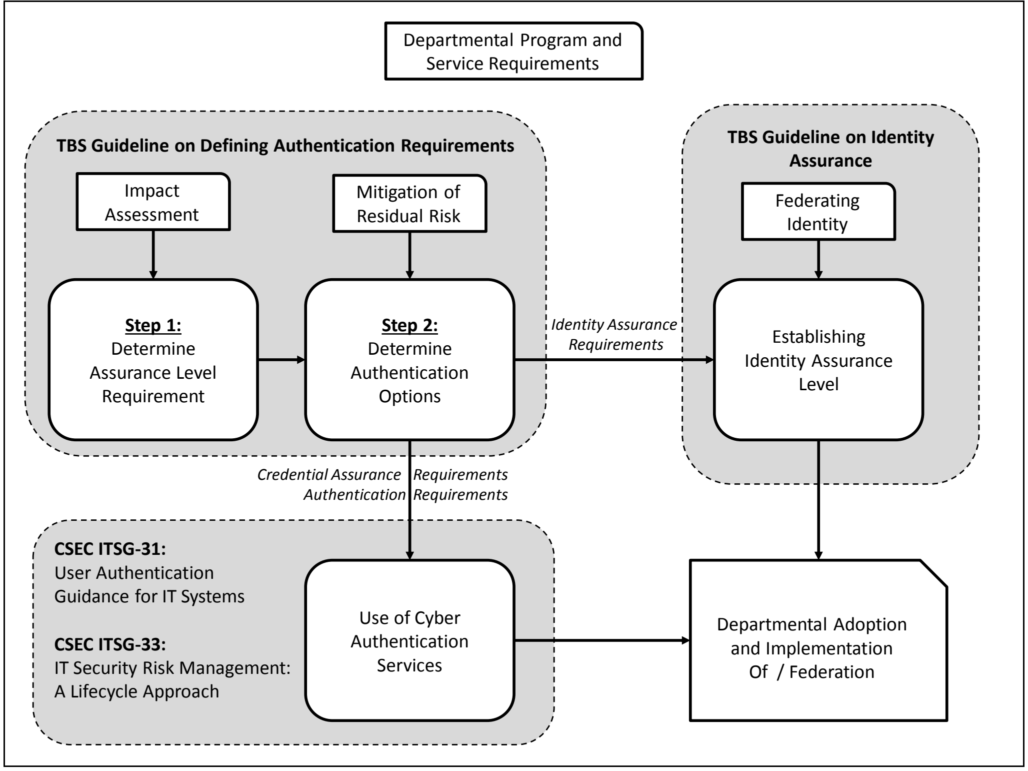
However, when the identity of a client is required (i.e. identity information), identity risk should be considered as the predominant risk. When identity information is involved, the potential theft or misuse of a credential (i.e., credential risk) is a direct contributing factor to identity risk.

Therefore, when identity is required for a program or services, departments should consider credential risk as a sub-component of identity risk.

2.5 Assurance Level Assessment

Figure 1 illustrates the related TBS and CSEC guidelines that are used in the assurance level assessment and the IT design process.

Figure 1: Related Guidelines


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

The TBS Guideline on Defining Authentication Requirements defines a two-step process that determines the following:

- **Assurance Level Requirement:** represents the overall level of confidence required to carry out a program activity, service or transaction. The assurance level assessment is conducted using the worksheet contain in Appendix A of this guideline. The assurance level requirement is determined in Step 1.

- **Identity assurance requirements**: The minimum requirements to establish the identity of an individual to a given level of assurance. Identity assurance requirement (along with other requirements listed below) is determined in Step 2. The guidelines on the implementing these requirements are set out in Section 3.0 of this document.

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

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

This guideline also provides recommendations on other mechanisms for mitigating risk:

- **Compensating factors:** Additional (i.e. non-standard) measures that can be used during the authentication process to reduce a risk.

- **Other Safeguards:** Other controls that exist within the larger system downstream from the authentication process.

Departments should be familiar with these related guidelines. Departments should have also conducted the assurance level assessment process prior to implementing requirements set out in Section 3.0.

3.0 Implementation Guidelines

3.1 Overview of Appendix C Requirements

Appendix C of the Standard on Identity and Credential Assurance is provided in Table 1 on page 11. The appendix specifies the four major requirements that must be fulfilled for establishing an identity assurance level: uniqueness, evidence of identity, accuracy of identity information, and linkage to individual.

The four requirements are listed below with a corresponding control objective statement and description.

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

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

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

   Evidence of identity supports the integrity and accuracy of the claims made by an individual. This includes gathering sufficient evidence of identity to support the claims, and to confirm the accuracy and linkage of identity information as these relate to the individual.

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

   Accuracy of identity information ensures that the identity information originates from and can be confirmed using an authoritative source. This includes ensuring the identity information is accurate, complete and up-to-date, as is necessary.

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

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

Table 1 on the following page specifies the minimum requirements related to each level of assurance. As departments begin the implementation of these requirements, the following should be considered:

- The Appendix C requirements are stated independently of delivery channel and technology used. This is to support the Government of Canada’s commitment to multi-channel access and service delivery. In implementing these requirements, departments should consider channel and service delivery alternatives that best suit the needs of clients, enable accessibility to a wide range of people with disabilities, and encourage adoption through trust and confidence.

- The requirements may be implemented in a staged, incremental approach. These requirements may be implemented in collaboration with other departments to assist in being ‘federation-ready’ (as described in Section 2.2).

Table 1: Appendix C: Minimum Requirements to Establish an Identity Assurance Level

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

Please refer to Appendix C of the standard for the authoritative version of Table 1.

3.2 Uniqueness and Context

The core function of uniqueness is to ensure that individuals can be distinguished from one another within a given context. Uniqueness is independent of level of assurance. Instead, uniqueness is dependent on the program or service context. This program or service context, in turn, drives the identity information requirements.

Uniqueness

Uniqueness ensures that the right service gets delivered to the right individual. Uniqueness eliminates or reduces the likelihood of error that a recipient receives services or benefits that are intended for someone else.

Uniqueness does not determine eligibility or entitlement for a service or benefit. Information that is collected to determine uniqueness can also be used for entitlement or benefits purposes, however the collection purposes are not related.

Uniqueness is also necessary for services that do *not* require identity (i.e., anonymous or pseudonymous services) Regardless of not knowing the identity of an individual, there still may be a requirement to distinguish between individuals for the purposes of repeatability. An example is the completion of an online survey; the identity of the respondent is not required, however the respondent may be required to complete the survey over the course of several days. It is necessary to have the *same* individual complete the parts of the survey but without requiring the knowledge of the identity of the respondent.

Context

Departments, as they deliver their programs and services, operate within a certain environment or circumstance which can be considered as the context. Context may be considered from the individual, the departmental, or the GC-wide perspective. For example, a context may be defined as the set of external services to citizens or the set of internal services to employees. A defined context should be distinct, but it may overlap with other contexts.

Understanding and defining context assists departments in determining the identity information that is necessary to fulfill their requirements. Context may also assist departments to determine commonalities with other departments (or jurisdictions) and to determine if identity information (or identity assurance processes) can be leveraged across contexts.

In defining uniqueness and context, departments should consider the following:

- The intended recipient of a service. Recipients may be external to the federal government (e.g., citizens, businesses, non-Canadians and non-profit organizations) or internal to government (e.g., departments).
- The size, characteristics and composition of the client population.
- Commonalities with other services (i.e. horizontal versus siloed approach)
- Departments with similar mandates.
- Use of shared services.

For all of these considerations, privacy must be considered

3.3 Identity Information

According to the Directive on Identity Management, departments that are required to ensure that they are transacting with a legitimate individual, organization or device are responsible for:

- Unique identification for the purposes of administering a federal program or service enabled by legislation; and
- Collection of identity information from the individual[3], organization or device before receiving a government service, participating in a government program or becoming a member of a government organization.

Defining Identity Information

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*.

An *identity attribute* is a property or characteristic associated with an identifiable individual. An *identity data element* is the same as an identity attribute.

Identity information is the set of identity attributes that is:

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

Identity information should not consist of attributes that are used to determine eligibility or entitlement. An exception is date of birth which may be used to determine age eligibility.

When defining identity information, departments should be aware of their legislative requirements as these may place certain constraints on the information that can or cannot be used.

Presently, there is no a consistent definition of identity across different legislation. Departments are advised to consult with their legal counsel to ensure that the defined identity information does not conflict with legislative requirements.

Departments should be familiar with and understand the potential applicability of the following sections in the Criminal Code including the definitions of 'identity documents' and 'identity information' as they apply within the context of the Code:

- **Section 56.1(1)** and **(2)** regarding the use of identity documents relating to another person.
- **Section 56.1(3)** regarding the definition of identity document as related to Section 56.1(1) and (2).
- **Section 57.(1)** to **(6)** regarding the use of the Canadian Passport.
- **Sections 402.1** regarding the definition of identity information. It should be noted that this is a narrower definition of identity information for the purposes of Sections 402.2 and 403 in relation of identity theft and identity fraud only.
- **Section 402.2** regarding the wrongful possession of identity information (i.e. identity theft).

[3] Information about an identifiable individual is considered to be personal information and is therefore subject to the Federal Privacy Act and PIPEDA. This is discussed later in the section

- **Section 403** regarding fraudulent personation of another person.

All identity information should be considered a subset of “personal information” as defined by the Privacy Act.

- The TBS Policy on Privacy Protection applies to identity information. This includes the applicability of all related privacy directives, standards and guidelines. As such, departments are expected identify, assess, monitor and mitigate any privacy risk involved in the collection, retention, use and disclosure of identity information.

- Identity information consisting of pseudonymous or anonymous attributes is considered as personal information.

Identity information may be collected, used or disclosed as part of a larger business process, such as registration, enrolment, or determination of entitlement. Some of this information may be used as identity information.

Departments should distinguish between the collection of identity information and program-specific information. Identity information that is collected (e.g. date of birth), may also be collected to determine an eligibility requirement (e.g., age). If information is collected for the purposes of identification and for purposes relating to other program or service requirements, the different collection purposes should be identified as these may have privacy implications.

Identity attributes used to uniquely distinguish between individuals (versus describing individuals) should be referred to as *identifiers*.

Identity attributes used as identifiers should be constant over time. In many cases, this is difficult to do, so departments may choose instead to assign an identifier to an individual. Typically, an identifier is a (numeric or alphanumeric) string that is generated independently of any other identity characteristic.

Other identity attributes may be used to additionally describe an individual. These attributes may not necessarily be unique to the individual (e.g. hair colour) and may change over time.

When departments define identity information, the following should be considered:

- Collection, and use of identity attributes should be kept to a minimum.

- An identifier may be an assigned identity attribute that is generated and managed by the program or service.

- Assigned identifiers may be kept internal to the program and service. Examples of internal identifiers are database unique keys, universally unique identifiers, etc.

- Assigned identifiers may be provided to other programs. However, this may be restricted due to privacy or legislation.

- Existing or previously assigned identifiers may be used. However, these identifiers may have privacy or legislative implications.

- Certain identifiers may be subject to legislative and policy restrictions. For example, the Directive on Social Insurance Number outlines specific restrictions on the collection, use and disclosure of the SIN.

- Identity information that is intended to distinguish or describe a real person, is subject to Accuracy of Identity Information requirements (see Section 3.5).

- Examples of identity information can include, name, date of birth, gender for individuals, business registration numbers for organizations, and serial numbers/network identifiers for telecommunications and computing devices.

- For privacy and security reasons, such as protecting the identities of individuals, certain identity attributes may be pseudonymous or anonymous. Examples of pseudonymous or anonymous identity attributes are the persistent anonymous identifier (PAI) used in GCKey and CBS, screen names, handles, userids, etc.

- Sensitivity of identity attributes should be considered. Unless required by legislation, individuals may not wish to disclose certain attributes due to their sensitive nature (e.g., date of birth for disclosure of age, address for disclosure of location, etc.). To reduce sensitivity, departments may collect only portions of certain identity attributes: e.g., ‘birth month plus last digit of birth year’ (instead of date of birth) or ‘city of residence’ (instead of complete mailing address)

Determining uniqueness may also be referred to as identity resolution. Identity resolution is the ability to resolve identity attributes to a unique individual (i.e. no other individual has the same set of attributes.)

Table 2 provides options for the combination of identity attributes can be used to resolve or distinguish a unique individual within a large population[4]. This table can be used as baseline in defining identity information requirements.

Table 2: Identity Attribute Combinations

Identity Resolution	**Option**	**Identity Attribute Combinations**
Sufficient to: uniquely distinguish or resolve 96% of population	1)	a. **Name:** (given name and surname) b. **Partial Current Address:** (postal code) or (city and province/territory), c. **Partial Date of Birth:** (month and day) or (year)
	2)	d. **Name:** (given name and surname), **e.** Full Date of Birth: (month, day, and year)
	3)	f. **Name:** (given name and surname) g. **Place of Birth:** (city or municipality) **h. Partial Date of Birth:** (month and day) or (year)

[4] This table is subset of table resulting from a draft US study that concluded certain attribute are sufficient to distinguish between individuals in 96% of cases involving the US population (approx. 320 million). The terminology in the table has been adjusted for the Canadian context. This table may not be applicable for different populations.

3.4 Evidence of Identity

Evidence of identity is a record from an authoritative source indicating an individual's identity information. Evidence of identity is used to establish an identity assurance level and individuals are required to provide evidence of identity to support their claims or self-assertions.

Foundational and Supporting Evidence of Identity

The Standard on Identity and Credential Assurance defines two categories of evidence of identity: *foundational evidence of identity* and *supporting evidence of identity*. The full definitions are below:

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

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

Collection of Evidence of Identity

Evidence of identity may be collected and used to determine other program entitlement or eligibility requirements. For example, the collection of the date of birth may be used to distinguish between individuals having the same name and to determine an eligibility requirement (e.g., required age for benefit)

Evidence of Identity requirements should be restricted for the following purposes:

- **To collect identity information required about the individual.** To ensure the necessary identity information is collected as required by the program or service.

- **To determine the accuracy of information.** To ensure that the identity information collected is accurate and up-to-date.

- **To determine linkage.** To ensure the identity information relates to the individual making the claim. (Note: linkage requirements do not apply to Level 1 or Level 2)

Evidence of identity requirements are specified independently of physical, electronic, or documentary form. An "instance" refers to evidence of identity (documentary, electronic, or physical) that is independent of another "instance", that is, from another and unrelated authoritative source.

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

- **Documentary Evidence:** Documentary evidence is widely understood to mean information written on paper. More generally, documentary evidence is any record of information that can be used as evidence. This includes records in electronic form, photographs, emails, audio recordings and log entries.

- **Electronic or Digital Evidence:** Electronic evidence is any data that is recorded or preserved on any medium in or by a computer system or other similar device. Examples are database records, audit logs, electronic word processing documents. In many cases, electronic records are printed, which then become documentary evidence.

Acceptability Criteria for Evidence of Identity

Table 3 sets out criteria for acceptability of foundational evidence of identity and supporting evidence of identity.

Table 3: Acceptability Criteria for Evidence of Identity

Evidence of Identity	Acceptability Criteria and Examples
Foundational Evidence of Identity	**Acceptability Criteria:** a. Evidence originates from an authoritative source that is: ii) Under the control of a federal or provincial/territorial government authority (or local equivalent abroad) iii) Used to maintain registration of vital events or determination of legal status. b. If identity information is incomplete or inconsistent with identity information as claimed by the individual (e.g. name change), additional supporting evidence may be required. c. If authoritative record or evidence is flagged for any reason (e.g. fraud, expiry, etc.) an appropriate identity notification should occur. (refer to Section 3.8). **Examples of authoritative sources/record 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
Supporting Evidence of Identity	**Acceptability Criteria:** d. Evidence originates from an authoritative source that is under the control of an approved organization (see note below). e. If authoritative record or associated documentary evidence is flagged for any reason (e.g. fraud, expiry, etc.) an appropriate identity notification should occur. (refer to Section 3.8) **If Accepted In Conjunction with Foundational Evidence of Identity (Level 3 and Level 4)** f. Supporting evidence of identity should consistent with the information that is provided by the foundational evidence of identity. g. In case of incomplete or inconsistent identity information (e.g. name change), additional supporting evidence may be required. h. An endorsement or certification that it is a true copy of an original **Examples of authoritative sources/record and documents:** • Driver licensing and registration used in the issuance of driver's licenses • Passport, Certificate of Indian status • Professional qualifications used in the issuance of professional credentials.
Notes: 1. The determination of an 'approved organization' is dependent on the program or service context. Approved organizations may be crown corporations, academic institutions, public agencies, commercial organizations, etc., that are subject to regulation and oversight. 2. Departments should formalize definitions and criteria on what constitutes an 'approved organization' within their context.	

Evidence of Identity Level Guidelines

Table 4 provides additional guidelines for evidence of identity for each level of assurance.

Table 4: Evidence of Identity Level Guidelines

Level	**Appendix C Requirement**	**Level Guidelines** (see Note 1 below)
Level 1	No restriction on what is provided as evidence	a. Departments should provide notice that any false or misleading statements may result in violation of terms or conditions. b. An audit log should be kept indicating when the evidence was presented and accepted.
Level 2	**One** instance of evidence of identity.	c. Only one instance of foundational <u>or</u> supporting evidence of identity is required. d. Departments may wish to specify that foundational is preferable over supporting evidence of identity. However, this should not be made a mandatory requirement.
Level 3	**Two** instances of evidence of identity (At least one must be foundational evidence of identity)	e. May be two instances of foundational evidence of identity <u>or</u> one instance of foundational evidence of identity and one instance of supporting evidence of identity. f. Evidence of identity should originate from different or independent authoritative sources (some authorities may issue more than one document) g. Should not be the same type of record or document from different authorities. For example, a birth certificate issued by two different jurisdictions.
Level 4	**Three** instances of evidence of identity (At least one must be foundational evidence of identity)	h. Departments may wish to further increase stringency of this requirement by requesting two instances of foundational evidence of identity. i. Any increase in stringency should be stated as an additional program risk management requirement.
Note 1: Guidelines specified at the lower level should be applied to the higher levels of assurance		

3.5 Accuracy of Identity Information

Accuracy of identity information ensures that the identity information originates from and can be confirmed using an authoritative source. This ensures the identity information is accurate, complete and up-to-date, as is necessary.

Accuracy is assured by validating identity information (or data attributes) against authoritative sources. If validation against authoritative sources is not feasible, other methods may be employed such as verifying/corroborating identity information using one or more instances of evidence of identity.

Determining the accuracy of identity information should also include the determination that the individual exists (or existed, in the case of a deceased individual). This determination should be provided by the authoritative source.

Depending upon program or service requirements and privacy considerations, departments may use different methods of validating identity information, such as providing a response that an attribute is “valid” or “invalid” (no additional information provided).

Determining the accuracy of identity information may be problematic due to factors such as name variants, name changes, cultural conventions, etc. Departments may employ the use matching and scoring algorithms to determine accuracy. In these cases, a match score may be used.

Identity attributes that are used an identifier (refer to Section 3.3) should be subject to an exact match.

In cases where the integrity of an identifier can be determined using a mathematical algorithm (e.g. checksum) these methods should be applied in addition to the validation process.

Table 5 lists guidelines for the accuracy of identity information recommended for each level of assurance.

Table 5: Accuracy of Information Level Guidelines

Level	**Appendix C Requirement**	**Level Guidelines** *(*see Note 1 below)
Level 1	Acceptance of self-assertion of identity information by an individual	a. Individuals are trusted to provide accurate information about who they are. b. There may be a likelihood that an individual may provide fictional or inaccurate information the resulting impacts are sufficiently low to not to require risk mitigation. c. Departments should provide notice to individuals that any false or misleading statements may result in reduced quality of service or be in violation of terms or conditions. d. An audit log should record when the self-assertion was made and the notices provided.
Level 2	Identity information acceptably matches assertion by an individual and evidence of identity **and** Confirmation that evidence of identity originates from appropriate authority	e. Individuals should be required to acknowledge that their identity information is consistent with the evidence of identity provided. f. Evidence of identity (documentary or electronic) should be confirmed as being legitimately issued by an authority that has been approved or recognized by the department. g. Determining accuracy of information should involve confirming the validity or integrity of the document including the information contained within (e.g. inspecting security features, checksums, etc.), validating electronic certificates (e.g. checking certificate revocation lists). h. Determining accuracy of information does not necessarily involve confirming accuracy using a remote electronic validation process (as there may be no facility for remote access or network connectivity) i. Departments may use informal matching criteria that determines accuracy within certain tolerances (e.g. name variances) j. An audit log should record 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	k. Departments should have in place formal matching criteria that determines accuracy within specified tolerances (e.g. name variances) l. Identity information should match within specified tolerances between all presented instances evidence of identity.

	identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source --- **or** inspection by trained examiner	m. Identity information that is presented using foundational evidence of identity should be validated using the most currently available authoritative record from an authoritative source (see Note 2). If necessary, multiple authoritative sources may be used. n. When the authoritative source is outside of Canadian jurisdiction, the accuracy of identity information is determined through a risk managed approach. o. In cases where the above guidelines cannot be applied, a trained examiner may be required to make the determination. p. An audit log should record the results of the confirmation process.
Level 4	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **and** Confirmation of the foundational evidence of identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source --- **or** inspection by trained examiner	q. Evidence of identity requirements equivalent to Level 3 requirements, however departments should in place more stringent matching criteria to determine accuracy within specified tolerances. r. Similar to Level 3, there may be cases where the above guidelines cannot be applied and a trained examiner makes the determination. Exception cases should be documented and each specific may be required to be approved separately. s. An audit log should record the results of the matching process, including when matches fall outside of specified tolerances.
Note 1: Guidelines specified at the lower level also should be applied to the higher levels *Note 2: An authoritative source may be responsible for providing a validated identity attribute <u>only</u> (i.e. not an identity assurance). An authoritative source, is not necessarily a member of a federation, but can used by an authoritative party, which is a member of a federation, to establish an identity assurance level, and therefore provide identity assurances.*		

3.6 Linkage to Individuals

Linkage is the determination that identity information relates to the individual making the claim.

Linkage ensures that identity information relates to the individual making the claim, and that this identity information does not relate to another individual. This includes ensuring the identity information relates to a real person (born and still alive, in most cases) and reflects how the individual is known or legally recognized within a jurisdiction or community.

Once a linkage is determined, this determination may be used to create a *binding*. Please refer to the discussion later in the section on the difference between linking and binding.

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

- **Knowledge-based confirmation:** Knowledge-based confirmation compares personal or private information (i.e. shared secrets) provided by the individual. Knowledge-based confirmation involves the use of information that should only be known exclusively to the individual and can only be legitimately answer by the individual.

- **Biological or behavioural characteristic confirmation:** Biological or behavioural characteristic confirmation compares biological (anatomical and physiological) to establish a link to an individual.

- **Trusted Referee confirmation:** Trusted referee confirmation is the process that relies on a trusted referee to establish a link to an individual. The trusted referee is determined by program-specific criteria. Examples of trusted referee include guarantor, notary and certified agent.

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

Linkage can be accomplished using one or a combination of the types of methods described above. Table 6 lists possible implementations for each of the linkage methods.

Table 6: Linkage Methods

Method Type	**Possible Implementations**
Knowledge-based confirmation	• **Static knowledge-based confirmation** – uses personal information that was collected or established at a specific point in time (e.g. during a registration process). • **Dynamic knowledge-based confirmation** – uses personal information that has been collected or generate over period of time (as opposed to a specific point in time).
Biological or behavioural characteristic confirmation:	• **Facial Comparison** Conducting manual facial comparisons between evidence of identity and the presenting individual or the use of facial recognition software performing automated one-to-one or one-to-many comparisons. • **Iris Comparison** Comparison of iris patterns of an individual's eyes with previously collected templates. • **Fingerprint Comparison** Use of the physical structure of an individual's fingerprint for recognition purposes. • **Voice Comparison** Detection and comparision of spoken works with a voiceprint • **Signature Comparison**. Comparison of the signature provided by an individual with a signature associated with evidence of identity. • **Data Analytics** Use of past historical data to identify characteristics, trends or behaviours that are attributable to the individual.
Trusted Referee confirmation (see Note below)	• **Guarantors** that have agreed to be responsible for the individual • **Notaries** that have the authority to administer oaths and attest to signatures in relation to in legal documents. • **Individuals** that are in a position of trust.
Physical Possession Confirmation	• **Document Authentication:** Authentication of a secure document that is issued for the exclusive use of the individual. This can include the authentication of specific security features.
Note: Departments should develop formal criteria for trusted referees.	

Table 7 lists recommended guidelines for linkage methods for each level of assurance

Table 7: Linkage Method Level Guidelines

Level	Appendix C Requirement	Level Guidelines *(*see Note 1 below)
Level 1	No requirement	a. Although there is no linkage requirement, departments should employ methods to ensure interaction is with a <u>real</u> person (i.e. not a robot)
Level 2	No requirement	b. Although there is no linkage requirement, department should employ some method to ensure interaction is with the <u>same</u> person (i.e. not a robot)
Level 3	At least **one** of the following linkage methods: i) Knowledge-based confirmation ii) Biological or behavioural characteristic confirmation iii) Trusted referee confirmation iv) Physical possession confirmation	c. Departments may wish to employ out-of-band (OOB) methods for linkage processes. Out-of-band methods employ communication channels or application services that are independent of, or separate from, the system used to carry out the transaction. Examples include, Short Message Services (SMS) or e-mail. d. OOB methods should be secure, private and exclusive to the individual. e. Audit logs should record linkage and OOB transactions (delivery, receipt, used in confirmation, etc.)
Level 4	At least **three** of the following linkage method: ii) Knowledge-based confirmation iii) Biological or behavioural characteristic confirmation iv) Trusted referee confirmation v) Physical possession confirmation	f. Audit logs should be able to resolve which linkage were used together to meet the linkage requirement.
Note 1: Guidelines recommended at the lower level also should be applied to the higher levels		

3.7 Linkage and Binding

Linkage and binding are different types of associations. In practice, these terms are used interchangeably, but there are key differences between the two concepts.

- *Linkage is the <u>determination</u> of an association of identity information to the right individual*. Linkage is determined by methods described in Table 6.

By comparison:

- *Binding is the <u>creation</u> of an association of identity information to the right individual*. Binding is usually performed *after* linkage and may be part of a registration or credential issuance process.

Linkage is carried out as part of the identity establishment process when there has been no previous interaction with the individual. An example is applying for a passport for the very first time.

Binding is carried out subsequent to an identity establishment process (where linkage has already taken place). Once the identity establishment process is complete, the identity information may be *bound* to a credential (i.e., *credential binding*).

An example of a physical credential binding process is the issuance of an employee ID card where the identity information is securely printed on a card. The card may also contain a secure chip which must be authenticated before the card can be used.

With the use of the electronic credentials, various binding models are being explored and implemented. Credentials may be bound only to identifiers, such as the persistent anonymous identifier (PAI) using the GCKey and Commercial Broker Service (described in Section 2.3).

In the case of GCKey and CBS, the PAI has no descriptive identity information and there is no need to carry out linkage as part of the credential issuance process. However, if departments intend to map the PAI to a program identifier that identifies an individual, they must perform the linkage as part of the mapping process.

In cases where an individual has lost a credential (or forgotten a password) a simple credential re-binding process may be sufficient (e.g., password reset). In other cases, the linkage requirement may need to be carried out once again to ensure it is same individual.

Once a credential has been bound to an established identity (i.e. identity information) by an authoritative party within a federation, the subsequent authentication and use of the credential may also be relied on for identity assurance. In other words, upon authentication of a credential, an authoritative party may also provide identity information bound to the credential (and by extension, associated with the individual using the credential).

3.8 Identity Assurance Processes

In many cases, departments have already implemented identity assurance processes as part of an existing business process. For example, a program or service registration or enrolment process may include steps to collect and validate identity information.

If identity information may be collected as part of a larger business process, departments should delineate the collection purposes related to identity information. Please refer to Section 3.3 for guidelines on the collection of identity information.

Departments should specify that information is being collected for different purposes: identity assurance purposes (e.g. validation), program purposes (e.g. eligibility, entitlement), or both. Departments should also be aware that the different collection purposes will have privacy implications which in may, in turn, restrict the use of the personal information collected.

Incorporation into Identity Lifecycle Models.

Departments may wish to formalize an identity lifecycle model. A lifecycle is broken into several major phases and may also include: identity proofing; user provisioning; credential issuance, use and authentication; and attribute use[5]. Many of the lifecycle phases defined in these are outside the scope of this guideline (e.g. credential issuance, use and authentication). Table 8 lists the phases that should be, at a minimum, incorporated into a lifecycle model.

Table 8: Identity Life Cycle Considerations

Life Cycle Phase	Description and Detail
Identity Establishment	• Carried out when an individual has no prior interaction with a program or service. • Results in a new authoritative record where none has existed previously. • Usually reserved for departments that intend to be authoritative providers within a federation. • Requires the implementation of all Appendix C requirements for a given level of assurance.
Identity Validation	• Carried out when an individual has had a previous interaction with a program or service. • Uses a previously established authoritative record. • Does not create a new authoritative record (unless the validation process is part of an identity establishment process described above). • Ensures that identity information is accurate, up-to-date and is uniquely associated with the same individual. • An identity validation process may leverage an existing credential binding.
Identity Notification	• Provides notification that identity information may have been exposed to other risk factors (e.g. fraudulent use detected, etc.). • Identity notifications can be provided to relying parties in conjunction with an identity validation or assurance service. • Relying parties may use these notifications to put in place additional safeguards or compensating factors. • If relying parties detect fraud (or any other incident or risk factor), they may provide notifications back to the authoritative party. • Identity notifications should not be used for entitlement or benefit decisions. These are separate from identity risk.

[5] These are the major phases as defined in the Gartner Report: Balancing the Identity and Risk Equation with Identity Assurance Frameworks, January 25, 2013 Publication No: G00246530

Identity assurance processes should be as efficient and transparent to the client as possible. Identity assurance processes that are not clear or are burdensome to the client may instead be a barrier to adoption of services.

3.9 Federation Considerations

Departments may assume the roles of an authoritative party or a relying party within their own department and without necessarily being a member of a federation. For example, a departmental human resources (HR) system may be considered as an authoritative party for a departmental security system that is responsible for issuing ID badges (this system would be considered as the relying party).

Table 9 is intended to assist departments in determining their role as an authoritative party, and/or a relying party, and their responsibilities when they participate in a federation. Table 9 may also be used by departments that wish to collaborate with other departments in implementing the requirements and they transition to a federation model.

Table 9: Considerations for Departmental Responsibilities

Departmental Role	**Not a member of a federation**	**As a member of a Federation**
Department in the role of an authoritative party	**Considerations for department:** • May be an authoritative party for own department. • May provide foundational or supporting evidence of identity that may be used by other departments. • May provide identity assurance for department only (i.e. cannot provide identity assurance outside of department) • May provide an identity validation service to other departments (does not share identity risk) • Is responsible for managing own departmental identity risk. **Departments should:** • Implement Appendix C requirements at the required assurance level. *Example: a departmental HR system that maintains an employee record.*	**Considerations for department:** • May be an authoritative party for participants in a federation (in addition to own department). • May provide foundational or supporting evidence of identity that may be used by other departments. • May provide identity assurances to relying party participants in a federation. • May share identity risk when providing identity assurances to relying party participants in a federation (to a level of assurance). **Departments should:** • Implement Appendix C requirements at the required assurance level, **and**, • Participate as authoritative party in a federation and comply with federation criteria and established by the Government of Canada CIO.
Department in the role of a relying party	**Considerations for department:** • May use foundational and supporting evidence of identity provided by another department • May use identity information validated by another department • Identity risk remains the responsibility of department. • Program-specific risk remains the responsibility of department **Departments should:** • Implement Appendix C requirements at the required assurance level, **or**, • Enter into an arrangement with another party to implement Appendix C requirements on its behalf (e.g. MOU, bilateral agreement, etc.) *Example: a departmental security system that relies on the departmental HR system to issue an ID badge.*	**Considerations for department:** • 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 department **Departments should:** • Participate in federation as a relying party **and,** • Comply with federation criteria established by Government of Canada CIO.

3.10 Fraud Considerations

Departments should be aware of the different methods of fraud.

Document Fraud

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

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

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

Records Fraud

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

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

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

Impostor Fraud

Impostor fraud is the fraudulent use of a fictitious or another person's identity information. Impostor fraud may involve:

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

- **Use of another person's evidence of identity where the other person is known.** In these cases, the fraudster may not be acting as an impostor but rather in an unauthorized capacity. Different methods must be used to confirm the legitimacy of the relationship.

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

4.0 Related Guidance and Tools

This section provides links of related TBS policy instruments that should be applied in conjunction with this guideline.

4.1 Policy on Government Security

The objective of the Policy on Government Security is to ensure deputy heads effectively manage security activities within departments and contribute to effective government-wide security management. It 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 departments.
- Directive on Identity Management The objective of this directive is to ensure effective identity management practices by outlining requirements to support departments 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 the determination of authentication options. Please refer to Section 2.5.
- **Guideline on Identity Assurance** (this document). This guideline provides guidance on the implementation of requirements specified in Appendix C of the Standard on Identity and Credential Assurance.

4.2 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 in administering the Act and 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 collection, retention, use, disclosure and disposal of personal information.

The Policy on Privacy Protection is supported by these directives:

- Directive on Privacy Impact Assessment requires that departments carry out a privacy impact assessment for new or substantially modified programs or activities that involve the creation, collection and handling of personal information

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

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

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

4.3 Policy on Information Management

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

The Policy on Information Management is supported by these directives:

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

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

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

4.4 Threat and Risk Assessments

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

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

Departments may want to use the Harmonized TRA analysis as additional considerations when implementing the minimum requirements. For example, the Harmonized TRA may be useful in addressing the highly specialized threat agents associated with the rapidly evolving online environment and the potential vulnerabilities introduced by newer technologies (e.g., tablets, mobile phones).

4.5 IT Security Guidelines

For guidance on authentication related to IT systems and electronic service delivery, departments should consult the following guidelines published by CSEC: ITSG-31 and ITSG-33.

- 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 departments.

4.6 Federation Standards and Protocols

Several documents have been developed to support Cyber Authentication governance and contracting of services. Department may wish to consult these documents which can be provided by contacting the Chief Information Officer Branch. Contact details are found in Section 5.2

- **Cyber-Authentication Technology Solutions Interface Architecture and Specification Version 2.0 (CATS2 IA&S)** Describes and defines the deployment profile for participation in the Government of Canada cyber-authentication environment. It describes the deployment profile and messaging interface required for credential authentication services. The deployment profile is based on the eGov Profile published by the Kantara Initiative and describes additional requirements and constraints specific to the Government of Canada.

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

5.0 Additional Information

5.1 Next Review Date

This document will be reviewed and updated as required.

5.2 Enquiries and Comments

Please direct any enquiries or comments about these guidelines to:

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

Telephone: (613) 952-2400
Fax: (613) 952-8536
Email: CyberAuthCyber@tbs-sct.gc.ca

6.0 References

Public Sector, Industry and International References

Pan-Canadian Assurance Model, March 2010 http://www.iccs-isac.org/en/km/transformative/pdf/assurance.asp

OECD, *Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.* June 2007 http://www.oecd.org/dataoecd/32/45/38921342.pdf

OMB, M-04-04. *E-Authentication Guidance for Federal Agencies*. December 16, 2003. http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

NIST, SP 800-63 Rev 2 DRAFT, Electronic Authentication Guideline, Feb 1, 2013 http://csrc.nist.gov/publications/PubsDrafts.html

Kantara Initiative
http://kantarainitiative.org/

North American Security Products Organization, Identity Verification Standard IDP-V (requires authorized access)
http://www.naspo.info/