Standard on Identity and Credential Assurance

1. Effective Date

1.1 This standard takes effect on February 1, 2013.

2. Application

2.1 This standard applies to all departments as defined in Schedules I, I.1, II, IV and V of the *Financial Administration Act*, unless excluded by specific acts, regulations or orders-in-council.

3. Context

3.1 This standard supports the objectives of the *Policy on Government Security* and the *Directive on Identity Management* by providing departments with requirements to ensure consistency in identity management practices.

3.2 This standard supports the Government of Canada's approach to federating identity. Federating identity enables departments and agencies to fulfill program and service requirements by relying on identity and credential assurance processes that have been carried out by other departments, jurisdictions and industry sectors.

3.3 This standard establishes requirements for departments to adopt a common methodology for assessing their identity and credential risks and for selecting appropriate controls or arrangements to mitigate those risks using a standardized assurance level framework.

3.4 Identity assurance is a measure of certainty that an individual, organization or device is who or what it claims to be. Identity risk is the risk that an individual, organization or device is not who or what it claims to be.

3.5 Credential assurance is 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, etc.) and that the credential has not been compromised (e.g., tampered with, modified). 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.

3.6 A standardized framework for identity and credential assurance levels is necessary to manage risk across government and to enable federation. A federation is a cooperative agreement between autonomous entities that have agreed to work together, supported by trust relationships and standards to support interoperability.

3.7 This standard applies to all government activities where each department must establish or rely on identities that are internal or external to the department.

3.8 Appendix B and Appendix C apply to the identities of individuals only.

4. Definitions

4.1 Definitions to be used in the interpretation of this standard are listed in Appendix A.

5. Standard Statement

5.1 Objective

To ensure that identity risk is managed consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors.

5.2 Expected Results

The expected results of this standard are as follows:

5.2.1 Identity risk is assessed and integrated into departments' risk management practices.

5.2.2 Departments' business processes and controls for managing identity are determined and implemented using a standardized assurance level framework.

5.2.3 Departments participate in arrangements for federated identity to meet identity and credential assurance requirements.

6. Requirements

Program and service delivery managers, in consultation with other functional specialists, are responsible for the activities described in sections 6.1, 6.2 and 6.3.

6.1 Assessment of Identity and Credential Risks and Selection of Controls

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.

6.1.3 Selecting identity and credential controls for achieving assurance level requirements using the standardized assurance levels specified in Appendix B.

6.1.4 Ensuring that the minimum requirements for establishing an identity assurance level as specified in Appendix C are met.

6.2 Federating Identity

6.2.1 Ensuring participation in federating identity using criteria established by the Government of Canada's Chief Information Officer.

6.3 Monitoring and Reporting

6.3.1 Overseeing the implementation of this standard in their department, monitoring compliance with it, bringing to the deputy head's attention significant difficulties, gaps in performance or compliance issues, and developing proposals to address them; and

6.3.2 Providing the Treasury Board of Canada Secretariat with information, when requested, that supports timely and accurate reporting on compliance and achievement of the expected results of this standard.

7. Government-Wide Monitoring and Reporting

7.1 The Treasury Board of Canada Secretariat will monitor compliance with this standard and the achievement of the expected results and will review identity and credential risk assessment and the controls and arrangements for federating identity, through a variety of means, including the following:

- Government-wide and departmental assessments and fact-based consultations;

- Examinations of Treasury Board submissions, departmental performance reports, and the results of audits, evaluations and studies; and
- Work performed in collaboration with departments.

7.2 Treasury Board of Canada Secretariat will review this standard and its effectiveness five years after the effective date (or earlier if warranted).

8. Consequences

8.1 The consequences of non-compliance with this standard are described in Section 7 of the *Policy on Government Security.*

9. Roles and Responsibilities of Government Organizations

9.1 The Chief Information Officer Branch supports the Treasury Board of Canada Secretariat in establishing and overseeing a whole-of-government approach to security and identity management as a key component of all management activities and in monitoring the adequacy of services to support these activities and practices across government.

9.2 This includes setting government-wide direction, establishing priorities and defining and formalizing security and identity management requirements for the Government of Canada and departments and establishing standards and designating the necessary authorities for identifying and authenticating individuals internal and external to the Government of Canada.

9.3 The Government of Canada Chief Information Officer Branch fulfills these responsibilities by:

9.3.1 Providing support to committees and working groups to address government-wide challenges and opportunities related to implementing this standard and its supporting instruments;

9.3.2 Communicating and engaging government-wide and with partners in other jurisdictions and sectors to develop common or compatible strategies, approaches, and processes to support federating identity; and

9.3.3 Establishing criteria for participating in arrangements for federating identity.

10. References

10.1 Relevant Legislation

- *Financial Administration Act*
- *Privacy Act*

10.2 Related Policy Instruments and Publications

- *Policy on Government Security*
- *Directive on Identity Management*
- *Federating Identity Management in the Government of Canada: A Backgrounder*
- *Policy on Privacy Protection*
- *Directive on Privacy Impact Assessment*
- *Directive on Privacy Practices*

11. Enquiries

For information on this policy instrument, please contact Treasury Board of Canada Secretariat Public Enquiries.

Appendix A: Definitions

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.

Appendix B: Standardized Assurance Levels for Managing Identity and Credential Risks

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 nil to minimal harm.

Table 2: Credential Assurance Levels

Level	Description
4	**Very high confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised.** Compromise could reasonably be expected to cause serious to catastrophic harm.
3	**High confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised.** Compromise could reasonably be expected to cause moderate to serious harm.
2	**Some confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised**. Compromise could reasonably be expected to cause minimal to moderate harm.
1	**Little confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that the credential has not been compromised**. Compromise could reasonably be expected to cause nil to minimal harm.

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	At least **three** of the following: i) Knowledge-based confirmation ii) Biological or

			behavioural characteristic confirmation iii) Trusted referee confirmation iv) Physical possession confirmation	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.