CAN/CIOSC 103-1:20XX (D1)

Second Edition

Digital Trust and Identity – Part 1: Fundamentals

35.030

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Table of Contents

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Foreword

CIO Strategy Council (CIOSC) is a not-for-profit corporation providing a national forum for public and private sector members to transform, shape, and influence the Canadian information and technology ecosystem.

CIOSC standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organizations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. CIOSC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about CIOSC, please contact:

CIO Strategy Council
500-1000 Innovation Dr.
Ottawa, ON K2K 3E7
ciostrategycouncil.com

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Introduction

This is the Second Edition of CAN/CIOSC 103-1:20XX, Digital Trust and Identity – Part 1: Fundamentals.

CAN/CIOSC 103-1:20XX was prepared by the CIO Strategy Council Technical Committee 4 (TC 4) on digital trust and identity, comprised of over 50 thought leaders and experts in identity management and related subjects. This Standard was approved by a Technical Committee formed balloting group, comprised of X producers, government/regulator policymakers, users, and others.

All units of measurement expressed in this Standard are in SI units using the International system (SI).

This Standard is subject to technical committee review beginning no later than one year from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation, or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application. This Standard is intended to be technology agnostic.

This Standard is intended to be used for conformity assessment.

ICS 35.030

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

- Page left intentionally blank -

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Digital Trust and Identity – Part 1: Fundamentals

1 Scope

This standard specifies minimum requirements and a set of controls for creating and maintaining trust in digital systems and services that, as part of an *Organization*'s mandate, assert and/or consume *Identity* and *Credentials* in data pertaining to *Persons* and *Organization*s. This standard may be applied to digital systems and services that are used within an *identity context*, and/or to those that are used and applied across *identity contexts* i.e., in a *Credential* and/or *Identity* federation.

This standard *shall* not be construed so as to:

a. Create non-compliance with any legal, regulatory, or contractual requirements, duties, standards, directives, and agreements that users of this standard may otherwise be under; nor

b. Favour or mandate any specific technology method, process, or application.

2 Normative References

There are no normative references in this document.

3 Terms and Definitions

For the purposes of this document, the following terms and definitions shall apply. Terms used in this Standard are in italic font. Important terms are capitalized.

Agency Relationship
a special case of a *Balanced Relationship* where the *Entities* are equals, but where one *Entity* (the Principal) appoints another *Entity* (the *Agent*) to act on the Principal's behalf for a specified purpose (e.g., power of attorney, an accounting firm filing taxes for a corporation). See also "*Relationship*", "*Balanced Relationship*", and "*Directed Relationship*".

Agent
an *Entity* that acts on behalf of another *Entity*.

assigned identifier
a numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between *Entities* within a population without the use of any other *identity attributes*.

assurance
confidence that a statement is true.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

assurance level
a level of confidence that a statement is true that may be relied on by others.

Atomic Entity
an *Entity* that cannot be decomposed into smaller units. *Persons* are *Atomic Entities*. See also “*Compound Entity*”.

atomic process
a set of logically related activities that results in the state transition of an object. The object’s output state can be relied on by other atomic processes.

Attribute
a property or characteristic of a thing. See also “*Entity Attribute*”, “*Relationship Attribute*”, “*Credential Attribute*”, and “*identity attribute*”.

authentication
see “*Credential Verification*”.

authenticator
something that a *Holder* controls that is used to prove that the *Holder* has retained control over an issued *Credential*.

authoritative source
a set of records maintained by an authority that meets established criteria.

Balanced Relationship
a *Relationship* where the *Entities* are equals (e.g., spouses in a marriage, partners in a business, corporations in a joint venture). See also “*Relationship*”, “*Agency Relationship*”, and “*Directed Relationship*”.

biological or behavioural characteristic confirmation
an *Identity Verification* method that uses biological (anatomical and physiological) characteristics (e.g., face, fingerprints, retinas) or behavioural characteristics (e.g., keyboard stroke timing, gait) to prove that the *Subject* presenting the *identity information* is in control of the *Identity*.

NOTE: *Biological or behavioural characteristic confirmation* is achieved by means of the challenge-response model: the biological or behavioural characteristics recorded on a document or in a data store are compared to the *Subject* presenting the *identity information*.

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

Claim
a *Claim* is expressed by means of one or more *Attributes*. *Claims* are asserted by *Issuers*. See also “*Subject Claim*” and “*Relationship Claim*”.

client
the intended recipient for a service output. External *clients* are generally *Persons* (Canadian citizens, permanent residents, etc.) and *Organizations* (public and private sector). Internal *clients* are generally employees and contractors.

Compound Entity
an *Entity* that is comprised of one or more *Atomic Entities* and/or one or more subordinate *Compound Entities*. *Organizations* are *Compound Entities*. See also “*Atomic Entity*”.

compound process
a set of *atomic processes* and/or other *compound processes* that results in a set of state transitions**.**

conformance criteria
a set of requirement statements that define what is necessary to ensure the integrity of an *atomic process*.

Consent Expiration
the process of suspending the validity of a “yes” consent decision as a result of exceeding an expiration date limit.

Consent Notice Formulation
the process of producing a consent notice statement that describes what *personal information* is being, or may be, collected; to which parties the *personal information* is being disclosed (as known at the time of presentation); for what purposes the *personal information* is being collected, used, or disclosed; the risk of harm and other consequences as a result of the collection, use, or disclosure; how the *personal information* will be handled and protected; the time period for which the consent notice statement is applicable; under whose jurisdiction or authority the consent notice statement is issued; and the rights of and process to revoke any consent given in whole or in part pursuant to such consent notice. This process should be carried out in accordance with any requirements of jurisdictional legislation and regulation.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Consent Notice Presentation
the process of presenting a consent notice statement to a *Person.*

Consent Registration
the process of storing the consent notice statement and the person's related consent decision. In addition, the identity information of the person, the version of the consent notice statement that was presented, the date and time that the consent notice statement was presented, and, if applicable, the expiration date or revocation date for the consent decision may be stored. Once the consent information has been stored, a notification on the consent decision made is issued to the relevant parties to the consent decision.

Consent Renewal
the process of extending the validity period of a "yes" consent decision by means of increasing an expiration date limit.

Consent Request
the process of asking a *Person* to agree to provide consent ("Yes") or decline to provide consent ("No") based on the contents of a presented consent notice statement, resulting in either a "yes" or "no" consent decision.

Consent Review
the process of making the details of a stored consent decision visible to the *Person* who provided the consent.

Consent Revocation
the process of suspending the validity of a "yes" consent decision as a result of an explicit withdrawal of consent by the *Person* (i.e., a "yes" consent decision is converted into a "no" consent decision).

contextual identity
an *Identity* that is used for a specific purpose within a specific *identity context*.

NOTE: Examples include banking, business permits, health services, drivers licensing, or social media. Depending on the *identity context*, a *contextual identity may* be tied to a *foundational identity* (e.g., a drivers licence) or may not be tied to a *foundational identity* (e.g., a social media profile). See also "*foundational identity*".

Credential
an assertion of identity, qualification, competence, authority, rights, privileges, permissions, status, eligibility, or asset ownership (or a combination of these). A *Credential* contains a set of one or more *Claims* asserted about one or more *Subjects*.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

credential assurance
confidence that a *Holder* has control over an issued *Credential* and that the issued *Credential* is valid.

credential assurance level
the level of confidence that a *Holder* has control over an issued *Credential* and that the issued *Credential* is valid.

Credential Attribute
a property or characteristic of a *Credential*.

Credential Authenticator Binding
the process of associating a *Credential* issued to a *Holder* with one or more *authenticators*. This process also includes *authenticator* life-cycle activities such as suspending *authenticators* (caused by a forgotten password or a lockout due to successive failed *Credential Verification* attempts, inactivity, or suspicious activity), removing *authenticators*, binding new *authenticators*, and updating *authenticators* (e.g., changing a password, updating security questions and answers, having a new facial photo taken).

Credential Issuance
the process of creating a *Credential* from a set of *Claims* about one or more *Subjects* and assigning the *Credential* to a *Holder*.

Credential Maintenance
the process of updating the *Credential Attributes* (e.g., expiry date, status of the *Credential*) of an issued *Credential*.

Credential Metadata
one or more Cr*edential Attributes* that describe the properties or characteristics of the *Credential*.

Credential Payload
a set of one or more *Claims* asserted about one or more *Subjects*.

Credential Proofs
one or more methods or mechanisms that are used to verify that the *Issuer* authored the *Credential*, that the *Credential* has not been tampered with, and that the *Credential* has been bound to a *Holder*.

Credential Recovery
the process of transforming a suspended *Credential* back to a usable state (i.e., an issued *Credential*).

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Credential Registration
a statement made by the *Issuer* that the *Issuer* issues a type of *Credential*. The statement may include a definition of the *Credential's* format.

Credential Revocation
the process of ensuring that an issued *Credential* is permanently flagged as unusable.

Credential Suspension
the process of transforming an issued *Credential* into a suspended *Credential* by flagging the issued *Credential* as temporarily unusable.

Credential Validation
the process of verifying that the issued *Credential* is valid (e.g., not tampered with, corrupted, modified, suspended, or revoked). The validity of the issued *Credential* can be used to generate a level of *assurance*.

Credential Verification
the process of verifying that a *Holder* has control over an issued *Credential*. Control of an issued *Credential* is verified by means one or more *authenticators*. The degree of control over the issued *Credential* can be used to generate a level of *assurance.*

digital ecosystem
a collection of various tools and systems, and the actors who create, interact with, use, and remake them.

Digital Identity
an electronic representation of an *Entity* that is exclusive to the *Entity*.

Digital Relationship
an electronic representation of an association between two or more *Entities*.

Digital Representation
an electronic representation of an *Entity* or an electronic representation of an association between two or more *Entities*.

Directed Relationship
a *Relationship* where the *Entities* are not equals (e.g., parent and child, parent corporation and subsidiary corporation, manager and subordinate). See also "*Relationship*", "*Agency Relationship*", and "*Balanced Relationship*".

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

eIDAS
Electronic Identification, Authentication, and Trust Services (*eIDAS*) is a European Union regulation that oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online such as electronic funds transfer or transactions with public services.

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

Entity
a thing with a distinct and independent existence, such as a *Person* or an *Organization*, that can be subject to legislation, policy, or regulations within a context, and which may have certain rights, duties, and obligations. An *Entity* can perform one or more of four roles (i.e., *Subject*, *Issuer*, *Holder*, or *Verifier*) in the *digital ecosystem*.

Entity Attribute
a property or characteristic of an *Entity*.

entity information
information about an identifiable *Entity*.

evidence of contextual identity (of an *Organization*)
evidence of identity that corroborates the *evidence of foundational identity* and assists in linking the *identity information* to an *Organization*. It may also provide additional information such as market activity, signature, or address. Examples include records of licences to carry on logging or mining activities, or to cultivate cannabis; and registrations of charitable status.

evidence of contextual identity (of a *Person*)
evidence of identity that corroborates the evidence of *foundational identity* and assists in linking the *identity information* to a *Person*. 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 services; and records of marriage, name change, or death originating from a jurisdictional authority.

evidence of foundational identity (of an *Organization*)
evidence of identity that established core *identity information* about an *Organization* such as legal name, date of event, address, status, primary contact. Examples are registration records, certificates of compliance, and incorporation records from an authority with the necessary jurisdiction.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

evidence of foundational identity (of a *Person*)
evidence of identity that establishes core *identity information* about a *Person* such as given name(s), surname, date of birth, and place of birth. Examples are records of birth, immigration, or citizenship from an authority with the necessary jurisdiction.

evidence of identity
a record from an *authoritative source* indicating an *Entity's Identity.* There are two categories of *evidence of identity*: foundational and contextual. See *"evidence of foundational identity"* and *"evidence of contextual identity".*

FATF
the Financial Action Task Force (*FATF*) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

FINTRAC
the Financial Transactions and Reports Analysis Centre of Canada (*FINTRAC*) is Canada's financial intelligence unit. Its mandate is to facilitate the detection, prevention, and deterrence of money laundering and the financing of terrorist activities.

foundation name
the name of an *Entity* as indicated on an official record identifying the *Entity* (e.g., provincial/territorial vital statistics record, federal immigration record, provincial/territorial business registry record, federal corporate registry record).

foundation registry (of *Organizations*)
a registry that maintains permanent records of *Organizations* that were created and registered in Canada. There are 14 such registries in Canada (the 13 provincial and territorial business registries and Corporations Canada [federal]).

foundation registry (of *Persons*)
a registry that maintains permanent records of *Persons* who were born in Canada, or *Persons* who were born outside Canada to a Canadian parent, or *Persons* who are foreign nationals who have applied to enter Canada. There are 14 such registries in Canada (the 13 provincial and territorial VSO registries and Immigration, Refugees, and Citizenship Canada [federal]).

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

foundational event
a significant discrete episode that occurs in the life span of a *Person* or an *Organization*. By law a *foundational event* must be recorded with a government entity and is subject to legislation and regulation. Examples of *foundational events* for *Persons* are live birth, stillbirth, adoption, legitimation, recognition of parenthood, immigration, legal residency, naturalized citizenship, name change, marriage, annulment of marriage, legal separation, divorce, and death. Examples of *foundational events* for *Organizations* are registration of charter, merger, amalgamation, surrender of charter, and dissolution.

foundational identity
an *Identity* that has been established or changed as a result of a *foundational event* (e.g., birth, *Person* legal name change, immigration, legal residency, citizenship, death, *Organization* legal name registration, *Organization* legal name change, bankruptcy). See also "*contextual identity*".

gender
refers to a social identity, such as man, woman, non-binary, or two-spirit.

Holder
an *Entity* that controls one or more *Credentials* from which a *Presentation* can be expressed to a *Verifier*. A *Holder* is usually, but not always, the *Subject* of a *Credential*.

NOTE: If the *Holder* is not the *Subject* of a *Credential*, then the *Holder* must have the legal status to represent the *Subject* (e.g., a legal guardian, or an attorney).

identifier
the set of *identity attributes* used to uniquely distinguish a particular *Entity* within a population.

Identity
a reference or designation used to uniquely distinguish a particular *Entity* within a population. There are two types of *Identity*: foundational and contextual. See *"foundational identity"* and *"contextual identity".*

identity assurance (of an *Organization*)
confidence that the *Organization identity information* is correct.

identity assurance (of a *Person*)
confidence that a *Person* is who they claim to be.

identity assurance level (of an *Organization*)
the level of confidence that the *Organization identity information* is correct.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

identity assurance level (of a *Person*)
the level of confidence that a *Person* is who they claim to be.

identity attribute
a property or characteristic associated with an identifiable *Entity* (also known as *"identity data element").* The *identity attributes* of an *Entity* are a subset of the *Entity's Entity Attributes*.

identity context
the environment or set of circumstances within which an *Organization* operates and within which it delivers its programs and services. *Identity context* is determined by factors such as mandate, target population (i.e., *clients,* customer base), and other responsibilities prescribed by legislation or agreements.

Identity Continuity
the process of dynamically confirming that the *Subject* has a continuous existence over time (i.e., "genuine presence"). This process can be used to ensure that there is no malicious or fraudulent activity (past or present) and to address *Identity* spoofing concerns.

identity data element
see *"identity attribute".*

Identity Establishment
The process of creating a record of *Identity* of a *Subject* within a population.

Identity Evidence Acceptance
the process of confirming that the *evidence of identity* presented (whether physical or electronic) is acceptable.

Identity Evidence Determination
the process of determining the acceptable *evidence of identity* (whether physical or electronic).

identity information
the set of *identity attributes* that is sufficient to distinguish one *Entity* from all other *Entities* within a population.

Identity Information Determination
the process of determining the *identity context*, the *identity information* requirements, and the *identifier.*

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

identity information notification
the disclosure of *identity information* about an *Entity* by an authoritative party to a relying party that is triggered by a *foundational event*, a change in their *identity information,* or an indication that their *identity information* has been exposed to a risk factor (e.g., the death of the *Person*, a charter surrender, use of expired documents, a privacy breach, fraudulent use of the *Identity information*).

identity information retrieval
the disclosure of *identity information* about an *Entity* by an authoritative party to a relying party that is triggered by a request from the relying party.

Identity Information Validation
the process of confirming the accuracy of *identity information* about a *Subject* as established by the *Issuer.*

Identity Linking
the process of mapping one or more *assigned identifiers* to a *Subject*.

Identity Maintenance
the process of ensuring that a *Subject*'s *identity information* is accurate, complete, and up-to-date.

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

identity model
a simplified (or abstracted) representation of an *identity management* methodology (also known as *"identity scheme*").

NOTE: Examples include centralized, federated, and decentralized *Identity models*.

Identity Resolution
the process of establishing the uniqueness of a *Subject* within a population through the use of *identity information*.

identity scheme
see *"identity model".*

Identity Verification
the process of confirming that the *identity information* is under the control of the *Subject*.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Issuer
an *Entity* that asserts one or more *Claims* about one or more *Subjects*, creates a *Credential* from these *Claims*, and assigns the *Credential* to a *Holder*.

knowledge-based confirmation
an *Identity Verification* method that uses *personal information* or shared secrets to prove that the *Subject* presenting the *identity information* is in control of the *Identity.*

NOTE: Knowledge-based confirmation is achieved by means of the challenge-response model: the *Subject* presenting the *identity information* is asked questions, the answers to which (in theory, at least) only they and the interrogator would know (e.g., financial information, credit history, shared secret, cryptographic key, mailed-out access code, password, personal identification number, *assigned identifier*).

legal name
see "*foundation name*", "*primary name*".

legal presence
lawful entitlement to be or reside in Canada.

Methods
the sets of rules that govern how actors in the *digital ecosystem* interact directly or indirectly with one another. Methods encompass such things as data models and schemas, communications protocols, conveyance mechanisms, cryptographic algorithms, databases, distributed ledgers, verifiable data registries, and similar schemes; and combinations of these.

NIST
the National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.

Organization
a legal *Entity* that is not a human being (referred to in law as a "juridical person").

organizational information
information about an identifiable *Organization*.

Person
a human being (referred to in law as a "natural person") including "minors" and others who might not be deemed to be *Persons* under the law.

personal information
information about an identifiable *Person*.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

physical possession confirmation
an *Identity Verification* method that requires physical possession or presentation of evidence (e.g., a *Credential*) to prove that the *Subject* presenting the *identity information* is in control of the *Identity*.

preferred name
the name by which a *Person* prefers to be informally addressed.

Presentation
information derived from one or more *Credentials*. The source *Credentials* may have been issued by different *Issuers*.

Presentation Confirmation
a determination by the *Verifier* of the correctness of the *Presentation*.

primary name
the name that an *Entity* uses for formal and legal purposes (also known as "*legal name*"). See also "*foundation name*".

Relationship
an association between two or more *Entities*. See also "*Agency Relationship*", "*Balanced Relationship*", and "*Directed Relationship*".

relationship assurance
confidence that the *Person(s)* is/are who they claim to be, that the *Organization(s) identity information* is correct, and that there is evidence of the *Relationship*.

relationship assurance level
the level of confidence that the *Person(s)* is/are who they claim to be, that the *Organization(s) identity information* is correct, and that there is evidence of the *Relationship*.

Relationship Attribute
a property or characteristic of an association between two or more an *Entities*.

Relationship Claim
a statement about an association that exists between two or more *Subjects*. A *Relationship Claim* is expressed by means of one or more *Relationship Attributes*.

Relationship Continuity
the process of dynamically confirming that a *Relationship* between two or more *Subjects* has a continuous existence over time.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Relationship Establishment
the process of creating a record of a *Relationship* between two or more *Subjects*.

Relationship Evidence Acceptance
the process of confirming that the evidence of a *Relationship* presented (whether physical or electronic) is acceptable.

Relationship Evidence Determination
the process of determining the acceptable evidence of a *Relationship* (whether physical or electronic).

relationship identifier
the set of *identifiers* of the *Entities* in the *Relationship* and the ”relationship type” *Relationship Attribute*.

relationship information
the set of *Relationship Attributes* that describes the association between two or more *Entitie*s.

Relationship Information Determination
the process of determining the relationship context, the *relationship information* requirements, and the *relationship identifier*.

Relationship Information Validation
the process of confirming the accuracy of information about a *Relationship* between two or more *Subjects* as established by the *Issuer*.

Relationship Maintenance
the process of ensuring that the information about a *Relationship* between two or more *Subjects* is accurate, complete, and up-to-date.

Relationship Reinstatement
the process of transforming a suspended *Relationship* back to an active state.

Relationship Resolution
the process of establishing the uniqueness of a *Relationship* within a population through the use of *relationship information* and *identity information*.

Relationship Revocation
the process of flagging a record of a *Relationship* as no longer in effect.

Relationship Suspension
the process of flagging a record of a *Relationship* as temporarily no longer in effect.

Relationship Verification
the process of confirming that the *relationship information* is under the control of the *Subjects*.

sex
refers to biological characteristics, such as male, female, or intersex.

signature
an electronic representation where, at a minimum: the *Person* signing the data can be associated with the electronic representation, it is clear that the *Person* intended to sign, the reason or purpose for signing is conveyed, and the data integrity of the signed transaction is maintained, including the original.

Signature Checking
the process of confirming that a *signature* is valid.

Signature Creation
the process of creating a *signature*.

shall
a requirement.

should
a recommendation.

Subject
an *Entity* about which *Claims* are asserted by an *Issuer*.

Subject Claim
a statement about a *Subject*. A *Subject Claim* is expressed by means of one or more *Entity Attributes*.

trust framework
a set of agreed on principles, definitions, standards, specifications, conformance criteria, and assessment approach.

trusted referee confirmation
an *Identity Verification* method that relies on a trusted referee to prove that the *Subject* presenting the *identity information* is in control of the *Identity*. The type of trusted referee and their acceptability is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries, accountants, and certified agents.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

UNCITRAL
the United Nations Commission on International Trade Law (*UNCITRAL*) is mandated to promote the progressive harmonization and unification of international trade law through conventions, model laws, and other instruments that address key areas of commerce, from dispute resolution to the procurement and sale of goods.

user
see “*Holder*”.

Verifier
an *Entity* that accepts a *Presentation* from a *Holder* for the purposes of delivering services or administering programs.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

4 Trust Framework

4.1 Fundamentals

4.1.1 General

4.1.1.1 Where an *Organization* will issue and/or consume *Identity* and/or *Credentials* as part of its *identity context*, including as part of a federation, the *Organization shall* define and implement criteria for selecting a *trust framework*[1] that will govern the operation of its *identity management* system and the rights and obligations of the federation participants, so as to ensure the trustworthiness of its *identity management* system and those of the federation participants. *Organizations should* consider the following when defining criteria for selecting a *trust framework*:

a. the *Organization's* context including its contractual obligations;
b. the industry sector in which the *Organization* operates including its policies and rules of general application;
c. jurisdictional legislation, regulations, and policies; and
d. applicable standards including this Standard.

4.1.1.2 The *Organization* may accept *Identity* and/or *Credentials* provided through an approved *trust framework* as an equivalent alternative to in-person service or resource delivery, by assessing the following:

a. *Identity* and service/resource specific information, i.e., whether *evidence of foundational identity* and/or *evidence of contextual identity* is required or appropriate to uniquely identify an *Entity* (see Clause 8.2.1.1), and what additional *entity information* is required to administer or deliver a service or resource;
b. *Identity assurance levels* and *credential assurance levels,* as outlined in Annex B;
c. Identity registration, i.e., the association and correctness between the *Identity* and *personal information* with a *Credential* issued to a *Person*; and
d. Notice and consent, i.e., whether the content of the notice given, and the collection, use, and disclosure of *personal information* obtained, is relevant and meaningful to the nature and duration of the consent obtained.

4.2 Identity Management

[1] Examples of trust frameworks include the Public Sector Profile of the Pan-Canadian Trust Framework (PCTF) in Canada, the UK Digital Identity and Attributes Trust Framework in the UK, and the Electronic Identification, Authentication, and Trust Services (*eIDAS*) in the European Union.

4.2.1 General

4.2.1.1 The *Organization shall*, absent legal directives, select *Identity attributes* to distinguish a unique *Identity* that meet the *Organization'*s needs and requirements, in a manner that balances risk, flexibility, and inclusiveness.

4.2.1.2 The *Organization shall* evaluate *Identity Verification* risks and/or *Credential Verification* risks by assessing potential impacts to a *Person*, an activity, a service, a transaction, or a sector.

4.2.1.3 The *Organization shall,* with respect to *Identity* and *Credential* processes, apply the required *Identity assurance levels* and/or *credential assurance levels* and related controls for achieving *assurance level* requirements.

4.2.1.4 The *Organization shall* monitor its *identity management* systems and processes to ensure their availability, integrity, and confidentiality, and *shall* evaluate the federation's *trust framework* for the same purpose.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

5 Leadership

5.1 Role of the Organization's Leadership

5.1.1 General

5.1.1.1 Top management shall demonstrate their commitment to the *Organization's Digital Identity* systems and services by:

a. ensuring that *Digital Identity* systems and services policy and objectives are established and are aligned with the strategic direction of the *Organization*;
b. communicating the importance of effective *Digital Identity* systems and services and ensuring that the resources needed for those systems and services are available;
c. ensuring that *Digital Identity* systems and services conform to cyber security policy, objectives, and program requirements;
d. establishing *Digital Identity* systems and services metrics, and tracking progress and performance; and
e. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

6 Planning

6.1 Addressing Risks and Opportunities

6.1.1 General

6.1.1.1 When planning for the *Organization's Digital Identity* systems and services, the *Organization shall* consider the issues and requirements outlined in Section 4, and determine the risks and opportunities that need to be addressed to:

- give assurance that the *Digital Identity* systems and services can achieve their intended result(s);
- prevent, or reduce, undesired effects; and
- achieve continual improvement.

6.1.1.2 The *Organization shall* plan:

a. actions to address these risks and opportunities; and
b. how to:
    - integrate and implement the actions into its *Digital Identity* systems and services processes; and
    - evaluate the effectiveness of these actions.

6.2 Objectives and Planning

6.2.1 General

6.2.1.1 The *Organization shall* establish objectives for its *Digital Identity* systems and services.

6.2.1.2 These objectives *shall*:

a. be consistent with the existing policies;
b. be measurable (if practicable);
c. take into account applicable requirements;
d. be monitored;
e. be communicated;
f. be updated as appropriate; and
g. be available as documented information.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

6.2.1.3 When planning how to achieve these objectives, the *Organization shall* determine:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed; and
- how the results will be evaluated.

6.3 Planning of Changes

6.3.1 General

6.3.1.1 When the *Organization* determines the need for changes to its *Digital Identity* systems and services, the changes shall be carried out in a planned manner.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

7 Support

7.1 Resources

7.1.1 General

7.1.1.1 The *Organization shall* determine the resources needed for the establishment, implementation, maintenance, and continual improvement of *Digital Identity* systems and services.

7.2 Competence

7.2.1 General

7.2.1.1 The *Organization shall* determine the necessary competence of person(s) doing work that affects the performance of *Digital Identity* systems and services.

7.2.1.2 The *Organization shall* ensure that the persons contemplated in 7.2.1.1 are competent on the basis of appropriate education, training, and experience.

7.2.1.3 The *Organization shall*, where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

7.3 Awareness

7.3.1 General

7.3.1.1 To ensure the successful implementation required by the Outcomes listed in Section 8, persons doing work related to *Digital Identity* systems and services *shall* be aware of:

- All manual and automated controls;
- All policies and procedures that they must follow; and
- The implications of not conforming to the requirements of this document, particularly the implications on the subjects of the *Digital Identity* systems and services.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

7.4 Communication

7.4.1 General

7.4.1.1 The *Organization shall* determine the internal and external communications relevant to the ongoing successful implementation of *Digital Identity* systems and services including:

- The subject of communications;
- When to communicate;
- With whom to communicate; and
- How to communicate.

7.5 Documented Information

7.5.1 General

7.5.1.1 The *Organization's Digital Identity* systems and services documentation *shall* include documented information required by this document.

7.5.1.2 The *Organization's Digital Identity* systems and services documentation *shall* include information determined by the *Organization* as being necessary for the effectiveness of the *Organization*'s *Digital Identity* systems and services.

7.5.2 Creating and Updating Documented Information

7.5.2.1 The *Organization's Digital Identity* systems and services documentation *shall* be created and updated to ensure appropriate identification and description (e.g., a title, date, author, or reference number).

7.5.2.2 The *Organization's Digital Identity* systems and services documentation *shall* be created and updated with appropriate review and approval for suitability and adequacy.

7.5.3 Control of Documented Information

7.5.3.1 The *Organization's Digital Identity* systems and services documentation *shall* be controlled to ensure it is available and suitable for use where and when it is needed.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

7.5.3.2 The *Organization's Digital Identity* systems and services documentation *shall* be controlled to ensure it is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity).

7.5.3.3 The *Organization shall* control *Digital Identity* systems and services documentation by addressing the following activities:

- Distribution, access, retrieval, and use;
- Storage and preservation, including preservation of legibility;
- Control of changes (e.g., version control); and
- Retention and disposition.

7.5.3.4 The *Organization's Digital Identity* systems and services documentation of external origin *shall* be identified as appropriate, and controlled.

7.5.4 *Digital Identity* Systems and Services Documentation

7.5.4.1 The *Organization shall* create, update, and control documentation of the scope of *Digital Identity* systems and services for the purpose of assessing conformity with this document.

7.5.4.2 The *Organization shall* create, update, and control documentation for *Digital Identity* systems and services to meet the objectives of the program.

NOTE: As an example, the *Organization* created, updated, and controlled documentation of the criteria for selecting a *trust framework* required by Section 4.1.1.1.

7.5.4.3 The *Organization shall* create, update, and control documentation of all the controls required to ensure the successful implementations required by the Outcomes listed in Section 8 and to support performance evaluation of the *Digital Identity* systems and services.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8 Operations: Processes

8.1 Identity Information Determination process

8.1.1 Purpose

8.1.1.1 The purpose of the *Identity Information Determination* process is to determine the *identity context,* the *identity information* requirements, and the *identifier*.

8.1.2 Outcomes

8.1.2.1 As a result of the successful implementation of the *Identity Information Determination* process, the *identity context*, the *identity information* requirements, and the *identifier* have been determined.

8.2 Identity Evidence Determination process

8.2.1 Purpose

8.2.1.1 The purpose of the *Identity Evidence Determination* process is to determine the acceptable *evidence of identity* (whether physical or electronic).

8.2.2 Outcomes

8.2.2.1 As a result of the successful implementation of the *Identity Evidence Determination* process, the acceptable *evidence of identity* has been determined.

8.3 Identity Evidence Acceptance process

8.3.1 Purpose

8.3.1.1 The purpose of the *Identity Evidence Acceptance* process is to confirm that the *evidence of identity* presented (whether physical or electronic) is acceptable.

8.3.2 Outcomes

8.3.2.1 As a result of the successful implementation of the *Identity Evidence Acceptance* process, the *evidence of identity* has been confirmed as being acceptable.

8.4 Identity Information Validation process

8.4.1 Purpose

8.4.1.1 The purpose of the *Identity Information Validation* process is to confirm the accuracy of *identity information* about a *Subject* as established by the *Issuer*.

8.4.2 Outcomes

8.4.2.1 As a result of the successful implementation of the *Identity Information Validation* process, the *identity information* has been confirmed with the *Issuer*.

8.5 Identity Resolution process

8.5.1 Purpose

8.5.1.1 The purpose of the *Identity Resolution* process is to establish the uniqueness of a *Subject* within a population through the use of *identity information*.

8.5.2 Outcomes

8.5.2.1 As a result of the successful implementation of the *Identity Resolution* process, the *identity information* is unique to one and only one *Subject*.

8.6 Identity Establishment process

8.6.1 Purpose

8.6.1.1 The purpose of the *Identity Establishment* process is to create a record of *Identity* of a *Subject* within a population.

8.6.2 Outcomes

8.6.2.1 As a result of the successful implementation of the *Identity Establishment* process, a record of *Identity* for the *Subject* exists.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.7 Identity Verification process

8.7.1 Purpose

8.7.1.1 The purpose of the *Identity Verification* process is to confirm that the *identity information* is under the control of the *Subject*.

8.7.2 Outcomes

8.7.2.1 As a result of the successful implementation of the *Identity Verification* process, the *identity information* has been verified as being under the control of the *Subject*.

8.8 Identity Continuity process

8.8.1 Purpose

8.8.1.1 The purpose of the *Identity Continuity* process is to dynamically confirm that the *Subject* has a continuous existence over time (i.e., “genuine presence”).

NOTE: This process can be used to ensure that there is no malicious or fraudulent activity (past or present) and to address *Identity* spoofing concerns.

8.8.2 Outcomes

8.8.2.1 As a result of the successful implementation of the *Identity Continuity* process, the *Identity* exists continuously over time in association with many transactions.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.9 Identity Maintenance process

8.9.1 Purpose

8.9.1.1 The purpose of the *Identity Maintenance* process is to ensure that a *Subject*'s *identity information* is accurate, complete, and up-to-date.

NOTE: The *Identity Maintenance* process involves records maintenance, including the possible deletion of records. It may be appropriate to delete records of *Identity* for reasons of accuracy (e.g., mistaken inclusion in an authoritative registry, such as a duplicate birth record), for reasons of policy (e.g., record retention policy, such as a 3-year retention limit on information about former customers), or for legal reasons (e.g., complying with a Privacy Commissioner's order).

8.9.2 Outcomes

8.9.2.1 As a result of the successful implementation of the *Identity Maintenance* process, the *identity information* is accurate, complete, and up-to-date.

8.10 Identity Linking process

8.10.1 Purpose

8.10.1.1 The purpose of the *Identity Linking* process is to map one or more *assigned identifiers* to a *Subject*.

8.10.2 Outcomes

8.10.2.1 As a result of the successful implementation of the *Identity Linking* process, one or more *assigned identifiers* have been mapped to the *Subject*.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.11 Relationship Information Determination process

8.11.1 Purpose

8.11.1.1 The purpose of the *Relationship Information Determination* process is to determine the relationship context, the *relationship information* requirements, and the *relationship identifier*.

8.11.2 Outcomes

8.11.2.1 As a result of the successful implementation of the *Relationship Information Determination* process, the relationship context, the *relationship information* requirements, and the *relationship identifier* have been determined.

8.12 Relationship Evidence Determination process

8.12.1 Purpose

8.12.1.1 The purpose of the *Relationship Evidence Determination* process is to determine the acceptable evidence of a *Relationship* (whether physical or electronic).

8.12.2 Outcomes

8.12.2.1 As a result of the successful implementation of the *Relationship Evidence Determination* process, the acceptable evidence of a *Relationship* has been determined.

8.13 Relationship Evidence Acceptance process

8.13.1 Purpose

8.13.1.1 The purpose of the *Relationship Evidence Acceptance* process is to confirm that the evidence of a *Relationship* presented (whether physical or electronic) is acceptable.

8.13.2 Outcomes

8.13.2.1 As a result of the successful implementation of the *Relationship Evidence Acceptance* process, the acceptable evidence of a *Relationship* has been confirmed as being acceptable.

8.14 Relationship Information Validation process

8.14.1 Purpose

8.14.1.1 The purpose of the *Relationship Information Validation* process is to confirm the accuracy of information about a *Relationship* between two or more *Subjects* as established by the *Issuer*.

8.14.2 Outcomes

8.14.2.1 As a result of the successful implementation of the *Relationship Information Validation* process, the *relationship information* has been confirmed with the *Issuer*.

8.15 Relationship Resolution process

8.15.1 Purpose

8.15.1.1 The purpose of the *Relationship Resolution* process is to establish the uniqueness of a *Relationship* within a population through the use of *relationship information* and *identity information*.

8.15.2 Outcomes

8.15.2.1 As a result of the successful implementation of the *Relationship Resolution* process, the *relationship information* and the *identity information* is unique to one and only one *Relationship*.

8.16 Relationship Establishment process

8.16.1 Purpose

8.16.1.1 The purpose of the *Relationship Establishment* process is to create a record of a *Relationship* between two or more *Subjects*.

8.16.2 Outcomes

8.16.2.1 As a result of the successful implementation of the *Relationship Establishment* process, a record of a *Relationship* exists.

8.17 Relationship Verification process

8.17.1 Purpose

8.17.1.1 The purpose of the *Relationship Verification* process is to confirm that the *relationship information* is under the control of the *Subjects*.

8.17.2 Outcomes

8.17.2.1 As a result of the successful implementation of the *Relationship Verification* process, the *relationship information* has been verified as being under the control of the *Subjects*.

8.18 Relationship Continuity process

8.18.1 Purpose

8.18.1.1 The purpose of the *Relationship Continuity* process is to dynamically confirm that a *Relationship* between two or more *Subjects* has a continuous existence over time.

8.18.2 Outcomes

8.18.2.1 As a result of the successful implementation of the *Relationship Continuity* process, the *Relationship* exists continuously over time in association with many transactions.

8.19 Relationship Maintenance process

8.19.1 Purpose

8.19.1.1 The purpose of the *Relationship Maintenance* process is to ensure that the information about a *Relationship* between two or more *Subjects* is accurate, complete, and up-to-date.

8.19.2 Outcomes

8.19.2.1 As a result of the successful implementation of the *Relationship Maintenance* process, the *relationship information* is up-to-date.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.20 Relationship Suspension process

8.20.1 Purpose

8.20.1.1 The purpose of the *Relationship Suspension* process is to flag a record of a *Relationship* as temporarily no longer in effect.

8.20.2 Outcomes

8.20.2.1 As a result of the successful implementation of the *Relationship Suspension* process, the *Relationship* is temporarily no longer in effect.

8.21 Relationship Reinstatement process

8.21.1 Purpose

8.21.1.1 The purpose of the *Relationship Reinstatement* process is to transform a suspended *Relationship* back to an active state.

8.21.2 Outcomes

8.21.2.1 As a result of the successful implementation of the *Relationship Reinstatement* process, the record of a *Relationship* has been updated.

8.22 Relationship Revocation process

8.22.1 Purpose

8.22.1.1 The purpose of the *Relationship Revocation* process is to flag a record of a *Relationship* as no longer in effect.

8.22.2 Outcomes

8.22.2.1 As a result of the successful implementation of the *Relationship Revocation* process, the *Relationship* is no longer in effect.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.23 Credential Issuance process

8.23.1 Purpose

8.23.1.1 The purpose of the *Credential Issuance* process is to create a *Credential* from a set of *Claims* about one or more *Subjects* and assign the *Credential* to a *Holder*.

8.23.2 Outcomes

8.23.2.1 As a result of the successful implementation of the *Credential Issuance* process, one or more *Claims* about one or more *Subjects* have been associated with the *Credential* and the *Credential* has been assigned to a *Holder*.

8.24 Credential Authenticator Binding process

8.24.1 Purpose

8.24.1.1 The purpose of the *Credential Authenticator Binding* process is to associate a *Credential* issued to a *Holder* with one or more *authenticators.*

NOTE: This process also includes *authenticator* life-cycle activities such as suspending *authenticators* (i.e., caused by a forgotten password or a lockout due to successive failed *Credential Verification* attempts, inactivity, or suspicious activity), removing *authenticators*, binding new *authenticators,* and updating a*uthenticators* (e.g., changing a password, updating security questions and answers, having a new facial photo taken).

8.24.2 Outcomes

8.24.2.1 As a result of the successful implementation of the *Credential Authenticator Binding* process, an issued *Credential* has been associated with one or more *authenticator*s.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.25 Credential Validation process

8.25.1 Purpose

8.25.1.1 The purpose of the *Credential Validation* process is to verify that the issued *Credential* is valid (i.e., not tampered with, corrupted, modified, suspended, or revoked).

NOTE: The validity of the issued *Credential* can be used to generate a level of *assurance.*

8.25.2 Outcomes

8.25.2.1 As a result of the successful implementation of the *Credential Validation* process, the issued *Credential* is valid.

8.26 Credential Verification process

8.26.1 Purpose

8.26.1.1 The purpose of the *Credential Verification* process is to verify that a *Holder* has control over an issued *Credential*.

NOTE: The degree of control over the issued *Credential* can be used to generate a level of *assurance.* Control of an issued *credential shall* be verified by means of one or more *authenticator*s.

8.26.2 Outcomes

8.26.2.1 As a result of the successful implementation of the *Credential Verification* process, the *Holder* has proven control of the issued *Credential*.

8.27 Credential Maintenance process

8.27.1 Purpose

8.27.1.1 The purpose of the *Credential Maintenance* process is to update the *Credential Attributes* (e.g., expiry date, status of the *Credential*) of an issued *Credential*.

8.27.2 Outcomes

8.27.2.1 As a result of the successful implementation of the *Credential Maintenance* process, the issued *Credential* has been updated.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.28 Credential Suspension process

8.28.1 Purpose

8.28.1.1 The purpose of the *Credential Suspension* process is to transform an issued *Credential* into a suspended *Credential* by flagging the issued *Credential* as temporarily unusable.

NOTE: This process is intended to support *credential assurance*. This process may be appropriate when there is evidence that a *Claim* is not accurate (e.g., a misspelled name), or when there is evidence that a *Holder* has not maintained control of a *Credential* (e.g., a stolen password).

8.28.2 Outcomes

8.28.2.1 As a result of the successful implementation of the *Credential Suspension* process, the *Holder* is not able to use the *Credential*.

8.29 Credential Recovery process

8.29.1 Purpose

8.29.1.1 The purpose of the *Credential Recovery* process is to transform a suspended *Credential* back to a usable state (i.e., an issued *credential*).

NOTE: This process is intended to support *credential assurance*. This process may be appropriate when there is evidence that a *Claim* is not accurate (e.g., a misspelled name), or when a *Holder*'s control of a suspended *Credential* has been restored (e.g., the password was changed by the *Holder*).

8.29.2 Outcomes

8.29.2.1 As a result of the successful implementation of the *Credential Recovery* process, the issued *Credential* has been updated.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.30 Credential Revocation process

8.30.1 Purpose

8.30.1.1 The purpose of the *Credential Revocation* process is to ensure that an issued *Credential* is permanently flagged as unusable.

8.30.2 Outcomes

8.30.2.1 As a result of the successful implementation of the *Credential Revocation* process, the *Holder* is not able to use the *Credential*.

8.31 Consent Notice Formulation process

8.31.1 Purpose

8.31.1.1 The purpose of the *Consent Notice Formulation* process is to produce a consent notice statement.

8.31.2 Outcomes

8.31.2.1 As a result of the successful implementation of the *Consent Notice Formulation* process, a consent notice statement exists.

NOTE: The consent notice statement *shall* describe:

a. what *personal information* is being, or may be, collected;
b. to which parties the *personal information* is being disclosed (as known at the time of presentation);
c. for what purposes the *personal information* is being collected, used, or disclosed;
d. the risk of harm and other consequences as a result of the collection, use, or disclosure;
e. how the *personal information* will be handled and protected;
f. the time period for which the consent notice statement is applicable;
g. under whose jurisdiction or authority the consent notice statement is issued; and
h. the rights of and process to revoke any consent given in whole or in part pursuant to such consent notice.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.32 Consent Notice Presentation process

8.32.1 Purpose

8.32.1.1 The purpose of the *Consent Notice Presentation* process is to present a consent notice statement to a *Person*.

8.32.2 Outcomes

8.32.2.1 As a result of the successful implementation of the *Consent Notice Presentation* process, a consent notice statement has been presented to a *Person*.

8.33 Consent Request process

8.33.1 Purpose

8.33.1.1 The purpose of the *Consent Request* process is to ask a *Person* to agree to provide consent ("Yes") or decline to provide consent ("No") based on the contents of a presented consent notice statement, resulting in either a "yes" or "no" consent decision.

8.33.2 Outcomes

8.33.2.1 As a result of the successful implementation of the *Consent Request* process, a consent decision exists.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.34 Consent Registration process

8.34.1 Purpose

8.34.1.1 The purpose of the *Consent Registration* process is to store the consent notice statement and the *Person*'s related consent decision.

8.34.2 Outcomes

8.34.2.1 As a result of the successful implementation of the *Consent Registration* process, a stored consent decision exists.

NOTE: The *Organization shall* store as a record the following information related to a consent decision:

a. the *identity information* of the *Person*;
b. the version of the consent notice statement that was presented;
c. the date and time that the consent notice statement was presented;
d. the 'Yes' or 'No' outcome of the consent decision and the date and time of the consent decision; and
e. if applicable, the expiration date and time of the consent decision, and/or the revocation date and time of the consent decision.

Once the consent information has been stored, a notification on the consent decision made *shall* be issued by the *Organization* to the relevant parties of the consent decision.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.35 Consent Review process

8.35.1 Purpose

8.35.1.1 The purpose of the *Consent Review* process is to make the details of a stored consent decision visible to the *Person* who provided the consent.

8.35.2 Outcomes

8.35.2.1 As a result of the successful implementation of the *Consent Review* process, a stored consent decision exists.

NOTE: The *Organization shall* define its *Consent Review* process to expose the minimal data required to confirm the 'Yes' or 'No' decision of the *Subject* to the consent notice statement presented, together with a copy of the consent notice statement for which the consent decision was given. Where the authorized reviewer is part of a federation *trust framework*, a record of such inquiry *shall* also be retained as part of the processes for *Identity Evidence Acceptance* and *Consent Request.* Further, where a subsequent *Consent Renewal, Consent Expiration*, or *Consent Revocation* occurs, this *shall* be made available as part of the *Consent Review* process and *shall* specifically be sent as a notice to the authorized reviewer who is part of a federation.

8.36 Consent Renewal process

8.36.1 Purpose

8.36.1.1 The purpose of the *Consent Renewal* process is to extend the validity period of a "yes" consent decision by means of increasing an expiration date limit.

8.36.2 Outcomes

8.36.2.1 As a result of the successful implementation of the *Consent Renewal* process, a stored consent decision has been updated.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.37 Consent Expiration process

8.37.1 Purpose

8.37.1.1 The purpose of the *Consent Expiration* process is to suspend the validity of a "yes" consent decision as a result of exceeding an expiration date limit.

8.37.2 Outcomes

8.37.2.1 As a result of the successful implementation of the *Consent Expiration* process, a stored consent decision has been updated.

8.38 Consent Revocation process

8.38.1 Purpose

8.38.1.1 The purpose of the *Consent Revocation* process is to suspend the validity of a "yes" consent decision as a result of an explicit withdrawal of consent by the *Person* (i.e., a "yes" consent decision is converted into a "no" consent decision).

8.38.2 Outcomes

8.38.2.1 As a result of the successful implementation of the *Consent Revocation* process, a stored consent decision has been updated.

8.39 Signature Creation process

8.39.1 Purpose

8.39.1.1 The purpose of the *Signature Creation* process is to create a signature.

8.39.2 Outcomes

8.39.2.1 As a result of the successful implementation of *Signature Creation* process, a signature exists.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

8.40 Signature Checking process

8.40.1 Purpose

8.40.1.1 The purpose of the *Signature Checking* process is to confirm that a signature is valid.

8.40.2 Outcomes

8.40.2.1 As a result of the successful implementation of *Signature Checking* process, a signature is valid.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Annex A
(Informative)

A Identity Attributes

A.1 General

A.1.1
Different sets of identity attributes may be specified as an identifier depending on program or service requirements and, in some cases, legislation.

A.1.2
When determining the set of *identity attributes* to be used as an *identifier*, the following factors shall be considered:

a. Universality;

   i. Every *Entity* within the program or service population *shall* possess an *identifier* set of *identity attributes*.

      NOTE: Even when an *identity attribute* is universal, widespread missing or incomplete values for the *Identity attribute* may render it useless as part of an *identifier* set. For example, many dates of birth for *Person*s born outside of Canada consist only of the year or the year and the month.

b. Uniqueness;

   i. The values associated with the *identity attributes shall* be sufficiently different for each Entity within the population of interest so that the Entities within the population of interest can be distinguished from one another.

      NOTE: For example, date of birth information by itself is insufficient to distinguish between *Person*s within a population because many people have the same birthdate.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

c. Constancy; and

   i. The values associated with the *identity attributes should* vary minimally (if at all) over time.

      NOTE: For example, having address information in the *identifier* set is problematic because a *Person*'s address is likely to change several times in their lifetime.

d. Collectability

   i. Obtaining a set of values for the *identity attributes should* be relatively easy.

      NOTE: For example, human DNA sequences are universal, unique, and very stable over time, but they are somewhat difficult to obtain.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Annex B
(Informative)

B Levels of Assurance Qualifiers

Identity Assurance Levels (Persons)	
Qualifier	**Description**
IP1	Little confidence required that a *Person* is who they claim to be.
IP2	Some confidence required that a *Person* is who they claim to be.
IP3	High confidence required that a *Person* is who they claim to be.
IP4	Very high confidence required that a *Person* is who they claim to be.

Identity Assurance Levels (Organizations)	
Qualifier	**Description**
IO1	Little confidence required that the *Organization identity information* is correct.
IO2	Some confidence required that the *Organization identity information* is correct.
IO3	High confidence required that the *Organization identity information* is correct.
IO4	Very high confidence required that the *Organization identity information* is correct.

Relationship Assurance Levels	
Qualifier	**Description**
R1	Little confidence required that the *Person(s)* is/are who they claim to be, that the *Organization(s) identity information* is correct, and that there is evidence of the *Relationship*.
R2	Some confidence required that the *Person(s)* is/are who they claim to be, that the *Organization(s) identity information* is correct, and that there is evidence of the *Relationship*.
R3	High confidence required that the *Person(s)* is/are who they claim to be, that the *Organization(s) identity information* is correct, and that there is evidence of the *Relationship*.
R4	Very high confidence required that the *Person(s)* is/are who they claim to be, that the *Organization(s) identity information* is correct, and that there is evidence of the *Relationship*.

Credential Assurance Levels	
Qualifier	**Description**
C1	Little confidence required that a *Holder* has control over an issued *Credential* and that the issued *Credential* is valid.
C2	Some confidence required that a *Holder* has control over an issued *Credential* and that the issued *Credential* is valid.
C3	High confidence required that a *Holder* has control over an issued *Credential* and that the issued *Credential* is valid.
C4	Very high confidence required that a *Holder* has control over an issued *Credential* and that the issued *Credential* is valid.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Annex C

(Informative)

C Accuracy of Identity Information

C.1 General

C.1.1

Accuracy ensures the quality of *identity information*. It ensures that the information represents what is true about an *Entity*, and that it is as complete and up to date as necessary.

C.1.2

For *identity information* to be considered accurate, three requirements shall be met:

a. The *identity information* is correct and up to date.

   NOTE: *Identity information* may change over time as a result of the occurrence of a *foundational event* (e.g., death of a *Person*, dissolution of a corporation). Ongoing updates to *identity information* may be required; otherwise, it becomes incorrect.

b. The *identity information* relates to a real *Entity*. *Identity information shall* be associated with an *Entity* which actually exists or existed at some point in time.

c. The *identity information* relates to the correct *Entity*.

   NOTE: In large populations, *Entities* may have the same or similar *identity information* as other *Entities* within the population. While the requirement for *Identity* uniqueness addresses this issue, the possibility of relating *identity information* to the wrong *Entity* still remains.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

C.1.3
The *Organization* shall ensure the accuracy of the *identity information* that is used within its programs and services.

> NOTE: The accuracy of *identity information* can be ensured by comparing it to an *authoritative source*. There are two methods by which this can be achieved. These two methods can be used independently or in combination, and an effective strategy usually requires the use of both:
>
> a. **Identity information retrieval**: On an as needed basis, request the *identity information* from an *authoritative source.* For example, a *Person*'s place of birth might be electronically retrieved from the federal registry of *Person*s born abroad; and
>
> b. **Identity information notification**: Subscribe to a notification service provided by an *authoritative source.* For example, death notifications might be received from a provincial vital statistics registry.
>
> If ensuring the accuracy of *identity information* by means of an *authoritative source* is not feasible, other methods may be employed, such as corroborating *identity information* using one or more instances of *evidence of identity*.

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

Bibliography

[1] Australia Trusted Digital Identity Framework

[2] BSI PAS 499:2019, Code of practice for digital identification and strong customer authentication.

[3] European Union. Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

[4] GPG 43, Requirements for Secure Delivery of Online Public Services

[5] GPG 44, Authentication Credentials in Support of HMG Online Services

[6] GPG 45, Identity Proofing and Verification of an Individual

[7] GPG 53, Transaction Monitoring for HMG Online Service Providers

[8] ISO/IEC 24760-1:2019, IT Security and Privacy -- A framework for identity management -- Part 1: Terminology and concepts

[9] ISO/IEC 24760-2:2015, Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements

[10] ISO/IEC 24760-3:2016, Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice

[11] ISO/IEC 27018, Information Technology – Security Techniques – Code of Practice for Protection of PII in Public Clouds Acting as PII Processors

[12] ISO/IEC 29100, Information Technology – Security Techniques – Privacy Framework

[13] ISO/IEC 29115:2013, Information technology -- Security techniques -- Entity authentication assurance framework

[14] ITSP.30.031 User Authentication Guidance for Information Technology Systems

[15] New Zealand Government, Digital Identity New Zealand
i. Evidence of Identity Standard
ii. Authentication Standards
iii. Identification Management

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.

[16] NIST Special Publication 800-63 Series, Digital Identity Guidelines

[17] The Public Sector Profile of the Pan-Canadian Trust framework (PCTF). Version 1.4, 2021

[18] Treasury Board Secretariat of Canada. Guideline on Defining Authentication Requirements. 2012

[19] Treasury Board Secretariat of Canada. Guideline on Identity Assurance. 2016

[20] Treasury Board Secretariat of Canada. Directive on Identity Management. 2019

[21] The UK Digital Identity and Attributes Trust Framework

© CIOSC 2022 – All rights reserved. Unauthorized reproduction is strictly prohibited.