CIOSC TS 115:202X (D3)

NATIONAL TECHNICAL SPECIFICATION

National Technical Specification for Digital Credentials and Digital Trust Services

35.030

WARNING

This document is not an official CIOSC Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as a National Technical Specification.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

CIO STRATEGY COUNCIL

- Page left intentionally blank -

Table of Contents

Foreword

The 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 technical specifications are developed in accordance with the Canadian Standards Development National Technical Specifications, 2019-08-02, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this National Technical Specification 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
1000 Innovation Drive, Suite 500
Ottawa, ON
K2K 3E7
ciostrategycouncil.com

Introduction

This is the First Edition of CIOSC TS 115:20XX, National Technical Specification for digital credentials and digital trust services.

CIOSC TS 115:20XX was prepared by the CIO Strategy Council Technical Committee on digital credentials, comprised of over XXXX thought leaders and experts in identity management, digital credentials, digital wallets, and related subjects. This Specification was approved by a Technical Committee formed balloting group, comprised of X producers, X government / regulators / policymakers, X users, and X general interests.

This Specification was developed in accordance with the SCC Canadian Standards Development National Technical Specifications, 2019-08-02.

All units of measurement expressed in this Specification are in SI (International System) units.

This Specification 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 Specification.

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

This Specification is intended to be used for conformity assessment.

We acknowledge and thank the Standards Council of Canada for its support in the development of the Specification.

ICS 35.030

- Page left intentionally blank -

Context

This Technical Specification is intended to support a prototype conformity assessment program for digital credentials and digital trust services and is intended to be a method of test to provide repeatable and reproducible procedures with consistent outcomes for the assessment of the products being assessed.

A digital credential is a set of machine-readable claims that can be verified. A digital credential can be used to increase efficiency of sharing trusted information while reducing or eliminating fraud due to misuse or modification. Digital credentials can be used to support many external or internal applications, including but not limited to secure identification to access online services, driving licences and passports, access to and presentation of health data, educational diplomas, and asset ownership.

An organization that issues a digital credential may carry out the role of Issuer, Holder, or Verifier.

This specification provides a small-scale set of conformity assessment criteria that can be used to support digital credential policy and regulatory objectives of the Canadian public sector, comprising of Federal, Provincial, Territorial and Indigenous governments.

This specification supports conformity assessment needs that can:

- provide market structure and clarity for digital credentials and digital trust services.
- enable interoperability, privacy protection and mutual support for digital credentials and digital trust services and products nationally and internationally.
- offer an avenue for product differentiation and competition between developers and providers.
- provide greater consumer confidence in digital credentials and digital trust services and products.
- provide a means for third-party assessment of the safety, efficacy, and ethical profile of digital credentials and digital trust services and products.
- provide Canadian governments with a standards-based tool suitable for use in policy and regulation.

This Technical Specification covers the following objects of conformity:

- Issuer Component
- Holder Component;
- Verifier Component; and
- Digital Trust Registry Component

Page left intentionally blank -

National Technical Specification for digital credentials and digital trust services

1 Scope

This National Technical Specification specifies a methodology for testing and criteria to be achieved to claim a system's compliance in issuing, managing, storing, presenting, or verifying machine-readable digital credentials.

NOTE: The requirements specified in the National Technical Specification are for testing and compliance purposes and do not replace or supersede applicable authority having jurisdiction standards, policies and guidelines. As such, the requirements are written in a manner to demonstrate compliance. By comparison, applicable authority having jurisdiction standards, policies and guidelines may mandate or recommend compliance for a particular implementation.

2 Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CAN/CIOSC 103-1:2020, *Digital Trust and Identity – Part 1: Fundamentals*

CSA ISO/IEC/IEEE 29119-4:2022, *Software and systems engineering – Software testing – Part 4: Test techniques* (ISO/IEC/IEEE 29119-4:2021, IDT)

EN 301-549, *Harmonized European Standard on Accessibility requirements for ICT products and services*

ISO/IEC 27001 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

ISO/IEC 27002 *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 27017 *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

ITSP.40.111, *Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information*

W3C *Decentralized Identifiers (DIDs) v1.0 Recommendations July 19, 2022*

3 Terms and Definitions

For the purposes of this document, the terms and definitions in CAN/CIOSC 103-1 and CSA ISO/IEC/IEEE 29119-4:2022 (ISO/IEC/IEEE 29119-4:2021, IDT) shall apply.

claim
A statement about a Subject

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.

credential format
The format used to specify identifier of the credential issuer, schema of issued credential, keys used to sign claims within the credential and cryptographic methods used. Revocation methods are optional

cryptographic module
The set of hardware, software, and/or firmware that implements cryptographic security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

decentralized identifier
A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically.

digital credential (also referred to as verifiable credential)
A portable digital record about a Subject (e.g., organization, individual, product) that can be held and shared through a user-controlled digital wallet/vault. It is the digital representation of a traditional physical certificate or information.

digital trust service
Enabling services for digital credentials, such as blockchain-based verifiable data registries, issuing and verifier services and digital wallets/vaults.

digital trust registry (also referred to as verifiable data registry)
A system that mediates the creation and verification of identifiers, keys, and other relevant data, such as credential schemas, revocation registries, issuer public keys, and so on, which might be required to use credentials.

entity
A thing with a distinct and independent existence, such as a person, organization, or device, 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 roles in the digital ecosystem.

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.

holder component
Information technology from which a presentation can be expressed to a verifier in forms such as a user-controlled digital wallet or digital trust service.

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.

issuer component
Information technology that provides a portable digital record about a Subject (e.g., organization, individual, product). It is the digital representation of a traditional physical certificate or information.

protected b (labelled as PROTECTED B)
A Government of Canada (GC) security level that applies to information or assets that, if compromised, could cause serious injury to an individual, organization or government.

storage component
A foundational layer for secure data storage, including personal data, including data models for storage and transport, syntax, data at rest protection.

subject
An entity about which claims are asserted by an issuer.

verifiable credential
A cryptographically secure set of information that is both of the following:

a. created in accordance with open standards that comply with all existing privacy protections; and
b. shared through a user-controlled, portable means that can be authenticated through publicly available services.

verifier
An entity that accepts a presentation from a holder for the purposes of delivering services or administering programs.

verifier component
information technology from which a digital credential can be verified authentic and valid.

4 Objects of conformity

4.1 Conformance

4.1.1 Conforming implementations shall pass respective normative specification-based techniques and requirements of this Specification. Test results including the test plan for executing specification-based techniques shall be reviewed before taking a final decision as to whether the object of conformity has been reliably demonstrated. A standardized expression shall be used for means of communicating the fulfilment of conformity assessment requirements.

NOTE: A statement of conformity may include non-fulfilment of specified requirements.

4.1.2 Implementations shall include one or more of the following service(s) and are considered in scope:

a. Issuer Component,
b. Holder Component;
c. Verifier Component; and/or
d. Digital Trust Registry Component

4.2 Methods of test

4.2.1 The following two specification-based testing techniques shall be used in accordance with ISO/IEC/IEEE 29119-4 to derive test cases that, when executed, generate evidence that test item requirements have been met or not:

a. Scenario testing
b. Requirements-based testing

NOTE: Additional specification-based test design techniques, structure-based test design techniques, and experience-based test design techniques may be used in accordance with ISO/IEC/IEEE 29119-4 where appropriate to provide added evidence and confidence that requirements in this Technical Specification are met.

4.2.2 Test results shall demonstrate conformance to the relevant specification or open standard specified in Clause 4.3.1 and remain in accordance with the conformity assessment requirements in Subsections 4.3, 4.4, and 4.5 and applicable Sections 9 through 12.

4.3 Data model, data interchange and file formats

4.3.1 Data model, data interchange and file formats used shall be published by a recognized body and may include one or several of the following examples:

a. JSON open standard
b. JSON-LD specification
c. W3C VC Data Model specification
d. ISO 18013-5

4.4 Scenario testing

4.4.1 A test plan for executing the test scenarios using the data model and data interchange and file formats specified in Clause 4.3.1 shall be sufficiently detailed with specific inputs, outputs, execution conditions, testing procedures and expected results in accordance with this Specification.

4.4.2 Test scenarios shall be executed on the service in scope. Each test scenario shall illustrate how the digital credential behaves in context. Test scenarios shall include one or several of the following dependent on the scope of the service:

a. Issue and Revoke Credential
b. Present Credential
c. Store Credential
d. Validate and Verify Credential
e. Retrieve Credential

4.4.3 The result of the test scenarios should be documented in a test report.

4.4.4 All test scenarios executed shall result and/or preserve the general characteristics of the digital credential in accordance with Section 5 through 8, and applicable Sections 9 through 12.

4.5 Requirements-based testing

4.5.1 The criteria specified in Sections 5 through 8 and applicable Sections 9 through 12 shall comprise the test model and a test case derived to cover each atomic requirements with at least one test case and executed in accordance with ISO/IEC/IEEE 29119-4.

5 Digital Credentials

5.1 Requirements

5.1.1 The digital credential shall be composed of three components:

a. Credential metadata: One or more credential attributes that describe the properties or characteristics of the credential;
b. Credential payload: A set of one or more claims asserted about one or more Subjects; and
c. Credential proofs: One or more methods or mechanisms that are used to verify that the issuer authored the credential and that the credential has not been tampered with.

5.1.2 Digital credentials shall:

a. contain claims about one or more Subjects;
b. reference a relevant event or activity;
c. identify the Issuer;
d. define a validity period;
e. be tamper-evident and unique within a specified population; and
f. be machine readable.

g. be revocable

5.1.3 The authorship of a digital credential shall be cryptographically verifiable.

5.1.4 The digital credential shall demonstrate that it can be stored within and presented from a minimum of two independent implementations.

5.1.5 The digital credential shall demonstrate that it can be cryptographically verified using a minimum of two independent implementations.

5.1.6 At least one authenticator shall be bound to a digital credential.

6 Storage

6.1 Requirements

6.1.1 All data shall be protected during data-in-transit and data-at-rest in accordance with Section 7.

NOTE: An organization may consider the use of CAN/CIOSC 100-1, Data governance – Part 1: Data-centric security, for the purposes of protecting the digital credential, and/or the issuer, holder and verifier component data at-rest, in-transit, and in-use.

6.1.2 All data held in device-based or cloud-based storage shall be encrypted in accordance with Section 7 of this Specification.

6.1.3 Cloud-based storage shall be implemented in accordance with ISO/IEC 27018 to protect personally identifiable information (PII) and ISO/IEC 29100 to protect personal information (PI).

7 Cryptographic Module

7.1 Requirements

7.1.1 Data shall be encrypted using a Cryptographic Module Validation Program – certified encryption module.

7.1.2 Data should be protected using CAN/CIOSC 100-1, Data governance – Part 1: Data-centric security.

7.1.3 Cryptographic algorithms shall be compliant with the recommendations for Protected B information in the CSE publication Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information (ITSP.40.111).

7.1.4 The cryptographic module shall ensure support for quantum-safe cryptography using cryptographic algorithms, cryptographic parameter sizes, key lengths and crypto periods which are configurable and which can be updated within protocols, applications and services to be consistent with transition guidance in time to meet specified transition dates.

8 Decentralized Identifier

8.1 Requirements

8.1.1 Decentralized Identifiers shall be implemented in accordance with the Decentralized Identifiers (DIDs) v1.0 W3C Recommendation.

9 Issuer Component

9.1 Requirements

9.1.1 The Issuer Component shall reference the digital credential to a record of a relevant event or activity.

9.1.2 The Issuer Component shall reference the digital credential with a decentralized identifier in accordance with Section 8 of this Specification.

9.1.3 The Issuer Component shall keep a record of the credential issuance, including information about the Holder to which a credential was assigned.

9.1.4 The Issuer Component shall identify the Issuer of the digital credential.

9.1.5 The Issuer Component shall require the Holder to complete administrator-initiated digital credential authenticator binding.

NOTE: As an example, the Holder supplying a new password when the administrator initiates a password reset.

9.1.6 The Issuer Component may provide to the Holder the ability to update the authenticators bound to a digital credential issued to the Holder. In this case, credential validation and verification test scenarios shall be performed first.

9.1.7 The Issuer Component shall provide to authorized personnel the ability to update the claims that were used to compose a digital credential and may provide them the ability to update the authenticators bound to a digital credential.

9.1.8 The Issuer Component shall record the initiating party for a digital credential attribute modification, and date of modification.

9.1.9 The Issuer Component shall provide a defined validity period on the digital credential.

NOTE: A defined validity period may be open-ended. For example, a period may have no specific expiry date.

9.1.10 The Issuer Component shall provide and preserve digital credentials in accordance with the general characteristics specified in Subsection 5.1 of this Specification.

9.1.11 The Issuer Component shall log and retain all digital credential events for a predefined period.

9.1.12 The Issuer Component shall provide the digital credential to a rightful Holder.

9.1.13 The Issuer Component shall provide a unique digital credential within a specified population.

9.1.14 The Issuer Component shall notify the Holder of any changes to digital credential information.

9.1.15 The Issuer Component shall have the ability to either suspend or revoke and re-issue the use of a digital credential issued to a Holder.

NOTE: As an example, the expiry date having been exceeded or the detection of suspicious activity.

9.1.16 The Issuer Component shall be designed to create a digital credential that receiving systems can parse or verify.

NOTE: It is strongly recommended that the Issuer Component, when deployed in a live environment, be retested against Section 5 and verified for compliance against this Specification.

9.1.17 The Issuer Component shall flag and notify the Issuer to undertake a reassessment of a digital credential relationship, potentially leading to suspension, when evidence of a potential change to underlying identity attributes or digital credential attributes is made known from an information provider.

9.1.18 The Issuer Component shall record the following information upon suspending a digital credential:

a. the effective date of suspension;
b. the reason for suspension; and
c. the initiating party for a suspension.

9.1.19 The Issuer Component should inform the Holder of the change in digital credential status.

9.1.20 The Issuer Component shall provide support for English and French, and should provide support for additional languages (e.g., Indigenous languages).

9.1.21 The Issuer Component shall conform to the Harmonized European Standard on Accessibility requirements for ICT products and services (EN 301-549)

9.1.22 The Issuer Component shall make available suspension information to the Holder and any Verifier.

9.1.23 The Issuer Component shall flag and notify the Issuer to undergo revalidation of a suspended digital credential, based on the system's policy and procedures, for the purposes of either recovery or revocation.

9.1.24 The Issuer Component shall initiate a process to render a digital credential unusable, potentially leading to revocation, if it detects indications of compromised information or compromised automated processing compromised authenticator.

9.1.25 The Issuer Component shall have the ability to recover a suspended digital credential.

9.1.26 The Issuer Component should provide to the Holder the ability to request the recovery of a suspended digital credential.

9.1.27 The Issuer Component shall perform identity verification of the Holder prior to digital credential recovery.

9.1.28 The Issuer Component shall record the following recovery information:

a. the effective date of recovery; and
b. the initiating party for the recovery action.

9.1.29 The Issuer Component shall make available recovery information to the Holder and any Verifier.

9.1.30 The Issuer Component shall have the ability to revoke a digital credential.

NOTE: As an example, due to an expiry date having been exceeded or the detection of suspicious activity.

9.1.31 The Issuer Component should provide to the Holder the ability to revoke a digital credential issued to the Holder.

9.1.32 The Issuer Component shall record the following information upon revoking a digital credential:

a. the effective date of revocation;
b. the reason for revocation; and
c. the initiating party for a revocation.

9.1.33 The Issuer Component shall inform the Holder of the change in digital credential status.

9.1.34 The Issuer Component shall make available the revocation information to the Holder and any Verifier.

9.1.35 The Issuer Component shall be designed to create and update claims with respect to the Subject(s) resulting from identity linking, identity verification, identity evidence determination, and identity continuity processes of the Issuer in accordance with CAN/CIOSC 103-1.

9.1.36 The Issuer Component shall ensure all stored information about digital credential issuance, including information about the Holder, is stored in in accordance with Section 6 of this Specification.

9.1.37 The Issuer Component shall encrypt all credential data and all other sensitive data, including personally identifiable information (PII) and personal information (PI), when it is shared with the Holder Component, in accordance with Section 7 of this Specification.

9.1.38 Where the Issuer Component is reliant upon a Digital Trust Registry for the issuance and verification of digital credentials, the Digital Trust Registry shall be implemented in accordance with Section 12 of this Specification.

10 Holder Component

10.1 Requirements

10.1.1 The Holder Component shall detect indications of digital credential misuse or compromise of the identity information.

NOTE: As an example, the expiry date having been exceeded or the detection of suspicious activity.

10.1.2 The Holder Component shall use password or biometric authentication to prevent unauthorized access.

a. The Holder Component should encourage the use of passwords that are in accordance with Best practices for passphrases and passwords (ITSAP.30.032).

b. The Holder Component shall limit the number of unsuccessful authentication attempts without negative consequences (e.g., suspending access to the Holder Component or wiping the contents of the Holder Component).

c. The Holder Component shall require re-authentication after being idle for a period of time, with that period of time being configurable by the Holder.

d. The Holder Component may support the ability to remotely allow, suspend or restore access to the Holder Component.

10.1.3 The Holder Component shall be able to request a digital credential from an Issuer.

a. The digital credential request shall allow Holder and Subject binding, where the Holder Component may be able to generate identifiers enabling proof of identifier control.

NOTE: Examples include pairwise decentralized identifiers, other decentralized identifiers, and other methods resulting in a URI identifier that can serve as a Subject in a Verifiable Credential or a Holder in a Verifiable Presentation

10.1.4 The Holder Component may be able to generate proofs of identifier control.

10.1.5 The Holder Component shall be able to request a digital credential from an Issuer in response to a Holder action.

10.1.6 The Holder Component may be able to request a digital credential using a subscribe model in which digital credentials representing earned credentials from one or more Issuers are requested/received/persisted so that the Holder Component stays up-to-date with available digital credentials from those Issuers.

10.1.7 The Holder Component shall be able to receive digital credentials from an Issuer.

10.1.8 The Holder Component shall be able to decline digital credentials from an Issuer.

10.1.9 The Holder Component shall be able to persist digital credentials with native format encoding to ensure that it can fully produce the original record intact.

10.1.10 The Holder Component shall store digital credentials with sufficient metadata to allow execution of the minimal functions in Section 6 of this Specification.

10.1.11 The Holder Component may be able to unpack the digital credential payload, but it is not required to do so.

10.1.12 The Holder Component shall be able to respond to a Holder's request to remove a digital credential and stop persisting that digital credential.

10.1.13 The Holder Component shall assign control over an issued digital credential so that the Holder's control of that digital credential may be subsequently verified.

10.1.14 The Holder Component shall have a mechanism to create and submit a verifiable presentation to a relying party in response to:

a. A Holder action.
b. A request for a verifiable presentation from a Verifier, if approved by the Holder.

10.1.15 The Holder Component may have a mechanism for receiving and processing presentation requests.

10.1.16 The Holder Component shall be able to manage connections (e.g., to Issuers, requesting parties, and other parties) in accordance with Section 7 requirements.

10.1.17 The Holder Component shall conform to the Harmonized European Standard on Accessibility requirements for ICT products and services (EN 301-549).

10.1.18 The Holder Component shall enable the Holder to manage privacy and sharing settings.

10.1.19 The Holder Component shall enable the user to control the sharing of digital credential data, in whole, in part, or as a derivation.

10.1.20 The Holder Component shall ensure there is Holder consent before sharing digital credential data and before accepting, declining, or removing digital credentials.

10.1.21 The Holder Component shall notify the Holder of any changes to the digital credentials.

10.1.22 The Holder Component shall preserve digital credentials in accordance with the general characteristics specified in Subsection 5.1 of this Specification.

10.1.23 The Holder Component shall provide support for English and French, and should provide support for additional languages (e.g., Indigenous languages).

10.1.24 The Holder Component shall store digital credentials in accordance with Section 6 of this Specification.

10.1.25 The Holder Component shall encrypt all data when it is shared with the Issuer Component or the Verifier Component, in accordance with Section 7 of this Specification.

11 Verifier Component

11.1 Requirements

11.1.1 The Verifier Component shall use acceptable methods to ensure that a digital credential is not tampered with, corrupted, or modified.

NOTE: Examples of acceptable methods include cryptographic methods or examination by a trained examiner.

11.1.2 The Verifier Component may resolve the digital credential with a decentralized identifier, in accordance with Section 8 of this Specification.

11.1.3 The Verifier Component shall not use a digital credential that is suspended or revoked to permit access to a good or service.

11.1.4 The Verifier Component shall determine whether the Holder has demonstrated control over a digital credential by means of one or more authenticators.

11.1.5 The Verifier Component shall inform the Holder when the Holder has demonstrated control over a digital credential by means of one or more authenticators.

11.1.6 The Verifier Component shall indicate an authentication failure when a digital credential is suspended or revoked, or when digital credential misuse or compromise is detected.

11.1.7 The Verifier Component shall provide support for English and French, and should provide support for additional languages (e.g., Indigenous languages).

11.1.8 The Verifier Component shall conform to the Harmonized European Standard on Accessibility requirements for ICT products and services (EN 301-549).

11.1.9 The Verifier Component shall preserve digital credentials, in accordance with the general characteristics specified in Subsection 5.1 of this Specification.

11.1.10 The Verifier Component shall encrypt all digital credential data and all other sensitive data, including personally identifiable information (PII) and personal information (PI), when it is shared with the Holder Component, in accordance with Section 7 of this Specification.

11.1.11 Where the Verifier Component is reliant upon a Digital Trust Registry for the verification of digital credentials, the Digital Trust Registry shall be implemented in accordance with Section 12 of this Specification.

11.1.12 The Verifier Component may inform the Issuer when it resolves a digital credential that is suspended, revoked or when a digital credential misuse or compromise is detected.

12 Digital Trust Registry Component

12.1 Requirements

12.1.1 The Digital Trust Registry Component shall store keys and other relevant data needed for the issuance and verification of digital credentials.

12.1.2 The Digital Trust Registry Component shall employ authentication and access control to prevent against unauthorized access, compromise, or destruction of data.

12.1.3 The Digital Trust Registry Component shall provide cryptographic assurances that the keys and other relevant data stored in the Digital Trust Registry have not been altered and are complete.

Annex A: Credentials Overview

(Informative)

What is a Credential?

The foundation of any transaction is trust. Trust is the confidence that any claim made by a transacting Entity can be relied on as being true. As examples, a transacting Entity may need to confirm the identity of the other Entity with which it is transacting, whether that other Entity has the authority to conduct a certain activity, or whether that other Entity owns a particular asset.7

Over time many types of Credentials have been developed and issued in order to solve lack of trust between Entities. These Credentials help to answer questions such as: “is this person permitted to drive a car in Ontario?”, “does this person meet the requirements needed to receive employment insurance benefits?”, “is this business licensed to cut timber in British Columbia?”, or “does this business qualify for a small business loan?”

In the most general sense, a Credential is an assertion of identity, qualification, competence, authority, rights, privileges, permissions, status, eligibility, or asset ownership (or a combination of these). More specifically, a Credential contains a set of one or more Claims asserted about one or more Subjects. The Credential is issued by one Entity, the Issuer, to another Entity, the Holder. The Issuer either possesses the de jure authority to issue the Credential or is granted through convention and consensus the de facto authority to issue the Credential.

Credentials contain two basic types of information. The first type of information is information about the Credential itself that is expressed by means of a set of Credential Attributes:

- Information that specifies the type of Credential;
- Information that identifies the Issuer of the Credential;
- Information that specifies the date that the Credential was issued;
- Information that specifies any constraints on the Credential (e.g., an expiry date, terms of use); and
- Information about the status of the Credential (i.e., whether the Credential is active, suspended, or revoked).

The second type of information contained within a Credential consists of a set of Attributes that describe the properties or characteristics of the Entities who are the Subjects of the Credential. These Entity Attributes are a selection of identity attributes of the Subjects and non-identity attributes of the Subjects. Some examples of non-identity attributes of a Subject are: the Subject's language of preference, the Subject's address of residence, and the Subject's total assets. If a Credential asserts that there is a Relationship between the Subjects, then the Credential will also include Relationship Attributes. All of these various Attributes are used to assert one or more Claims about one or more Subjects.

Types of Credentials

The following is a non-exhaustive list of the many types of Credentials that exist, along with some examples of their documentation:

- Citizenship and Legal Residency Credentials (e.g., birth certificate, citizenship certificate, permanent residence certificate, passport)
- Service Enrolment Credentials (e.g., Provincial/Territorial health services card, private health services insurance card, private dental services insurance card, private travel insurance card, loyalty reward program card, group or club membership card)
- Operator Licensing Credentials (e.g., automobile driver's licence, heavy equipment operator's licence)
- Business Credentials (e.g., licences, permits, inspection certificates)
- Financial Services Credentials (e.g., bank debit card, credit card)
- Asset Ownership Credentials (e.g., motor vehicle registration, deed to a property, proof of motor vehicle insurance)
- Health Credentials (e.g., "vaccine passport", vaccination certificate)
- Academic Credentials (e.g., diploma, degree, certificate, certification, school transcript)
- Employment Credentials (e.g., letter of employment)
- Trade or Professional Membership Credentials (e.g., Union of Electricians membership card)
- Diplomatic Credentials (e.g., ambassadorial letters of introduction)
- Journalist Credentials (e.g., press pass)
- Security Clearance Credentials (e.g., building access pass, secure zone access pass)
- System Access Credentials (e.g., username/password combination)

The Credential Model

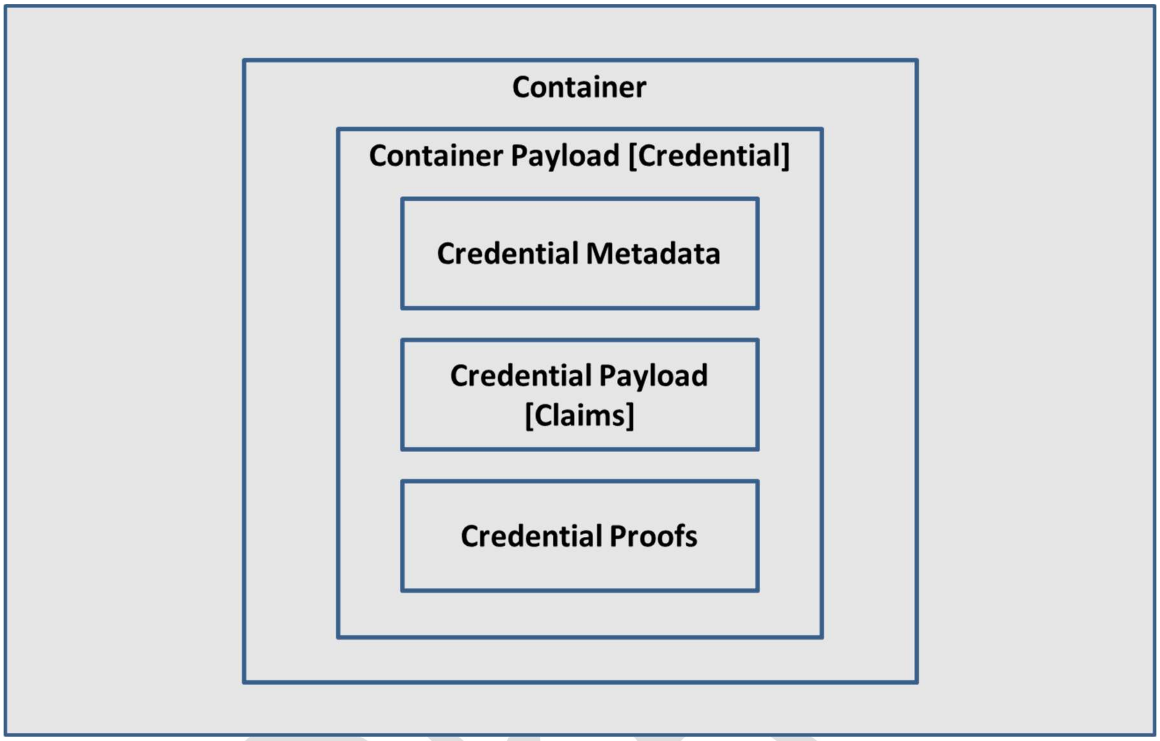

Figure 1: The Credential Model

In the Credential Model, a Credential is composed of three components:

- **Credential Metadata**: One or more Credential 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.

It should be noted that although a Verifier can verify the authorship of a Credential and can inspect a Credential for evidence of tampering, the veracity of the Credential Payload itself cannot be verified by a Verifier (i.e., the fact of a Claim (e.g., “the sky is green”) cannot be verified). By accepting a Credential, a Verifier is stating that the Verifier has confidence that the Issuer of the Credential has properly ascertained the veracity of the Claims prior to creating the Credential Payload.

The Holder of a Credential is usually given some form of documentation as evidence of being in possession of the Credential. For many years Credential documentation consisted mainly of a piece of paper or a plastic card. Over time authentication features (including electronic authentication features) were built into the plastic card. Increasingly, Credentials are being issued in an electronic form. The documentary evidence of a Credential can be thought of as a *container* or as a substrate for transporting the Credential. The Credential is placed inside the container and becomes the *payload of the container*.

Claims Assertion Models

The Claims Assertion Model of a Subject Claim

A Subject Claim is a statement about a Subject. A Subject Claim is expressed by means of one or more Entity Attribute*s*. Figure 2 illustrates the claims assertion model of a Subject Claim.

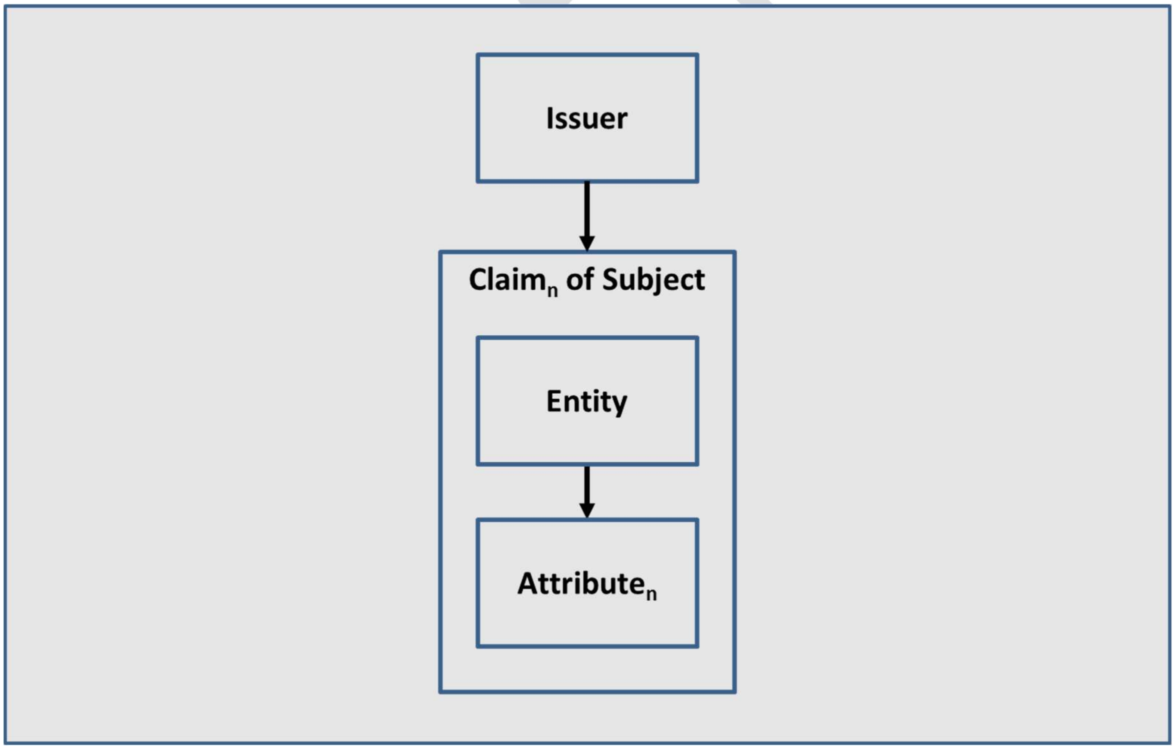

Figure 2: The Claims Assertion Model of a Subject Claim

The Claims Assertion Model of a Relationship Claim

A Relationship Claim is 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. Figure 3 illustrates the claims assertion model of a Relationship Claim.

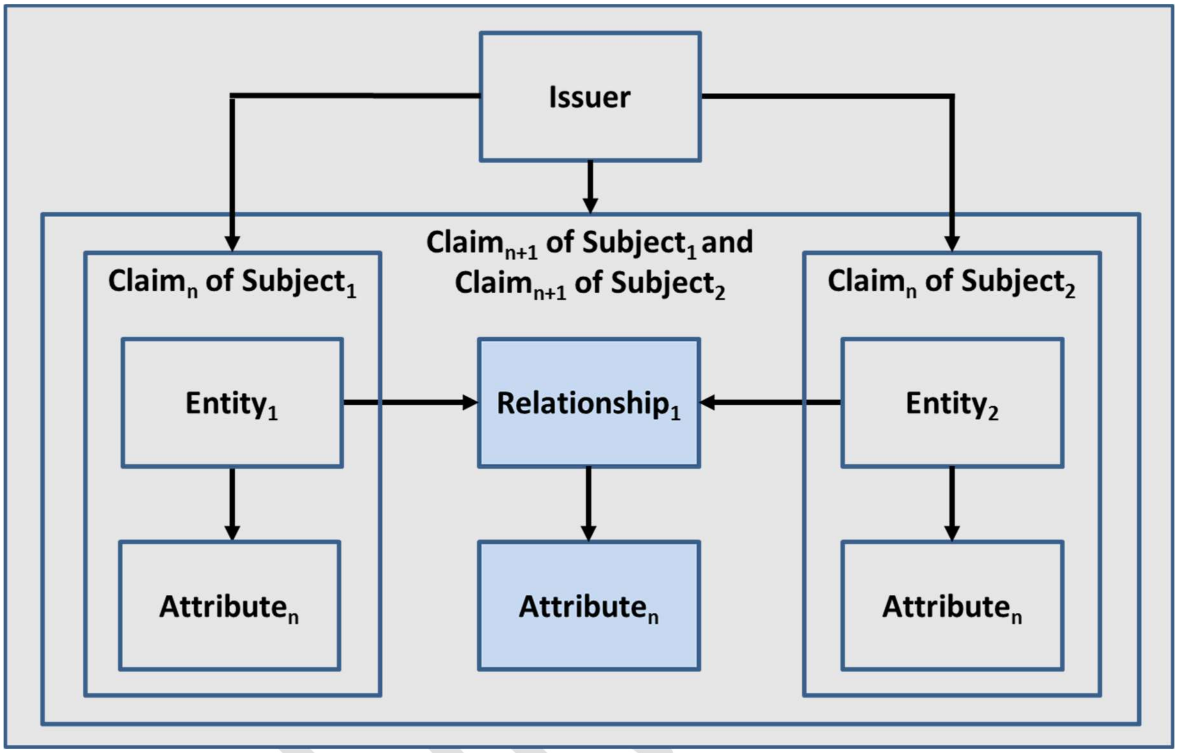

Figure 3: The Claims Assertion Model of a Relationship Claim

The Credential Issuance Model

An Issuer asserts one or more Claims about one or more Subjects, creates a Credential from these Claims, and assigns the Credential to a Holder. Figure 4 illustrates the credential issuance model.

NOTE: Some implementations of a Credential Issuance Process may include other steps and outputs. The definition above is the minimum necessary for conformance with this specification, but not necessarily sufficient to meet the documented goals of a digital credential management system.

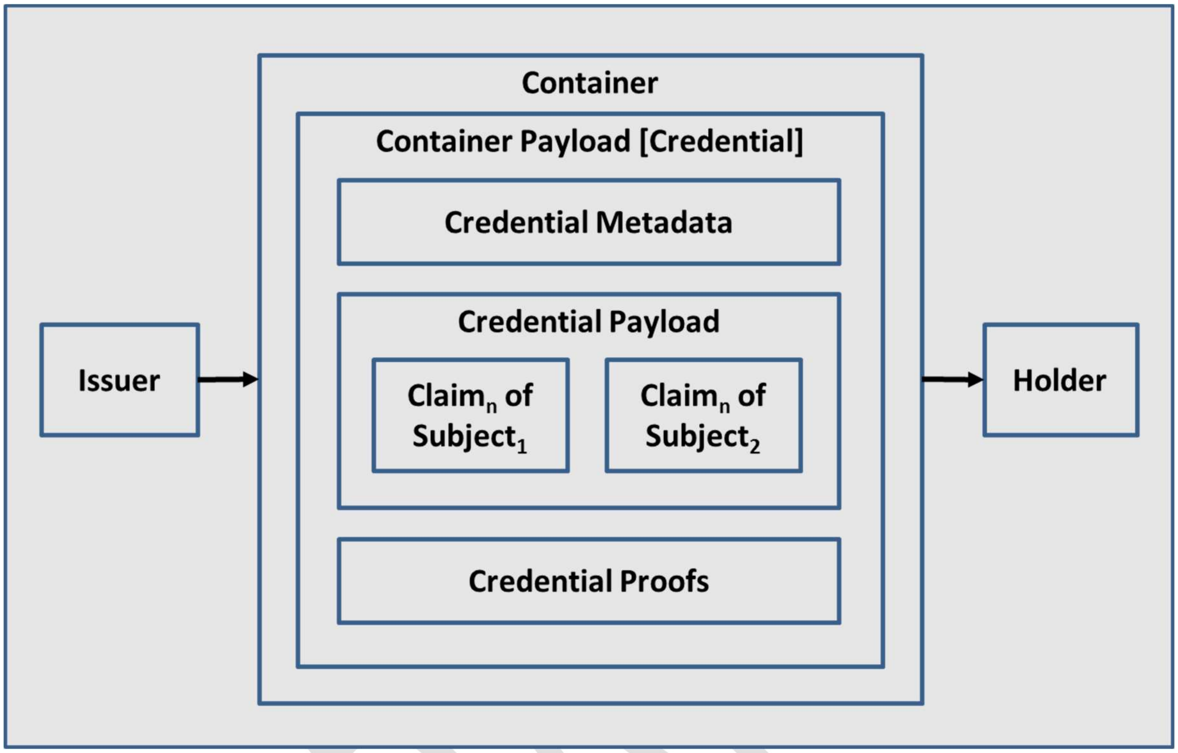

Figure 4: The Credential Issuance Model

Annex B: Credential Verification in Detail

(informative)

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

The Credential Verification process is dependent on the Credential Authenticator Binding process (i.e., the process of associating a Credential issued to a Holder with one or more authenticators). The Credential Authenticator Binding process also includes authenticator life-cycle activities such as suspending authenticators (caused by a forgotten password or a lockout due to successive failed credential verifications, 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).

Authenticators

An authenticator is something that a Holder controls that is used to prove that the Holder has retained control over an issued Credential. There are three types of authenticators:

- Something the Holder has (e.g., a cryptographic key or a one-time-password).
- Something the Holder knows (e.g., a password, a response to a challenge question).
- Something the Holder is or does (e.g., face, fingerprints, retinas, keyboard stroke timing, gait).

The authenticators when bound to a Credential will be subsequently used to prove, with a specified level of assurance, that the Credential is referring to the same Holder that was originally bound to the Credential.

It should be noted that given the irrevocability of biological characteristics (e.g., face, fingerprints, retinas), industry standards are generally cautious in regards to the exclusive use of biological characteristics for Credentials. A biological characteristic is not the same as a secret which can be changed periodically; a biological characteristic cannot be easily changed. Moreover, a Holder's biological characteristic can be replicated. For example, a threat actor may obtain a copy of the Holder's fingerprint, construct a replica, and pass Credential Verification (assuming that the Credential Verification process does not block such attacks by employing robust liveness detection techniques).

However, a biological characteristic may be used to unlock access to an authenticator stored within a local device in order to facilitate remote Credential Verification with a service. An example of such a scenario is the use of facial recognition software to unlock access to a mobile one-time passcode or other locally stored and generated mobile authenticator.

Bibliography

[1] Australia Trusted Digital Identity Framework

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

[3] CASCO Conformity Assessment Toolbox

[4] CAN/CIOSC 103-1:2020, Digital Trust and Identity – Part 1: Fundamentals

[5] Digital Credentials Consortium

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

[7] Government of Canada Digital Credentials

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

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

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

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

[12] ICAO MRTD Doc 9303 series of standards, Machine Readable Travel Documents

[13] ISO 18013-5, Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

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

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

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

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

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

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

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

[21] ITSAP.30.032 Best practices for passphrases and passwords

[22] New Zealand Government, Digital Identity New Zealand

i. Evidence of Identity Standard
ii. Authentication Standards
iii. Identification Management

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

[24] Ontario's Digital ID: Technology and Standards

[25] OpenID Connect Specifications

[26] Open Wallet Foundation

[27] The Public Sector Profile of the Pan-Canadian Trust framework, Version 1.4, Assessment Workbook, Consultation Draft v0.1, 2021-12

[28] The Public Sector Profile of the Pan-Canadian Trust framework, Version 1.4, Consolidated Overview, Consultation Draft v0.1, 2021-12

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

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

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

[32] Verifiable Credentials Explained

[33] W3C. Verifiable Credentials Data Model 1.0

[34] W3C. Verifiable Credentials Implementation Guidelines 1.0

[35] W3C. Verifiable Credentials Use Cases

[36] World Bank National Digital Identity and Government Sharing in Singapore