Table of Contents

1 TS-115

CIO Strategy Council

1.1 Technical Specification

2 Introduction

The 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 provides repeatable and reproducible procedures with consistent outcomes for the assessment of the products being assessed.

This specification provides a small-scale set of conformity assessment criteria that are based on digital credential policy and regulatory objectives of Canadian governments.

This specification supports conformity assessment needs that can:

- provide market structure and clarity for digital credentials and digital trust services.
- enable interoperability and mutual support for digital credentials and digital trust services 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, thus potentially helping with adoption.
- provide a means for third-party assessment of the safety, efficacy, and ethical profile of digital credentials and digital trust services.
- provide Canadian governments with a standards-based tool for establishing regulations for digital credentials and digital trust services.

3 Objects of Conformity Assessment Schedule

Objects of Conformity Assessment definitions are adapted from selected techical specifications and standards and agreed to by the working group. The definition reflects a common understanding of what is required to define scope of method of test for the purposes of conformity.

The objects of conformity assessment definitions are intended to be:

- **CONCISE** as agreed on by the technical experts.
- **NORMATIVE** in relation to the conformity assessment scheme, scope, requirements and method of test.
- **NON-NORMATIVE** in relation to other standards, specifications and recommendations.
- **SUBSTANTIVE** to assist in the mapping and scoping of product, process or service components for the purposes of conformity assessment.

Status field has the following values:

- **PROPOSED** - proposed by technical experts and contributors.
- **DRAFT** - in active draft by the techical experts with link to object of conformity assessment specification (template example)
- **PILOT** - approved by the sponsor for pilot as part of a prototype conformity asssessment program (note: material may still be in draft phase)
- **RELEASED** - material is finalized and released as part of a published deliverable.

3.1 Objects of Conformity Asessment Definitions

Defined and listed in the table below

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Digital Credential	`A portable digital record about a subject (e.g., organization, individual, product) that can be held and shared through a user-controlled wallet. It is the digital representation of a traditional physical certificate or information.`	DRAFT

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Digital Trust Service	Digital trust services is enabling service for digital credentials, such as a blockchain-based verifiable data registry, issuing and verifying services, and, digital wallets.	PROPOSED
Identifier	The set of identity attributes used to uniquely distinguish a particular Entity within a population.	PROPOSED
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.	DRAFT
Verifier	An Entity that accepts a Presentation (Proof) from a Holder for the purposes of delivering services, administering programs or yielding an ACCEPT or REJECT decision.	PROPOSED
Key	A key is data structure that represents a cryptographic key.	PROPOSED

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Presentation	A Presentaion is information derived from one or more Credentials. The source Credentials may have been issued by different Issuers.	PROPOSED
Signature	An electronic representation where, at a minimum: the Entity signing the data can be associated with the electronic representation, it is clear that the Entity intended to sign, the reason or purpose for signing is conveyed, and the data integrity of the signed transaction is maintained, including the original. **Alternate definition:** A key represents content secured with a digital signature or message authentication code	PROPOSED
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.	PROPOSED

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Cryptographic Proof	A Cryptographic Proof is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true without conveying additional information apart from the fact that the statement is true.	PROPOSED
Storage	TO DO	PROPOSED
Schema Object	A Schema object is used to list a set of attributes and data types. Issuers of Verifiable Credentials may reference schemas within Credentials they issue in order to provide a layer of semantic interoperability with other issuers utilising the same schema.	PROPOSED
Credential Format	A Credential Format is used to specify: 1. Identifier of the credential issuer, 2. Schema of issued credential. 3. Keys used to sign claims within the credential 4. Cryptographic methods used. 5. Revocation methods (optional)	DRAFT

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Credential Proof	see Cryptographic Proof	TODO
Credential Exchange	Credential Exchange is the set of protocols required to 1. Issue a Credential to a Holder, 2) Present a Proof to a Verifier	TODO
Credential Binding	Credential Binding is the process of associating a Credential issued to a Holder	TODO
Credential Data Model	A credential data model organizes elements of data and standardizes how they relate to one another and to the properties of real-world	PROPOSED
DID Methods	description	TODO
Revocation Registry	A Revocation Registry contains information required for verifiers to verify whether a revokable verifiable credential has been revoked by the issuer since issuance.	PROPOSED

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Trust Registry	`A Trust Registry answers queries about whether a particular party is trusted and authorized to perform a particular action in a particular context. A system role that mediate the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries and issuer public keys.`	PROPOSED
Messaging Protocol	`A Messaging Protocol supports identifier-based relationships, credential exchanges, and specialized application workflows in a manner that ensures privacy and security.`	PROPOSED

3.1.1 Other Objects of Conformity Assessment for consideration (from DHS)

- Signing Algorithm
- Revocation Algorithm
- Key Management - Issuer
- Key Management - Holder
- Encoding Scheme
- Rich Schemas / Semantic
- Selective Disclosure

- Predicates

3.2 Recognized Bodies

A recognized body is any organization that develops a standards, specifications or recommendation that is used is conjuction with conformity assessment scheme.

(To be reviewed:)

- DIF
- FIDO
- Hyperledger
- IETF
- ISO
- ICAO
- ToIP
- W3C

3.3 ISO Conventions for Requirements

- **Requirements -** SHALL, SHALL NOT
- **Recommendations -** SHOULD, SHOULD NOT
- **Permission -** MAY, MAY NOT
- **Possibility and Capability -** CAN, CANNOT

4 Object of Conformity Assessment Specification: Digital Credential

4.1 Part 1: Object of Conformity Assessment Specifications

Normative definition and description used for the purposes of the object of conformity assessment.

> **Digital Credential** is a portable digital record about a subject (e.g., organization, individual, product) that can be held and shared through a user-controlled wallet. It is the digital representation of a traditional physical certificate or information. Statement of Work

4.1.1 Related Definitions

Non-normative definitions which may assist in interpretation and application of the conformity.

- 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. (TS-115 D1)

- **Credential** 103-1 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.
- **Verifiable Credential** California means 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. (B) Shared through a user-controlled, portable means that can be authenticated through publicly available services.

Further definitions may provided by the evaluator or vendor:

- Relevant definitions

4.1.2 Appropriate Use Cases

- Provide descriptions of appropriate use cases that situate the context where the object of conformity is being used.

4.1.3 Selection of Product, Service or Process

- Provide descriptions of selected the products, services or process that are being tested in relation to the conformity assessment requirements._

4.1.4 Determination of Activities and Methods of Test

- Provide a description of activities undertaken and methods of test. used to btain information regarding the fulfillment of the conformity assessment requirements.

4.2 Part 2: Object of Conformity Asssessment Requirements

1. A demonstrable use case SHALL be provided to illustrate how the object of conformity behaves in context.
2. A description of the components being assessed SHALL be provided that demonstrates the object of conformity assessment
3. A digital credential SHALL be 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; and
   - 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.
4. A digital credentials SHALL be tamper-evident.
5. The authorship of a digital credential SHALL be cryptographically verifiable.

6. A digital credential format SHALL demonstrate conformity to one or several of the following specifications
   - JSON
   - JSON-LD
   - W3C VC Data Model
7. A digital credential SHALL demonstrate that it can be stored within and presented from a minimum of two independent implementations.
8. A diigtal credential SHALL demonstrate that it can be cryptograhically verified using a minimum of two independent implementations.

4.3 Part 3: Determination of Outputs, Review and Attestation

4.3.1 Determination of Outputs

Determination of outputs that are used as input into the review, decision and attestation stage.

4.3.2 Review and Decision

Review is the final stage of checking before taking the decision as to whether or not the object of conformity assessment e.g. product, service and system, has been reliably demonstrated to fulfil the specified requirements.

4.3.3 Attestation

The "statement of conformity", a standardizedc expression used to include then means of communicating that fulfilment of conformity assessment requirements has been demonstrated. It should be noted that a "statement of conformity" may include non fulfilment of specified requirements.

5 Object of Conformity Assessment Specification: Issuer

5.1 Part 1: Object of Conformity Assessment Definition

Normative definition and description used for the purposes of the object of conformity assessment.

> **Issuer** is 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.* CAN/CIOSC 103-1:2020

5.1.1 Related Definitions

Claim is a statement about a *Subject.* CAN/CIOSC 103-1:2020

Credential is a set of one or more *claims* asserted about one or more *Subjects.* CAN/CIOSC 103-1:2020

Entity is 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.* CAN/CIOSC 103-1:2020

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.* CAN/CIOSC 103-1:2020

5.2 Appropriate Use Cases

A description of an appropriate use case that situates the context where the object of conformity is being used.

5.2.0.1 Issue Credential

5.2.0.1.1 Actors

- Issuer
- Holder

5.2.0.1.2 Description An *Issuer* asserts *claims* about one or more *Subjects*, creates a *Credential* from these *claims*, and assigns the *Credential* to an appropriate *Holder.*

5.2.0.1.3 Preconditions

1. The *Issuer* has created or updated claims that have resulted from its *identity linking*, *identity verification*, *identity evidence determination*, and *identity continuity* processes with respect to the *Subject(s)* per CAN/CIOSC 103-1:2020
2. *Claims* relate to one or more *Subjects.*
3. A format is defined for *Credentials* that are to be issued.
4. The *Issuer* has a defined *Credential Issuance process* per CAN/CIOSC 103-1:2020.
5. The *Issuer* has a defined policy for selecting, identifying, and authenticating an appropriate *Holder* of a *Credential* relating to the *Subject.*
6. The *Issuer* has followed their policy to recognize an appropriate *Holder.*

5.2.0.1.4 Triggers – this is the event that causes the use case to be initiated.

1. An appropriate *Holder* has made a request for a *Credential.*

2. A *business event* or *vital event* (a *foundational event*) or other event, that relates to a *Subject*, occurs which may invalidate previously asserted *claims* that were included in issued *Credentials.* (See also Revoke Credential.)

5.2.0.1.5 Postconditions

1. A *Holder* is assigned control over an issued *Credential* so as the *Holder*'s control of the *Credential* may be subsequently verified.

5.2.0.2 Revoke Credential

5.2.0.2.1 Actors

- Issuer

5.2.0.2.2 Description An *Issuer* revokes a *Credential* it has issued so that a *Verifier* recognizes that the *Issuer* no longer asserts one or more *claims* the *Credential* contains.

5.2.0.2.3 Preconditions

1. The *Issuer* has issued a *Credential* to an appropriate *Holder.*

5.2.0.2.4 Triggers – this is the event that causes the use case to be initiated.

1. An appropriate *Holder* has made a request of the *Issuer* that causes a change to one or more *claims* in a *Credential.*
2. A *business event* or *vital event* (a *foundational event*) or other event, that relates to a *Subject*, occurs which invalidates previously asserted *claims* that were included in an issued *Credential.*

5.2.0.2.5 Postconditions

1. Information about the status of the previously-issued *Credential* is updated to indicate that the *Issuer* no longer asserts one or more *Claims* the *Credential* contains.
2. This updated information about the status of the *Credential* is available for *Verifiers* to use as they verify *Credentials* that are presented to them.

5.2.1 Selection of Product, Service or Process

- Provide descriptions of selected the products, services or process that are being tested in relation to the conformity assessment requirements._

5.2.2 Determination of Activities and Methods of Test

- Provide a description of activities undertaken and methods of test. used to btain information regarding the fulfillment of the conformity assessment requirements.

5.3 Part 2: Object of Conformity Asssessment Requirements

1. The *Issuer* has creates or updates claims that have resulted from its *identity linking*, *identity verification*, *identity evidence determination*, and *identity continuity* processes with respect to the *Subject(s)* per CAN/CIOSC 103-1:2020
2. *Claims* relate to one or more *Subjects*.
3. A format is defined for *Credentials* that are to be issued.
4. The *Issuer* has a defined *Credential Issuance process* per CAN/CIOSC 103-1:2020.
5. The *Issuer* has a defined policy, or a documented business rule, for selecting, identifying, and authenticating an appropriate *Holder* of a *Credential* relating to the *Subject(s)*.
6. The *Issuer* has followed their policy, or obeyed their business rule, to recognize an appropriate *Holder*.

5.3.1 Additional Guidance

1. When a *Subject* of a *Credential* is a *Person*, that *Person* may frequently also be the *Holder* of a *Credential*.

5.4 Part 3: Determination of Outputs, Review and Attestation

5.4.1 Determination of Outputs

Determination of outputs that are used as input into the review, decision and attestation stage.

5.4.2 Review and Decision

Review is the final stage of checking before taking the decision as to whether or not the object of conformity assessment e.g. product, service and system, has been reliably demonstrated to fulfil the specified requirements.

5.4.3 Attestation

The "statement of conformity", a standardizedc expression used to include then means of communicating that fulfilment of conformity assessment requirements has been demonstrated. It should be noted that a "statement of conformity" may include non fulfilment of specified requirements.

6 References

Link to relevant references. All references are provided without warrant or endorsement and are intended for informative purposes only.

6.1 Conformity Assessment

- Conformity Assessment for standards writers
- Introduction to Conformity Assessment ISO/CASCO
- Conformity assessment for standards writers Do's and don'ts
- CASCO Conformity Assessment Toolbox

6.2 Digital Credential Ecosystems

- Digital Credentials Consortium
- Grongingen Declaration Network
- European Self Sovereign Identity Framework
- Open Wallet Foundation
- Open Wallet Foundation GitHub Repo
- Ontario's Digital ID: Technology and standards
- DHS
- Verifiable Credentials Explained
- VC WG TPAC Sept 2022
- W3C VC Use Cases
- VC Issuing Protocols
- W3C Verifiable Conditions
- W3C DECENTRALIZED IDENTIFIER AND VERIFIABLE CREDENTIALS APPLICATIONS COMMUNITY GROUP
- RWOT Verifiable Credential Market Signals
- EBSI Specification
- ISO/IEC 18013-5 Personal identification — ISOcompliant driving licence —Part 5:Mobile driving licence (mDL) application
- Findy
- Procivis Proposal to reconcile Aries and ISO 18013-5
- Hyperledger Aries
- MIT Learner Wallet Specification
- W3C VCWG Technical Plenary
- ToIP Governance Use Cases
- TRAIN - Trust Management Infrastructure
- Centre Verite DOCS

6.3 Government (including Legal and Regulatory)

- Government of Canada Digital Credentials
- User-Centric Verifiable Digital Credentials
- Public Sector Profile of the Pan-Canadian Trust Framework V1.4

- California Legislature: SB-786 County birth, death, and marriage records: blockchain
- DHS Scaling Interoperability
- DHS Implementation Profile
- EBSI Publications
- European Digital Identity Framework
- Europen Digital Identity Wallet Consortium
- Digital Identity Lab Building the trust needed to accelerate adoption of a digital verifiable credential ecosystem for all Canadians

6.4 Specifications, Standards and Recommendations for Conformity Assessment

References to specifications,standards and recommendations for consideration as part of the conformity assessment scheme.

- CAN/CIOSC 103-1 Digital Trust and Identity - Part 1 - Fundamentals
- DIF DIDComm Messaging Specification
- DIF Well Known DID Configuration
- DIF Peer DID Method Specification
- DIF Confidential Data Storage
- DIF BBS Signature Scheme
- DIF Presentation Exchange
- DIF Credential Manifest
- DIF Wallet and Credential Interactions
- FIDO Alliance Specifications
- Hyperledger AnonCreds
- Hyperledger Aries Interop Profile
- ICAO Guiding Core Principles for the Development of Digital Travel Credential
- ICAO Machine Readable Travel Documents
- IETF SD-JWT
- IETF CBOR Web Token RFC 8392
- IETF JSON Web Proof
- IETF Multibase Format
- IETF Multiformatt Code Registrations
- IETF OAUTH 2.0 Pushed Authorization Requests
- ISO 18013-5:2021 Personal Identification Part 5: Mobile Driving Licence
- ITU Public-key and attribute certificate frameworks
- ITU Recommendation X.509 (10/19)
- OAuth Working Group Specifications: Active Drafts and RFCs
- OpenID for Verifiable Credential Issuance
- OpenID for Verifiable Presentations
- OpenID for Self-Issued OpenID Provider v2
- ToIP Trust Registry V1 Protocol Specification
- W3C Decentralized Identifiers v1.0

- W3C Verifiable Credentials Data Model
- W3C JSON-LD 1.1
- W3C Verifiable Credential JWT
- W3C did:key Method Specificatin
- W3C did:web Method Specification

6.5 Services, Test Suites and Demonstration Instances

- Universal Resolver: GitHub Repo
- Universal Resolver: DIF Hosted Instance
- W3C Verifiable Credentials Working Group Test Suite
- IDLAB W3C VC Conformance Assessment and Testing Report
- IDLAB Assessment Programs
- Hyperledger Aries Agent Test Harness
- Hyperleger Aries Mobile Test Harness
- Hyperledger Aries Interoperability Information
- Tonomy DID-JWT-VC implementation
- W3C Status List 2021

6.6 Industry/Vendor Reports, Blogs, Media Articles, etc

- Sept 29, 2022 The Importance of Open Source Digital Wallets to the Future of the Internet
- Sept 21, 2022 Decoupling AnonCreds from Hyperledger Indy
- July 27, 2022 Aries Agent Test Harness Enhancemement Project
- Oct 27, 2021 continuumloop Digital Wallet Report
- Apr 28, 2019 continuumloop The Current and Future State of Digital Wallets
- Cryptography Review of W3C Verifiable Credentials Data Model (VCDM) and Decentralized Identifiers (DIDs) Standards and Cryptography Implementation Recommendations
- Cross Community Architecture Survey
- Tonomy - How Best to Implement and in which VC Library?
- VC Library Research
- W3C VC & W3C DID Cryptography Review
- European Parliament: Updating the European Digital Identity Framework

6.7 Academic Research and Papers

- Stanford Proofs in Cryptography
- Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors 2022, 22, 5641

6.8 Libraries

Implementation libraries

- DIF did-jwt-vc
- DIF did-resolver
- DIF web-did-resolver
- DIF key-did-resolver
- Verite Governance Overview

6.9 Vendor Solutions, Products and Services

Currently in the market

- Apple Passkeys
- Credivera
- Microsoft Entra
- Trinsic
- Mattr

–end–