Table of Contents

1 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 assess.

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.

CIO Strategy Council

2 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.

2.1 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
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

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
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
Presentation	A Presentaion isinformation derived from one or more Credentials. The source Credentials may have been issued by different Issuers.	PROPOSED

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
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 description	PROPOSED
DID Methods		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

2.1.1 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

2.2 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 Object of Conformity Assessment Specification: Digital Credential

3.1 Part 1: Object of Conformity Assessment Definition

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

3.1.1 Related Definitions

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

- **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 provided by the evaluator or vendor: * Relevant definitions

3.2 Part 2: Use Cases

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

3.2.1 Conformity Asssessment Requirements

1. A relevant use case MUST be provided to illustrate how the object of conformity behaves in context.

3.2.2 Additional Guidance

- ...

3.3 Part 3: Selection of Product, Service and Process

Selection of the product, service and/or process that is being tested in relation to the specified requirements.

3.3.1 Conformity Asssessment Requirements

1. A description of the components being assessed MUST be provided that demonstrates the object of conformity assessment

3.3.2 Additional Guidance

- ...

3.4 Part 4: Determination of Activities

Determination of activities to obtain information regarding the fulfillment of the specified requirements. For the purposes of this scheme, activities are the methods of test.

3.4.1 Conformity Asssessment Requirements

1. Digital credentials SHALL be tamper-evident.
2. The authorship of a digital credential SHALL be cryptographically verified.
3. Method of test MUST prove that is digital credential is tamper-evident

3.4.2 Additional Guidance

- ...

3.5 Part 5: Determination of Outputs

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

3.5.1 Conformity Asssessment Requirements

1. TBD

3.5.2 Additional Guidance

- ...

3.6 Part 6: Review Decision

3.6.1 Review

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.

3.6.2 Conformity Asssessment Requirements

1. TBD

3.6.3 Additional Guidance

- ...

3.7 Part 7:Attestation

The creation of a "statement of conformity", which is a generic expression used to include all means of communicating that fulfilment of specified requirements has been demonstrated. It should be noted that a "statement of conformity" can include non fulfilment of specified requirements.

3.7.1 Conformity Asssessment Requirements

1. TBD

3.7.2 Additional Guidance

...

3.8 Part 8: Other Considerations

other requirements that may be part of object of conformity of assessess

3.8.1 Credential Data Models

Credential data models are composed of three main components: credential metadata, credential attributes (claims) and cryptographic material which allows a holder to prove the authenticity of presented data to a verifier.

3.8.2 Encoding / Decoding Formats

A format is a means to structure and convey information. This may also include encoding and decoding.

3.8.3 Technical schemes

Credential formats MUST demonstrate conformity to one or several of the following specifications

- JSON
- JWT

4 Object of Conformity Assessment Specification: Issuer

4.1 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

4.1.1 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

4.2 Part 2: Use Cases

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

4.2.1 Issue Credential

4.2.1.1 Actors

- Issuer
- Holder
- Subject(s)

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

4.2.1.3 Preconditions

1. *Claims* are associated with one or more *Subjects*.
2. *Claims* that are to be included in a *Credential* are available for that purpose.
3. A format for *Credentials* that are to be issued is defined.
4. A process for assigning a *Credential* to an appropriate *Holder* is defined.

4.2.1.4 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*, that relates to a *Subject*, occurs which may invalidate previously asserted *claims* that were included in issued *Credentials*. ("A life-cycle event")

4.2.1.5 Postconditions

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

4.2.2 Conformity Asssessment Requirements

- ...

4.2.3 Additional Guidance

- ...

4.3 Part3: Selection of Product, Service and Process

Selection of the product, service and/or process that is being tested in relation to the specified requirements.

4.3.1 Conformity Asssessment Requirements

1. A description of the components being assessed MUST be provided that demonstrates the object of conformity assessment

4.3.2 Additional Guidance

- ...

4.4 Part 4: Determination of Activities

Determination of activities to obtain information regarding the fulfillment of the specified requirements. For the purposes of this scheme, activities are the methods of test.

4.4.1 Conformity Asssessment Requirements

1. TBD

4.4.2 Additional Guidance

- ...

4.5 Part 5: Determination of Outputs

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

4.5.1 Conformity Asssessment Requirements

1. An *Issuer* must document how its Credential Issuance process to meet the required outcome(s) documented in CAN/CIOSC 103-1:2020.
2. An *Issuer* must document how its Identity Continuity process to meet the required outcome(s) documented in CAN/CIOSC 103-1:2020.
3. An *Issuer* must document how its Identity Linking process to meet the required outcome(s) documented in CAN/CIOSC 103-1:2020.
4. An *Issuer* must document how its Identity-Credential Binding process to meet the required outcome(s) documented in CAN/CIOSC 103-1:2020.
5. An *Issuer* must document how its Credential-Authenticator Binding process to meet the required outcome(s) documented in CAN/CIOSC 103-1:2020.

4.5.2 Additional Guidance

- ...

4.6 Part 6: Review Decision

4.6.1 Review

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.

4.6.2 Conformity Asssessment Requirements

1. TBD

4.6.3 Additional Guidance

- ...

4.7 Part 7:Attestation

The creation of a "statement of conformity", which is a generic expression used to include all means of communicating that fulfilment of specified requirements has been demonstrated. It should be noted that a "statement of conformity" can include non fulfilment of specified requirements.

4.7.1 Conformity Asssessment Requirements

1. TBD

4.7.2 Additional Guidance

...

5 References

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

5.1 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

5.2 Digital Credential Ecosystems

- Digital Credentials Consortium
- 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 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

5.3 Government (including Legal and Regulatory)

- Government of Canada Digital Credentials
- User-Centric Verifiable Digital Credentials
- 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

5.4 Specifications, Standards and Recommendations for Conformity Assessment

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

- Hyperledger AnonCreds
- Hyperledger Aries Interop Profile
- W3C Decentralized Identifiers v1.0
- W3C Verifiable Credentials Data Model
- W3C Verifiable Credential JWT
- ISO 18013-5:2021 Personal Identification Part 5: Mobile Driving Licence
- IETF SD-JWT
- IEFT CBOR Web Token RFC 8392
- IETF JSON Web Proof
- ToIP Trust Registry V1 Protocol Specification
- DIF DIDComm Messaging Specification
- DIF Well Known DID Configuration
- DIF Peer DID Method Specification
- DIF Confidential Data Storage
- DIF BBS Signature Scheme
- ICAO Guiding Core Principles for the Development of Digital Travel Credential
- ICAO Machine Readable Travel Documents

- OAuth Working Group Specifications: Active Drafts and RFCs
- ITU Public-key and attribute certificate frameworks
- ITU Recommendation X.509 (10/19)
- OpenID for Verifiable Credential Issuance
- OpenID for Verifiable Presentations
- OpenID for Self-Issued OpenID Provider v2
- FIDO Alliance Specifications

5.5 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

5.6 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?

5.7 Academic Research and Papers

*Stanford Proofs in Cyptography

–end–