

# Contents

<b>Introduction</b>	<b>2</b>
<b>Objects of Conformity Assessment Schedule</b>	<b>3</b>
Objects of Conformity Assessment Definitions . . . . .	3
Other Proposed (from DHS) . . . . .	6
Recognized Bodies . . . . .	6
<b>Object of Conformity Assessment Specification: Digital Credential</b>	<b>7</b>
Part 1: Object of Conformity Assessment Definition . . . . .	7
Related Definitions . . . . .	7
Part 2: Use Cases . . . . .	7
Conformity Assessment Requirements . . . . .	7
Additional Guidance . . . . .	7
Part 3: Selection of Product, Service and Process . . . . .	7
Conformity Assessment Requirements . . . . .	8
Additional Guidance . . . . .	8
Part 4: Determination of Activities . . . . .	8
Conformity Assessment Requirements . . . . .	8
Additional Guidance . . . . .	8
Part 5: Determination of Outputs . . . . .	8
Conformity Assessment Requirements . . . . .	8
Additional Guidance . . . . .	8
Part 6: Review Decision . . . . .	8
Review . . . . .	8
Conformity Assessment Requirements . . . . .	8
Additional Guidance . . . . .	9
Part 7: Attestation . . . . .	9
Conformity Assessment Requirements . . . . .	9
Additional Guidance . . . . .	9
Part 8: Other Considerations . . . . .	9
Credential Data Models . . . . .	9
Encoding / Decoding Formats . . . . .	9
Technical schemes . . . . .	9
<b>Object of Conformity Assessment Specification: Issuer</b>	<b>10</b>
Part 1: Object of Conformity Assessment Definition . . . . .	10
Related Definitions . . . . .	10
Part 2: Use Cases . . . . .	10
Issue Credential . . . . .	10
Conformity Assessment Requirements . . . . .	11
Additional Guidance . . . . .	11
Part3: Selection of Product, Service and Process . . . . .	11
Conformity Assessment Requirements . . . . .	11
Additional Guidance . . . . .	11

Part 4: Determination of Activities . . . . .	11
Conformity Assessment Requirements . . . . .	11
Additional Guidance . . . . .	12
Part 5: Determination of Outputs . . . . .	12
Conformity Assessment Requirements . . . . .	12
Additional Guidance . . . . .	12
Part 6: Review Decision . . . . .	12
Review . . . . .	12
Conformity Assessment Requirements . . . . .	12
Additional Guidance . . . . .	12
Part 7: Attestation . . . . .	12
Conformity Assessment Requirements . . . . .	13
Additional Guidance . . . . .	13
<b>References</b>	<b>13</b>
Conformity Assessment . . . . .	13
Digital Credential Ecosystems . . . . .	13
Government (including Legal and Regulatory) . . . . .	14
Specifications, Standards and Recommendations for Conformity Assessment . . . . .	14
Services, Test Suites and Demonstration Instances . . . . .	14
Industry Reports, Blogs, Media Articles, etc. . . . .	15

## 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. ls

## Objects of Conformity Assessment Schedule

Objects of Conformity Assessment definitions are adapted from selected technical specifications and standards. The definition reflects an agreed on understanding of what is required of the object for the purposes of conformity assessment testing.

These 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 the working group \* ADOPTED - adopted by the working group \* FINALIZED - definition finalized by the working group. \* SPEC Link to specification (template example)

## Objects of Conformity Assessment Definitions

Defined and listed in the table below

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
<b>Digital Credential</b>	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.	SPEC
<b>Digital Trust Services</b>	Digital trust services are enabling services for digital credentials, such as a blockchain-based verifiable data registries, issuing and verifying services, and digital wallets.	PROPOSED

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
<b>Identifier</b>	The set of identity attributes used to uniquely distinguish a particular Entity within a population. CIOSC	PROPOSED
<b>Issuer</b>	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.	SPEC
<b>Verifier</b>	An Entity that accepts a Presentation from a Holder for the purposes of delivering services or administering programs. PROPOSED	
Presentation	information derived from one or more Credentials. The source Credentials may have been issued by different Issuers.	PROPOSED
<b>Signature</b>	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.	PROPOSED

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
<b>Holder</b>	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
<b>Storage</b>	TO DO	PROPOSED
<b>Schema Object</b>	Schemas are used to list a set of attributes. 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
<b>Credential Format</b>	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)	SPEC
<b>Revocation Registry</b>	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
<b>Trust Registry</b>	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
<b>Messaging Protocol</b>	A Messaging Protocol supports identifier-based relationships, credential exchanges, and specialized application workflows in a manner that ensures privacy and security.	PROPOSED

#### Other Proposed (from DHS)

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

#### Recognized Bodies

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

(To be reviewed:) \* DIF \* FIDO \* Hyperledger \* IETF \* ISO \* ICAO \* ToIP \* W3C \*

# Object of Conformity Assessment Specification: Digital Credential

## 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

### 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

## Part 2: Use Cases

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

### Conformity Assessment Requirements

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

### Additional Guidance

- ...

## 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.*

### **Conformity Assessment Requirements**

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

### **Additional Guidance**

- ...

## **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.*

### **Conformity Assessment 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

### **Additional Guidance**

- ...

## **Part 5: Determination of Outputs**

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

### **Conformity Assessment Requirements**

1. TBD

### **Additional Guidance**

- ...

## **Part 6: Review Decision**

### **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.*

### **Conformity Assessment Requirements**

1. TBD



## Additional Guidance

- ...

## 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.*

## Conformity Assessment Requirements

1. TBD

## Additional Guidance

...

## Part 8: Other Considerations

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

## 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.

## Encoding / Decoding Formats

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

## Technical schemes

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

- JSON
- JWT

# Object of Conformity Assessment Specification: Issuer

## 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

### 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

## Part 2: Use Cases

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

### Issue Credential

#### Actors

- Issuer
- Holder
- Subject(s)

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

#### 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.

**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”)

**Postconditions**

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

**Conformity Assessment Requirements**

- ...

**Additional Guidance**

- ...

### **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.*

**Conformity Assessment Requirements**

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

**Additional Guidance**

- ...

### **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.*

**Conformity Assessment Requirements**

1. TBD

#### **Additional Guidance**

- ...

### **Part 5: Determination of Outputs**

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

#### **Conformity Assessment 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.

#### **Additional Guidance**

- ...

### **Part 6: Review Decision**

#### **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.*

#### **Conformity Assessment Requirements**

1. TBD

#### **Additional Guidance**

- ...

### **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.*

## **Conformity Assessment Requirements**

1. TBD

## **Additional Guidance**

...

## **References**

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

## **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

## **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
- 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

## **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
- European Digital Identity Wallet Consortium

## **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
- IETF CBOR Web Token RFC 8392
- 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

## **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

### **Industry 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 Enhancement 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