Table of Contents

# Objects of Conformity Assessment Schedule

Objects of Conformity Assessment definitions are adapted from a variety of techical specifications and standards.

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 grou. \* SPEC [Link to specification (template example)](./objca-template.md)

| Object of Conformity Assessment | Object of Conformity Assessment Definition | Status |
| --- | --- | --- |
| **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. | [SPEC](./objca-digital-credential.md) |
| **Identifier** | The set of identity attributes used to uniquely distinguish a particular Entity within a population. CIOSC | 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. | [SPEC](./objca-issuer.md) |
| **Verifier** | 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 |
| **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. | 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 |
| **Storage** | TO DO | PROPOSED |
| **Schema Object** | 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 |
| **Credential Definition** | Credential Definitions are used to specify the following information: 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) |  |
| **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 |
| **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 |

# 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](/docs/statement-of-work.md)

### 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](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB786#93ENR) 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*](./use-cases.md) *that situates the context where the object of conformity is being used.*

### Conformity Asssessment Requirements

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

### 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 Asssessment 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*](./methods-of-tests.md)*.*

### 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

### Additional Guidance

* …

## Part 5: Determination of Outputs

*Determination of* [*outputs*](../scheme-definitions.md) *that are used as input into the review, decision and attestation stage.*

### Conformity Asssessment 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 Asssessment 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 Asssessment 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](https://www.json.org/json-en.html)
* [JWT](https://www.rfc-editor.org/rfc/rfc7519)

# 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](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/)

### Related Definitions

**Claim** is a statement about a *Subject*. [CAN/CIOSC 103-1:2020](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/)

**Credential** is a set of one or more *claims* asserted about one or more *Subjects*. [CAN/CIOSC 103-1:2020](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/)

**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](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/)

**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](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/)

## Part 2: Use Cases

*A description of an appropriate* [*use case*](./use-cases.md) *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 Asssessment 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 Asssessment 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*](./methods-of-tests.md)*.*

### Conformity Asssessment Requirements

1. TBD

### Additional Guidance

* …

## Part 5: Determination of Outputs

*Determination of* [*outputs*](../scheme-definitions.md) *that are used as input into the review, decision and attestation stage.*

### 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](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/).
2. An *Issuer* must document how its Identity Continuity process to meet the required outcome(s) documented in [CAN/CIOSC 103-1:2020](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/).
3. An *Issuer* must document how its Identity Linking process to meet the required outcome(s) documented in [CAN/CIOSC 103-1:2020](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/).
4. An *Issuer* must document how its Identity-Credential Binding process to meet the required outcome(s) documented in [CAN/CIOSC 103-1:2020](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/).
5. An *Issuer* must document how its Credential-Authenticator Binding process to meet the required outcome(s) documented in [CAN/CIOSC 103-1:2020](https://ciostrategycouncil.com/standards/find-a-standard/standards-in-digital-trust/digital-trust-fundamentals/).

### 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 Asssessment 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 Asssessment Requirements

1. TBD

### Additional Guidance

…