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

Objects of Conformity Assessment definitions ("object definitions") are adapted from selected technical specifications and standards and agreed to by the technical experts The definition reflects a common understanding and is used to define scope of the process, service or component and to specify the appropriate methods of test used for the purposes of conformity assessment.

3.1 Object Definitions

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

Where possible, the object definitions are developed to be interpreted as a single process, service or component. If the definition implies a role, then this will be specified as part of the definition. If an object definition consists of several components (i.e. a composite object), this is further specified in the object template.

3.2 Minimal Viable Set for TS-115

Conformity assessment object definitions being developed by the technical experts for inclusion in TS-115

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
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
Decentralized Identifier	A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically.	DRAFT
Issuer	A process, service or component that generates and signs the digital credential	DRAFT
Holder	A process, service or component from which a Presentation can be expressed to a Verifier. A Holder is usually under the control of a User	DRAFT
Verifier	A process, service or component that verifies the presentation of a credential to yield an ACCEPT or REJECT decision	DRAFT
Storage	A foundational layer for secure data storage, including personal data, including data models for storage and transport, syntax, data at rest protection, CRUD API, access control, synchronization, and a minimum viable HTTP-based interface compatible with W3C DIDs/VCs.	DRAFT
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.	DRAFT

3.3 Priority List

Conformity assessment object definitions that will be included in subsequent document releases.

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Holder Binding	Holder Binding is the process of associating a Credential issued to a Holder and limiting its control to the associated Holder	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
Digital Trust Service	A Digital Trust Service is an enabling service that can include one or several of the followiing: digital credentials, verifiable data registries, issuing services, verifying services, and, digital wallet services.	PROPOSED
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	PROPOSED
Credential Proof	A generalized proof (or set of proofs) that can be used to demonstrate one or more of: that the credential is valid, that the information (or derived information) is consistent with the intent for which it was issued, that the credential has not been tampered with, and, that the credential is being presented by the Holder (or authorized delegate) to whom it was issued. The proofs may employ cryptographic, or non-cryptographic means	PROPOSED

3.4 Others

Conformity assessment object definitions that are under consideration and may be included in subsquent document releases.

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
Assigned Identifier	A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between Entities within a population without the use of any other identity attributes.	PROPOSED
Verifiable Identifier	A type of identifier which its control can be independently verified (generally by cryptographic means	PROPOSED
Key	A key is data structure that represents a key or a secret.	PROPOSED
Presentation	A Presentation is information derived from one or more Credentials. The source Credentials may have been issued by different Issuers.	PROPOSED
Schema	A Schema is used to define a set of attributes and data types in order to provide a layer of semantic interoperability with other entities utilising the same schema.	PROPOSED
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
Revocation Method	A Revocation Method generates the necessary information required to indicate whether a credential has been revoked by the issuer since issuance.	PROPOSED
Facial Comparison	Facial comparision is the use of a facial recognition algorthim to yield a matching or confidence score (e.g MATCH/NO MATCH, PERCENT SIMILARITY)	PROPOSED
Trust Registry	A Trust Registry answers queries about whether an entity or object is trusted or is authorized to perform an action within a given context.	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
Selective Disclosure	The ability of a user to make nuanced decisions about what information to share.	PROPOSED

Object of Conformity Assessment	Object of Conformity Assessment Definition	Status
Predicate	The ability of a user to check a value against a certain condition, disclosing only true or false without revealing the value.	PROPOSED
Rich Schema	Hierarchically composable graph-based representations of complex data.	PROPOSED

3.5 Recognized Bodies

Recognized bodies are any organizations that develop standards, specifications or recommendations and which have established governance and processes that ensure fair development and ongoing maintenance of published materials. Standards, specificatios and recommendations used in conjunction for conformity assessment SHALL be published by a recognized body.

Recognized bodies (under review)

Acronym/Short Name	Official Name	Website
DIF	Decentralized Identity Foundation	https://identity.foundation
FIDO	FIDO Alliance	https://fidoalliance.org/
Hyperledger	Hyperledger Foundation, Aries	https://www.hyperledger.org/use/aries
IETF	Internet Engineering Task Force	https://www.ietf.org/
NIST	National Institute for Standards and Technology	https://www.nist.gov/
ISO	International Organization for Standardization	https://www.iso.org/home.html
ICAO	International Civil Aviation Organization	https://www.icao.int/Pages/default.aspx
ToIP	Trust Over IP Foundation	https://trustoverip.org/
W3C	Worldwide Web Consortium	https://www.w3.org

3.6 ISO Conventions for Requirements

Recommended terminology for conformity assessment requirements:

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

3.7 Technology Readiness Levels

Technology Readiness Levels (TRL) describe the different stages of pre-commercial development.

All objects of conformity SHOULD be assessed at TRL 7 or greater

TRL	Short Definition	Description	Example of Activities
1	Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D).	Activities might include paper studies of a technology's basic properties.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions.	Activities are limited to analytic studies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology.	Activities include components that are not yet integrated or representative.
4	Component(s)/subsystem(s) and/or process validation in a laboratory environment.	Basic technological components are integrated to establish that they will work together.	Activities include integration of "ad hoc" hardware in the laboratory.

TRL	Short Definition	Description	Example of Activities
5	Semi-integrated component(s)/subsystem(s) and/or process validation in a simulated environment.	The basic technological components are integrated for testing in a simulated environment.	Activities include laboratory integration of components.
6	System and/or process prototype demonstration in a simulated environment.	A model or prototype that represents a near desired configuration.	Activities include testing a model or prototype in a simulated or laboratory environment.
7	Prototype system ready (form, fit, and function) for demonstration in an appropriate operational environment.	Prototype is ready for demonstration in an operational environment and is at planned operational level.	Activities include prototype field testing in a real-world operational setting.
8	Actual technology completed and qualified through tests and demonstrations.	Technology has been proven to work in its final form and under expected conditions.	Activities include developmental testing and evaluation of whether it will meet operational requirements.
9	Actual technology proven through successful deployment in an operational setting.	Actual application of the technology in its final form and under real-life conditions, such as those encountered in operational tests and evaluations.	Activities include using the innovation under operational conditions.

Source: ISC Technology Readiness Scale

4 Object of Conformity Assessment Specification: Digital Credential

4.1 Part 1: Object of Conformity Assessment Specifications

4.1.1 Definition

A **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

4.1.2 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** 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. CAN/CIOSC 103-1
- **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.
- **Credential** A document, object, or data structure that vouches for the identity of a person or other entity through some method of trust and authentication. World Bank

4.1.3 Key Characteristics

In general, a well-formed digital credential has three components:

1. **Metadata** Provides information about the credential.
2. **Payload** Contains the actual content of the credential, which is attested by the issuer of the credential. The content may consist of a set of one or claims, and any additional information that the issuer intends to be relied on by other parties.

3. **Proof** A method to detect to tampering and to verify the authorship of the credential.

4.1.4 Appropriate Use Cases

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

Digital Credentials may be employed in a wide variety of use cases. For the purposes of testing, the use cases SHALL be centred around the key functionalities associated with the digital credential. These are:

1. Issue Credential
2. Present Credential.
3. Store Credential.
4. Verify Credential
5. Retrieve Credential
6. Revoke Credential

Please refer to W3C Verifiable Credentials Use Cases for additional detail.

4.1.5 Selection of Product, Service or Process

4.1.6 Determination of Activities and Methods of Test

1. Methods of test SHALL include one or more the following:
   - Black box testing
   - Automated testing where feasible
   - Manual testing with documented scripts
2. Methods of test SHALL reference a recommendation, standard, or specification published by a recognized body.
3. All conformity assessment requirements SHALL be verifiable via the appropriate method of test

4.2 Part 2: Object of Conformity Assessment Requirements

1. The relevant specifications or standards used for the method of test SHALL published by a recognized body. These MAY include one or several of the following:
   - JSON
   - JSON-LD
   - W3C VC Data Model
   - ISO 18013-5
2. A test plan that demonstrate conformance to the relevant specification or standard. The test plan should be sufficiently detailed to include specific test cases with specific inputs, outputs, execution conditions, testing procedures and expected results.

3. Use cases SHALL be provided to illustrate how the digital credential behaves in context. Thes MAY include one or several of the following:
    - Issue Credential
    - Present Credential.
    - Store Credential.
    - Verify Credential
    - Retrieve Credential
    - Revoke Credential
4. 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.
5. A digital credentials SHALL be tamper-evident.
6. The authorship of a digital credential SHALL be cryptographically verifiable.
7. A digital credential SHALL demonstrate that it can be stored within and presented from a minimum of two independent implementations.
8. A digital credential SHALL demonstrate that it can be cryptographically 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

4.3.3 Attestation

5 Object of Conformity Assessment Specification: Credential Format

5.1 Part 1: Object of Conformity Assessment Definition

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)

5.1.1 Related Definitions

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

5.1.2 Appropriate Use Cases

The use case SHOULD describe a HOLDER scenario or an ISSUER scenario.

5.1.3 Selection of Product, Service or Process

Examples of credential formats COULD be:

- LD Proofs with BBS+
- ISO mDL
- JWT
- JWT (hash and salt)
- JSON-JWT
- JSON-LD
- JSON-LD with LD Signatures
- JSON-LD ZKP with BBS+
- JWP
- X.509
- Verifiable PDF

5.1.4 Determination of Activities and Methods of Test

5.2 Part 2: Object of Conformity Assessment Requirements

5.3 Part 3: Determination of Outputs, Review and Attestation

5.3.1 Determination of Outputs

5.3.2 Review and Decision

5.3.3 Attestation

6 Object of Conformity Assessment Specification: Decentralized Identifier

6.1 Part 1: Object of Conformity Assessment Specifications

A DID is a simple text string consisting of three parts: 1) the *did* URI scheme identifier, 2) the identifier for the *DID method*, and 3) the DID method-specific identifier.

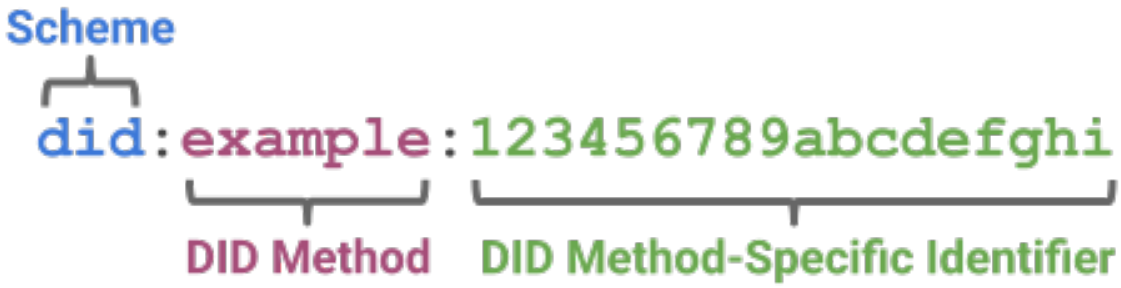

Image: W3C Decentralized Identifiers (DIDs) v1.0

6.1.1 Related Definitions

6.1.2 Appropriate Use Cases

6.1.3 Selection of Product, Service or Process

6.1.4 Determination of Activities and Methods of Test

6.2 Part 2: Object of Conformity Assessment Requirements

1. Decentralized Identifiers SHALL conform with W3C's recommendations for Decentralized Identifiers (DIDs) v1.0

6.3 Part 3: Determination of Outputs, Review and Attestation

6.3.1 Determination of Outputs

6.3.2 Review and Decision

6.3.3 Attestation

7 Object of Conformity Assessment Specification: Issuer

7.1 Part 1: Object of Conformity Assessment Definition

> **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

7.1.1 Related Definitions

Issuer Role is a role in which an entity asserts one or more claims about one or more Subjects, creates a credential from these claims, and assigns the credential to a Holder.

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

7.2 Appropriate Use Cases

7.2.0.1 Issue Credential

7.2.0.1.1 Actors

- Issuer
- Holder

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

7.2.0.1.3 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*.

7.2.0.1.4 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.)

7.2.0.1.5 Postconditions

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

7.2.0.2 Revoke Credential

7.2.0.2.1 Actors

- Issuer

7.2.0.2.2 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.

7.2.0.2.3 Preconditions

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

7.2.0.2.4 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*.

7.2.0.2.5 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.

7.2.1 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._

7.2.2 Determination of Activities and Methods of Test

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

7.3 Part 2: Object of Conformity Assessment 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*.

7.3.1 Additional Guidance

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

7.4 Part 3: Determination of Outputs, Review and Attestation

7.4.1 Determination of Outputs

7.4.2 Review and Decision

7.4.3 Attestation

8 Object of Conformity Assessment Specification: Holder

8.1 Part 1: Object of Conformity Assessment Specifications

Holder A process, service or component from which a Presentation can be expressed to a Verifier. A Holder is usually under the control of a User

8.1.1 Related Definitions

Holder Role A role in which 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.

8.1.2 Appropriate Use Cases

8.1.3 Selection of Product, Service or Process

8.1.4 Determination of Activities and Methods of Test

8.2 Part 2: Object of Conformity Assessment Requirements

1. The Holder Component SHALL detect indications of credential misuse or compromise of the identity information. *NOTE:* As an example, the expiry date having been exceeded or the detection of suspicious activity.
2. The Holder Component SHALL be able to request a credential from an issuer
    - The credential request SHALL allow the request to enable holder and subject binding where:
        - The Holder Component MAY be able to generate identifiers enabling proof of identifier control
            * Examples include pairwise decentralized identifiers, other decentralized identifiers, and other methods resulting in a URI identifier that can serve as subject in a Verifiable Credential or a holder in a Verifiable Presentation
    - The Holder Component MAY be able to generate proofs of identifier control
3. The Holder Component SHALL be able to request a credential in response to a holder action.
4. The Holder Component MAY be able to request a credential using a subscribe model in which verifiable credentials representing earned credentials from one or more issuers are requested/received/persisted so that the Holder component stays up-to-date with available credentials from those issuers.
5. The Holder Component SHALL be able to receive credentials.
6. The Holder Component SHALL be able to decline credentials.
7. The Holder Component SHALL be able to persist credentials with native format encoding from approved standards to ensure that it can fully produce the original record intact.
8. The Holder Component SHALL store credentials with sufficient metadata to allow execution of the minimal functions described in these requirements.
9. The Holder Component MAY be able to unpack the credential payload, but it is not required to do so.
10. The Holder Component MAY be able to request, listen for, or subscribe to credential updates, if offered, and if the holder chooses to enable.
    - The holder SHALL be able to decline a credential received via subscription.
11. The Holder Component SHALL be able to respond to a holder's request to remove a credential and stop persisting that credential.

12. The Holder Component SHALL assign control over an issued credential so as the Holder's control of the Credential MAY be subsequently verified.
13. The Holder Component SHALL have a mechanism to create and submit a Verifiable Presentation to a relying party in response to:
    - A Holder component owner action
    - A request for a Verifiable Presentation obtained by a verifier, if approved by the Holder component owner.
14. A Holder Component MAY have a mechanism for receiving and processing presentation requests.
15. A Holder Component MAY be able to generate identifiers enabling proof of identifier control.
    - Examples include pairwise decentralized identifiers, other decentralized identifiers, and other methods resulting in a URI identifier that can serve as subject in a Verifiable Credential or a holder in a Verifiable Presentation.
16. A Holder Component SHALL be able to manage connections (e.g. to issuers, requesting parties, and other parties)
17. A Holder component SHALL be able to manage privacy and sharing settings.
18. A Holder Component MAY be used in conjunction with digital credentials. If so, the following requirements SHALL be considered:
    - Ensuring adherence to applicable wallet security standards and specifications;
    - Enabling receipt and presentation of credentials according to applicable credential standards and specifications;
    - Enabling the user to control the sharing of credential data, in whole, in part, or as a derivation;
    - Notifying the user of any changes to credentials;
    - Ensuring consent of the user prior to any transaction; and
    - Ensuring adherence to applicable accessibility requirements.
19. The Holder Component SHALL preserve digital credentials in accordance with the general characteristics specified in the Digital Credential subsection of this Specification.

8.3 Part 3: Determination of Outputs, Review and Attestation

8.3.1 Determination of Outputs

8.3.2 Review and Decision

8.3.3 Attestation

9 Object of Conformity Assessment Specification: Verifier

9.1 Part 1: Object of Conformity Assessment Specifications

Verifier A process, service or component that verifies the presentation of a credential to yield an ACCEPT or REJECT decision.

9.1.1 Related Definitions

Verifier Role A role in which an entity accepts a Presentation (Proof) from a prover (usually a Holder) for the purposes of delivering services, administering programs or yielding an ACCEPT or REJECT decision.

9.1.2 Appropriate Use Cases

9.1.3 Selection of Product, Service or Process

9.1.4 Determination of Activities and Methods of Test

9.2 Part 2: Object of Conformity Assessment Requirements

1. The Verifier Component shall use acceptable methods to ensure that a credential is not tampered with, corrupted, or modified. NOTE: Examples of acceptable methods are cryptographic methods or examination by a trained examiner.
2. The Verifier Component shall not use a credential that is suspended or revoked to permit access to a good or service.
3. The Verifier Component shall detect whether the Holder has demonstrated control over a credential by means of one or more authenticators.
4. The Verifier Component shall inform the Holder when the Holder has demonstrated control over a credential by means of one or more authenticators.
5. The Verifier Component shall indicate an authentication failure when a credential is suspended or revoked, or when credential misuse or compromise is detected.
6. The Verifier Component shall preserve digital credentials in accordance with the general characteristics specified in the Digital Credential subsection of this Specification.

9.3 Part 3: Determination of Outputs, Review and Attestation

9.3.1 Determination of Outputs

9.3.2 Review and Decision

9.3.3 Attestation

10 Object of Conformity Assessment Specification: Storage

10.1 Part 1: Object of Conformity Assessment Specifications

Storage A foundational layer for secure data storage, including personal data, including data models for storage and transport, syntax, data at rest protection, CRUD API, access control, synchronization, and a minimum viable HTTP-based interface compatible with W3C DIDs/VCs.

10.1.1 Related Definitions

10.1.2 Appropriate Use Cases

10.1.3 Selection of Product, Service or Process

10.1.4 Determination of Activities and Methods of Test

10.2 Part 2: Object of Conformity Assessment Requirements

1. All Storage SHALL use required cryptographic modules as outlined in Cryptographic Module to secure personal information
2. In a cloud computing environment, Storage SHALL implement ISO/IEC 27018 measures to protect personally identifiable information (PII) and personal information (PI) in accordance with ISO/IEC 29100

10.3 Part 3: Determination of Outputs, Review and Attestation

10.3.1 Determination of Outputs

10.3.2 Review and Decision

10.3.3 Attestation

11 Object of Conformity Assessment Specification: Cryptographic Module

11.1 Part 1: Object of Conformity Assessment Specifications

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.

11.1.1 Related Definitions

11.1.2 Appropriate Use Cases

11.1.3 Selection of Product, Service or Process

11.1.4 Determination of Activities and Methods of Test

11.2 Part 2: Object of Conformity Assessment Requirements

1. All cryptographic algorithms and parameters SHALL conform with ITSP.40.111 - Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information
2. All data (both at rest and/or in transit) SHALL be treated at PROTECTED B
3. Passphrases and passwords SHOULD follow recommended best practices ITSAP.30.032 - Best practices for passphrases and passwords
4. Sanitization of all data SHALL be done using the following recognized methods:

- Crypto erase (CE): This method securely deletes the encryption key used to encrypt data on the media. The encrypted data remains on the media, and SHALL be erased using the Overwrite and Secure Erase method.
- Overwrite and secure erase (SE): This method uses software to write multiple passes (3 or more series) of random binary code (zeros and ones) on the storage media to prevent anyone from reading the previous data.

11.3 Part 3: Determination of Outputs, Review and Attestation

11.3.1 Determination of Outputs

11.3.2 Review and Decision

11.3.3 Attestation

12 References

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

12.1 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

12.2 Digital Credential Ecosystems

- Digital Credentials Consortium
- Grongingen Declaration Network
- European Self Sovereign Identity Framework
- eSSIF-Lab 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

12.3 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
- World Bank National Digital Identity and Government Data Sharing in Singapore

12.4 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
- DIF Wallet and Credential Interactions
- FIDO Alliance Specifications
- Hyperledger AnonCreds Proposal
- Hyperledger AnonCreds Specification
- 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 Connect Specifications
- 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

12.5 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
- TBD Verifiable Credential Selector

12.6 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
- Digital Credentials Consortium: Credentials to Employment: The Last Mile
- RWOT Enterprise Stakeholder Map
- RWOT Credential Profile Matrix
- T3 Innovation Network: APPLYING SELF-SOVEREIGN IDENTITY PRINCIPLES TO INTEROPERABLE LEARNING RECORDS
- VC <> mDL Project Stakeholder Interviews
- VC <> mDL Summary Report
- IDUnion Concepts for Wallet Security in SSI

12.7 Working Groups

- ISO/IEC JTC 1/SC 17 Cards and Security Devices
- W3C Verifiable Credentials Working Group
- OpenID Connect Working Group

12.8 Academic Research and Papers

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

12.9 Libraries

Implementation libraries

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

12.10 Vendor Solutions, Products and Services

Currently in the market

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

–end–