International Standard

ISO/IEC 26451

Information technology — Eclipse decentralized claims protocol

First edition
2026-11

Reference number
ISO/IEC 26451:2026(en)

© ISO/IEC 2026

Eclipse Decentralized Claims Protocol - v1.0

This document is licensed under The Apache License, Version 2.0.
Copyright © 2025 The Eclipse Foundation AISBL

Abstract

Dataspaces require the ability to communicate participant identities and credentials to secure data access. This specification defines a set of protocols for asserting participant identities, issuing verifiable credentials, and presenting verifiable credentials using a decentralized architecture for verification and trust.

Table of Contents

1. Abstract
2. 1. Terminology
    a. 1.1 Claim
    b. 1.2 DID
    c. 1.3 Holder
    d. 1.4 Issuer
    e. 1.5 Resource
    f. 1.6 Subject
    g. 1.7 Verifiable Credential
    h. 1.8 Verifiable Presentation
    i. 1.9 Verifiable Data Registry
    j. 1.10 Verifier
3. 2. Dataspace Ecosystem Overview
    a. 2.1 Interrelation to the Dataspace Protocol
    b. 2.2 Systems
        i. 2.2.1 Dataspace Governance Authority Systems
        ii. 2.2.2 Participant Agent Systems
        iii. 2.2.3 Credential Issuer Systems
4. 3. Trust Model and Information Flow Architecture
    a. 3.1 Consent
    b. 3.2 Trust Relationships
    c. 3.3 Transport Security
5. 4. Base Concepts

    a. 4.1 Decentralization
    b. 4.2 Identities
    c. 4.3 Self-Issued ID Tokens
        i. 4.3.1 Verifiable Presentation Access Token
        ii. 4.3.2 Obtaining Self-Issued ID Tokens
        iii. 4.3.3 Validating Self-Issued ID Tokens
    d. 4.4 Schemas, Contexts, and Message Processing
        i. 4.4.1 The Decentralized Claims Protocol Context
    e. 4.5 The Base URL
6. 5. Verifiable Presentation Protocol
    a. 5.1 Presentation Flow
    b. 5.2 Credential Service Endpoint Discovery
    c. 5.3 Credential Service Security
        i. 5.3.1 Submitting an Access Token
    d. 5.4 Resolution API
        i. 5.4.1 Presentation Query Message
        ii. 5.4.2 Presentation Response Message
        iii. 5.4.3 Presentation Validation
7. 6. Credential Issuance Protocol
    a. 6.1 Issuance Flow
    b. 6.2 Issuer Service Endpoint Discovery
    c. 6.3 Issuer Service Base URL
    d. 6.4 Credential Request API
        i. 6.4.1 Credential Request Message
    e. 6.5 Storage API
        i. 6.5.1 Credential Message
        ii. 6.5.2 Credential Container
    f. 6.6 Credential Offer API
        i. 6.6.1 Credential Offer Message
        ii. 6.6.2 CredentialObject
    g. 6.7 Issuer Metadata API
        i. 6.7.1 IssuerMetadata
    h. 6.8 Credential Request Status API
        i. 6.8.1 CredentialStatus

© ISO/IEC 2026 – All rights reserved

    i. 6.9 Key Rotation and Revocation
        i. 6.9.1 Key rotation
        ii. 6.9.2 Key revocation
    j. 6.10 Verifiable Credential Revocation
8. 7. Conformance
9. A. Profiles of the Decentralized Claims Protocol
    a. A.1 DCP Profile Definitions
        i. A.1.1 Homogeneity requirement
    b. A.2 Profile Authoring Recommendations
10. B. Notes
    a. B.1 List of Figures
11. C. References
    a. C.1 Normative references
    b. C.2 Informative references

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Eclipse Foundation AISBL (as Eclipse Decentralized claims Protocol v1.0) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Information technology — Eclipse decentralized claims protocol

1. Terminology

The following terms are used to describe concepts in this specification.

1.1 Claim

An assertion made about a Subject (1.6).

1.2 DID

A decentralized identifier as defined by Decentralized Identifiers (DIDs) v1.0.

1.3 Holder

An entity that possesses a set of identity resources as defined by the VC DataModel version of the selected profile (A). The holder will typically be the subject of a Verifiable Credential (1.7).

1.4 Issuer

An entity that asserts claims (1.1) about one or more subjects by issuing a Verifiable Credential (1.7) to a Holder (1.3).

1.5 Resource

A resource is an entity managed by the Credential Service such as a Verifiable Credential (1.7) or Verifiable Presentation (1.8).

1.6 Subject

The target of a set of claims contained in a Verifiable Credential (1.7) as defined by the VC DataModel version of the selected profile (A). In a dataspace, a subject will be a participant.

1.7 Verifiable Credential

A tamper-evident credential whose authorship can be cryptographically verified as defined by the VC DataModel version of the selected profile (A).

1.8 Verifiable Presentation

A tamper-evident presentation of information whose authorship can be cryptographically verified as defined by VC DataModel version of the selected profile (A).

1.9 Verifiable Data Registry

Maintains identifiers such as DIDs (1.2) and Verifiable Credential (1.7) schemas in a dataspace.

© ISO/IEC 2026 – All rights reserved

1.10 Verifier

An entity that receives a Verifiable Credential (1.7), optionally presented inside a Verifiable Presentation (1.8) as defined by the VC DataModel version of the selected profile (A).

2. Dataspace Ecosystem Overview

This section describes the core actors and systems in a dataspace ecosystem that are pertinent to this specification. It adheres to the model defined by the Dataspace Protocol [dsp-base]:

- A Dataspace is a policy-based data sharing context between two or more entities.
- The Dataspace Governance Authority is responsible for operational management of a dataspace (2), including participant (2) registration and designation of trust credential issuers.
- A Participant is a member of the dataspace (2). Members MAY take on different roles, which are attested to by verifiable credentials.
- A Participant Agent performs tasks such as publishing a catalog or engaging in data transfer. Note that a participant agent is a logical construct and does not necessarily correspond to a single runtime process.
- An Identity Provider is a service that generates identity tokens used to verify the identity of a Participant Agent (2). Each participant (2) will use their own identity provider to generate a self-signed identity token.
- A Credential Issuer issues Verifiable Credentials (1.7) used by participant agents (2) to allow access to assets and verify usage control.

2.1 Interrelation to the Dataspace Protocol

The Dataspace Protocol (DSP) [dsp-base] is designed as a layered protocol, which is independent of the identity and trust system used. The Decentralized Claims Protocol fills this gap by providing such an orthogonal overlay for identity and trust in a decentralized manner.

2.2 Systems

2.2.1 Dataspace Governance Authority Systems

Registration System

The registration system is responsible for participant (2) registration, onboarding, and management in a dataspace. The registration system is run by the Dataspace Governance Authority (2) and is outside the scope of this specification.

2.2.2 Participant Agent Systems

Participants (2) will run one or more agent systems that interact in the dataspace. These systems MAY offer data catalogs, perform data transfers, or provide application functionality. A participant (2) MAY run the following identity-related agents. Note that this is a logical description and MAY not represent an actual deployment topology.

© ISO/IEC 2026 – All rights reserved

Security Token Service (STS).

The STS creates self-issued authorization tokens that contain identity claims used by participant agents (2) under the control of the same participant (2).

Credential Service (CS)

The CS manages Verifiable Credentials (1.7). This includes read and write endpoints for Verifiable Presentations (1.8) and Verifiable Credentials (1.7).

DID Service (DIDS).

The DIDS creates, signs, and publishes DID documents.

2.2.3 Credential Issuer Systems

Issuer Service (IS)

The Issuer Service is run by a trust anchor and manages the lifecycle of Verifiable Credentials (1.7) in a dataspace. A dataspace MAY contain multiple Issuer Services run by different trust anchors. The Issuer Service:

- Issues Verifiable Credentials (1.7) for dataspace participants (2).
- Manages revocation lists for Verifiable Credentials (1.7) types it issues based on Verifiable Credentials Status List v2021.
- Provides cryptographic material used to verify Verifiable Presentations (1.8) and Verifiable Credentials (1.7).

3. Trust Model and Information Flow Architecture

This specification is based on the Issuer-Holder-Verifier model as described in the VC DataModel version of the selected profile (A):

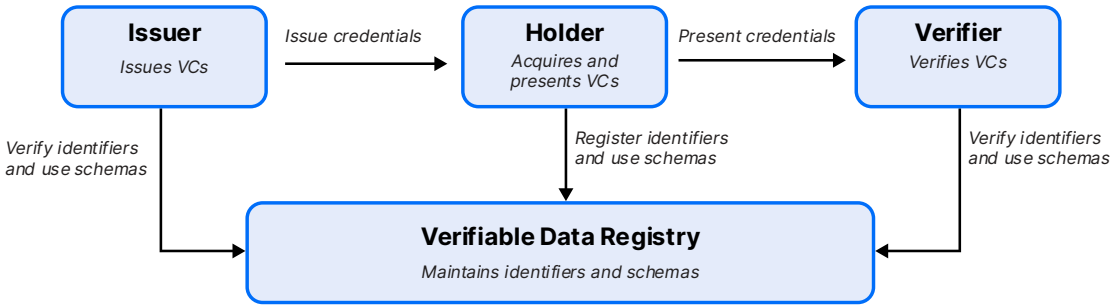


Figure 1 The Issuer-Holder-Verifier Model

In this model, the Issuer (1.4) creates a Verifiable Credential (1.7) and provides it to the Holder (1.3), which can then present the Verifiable Credential (1.7) to the Verifier (1.10).

The Verifier (1.10) decides which Verifiable Credentials (1.7) it will accept and the Holder (1.3) decides which Verifiable Credentials (1.7) it will present. All parties rely on a Verifiable Data Registry (1.9) to obtain identifier information and metadata about Verifiable Credentials (1.7), such as schemas. Furthermore, parties communicate with each other using the protocols defined in the Dataspace Protocol specification [dsp-base] and this specification.

© ISO/IEC 2026 – All rights reserved

The Issuer-Holder-Verifier model is mapped to the following architecture in this specification:

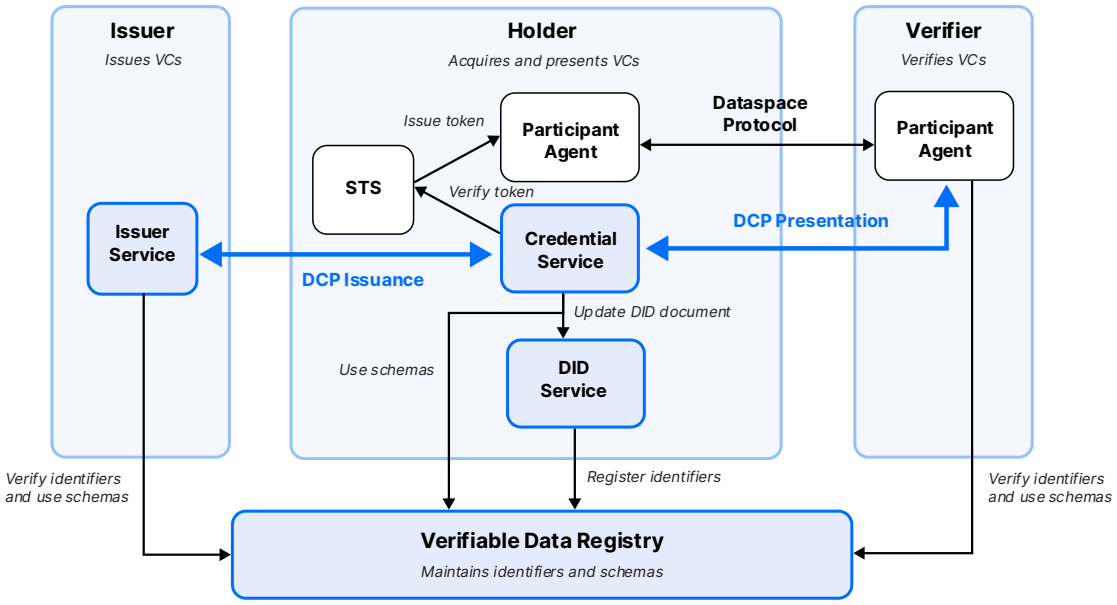


Figure 2 Information Flow Architecture

- Identity and claims information is exchanged between a Holder (1.3) and a Verifier (1.10) in the context of Dataspace Protocol message interactions [dsp-base]. These messages will contain metadata such as Offers and Agreements that determine the Verifiable Credentials (1.7) a Holder (1.3) MUST present to a Verifier (1.10).
- The Issuer Service (2.2.3) issues credentials to a Holder (1.3)'s Credential Service (2.2.2) using the protocol defined in Section 6. Credential Issuance Protocol. As part of this process, the Issuer Service (2.2.3) will verify the Holder (1.3)'s identifier using the Verifiable Data Registry (1.9). Since DID (1.2)s are mandatory in this specification, the registry will be used to resolve the Holder (1.3)'s DID document and cryptographic material.
- The Holder (1.3) runs three logical services: a Participant Agent (2), an STS (2.2.2), and a Credential Service (2.2.2). The Participant Agent (2) engages in dataspace communications with the Verifier (1.10) agent [dsp-base]. As part of these interactions, the Participant Agent (2) will include a Self-Issued ID Token as defined in Section 4.3 Self-Issued ID Tokens. This token will be obtained from the STS (2.2.2) controlled by the Holder (1.3). Note that the STS (2.2.2) is an internal system and therefore out of scope for the current specification. It MAY be a standalone service or part of the Participant Agent (2) or Credential Service (2.2.2). The Self-Issued ID Token will contain an access token bound to the Verifier (1.10) that will be used to request a Verifiable Presentation (1.8). The Holder (1.3)'s Credential Service (2.2.2) will verify the access token with the STS (2.2.2).
- The Verifier (1.10) runs a Participant Agent (2) that engages in dataspace message exchanges with the Holder (1.3) agent [dsp-base]. When it receives a request, it will resolve the Holder (1.3)'s DID document from the Verifiable Data Registry (1.9). The Participant Agent (2) will resolve the Credential Service (2.2.2) endpoint from the DID document. The Participant Agent (2) will send a request for a Verifiable Presentation (1.8) to the Credential Service (2.2.2) using the protocol defined in Section 5. Verifiable Presentation Protocol. This request will include the access token as a claim in the Self-Issued ID Token received from the Holder (1.3)'s agent. The Participant Agent (2) will then match the credentials returned in

© ISO/IEC 2026 – All rights reserved

the Verifiable Presentation (1.8) against the policy constraints associated with the original dataspace request.