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



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved.

This ISO publication is protected by copyright and is owned by ISO and/or its licensors.

The content of this ISO publication is provided under licence, not sold. Use is subject to the applicable licence terms issued by ISO, an ISO member body, or an authorized third-party distributor.

Except as required for implementation or expressly permitted by a separate licence, no part of this ISO publication may be reproduced, distributed, modified, used, or made available in any form or by any means – electronic or mechanical, including photocopying, scanning, recording, or posting on internal or external digital platforms.

Any use beyond the scope of the granted rights is prohibited and may result in legal action.

ISO copyright office
CP 401 • CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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