International Standard

ISO/IEC 25831-2

Information technology — OpenID identity assurance 1.0 —

Part 2: Schema definition

First edition
2026-05

Reference number
ISO/IEC 25831-2:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

OpenID Identity Assurance Schema Definition 1.0 **4**

Foreword 4

Introduction 5

1. Scope 5

2. Normative references 5

3. Terms and definitions 5

4. Requirements 6

5. Verified claims 7

5.1. General 7

5.2. Base elements 8

5.3. Claims element 8

5.4. Verification element 9

5.5. Examples 17

6. Security considerations 22

7. Bibliography 22

8. IANA considerations 22

8.1. JSON Web Token claims registration 22

Annex A. Copyright notice & license 23

© ISO/IEC 2026 – All rights reserved

OpenID Identity Assurance Schema Definition 1.0

Foreword

ISO (the International Organization for Standarization) 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 their 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

© ISO/IEC 2026 – All rights reserved

the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/sio/foreward.html. In the IEC, see www.iec.ch/understand-standards.

This document was prepared by the OpenID Foundation (OIDF) (as Identity Assurance 1.0) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical CommitteeISO/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.

Introduction

This specification defines a schema for describing assured identity claims and a range of associated identity assurance metadata. Much of this definition will be optional as it depends on which processes were run, and the operational requirements for data-minimization, which elements of the JSON schema described in this document will be needed for a specific transaction.

1. Scope

This specification defines the schema of JSON objects used to describe identity assurance relating to a natural person. It consists of the definition of a new claim called `verified_claims` that will be registered with the IANA "JSON Web Token Claims Registry" established by [RFC 7519]. As part of the definition of the `verified_claims` claim there is also an element defined called `verification` that provides a flexible container for identity assurance metadata. It is anticipated that the `verification` element may be used by other spec authors and implementers where the verification metadata is needed independently of the end-user verified claims.

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applied. For undated references, the latest edition of the referenced document (including any amendments) applies.

© ISO/IEC 2026 – All rights reserved

- **OpenID** OpenID Connect Core 1.0 incorporating errata set 1
- **RFC 7519** JSON Web Token (JWT)

3. Terms and definitions

For the purposes of this document, the following terms and definitions apply:

- Claim – piece of information asserted about an entity
- Claims provider – server that can return claims and verified claims about an entity

Note 1 to entry : A claim provider could be an OpenID Connect provider, a verifiable claim issuer or other application component that provides verified claims.

- Claims recipient – application that receives claims from the claim provider
- Identity proofing – process in which an end-user provides evidence to a provider reliably identifying themselves, thereby allowing the provider to assert that identification at a useful assurance level
- Identity verification – process conducted by the provider to verify the end-user's identity
- Identity assurance – process in which the provider asserts identity data of a certain end-user with a certain assurance towards another consuming entity (such as a relying party or verifier as described in [W3C_VCDM]), typically expressed by way of an assurance level

Note 1 to entry: Depending on legal requirements, the provider can be required to provide evidence of the identity verification process to the consuming entity.

- Verified claims – claims about an end-user, typically a natural person, whose binding to a particular end-user account was verified in the course of an identity verification process

4. Requirements

The RP will be able to request the minimal data set it needs (data minimization) and to express requirements regarding this data, the evidence and the identity verification processes employed by the OP.

© ISO/IEC 2026 – All rights reserved