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)

COPYRIGHT PROTECTED DOCUMENT

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

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

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.

- **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.

This extension will be usable by OPs operating under a certain regulation related to identity assurance, such as eIDAS, as well as other OPs operating without such a regulation.

It is assumed that OPs operating under a suitable regulation can assure identity data without the need to provide further evidence since they are approved to operate according to well-defined rules with clearly defined liability. For example in the case of eIDAS, the peer review ensures eIDAS compliance and the respective member state assumes the liability for the identities asserted by its notified eID system.

Every other OP not operating under such well-defined conditions could receive a request to provide the RP data about the identity verification process along with identity evidence to allow the RP to conduct their own risk assessment and to map the data obtained from the OP to other laws. For example, if an OP verifies and maintains identity data in accordance with an anti-money laundering law, an RP might choose to use the identity attributes in a different regulatory context, such as eHealth or the previously mentioned eIDAS.

The concept of this document is that the OP can provide identity data along with metadata about the identity assurance process. It is the responsibility of the RP to assess this data and map it into its own legal context.

From a technical perspective, this means this document allows the OP to provide verified claims along with information about the respective trust framework, but also supports the externalization of information about the identity verification process.

The representation defined in this document can be used to provide RPs with verified claims about the end-user via any appropriate channel. In the context of OpenID Connect, verified claims can be provided in ID Tokens or as part of the UserInfo response. It is also possible to utilize the format described here in OAuth access tokens or token introspection responses to provide resource servers with verified claims.

This extension is intended to be truly international and support identity assurance across different jurisdictions. The extension is therefore extensible to support various trust frameworks, identity evidence and assurance processes.

In order to give implementers as much flexibility as possible, this extension can be used in conjunction with existing OpenID Connect claims and other extensions within the same OpenID Connect assertion (e.g., ID Token or UserInfo response) utilized to convey claims about end-users.

For example, OpenID Connect [OpenID] defines claims for representing family name and given name of an end-user without a verification status. These claims can be used in the same OpenID Connect assertion beside verified claims represented according to this extension.

In the same way, existing claims to inform the RP of the verification status of the phone_number and email claims can be used together with this extension.

Even for representing verified claims, this extension utilizes existing OpenID Connect claims if possible and reasonable. The extension will, however, ensure RPs cannot (accidentally) interpret unverified claims as verified claims.

In order to fulfill the requirements of some jurisdictions on identity assurance, the OpenID Connect for IDA claims [OpenID4IDAClaims] specification defines a number of claims for conveying end-user data in addition to the claims defined in the OpenID Connect specification [OpenID].

5. Verified claims

5.1. General

This specification defines a generic mechanism to add verified claims to JSON-based assertions. It uses a container element, called `verified_claims`, to provide the claim recipient with a set of claims along with the respective metadata and verification evidence related to the verification of these claims. This way, claim recipients cannot mix up verified claims and unverified claims and accidentally process unverified claims as verified claims.

The following example would assert to the claim recipient that the claim provider has verified the claims provided (`given_name` and `family_name`) according to an example trust framework `trust_framework_example`:


```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "trust_framework_example"
    },
    "claims": {
      "given_name": "Max",
      "family_name": "Meier"
    }
  }
}
```

This document requires that RPs use the schema defined in [IDA-verified-claims]. There are places in the JSON structure where that schema can be extended by implementers but deviation from the schema as defined would not be correct use of this document.

5.2. Base elements

`verified_claims`: A single object or an array of objects, each object comprising the following sub-elements:

- `claims`: Required. Object that is the container for the verified claims about the end-user.
- `verification`: Required. Object that contains data about the verification process.

Note: Implementations shall ignore any sub-element not defined in this specification or extensions of this specification. Extensions to this specification that specify additional sub-elements under the `verified_claims` element may be created by the OpenID Foundation, ecosystem or scheme operators or indeed singular implementers using this specification.

A machine-readable syntax definition of `verified_claims` is given as JSON schema in [verified_claims.json], it can be used to automatically validate JSON documents containing a `verified_claims` element. The provided JSON schema files are a non-normative implementation of this specification and any discrepancies that exist are either implementation bugs or interpretations.

Extensions of this specification, including trust framework definitions, can define further constraints on the data structure.

5.3. Claims element

The `claims` element contains the claims about the end-user which were verified by the process and according to the policies determined by the corresponding `verification` element described in the next section.

The `claims` element may contain any of the following claims as defined in section 5.1 of the OpenID Connect specification [OpenID]

- `name`
- `given_name`
- `middle_name`
- `family_name`
- `birthdate`