International Standard

ISO/IEC 25831-1

Information technology — OpenID identity assurance 1.0 —

Part 1: General

First edition
2026-05

Reference number
ISO/IEC 25831-1:2026(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 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 extension to OpenID Connect standardizes how relying parties request and receive identity information with additional assurance metadata. This document is aimed at enabling use cases requiring strong assurance, for example, to comply with regulatory requirements such as anti-money laundering laws or access to health data, risk mitigation, or fraud prevention.

In such use cases, the relying party (RP) needs to understand the trustworthiness or assurance level of the claims about the end-user that the OpenID provider (OP) is willing to communicate, along with process-related information and evidence used to verify the end-user claims.

The `acr` claim, as defined in section 2 of the OpenID Connect specification [OpenID], is suited to assure information about the authentication performed in an OpenID Connect transaction. Identity assurance, however, requires a different representation. While authentication is an aspect of an OpenID Connect transaction, assurance and associated verification and validation details, are properties of a certain claim or a group of claims. Several of them will typically be conveyed to the RP as the result of an OpenID Connect transaction.

For example, the assurance an OP typically will be able to give for an e-mail address will be "self-asserted" or "verified". The family name of an end-user, in contrast, might have been verified in accordance with the respective anti-money laundering law by showing an ID card to a trained employee of the OP operator.

Identity assurance requires a way to convey assurance data along with and coupled to the respective claims about the end-user. This document defines a suitable representation and mechanisms the RP will utilize to request verified claims about an end-user along with

assurance data and for the OP to represent these verified claims and accompanying assurance data.

1. Scope

This document is a definition of the technical mechanism to allow a relying party to request one or more verified claims about the end-user and to enable an OpenID provider to provide a relying party with a verified claim ("the tools").

Additional facets needed to deploy a complete solution for identity assurance, such as legal aspects (including liability), trust frameworks, or commercial agreements are out of scope. It is up to the particular deployment to complement the technical solution based on this document with the respective definitions ("the rules").

Note: Although such aspects are out of scope, the aim of the specification is to enable implementations of the technical mechanism to be flexible enough to fulfill different legal and commercial requirements in jurisdictions around the world. Consequently, such requirements will be discussed in this document as examples.

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.

- **OIDC** OpenID Connect Core 1.0 incorporating errata set 1
- **RFC 7519** JSON Web Token (JWT)
- **OIDC4IDA** OpenID Identity Assurance 1.0 predefined identifier values

3. Terms and definitions

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

3.1. claim

Piece of information asserted about an entity.

3.2. identity proofing

Process in which an end-user provides evidence to an OpenID Connect provider (OP) or claim provider reliably identifying themselves, thereby allowing the OP or claim provider to assert that identification at a useful assurance level.

3.3. identity verification

Application that receives claims from the claim provider.

3.4. identity assurance

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.

3.5. verified claim

Process conducted by the provider to verify the end-user's identity.

3.6. claim provider

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.

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. Verified claims schema

The basic idea is to use a container element, called `verified_claims`, to provide the RP with a set of claims along with the respective metadata and verification evidence related to the verification of these claims. This way, it is explicit which claims are verified, reducing the risk of RPs accidentally processing unverified claims as verified claims.

This document uses the [IDA-verified-claims] document as the definition of the schema for representation of assured digital identity attributes and identity assurance metadata.

The following example would assert to the RP that the OP 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. Verified claims delivery

A `verified_claims` element can be added to an OpenID Connect UserInfo response and/or an ID Token.

Here is an example of the payload of an ID token including verified claims:

```
{
  "iss": "https://server.example.com",
  "sub": "248289761",
  "aud": "https://rs.example.com/",
  "exp": 1544645174,
  "client_id": "s6BhdRkqt3_",
  "verified_claims": {
    "verification": {
      "trust_framework": "example"
    },
    "claims": {
      "given_name": "Max",
      "family_name": "Mustermann"
    }
  }
```

```
}
```

An OP or Authorization Server (AS) can also include aggregated or distributed `verified_claims` in the above assertions (see Section 6 for more details).

5.3. Requesting end-user claims

Verified claims can be requested on the level of individual claims about the end-user by utilizing the `claims` parameter as defined in section 5.5 of the OpenID Connect specification [OpenID].

Note: A machine-readable definition of the syntax to be used to request `verified_claims` is given as JSON schema in [verified_claims_request.json], which can be used to automatically validate `claims` request parameters. The provided JSON schema files are a non-normative implementation of this document and any discrepancies that exist are either implementation bugs or interpretations.

To request verified claims, the `verified_claims` element is added to the `userinfo` or the `id_token` element of the `claims` parameter.

Since `verified_claims` contains the effective claims about the end-user in a nested `claims` element, the syntax is extended to include expressions on nested elements as follows. The `verified_claims` element includes a `claims` element, which in turn includes the desired claims as keys. For each claim, the value is either `null` (default), or an object. The object may contain restrictions using `value` or `values` as defined in [OpenID] and/or the `essential` key as described below. An example is shown in the following:

```
{
  "userinfo": {
    "verified_claims": {
      "verification": {
        "trust_framework": null
      },
      "claims": {
        "given_name": null,
        "family_name": null,
```

```
        "birthdate": null
      }
    }
  }
}
```

Use of the `claims` parameter allows the RP to request specified claims about the end-user needed for its use case. This allows RPs to fulfill the requirements for data minimization by requesting only claims needed for its use case.

Note: it is not possible to request sub-claims (for example the `country` subclaim of the `address` claim) using mechanisms from OpenID Connect Core or this document.

RPs can use the `essential` field as defined in section 5.5.1 of the OpenID Connect specification [OpenID]. The following example shows this for the family and given names.


```
{
  "userinfo": {
    "verified_claims": {
      "verification": {
        "trust_framework": null
      },
      "claims": {
        "given_name": {
          "essential": true
        },
        "family_name": {
          "essential": true
        },
        "birthdate": null
```

```
      }
    }
  }
}
```

5.4. Requesting verification data

RPs request verification data in the same way they request claims about the end-user. When the claims request parameter is being used, the syntax is based on the rules given in Section 5.3 and extends them for navigation into the structure of the `verification` element.

Elements within `verification` are requested by adding the respective element as shown in the following example:

```
{
  "userinfo": {
    "verified_claims": {
      "verification": {
        "trust_framework": null,
        "time": null
      },
      "claims": {
        "given_name": null,
        "family_name": null,
        "birthdate": null
      }
    }
  }
}
```