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)

© 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 1.0 **4**

Foreword 4

Introduction 5

1. Scope 5

2. Normative references 6

3. Terms and definitions 6

3.1. claim 6

3.2. identity proofing 6

3.3. identity verification 6

3.4. identity assurance 6

3.5. verified claim 6

3.6. claim provider 6

4. Requirements 7

5. Verified claims 8

5.1. Verified claims schema 8

5.2. Verified claims delivery 9

5.3. Requesting end-user claims 9

5.4. Requesting verification data 10

5.5. Defining further constraints on verification data 13

5.6. Requesting claims sets with different verification requirements 15

5.7. Returning less data than requested 17

5.8. Requesting sets of claims by scope 19

6. Aggregated and distributed claims 19

© ISO/IEC 2026 – All rights reserved

6.1. Aggregated and distributed claims assertions 19

6.2. Aggregated and distributed claims validation 23

7. Requesting verified claims 24

8. OP metadata 25

9. Privacy considerations 26

10. Security Considerations 27

10.1. Security profile 27

10.2. End-user authentication 27

11. Implementation and interoperability 28

12. Predefined values 28

13. Bibliography 28

14. IANA considerations 28

14.1. Media type registration 28

15. Example requests 29

15.1. Verification of claims by a document 29

15.2. Verification of claims by trust_framework and evidence types 30

15.3. Verification of claims by trust_framework and check_method 31

15.4. Verification of claims by electronic_signature 32

16. Example responses 32

16.1. Document 32

16.2. Document and verifier details 35

17.3. Evidence with all assurance details 36

17.4. Notified eID system (eIDAS) 40

17.5. Electronic_record 40

© ISO/IEC 2026 – All rights reserved

17.6. Vouch 41

17.7. Multiple verified claims 42

17.8. Claims provided by the OP and external sources 43

17.9. Self-Issued OpenID provider and external claims 44

18. Example requests and responses 44

18.1. Verified claims in UserInfo response 44

18.2. Verified claims in ID Tokens 45

Annex A. Acknowledgements 47

Annex B. Copyright notice & license 48

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved

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

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved