International Standard

ISO/IEC 26135

Information technology — OpenID connect — OpenID connect session management 1.0

First edition
2024-10

Reference number
ISO/IEC 26135:2024(en)

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

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 the OpenID Foundation (OIDF) (as OpenID Connect Session Management 1.0) 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 2024 – All rights reserved

Abstract

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

This document describes how to manage sessions for OpenID Connect, including when to log out the End-User.

© ISO/IEC 2024 – All rights reserved

Table of Contents

1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
2. Creating and Updating Sessions
3. Session Status Change Notification
   3.1. RP iframe
   3.2. OP iframe
   3.3. OpenID Provider Discovery Metadata
4. Validation
5. Implementation Considerations
   5.1. User Agents Blocking Access to Third-Party Content
6. Security Considerations
7. IANA Considerations
   7.1. OAuth Parameters Registry
      7.1.1. Registry Contents
   7.2. OAuth Authorization Server Metadata Registry
      7.2.1. Registry Contents
8. References
   8.1. Normative References
   8.2. Informative References

© ISO/IEC 2024 – All rights reserved

Information technology — OpenID Connect — OpenID Connect Session Management 1.0

1. Introduction

TOC

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 [RFC6749] protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

This specification complements the OpenID Connect Core 1.0 [OpenID.Core] specification by defining how to monitor the End-User's login status at the OpenID Provider on an ongoing basis so that the Relying Party can log out an End-User who has logged out of the OpenID Provider.

Both this specification and the OpenID Connect Front-Channel Logout 1.0 [OpenID.FrontChannel] specification use front-channel communication, which communicate logout requests from the OP to RPs via the User Agent. In contrast, the OpenID Connect Back-Channel Logout 1.0 [OpenID.BackChannel] specification uses direct back-channel communication between the OP and RPs being logged out. The OpenID Connect RP-Initiated Logout 1.0 [OpenID.RPInitiated] specification complements these specifications by defining a mechanism for a Relying Party to request that an OpenID Provider log out the End-User. This specification can be used separately from or in combination with these other three specifications.

1.1. Requirements Notation and Conventions

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

In the .txt version of this document, values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value. In the HTML version of this document, values to be taken literally are indicated by the use of `this fixed-width font`.

© ISO/IEC 2024 – All rights reserved

1.2. Terminology

TOC

This specification uses the terms "Authorization Endpoint", "Authorization Server", "Client", and "Client Identifier" defined by OAuth 2.0 [RFC6749], the term "User Agent" defined by RFC 7230 [RFC7230], and the terms defined by OpenID Connect Core 1.0 [OpenID.Core].

This specification also defines the following term:

Session

> Continuous period of time during which an End-User accesses a Relying Party relying on the Authentication of the End-User performed by the OpenID Provider.

IMPORTANT NOTE TO READERS: The terminology definitions in this section are a normative portion of this specification, imposing requirements upon implementations. All the capitalized words in the text of this specification, such as "Session", reference these defined terms. Whenever the reader encounters them, their definitions found in this section must be followed.

2. Creating and Updating Sessions

TOC

In OpenID Connect, the session at the RP typically starts when the RP validates the End-User's ID Token. Refer to the OpenID Connect Core 1.0 [OpenID.Core] specification to find out how to obtain an ID Token and validate it. When the OP supports session management, it MUST also return the Session State as an additional `session_state` parameter in the Authentication Response and SHOULD also return the Session State as an additional `session_state` parameter in the Authentication Error Response. The OpenID Connect Authentication Response is specified in Section 3.1.2.5 of OpenID Connect Core 1.0. The OpenID Connect Authentication Error Response is specified in Section 3.1.2.6 of OpenID Connect Core 1.0.

© ISO/IEC 2024 – All rights reserved