International Standard

ISO/IEC 26137

Information technology — OpenID connect — OpenID connect back-channel logout 1.0 incorporating errata set 1

First edition
2024-10

Reference number
ISO/IEC 26137:2024(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

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 Back-Channel Logout 1.0 incorporating errata set 1) 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.

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 specification defines a logout mechanism that uses direct back-channel communication between the OP and RPs being logged out; this differs from front-channel logout mechanisms, which communicate logout requests from the OP to RPs via the User Agent.

Table of Contents

Information technology — OpenID Connect — OpenID Connect Back-Channel Logout 1.0 incorporating errata set 1

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 defines a logout mechanism that uses direct back-channel communication between the OP and RPs being logged out; this differs from front-channel logout mechanisms, which communicate logout requests from the OP to RPs via the User Agent.

An upside of back-channel communication is that it can be more reliable than communication through the User Agent, since in the front-channel, the RP's browser session must be active for the communication to succeed. (If the RP's browser tab was subsequently used to navigate to an unrelated page, the RP session will be active unless the user uses the back button to return to it.) Both the OpenID Connect Session Management 1.0 [OpenID.Session] and OpenID Connect Front-Channel Logout 1.0 [OpenID.FrontChannel] specifications use front-channel communication, which communicate logout requests from the OP to RPs via the User Agent.

A downside of back-channel communication is that the session state maintained between the OP and RP over the front-channel, such as cookies and HTML5 local storage, are not available when using back-channel communication. As a result, all needed state must be explicitly communicated between the parties. Furthermore, RPs must implement an application-specific method of terminating RP sessions with the OP upon receiving back-channel logout requests; this can be more complicated than simply clearing cookies and HTML5 local storage state, which is often all that has to happen to implement logout in response to front-channel logout requests.

Another significant limitation of back-channel logout is that the RP's back-channel logout URI must be reachable from all the OPs used. This means, for instance, that the RP cannot be behind a firewall or NAT when used with public OPs.

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 OpenID Connect RP-Initiated Logout 1.0, OpenID Connect Session Management 1.0, and/or OpenID Connect Front-Channel Logout 1.0.

The previous version of this specification is:

- OpenID Connect Back-Channel Logout 1.0 (final) [OpenID.BackChannel.Final]

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 specification, 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 specification, values to be taken literally are indicated by the use of `this fixed-width font`.

1.2. Terminology

TOC

This specification uses the terms "Authorization Server", "Client", and "Client Identifier" defined by OAuth 2.0 [RFC6749], the term "User Agent" defined by RFC 7230 [RFC7230], the terms "Session" and "Session ID" defined by OpenID Connect Front-Channel Logout 1.0 [OpenID.FrontChannel] and the terms defined by OpenID Connect Core 1.0 [OpenID.Core] and JSON Web Token (JWT) [JWT].

This specification also defines the following term:

Logout Token

: JSON Web Token (JWT) [JWT] similar to an ID Token that contains Claims about the logout action being requested.

2. Back-Channel Logout

TOC

2.1. Indicating OP Support for Back-Channel Logout

TOC

If the OpenID Provider supports OpenID Connect Discovery 1.0 [OpenID.Discovery], it uses this metadata value to advertise its support for back-channel logout:

backchannel_logout_supported

> OPTIONAL. Boolean value specifying whether the OP supports back-channel logout, with `true` indicating support. If omitted, the default value is `false`.

It SHOULD also register this related metadata value:

backchannel_logout_session_supported

> OPTIONAL. Boolean value specifying whether the OP can pass a `sid` (session ID) Claim in the Logout Token to identify the RP session with the OP. If supported, the `sid` Claim is also included in ID Tokens issued by the OP. If omitted, the default value is `false`.

The `sid` (session ID) Claim used in ID Tokens and as a Logout Token parameter has the following definition (which is identical to the corresponding definition in OpenID Connect Front-Channel Logout 1.0 [OpenID.FrontChannel]):

sid

> OPTIONAL. Session ID - String identifier for a Session. This represents a Session of a User Agent or device for a logged-in End-User at an RP. Different `sid` values are used to identify distinct sessions at an OP. The `sid` value need only be unique in the context of a particular issuer. Its contents are opaque to the RP. Its syntax is the same as an OAuth 2.0 Client Identifier.

2.2. Indicating RP Support for Back-Channel Logout

TOC

Relying Parties supporting back-channel-based logout register a back-channel logout URI with the OP as part of their client registration.

The back-channel logout URI MUST be an absolute URI as defined by Section 4.3 of [RFC3986]. The back-channel logout URI MAY include an `application/x-www-form-urlencoded` formatted query component, per Section 3.4 of [RFC3986], which MUST be retained when adding additional query parameters. The back-channel logout URI MUST NOT include a fragment component.

If the RP supports OpenID Connect Dynamic Client Registration 1.0 [OpenID.Registration], it uses this metadata value to register the back-channel logout URI:

backchannel_logout_uri

> OPTIONAL. RP URL that will cause the RP to log itself out when sent a Logout Token by the OP. This URL SHOULD use the `https` scheme and MAY contain port, path, and query parameter components; however, it MAY use the `http` scheme, provided that the Client Type is `confidential`, as defined in Section 2.1 of OAuth 2.0 [RFC6749], and provided the OP allows the use of `http` RP URIs.

It SHOULD also register this related metadata value:

backchannel_logout_session_required

> OPTIONAL. Boolean value specifying whether the RP requires that a `sid` (session ID) Claim be included in the Logout Token to identify the RP session with the OP when the `backchannel_logout_uri` is used. If omitted, the default value is `false`.

2.3. Remembering Logged-In RPs

TOC

OPs supporting back-channel logout need to keep track of the set of logged-in RPs so that they know what RPs to contact at their back-channel logout URIs to cause them to log out. Some OPs track this state