International Standard

ISO/IEC 26134

Information technology — OpenID connect — OpenID connect RP-initiated logout 1.0

First edition
2024-10

Reference number
ISO/IEC 26134:2024(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 RP-Initiated Logout 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.

Abstract

TOC

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 mechanism for a Relying Party to request that an OpenID Provider log out the End-User.

Table of Contents

Information technology — OpenID Connect — OpenID Connect RP-Initiated Logout 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 enabling the Relying Party to request that an End-User be logged out by the OpenID Provider.

This specification can be used separately from or in combination with OpenID Connect Session Management 1.0 [OpenID.Session], OpenID Connect Front-Channel Logout 1.0 [OpenID.FrontChannel], and/or OpenID Connect Back-Channel Logout 1.0 [OpenID.BackChannel].

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`.

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].

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 "Relying Party", reference these defined terms. Whenever the reader encounters them, their definitions found in this section must be followed.

This specification also defines the following term:

Logout Endpoint

> The endpoint at the OpenID Provider that is the target of RP-Initiated Logout requests.

2. RP-Initiated Logout

TOC

An RP requests that the OP log out the End-User by redirecting the End-User's User Agent to the OP's Logout Endpoint. This URL is normally obtained via the `end_session_endpoint` element of the OP's Discovery response or may be learned via other mechanisms.

This specification defines the following parameters that are used in the logout request at the Logout Endpoint:

id_token_hint

> RECOMMENDED. ID Token previously issued by the OP to the RP passed to the Logout Endpoint as a hint about the End-User's current authenticated session with the Client. This is used as an indication of the identity of the End-User that the RP is requesting be logged out by the OP.

logout_hint

> OPTIONAL. Hint to the Authorization Server about the End-User that is logging out. The value and meaning of this parameter is left up to the OP's discretion. For instance, the

value might contain an email address, phone number, username, or session identifier pertaining to the RP's session with the OP for the End-User. (This parameter is intended to be analogous to the `login_hint` parameter defined in Section 3.1.2.1 of OpenID Connect Core 1.0 [OpenID.Core] that is used in Authentication Requests; whereas, `logout_hint` is used in RP-Initiated Logout Requests.)

client_id

OPTIONAL. OAuth 2.0 Client Identifier valid at the Authorization Server. When both `client_id` and `id_token_hint` are present, the OP MUST verify that the Client Identifier matches the one used when issuing the ID Token. The most common use case for this parameter is to specify the Client Identifier when `post_logout_redirect_uri` is used but `id_token_hint` is not. Another use is for symmetrically encrypted ID Tokens used as `id_token_hint` values that require the Client Identifier to be specified by other means, so that the ID Tokens can be decrypted by the OP.

post_logout_redirect_uri

OPTIONAL. URI to which the RP is requesting that the End-User's User Agent be redirected after a logout has been performed. This URI 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. The URI MAY use an alternate scheme, such as one that is intended to identify a callback into a native application. The value MUST have been previously registered with the OP, either using the `post_logout_redirect_uris` Registration parameter or via another mechanism. An `id_token_hint` is also RECOMMENDED when this parameter is included.

state

OPTIONAL. Opaque value used by the RP to maintain state between the logout request and the callback to the endpoint specified by the `post_logout_redirect_uri` parameter. If included in the logout request, the OP passes this value back to the RP using the `state` parameter when redirecting the User Agent back to the RP.

ui_locales

OPTIONAL. End-User's preferred languages and scripts for the user interface, represented as a space-separated list of BCP47 [RFC5646] language tag values, ordered by preference. For instance, the value "fr-CA fr en" represents a preference for French as spoken in Canada, then French (without a region designation), followed by English (without a region designation). An error SHOULD NOT result if some or all of the requested locales are not supported by the OpenID Provider.

OpenID Providers MUST support the use of the HTTP `GET` and `POST` methods defined in RFC 7231 [RFC7231] at the Logout Endpoint. RPs MAY use the HTTP `GET` or `POST` methods to send the logout request to the OP. If using the HTTP `GET` method, the request parameters are serialized using URI Query String Serialization. If using the HTTP `POST` method, the request parameters are serialized using Form Serialization.

When an `id_token_hint` parameter is present, the OP MUST validate that it was the issuer of the ID Token. The OP SHOULD accept ID Tokens when the RP identified by the ID Token's `aud` claim and/or `sid` claim has a current session or had a recent session at the OP, even when the `exp` time has passed. If the ID Token's `sid` claim does not correspond to the RP's current session or a recent session at the OP, the OP SHOULD treat the logout request as suspect, and MAY decline to act upon it.

At the Logout Endpoint, the OP SHOULD ask the End-User whether to log out of the OP as well. Furthermore, the OP MUST ask the End-User this question if an `id_token_hint` was not provided or if the supplied ID Token does not belong to the current OP session with the RP and/or currently logged in End-User. If the End-User says "yes", then the OP MUST log out the End-User.

As part of the OP logging out the End-User, the OP uses the logout mechanism(s) registered by the RPs to notify any RPs logged in as that End-User that they are to likewise log out the End-User. RPs can use any of OpenID Connect Session Management 1.0 [OpenID.Session], OpenID Connect Front-Channel Logout 1.0 [OpenID.FrontChannel], and/or OpenID Connect Back-Channel Logout 1.0 [OpenID.BackChannel] to receive logout notifications from the OP, depending upon which of these mechanisms the OP and RPs mutually support. The RP initiating the logout is to be included in these notifications before the post-logout redirection defined in Section 3 is performed.

It is up to the RP whether to locally log out the End-User before redirecting the User Agent to the OP's Logout Endpoint. On one hand, if the End-User approves the logout at the OP, the RP initiating the logout should receive a logout message from the OP and can perform a local logout at that time. On the other hand, some logout notification methods from the OP to the RP are unreliable and therefore the notification might not be received. Also, the End-User might not approve the OP logging out, in which case the RP would not receive a logout notification.

2.1. OpenID Provider Discovery Metadata

TOC

To support OpenID Connect RP-Initiated Logout, the RP needs to obtain the RP-Initiated Logout related OP metadata. This OP metadata is normally obtained via the OP's Discovery response, as described in OpenID Connect Discovery 1.0 [OpenID.Discovery], or MAY be learned via other mechanisms.

This OpenID Provider Metadata parameter MUST be included in the Server's discovery responses when RP-Initiated Logout and Discovery are supported:

end_session_endpoint

> REQUIRED. URL at the OP to which an RP can perform a redirect to request that the End-User be logged out at the OP. This URL MUST use the `https` scheme and MAY contain port, path, and query parameter components.

---

3. Redirection to RP After Logout

TOC

In some cases, the RP will request that the End-User's User Agent to be redirected back to the RP after a logout has been performed. Post-logout redirection is only done when the logout is RP-initiated, in which case the redirection target is the `post_logout_redirect_uri` parameter value sent by the initiating RP. An `id_token_hint` carring an ID Token for the RP is also RECOMMENDED when requesting post-logout redirection; if it is not supplied with `post_logout_redirect_uri`, the OP MUST NOT perform post-logout redirection unless the OP has other means of confirming the legitimacy of the post-logout redirection

target. The OP also MUST NOT perform post-logout redirection if the `post_logout_redirect_uri` value supplied does not exactly match one of the previously registered `post_logout_redirect_uris` values. The post-logout redirection is performed after the OP has finished notifying the RPs that logged in with the OP for that End-User that they are to log out the End-User.

This specification defines this Dynamic Registration parameter for this purpose, per Section 2.1 of OpenID Connect Dynamic Client Registration 1.0 [OpenID.Registration].

3.1. Client Registration Metadata

TOC

This Client Metadata parameter MAY be included in the Client's Registration information when RP-Initiated Logout and Dynamic Registration are supported:

post_logout_redirect_uris

OPTIONAL. Array of URLs supplied by the RP to which it MAY request that the End-User's User Agent be redirected using the `post_logout_redirect_uri` parameter after a logout has been performed. These URLs SHOULD use the `https` scheme and MAY contain port, path, and query parameter components; however, they 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.

---

4. Validation and Error Handling

TOC

If any of the validation procedures defined in this specification fail, any operations requiring the information that failed to correctly validate MUST be aborted and the information that failed to validate MUST NOT be used. Note that because RP-Initiated Logout Requests are intended to be idempotent, it is explicitly not an error for an RP to request that a logout be performed when the OP does not consider that the End-User is logged in with the OP at the requesting RP.

As described in Section 3, when the OP detects errors in the RP-Initiated Logout request, the OP MUST not perform post-logout redirection to an RP. Beyond that, the OP has discretion on what information to display to the End-User in the resulting page at the OP and what actions to enable the End-User to perform next. It MAY display an error message. It MAY ask the End-User whether to log out of the OP.

Note that giving the End-User the opportunity to log out may have security benefits, especially in kiosk scenarios. The End-User initiating a logout action at the RP may expect to be completely logged out, including from the OP. Not giving the End-User the opportunity to log out at the OP and leaving the End-User logged in would likely violate the End-User's security expectations about being completely logged out.

---

5. Implementation Considerations

TOC

This specification defines features used by both Relying Parties and OpenID Providers that choose to implement RP-Initiated Logout. All of these Relying Parties and OpenID Providers MUST implement the features that are listed in this specification as being "REQUIRED" or are described with a "MUST". No other implementation considerations for implementations of RP-Initiated Logout are defined by this specification.

---

6. Security Considerations

TOC

Logout requests without a valid `id_token_hint` value are a potential means of denial of service; therefore, OPs should obtain explicit confirmation from the End-User before acting upon them.

7. IANA Considerations

TOC

7.1. OAuth Authorization Server Metadata Registry

TOC

This specification registers the following metadata name in the IANA "OAuth Authorization Server Metadata" registry [IANA.OAuth.Parameters] established by [RFC8414].

7.1.1. Registry Contents

TOC

- Metadata Name: `end_session_endpoint`
- Metadata Description: URL at the OP to which an RP can perform a redirect to request that the End-User be logged out at the OP
- Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
- Specification Document(s): Section 2.1 of this document

7.2. OAuth Dynamic Client Registration Metadata Registration

TOC

This specification registers the following client metadata definition in the IANA "OAuth Dynamic Client Registration Metadata" registry [IANA.OAuth.Parameters] established by [RFC7591]:

7.2.1. Registry Contents

TOC

- Client Metadata Name: `post_logout_redirect_uris`

- Client Metadata Description: Array of URLs supplied by the RP to which it MAY request that the End-User's User Agent be redirected using the `post_logout_redirect_uri` parameter after a logout has been performed
- Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
- Specification Document(s): Section 3.1 of this document

---

8. References

TOC

8.1. Normative References

TOC

[IANA.OAuth.Parameters] IANA, "OAuth Parameters."

[OpenID.BackChannel] Jones, M. and J. Bradley, "OpenID Connect Back-Channel Logout 1.0," September 2022.

[OpenID.Core] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0," November 2014.

[OpenID.Discovery] Sakimura, N., Bradley, J., Jones, M., and E. Jay, "OpenID Connect Discovery 1.0," November 2014.

[OpenID.FrontChannel] Jones, M., "OpenID Connect Front-Channel Logout 1.0," September 2022.

[OpenID.Registration] Sakimura, N., Bradley, J., and M. Jones, "OpenID Connect Dynamic Client Registration 1.0," November 2014.

[OpenID.Session] de Medeiros, B., Agarwal, N., Sakimura, N., Bradley, J., and M. Jones, "OpenID Connect Session Management 1.0," September 2022.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

[RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages," BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework," RFC 6749, DOI 10.17487/RFC6749, October 2012.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing," RFC 7230, DOI 10.17487/RFC7230, June 2014.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content," RFC 7231, DOI 10.17487/RFC7231, June 2014.

8.2. Informative References

TOC

[RFC7591] Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, "OAuth 2.0 Dynamic Client Registration Protocol," RFC 7591, DOI 10.17487/RFC7591, July 2015.

[RFC8414] Jones, M., Sakimura, N., and J. Bradley, "OAuth 2.0 Authorization Server Metadata," RFC 8414, DOI 10.17487/RFC8414, June 2018.

ICS 35.030
Price based on 10 pages

iso.org