International Standard

ISO/IEC 26136

Information technology — OpenID connect — OpenID connect front-channel logout 1.0

First edition
2024-10

Reference number
ISO/IEC 26136:2024(en)

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 Front-Channel 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

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 front-channel communication via the User Agent between the OP and RPs being logged out that does not need an OpenID Provider iframe on Relying Party pages. Other protocols have used HTTP GETs to RP URLs that clear login state to achieve this. This specification does the same thing.

Table of Contents

Information technology — OpenID Connect — OpenID Connect Front-Channel 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 defines a logout mechanism that uses front-channel communication via the User Agent between the OP and RPs being logged out that does not need an OpenID Provider iframe on Relying Party pages, as OpenID Connect Session Management 1.0 [OpenID.Session] does. Other protocols have used HTTP GETs to RP URLs that clear login state to achieve this; this specification does the same thing.

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; this differs from front-channel logout mechanisms, which communicate logout requests from the OP to RPs via the User Agent. 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 Back-Channel Logout 1.0.

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", "Client Identifier", and "Redirection URI" 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 terms:

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.

Session ID

> Identifier for a Session.

---

2. Relying Party Logout Functionality

TOC

RPs supporting HTTP-based logout register a logout URI with the OP as part of their client registration. The domain, port, and scheme of this URL MUST be the same as that of a registered Redirection URI value.

The logout URI MUST be an absolute URI as defined by Section 4.3 of [RFC3986]. The 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 logout URI MUST NOT include a fragment component.

The OP renders `<iframe src="frontchannel_logout_uri">` in a page with the registered logout URI as the source to trigger the logout actions by the RP. Upon receiving a request to render the logout URI in an iframe, the RP clears state associated with the logged-in session, including any cookies and HTML5 local storage. If the End-User is already logged out at the RP when the logout request is received, the logout is considered to have succeeded.

The OP MAY add these query parameters when rendering the logout URI, and if either is included, both MUST be:

iss

Issuer Identifier for the OP issuing the front-channel logout request.

sid

Identifier for the Session.

The RP MAY verify that any `iss` and `sid` parameters match the `iss` and `sid` Claims in an ID Token issued for the current session or a recent session of this RP with the OP and ignore the logout request if they do not.

The RP's response SHOULD include the `Cache-Control` HTTP response header field with a `no-store` value, keeping the response from being cached to prevent cached responses from interfering with future logout requests. An example of this is:

```
Cache-Control: no-store
```

In the case that the RP is also an OP serving as an identity provider to downstream logged-in sessions, it is desirable for the logout request to the RP to likewise trigger downstream logout requests. This is achieved by having the RP serve content in the iframe that contains logout requests to the downstream sessions, which themselves are nested iframes rendering the downstream logout URIs.

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

frontchannel_logout_uri

OPTIONAL. RP URL that will cause the RP to log itself out when rendered in an iframe 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. An `iss` (issuer) query parameter and a `sid` (session ID) query parameter MAY be included by the OP to enable the RP to validate the request and to determine which of the potentially multiple sessions is to be logged out; if either is included, both MUST be.

It SHOULD also register this related metadata value:

frontchannel_logout_session_required

OPTIONAL. Boolean value specifying whether the RP requires that `iss` (issuer) and `sid` (session ID) query parameters be included to identify the RP session with the OP when the `frontchannel_logout_uri` is used. If omitted, the default value is `false`.

---

3. OpenID Provider Logout Functionality

TOC

OPs supporting HTTP-based logout need to keep track of the set of logged-in RPs so that they know what RPs to contact at their logout URIs to cause them to log out. Some OPs track this state using a "visited sites" cookie. OPs contact them in parallel using a dynamically constructed page with HTML `<iframe src="frontchannel_logout_uri">` tags rendering each logged-in RP's logout URI.

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

frontchannel_logout_supported

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

It SHOULD also register this related metadata value:

frontchannel_logout_session_supported

OPTIONAL. Boolean value specifying whether the OP can pass `iss` (issuer) and `sid` (session ID) query parameters to identify the RP session with the OP when the `frontchannel_logout_uri` is used. 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 `frontchannel_logout_uri` parameter has the following definition:

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.

3.1. Example Front-Channel Logout URL Usage

TOC

In this non-normative example, the RP has registered the `frontchannel_logout_uri` value `https://rp.example.org/frontchannel_logout"` with the OP. In the simple case, in which `frontchannel_logout_session_required` is false, the OP causes the front-channel logout to occur by rendering this URL in an iframe:

```
https://rp.example.org/frontchannel_logout
```

In a second example, in which `frontchannel_logout_session_required` is true, Issuer and Session ID values are also sent. This example uses an Issuer value of `https://server.example.com` and a Session ID value of `08a5019c-17e1-4977-8f42-65a12843ea02`. In this case, the OP causes the front-channel logout to occur by rendering this URL in an iframe (with line breaks for display purposes only):

```
https://rp.example.org/frontchannel_logout
  ?iss=https%3A%2F%2Fserver.example.com
  &sid=08a5019c-17e1-4977-8f42-65a12843ea02
```


4. Implementation Considerations

TOC

This specification defines features used by both Relying Parties and OpenID Providers that choose to implement Front-Channel 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".

4.1. User Agents Blocking Access to Third-Party Content

TOC

Note that at the time of this writing, some User Agents (browsers) are starting to block access to third-party content by default to block some mechanisms used to track the End-User's activity across sites. Specifically, the third-party content being blocked is website content with an origin different that the origin of the focused User Agent window. Site data includes cookies and any web storage APIs (sessionStorage, localStorage, etc.).

This can prevent the ability for notifications from the OP at the RP from being able to access the RP's User Agent state to implement local logout actions. In particular, the `frontchannel_logout_uri` might not be able to access the RP's login state when rendered by the OP in an iframe because the iframe is in a different origin than the OP's page. Therefore, deployments of this specification are recommended to include defensive code to detect this situation, and if possible, notify the End-User that the requested RP logouts could not be performed. The details of the defensive code needed are beyond the scope of this specification; it may vary per User Agent and may vary over time, as the User Agent tracking prevention situation is fluid and continues to evolve.

OpenID Connect Back-Channel Logout 1.0 [OpenID.BackChannel] is not known to be affected by these developments.

5. Security Considerations

TOC

Collisions between Session IDs and the guessing of their values by attackers are prevented by including sufficient entropy in Session ID values.

6. IANA Considerations

TOC

6.1. JSON Web Token Claims Registration

TOC

This specification registers the following Claim in the IANA "JSON Web Token Claims" registry [IANA.JWT.Claims] established by [JWT].

6.1.1. Registry Contents

TOC

- Claim Name: `sid`
- Claim Description: Session ID
- Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
- Specification Document(s): Section 3 of this specification

6.2. OAuth Dynamic Client Registration Metadata Registration

TOC

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

6.2.1. Registry Contents

TOC

- Client Metadata Name: `frontchannel_logout_uri`
- Client Metadata Description: RP URL that will cause the RP to log itself out when rendered in an iframe by the OP

- Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
- Specification Document(s): Section 2 of this specification
- Client Metadata Name: `frontchannel_logout_session_required`
- Client Metadata Description: Boolean value specifying whether the RP requires that a `sid` (session ID) query parameter be included to identify the RP session with the OP when the `frontchannel_logout_uri` is used
- Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
- Specification Document(s): Section 2 of this specification

6.3. 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].

6.3.1. Registry Contents

TOC

- Metadata Name: `frontchannel_logout_supported`
- Metadata Description: Boolean value specifying whether the OP supports HTTP-based logout, with `true` indicating support
- Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
- Specification Document(s): Section 3 of this document