|  |
| --- |
| **[TOC](" \l "toc)** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Draft | M. Jones | |  | Microsoft | |  | August 3, 2015 | |

# OpenID Connect HTTP-Based Logout 1.0 - draft 02

### 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 an HTTP-based logout mechanism 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. It also reuses the RP-initiated logout functionality specified in Section 5 of OpenID Connect Session Management 1.0 (RP-Initiated Logout).

### Table of Contents

[**1.**](#Introduction)  Introduction  
    [**1.1.**](#rnc)  Requirements Notation and Conventions  
    [**1.2.**](#Terminology)  Terminology  
[**2.**](#RPLogout)  Relying Party Logout Functionality  
[**3.**](#OPLogout)  OpenID Provider Logout Functionality  
[**4.**](#RPInitiated)  RP-Initiated Logout Functionality  
[**5.**](#Security)  Security Considerations  
[**6.**](#IANA)  IANA Considerations  
    **[6.1.](" \l "ClaimsRegistry)**  JSON Web Token Claims Registration  
        **[6.1.1.](" \l "ClaimsContents)**  Registry Contents  
    **[6.2.](" \l "DynRegRegistrations)**  OAuth Dynamic Client Registration Metadata Registration  
        **[6.2.1.](" \l "DynRegContents)**  Registry Contents  
**[7.](" \l "rfc.references1)**  References  
    **[7.1.](" \l "rfc.references1)**  Normative References  
    **[7.2.](" \l "rfc.references2)**  Informative References  
[**Appendix A.**](#Acknowledgements)  Acknowledgements  
[**Appendix B.**](#Notices)  Notices  
[**Appendix C.**](#History)  Document History  
[**§**](#rfc.authors)  Author's Address

|  |
| --- |
| [**TOC**](#toc) |

### 1.  Introduction

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 [[RFC6749] (Hardt, D., Ed., “The OAuth 2.0 Authorization Framework,” October 2012.)](#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 an HTTP-based logout mechanism 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. It also reuses the RP-initiated logout functionality specified in Section 5 of [OpenID Connect Session Management 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., Mortimore, C., and E. Jay, “OpenID Connect Session Management 1.0,” August 2015.)](" \l "OpenID.Session) [OpenID.Session] (RP-Initiated Logout). This specification can be used separately from or in combination with OpenID Connect Session Management 1.0.

|  |
| --- |
| [**TOC**](#toc) |

### 1.1.  Requirements Notation and Conventions

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 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.)](#RFC2119) [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.

|  |
| --- |
| [**TOC**](#toc) |

### 1.2.  Terminology

This specification uses the terms "Access Token", "Authorization Code", "Authorization Endpoint", "Authorization Grant", "Authorization Server", "Client", "Client Identifier", "Client Secret", "Protected Resource", "Redirection URI", "Refresh Token", "Resource Owner", "Resource Server", "Response Type", and "Token Endpoint" defined by [OAuth 2.0 (Hardt, D., Ed., “The OAuth 2.0 Authorization Framework,” October 2012.)](#RFC6749) [RFC6749], the term "User Agent" defined by [RFC 7230 (Fielding, R., Ed. and J. Reschke, Ed., “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing,” June 2014.)](#RFC7230) [RFC7230], and the terms defined by [OpenID Connect Core 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “OpenID Connect Core 1.0,” November 2014.)](#OpenID.Core) [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.

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.

|  |
| --- |
| [**TOC**](#toc) |

### 2.  Relying Party Logout Functionality

RPs supporting HTTP-based logout register a logout URI with the OP as part of their client registration.

The logout URI MUST be an absolute URI as defined by [[RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.)](" \l "RFC3986) Section 4.3. The logout URI MAY include an application/x-www-form-urlencoded formatted query component ([[RFC3986] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.)](" \l "RFC3986) Section 3.4), which MUST be retained when adding additional query parameters. The logout URI MUST NOT include a fragment component.

The OP renders <iframe src="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.

The RP's response SHOULD include Cache-Control directives keeping the response from being cached to prevent cached responses from interfering with future logout requests. It is RECOMMENDED that these directives be used:

Cache-Control: no-cache, no-store

Pragma: no-cache

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 (Sakimura, N., Bradley, J., and M. Jones, “OpenID Connect Dynamic Client Registration 1.0,” November 2014.)](#OpenID.Registration) [OpenID.Registration], it uses this metadata value to register the logout URI:

logout\_uri

OPTIONAL. RP URL that will cause the RP to log itself out when rendered in an iframe by the OP. 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.

It SHOULD also register this related metadata value:

logout\_session\_required

OPTIONAL. Boolean value specifying whether the RP requires that a sid (session ID) query parameter be included to identify the RP session at the OP when the logout\_uri is used. If omitted, the default value is false.

|  |
| --- |
| [**TOC**](#toc) |

### 3.  OpenID Provider Logout Functionality

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="logout\_uri"> tags rendering each logged-in RP's logout URI.

If the OP supports [OpenID Connect Discovery 1.0 (Sakimura, N., Bradley, J., Jones, M., and E. Jay, “OpenID Connect Discovery 1.0,” November 2014.)](#OpenID.Discovery) [OpenID.Discovery], it uses this metadata value to advertise its support for HTTP-based logout:

http\_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:

logout\_session\_supported

OPTIONAL. Boolean value specifying whether the OP can pass a sid (session ID) query parameter to identify the RP session at the OP when the 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 logout\_uri parameter has the following definition:

sid (session ID)

OPTIONAL. String identifier for a Session - a pairing of an OP to a User Agent or device for a logged-in End-User. Its contents are unique to the OP and opaque to the RP. It MUST have sufficient entropy to prevent collisions between Session IDs generated by different OPs and to prevent it from being guessed by potential attackers. Its syntax is the same as an OAuth 2.0 Client Identifier.

|  |
| --- |
| [**TOC**](#toc) |

### 4.  RP-Initiated Logout Functionality

This specification incorporates the RP-initiated logout functionality specified in Section 5 of [OpenID Connect Session Management 1.0 (Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., Mortimore, C., and E. Jay, “OpenID Connect Session Management 1.0,” August 2015.)](" \l "OpenID.Session) [OpenID.Session] by reference. A summary follows.

RPs supporting HTTP-based logout and [OpenID Connect Dynamic Client Registration 1.0 (Sakimura, N., Bradley, J., and M. Jones, “OpenID Connect Dynamic Client Registration 1.0,” November 2014.)](#OpenID.Registration) [OpenID.Registration] MAY register this metadata value:

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.

Post-logout redirection is only done when the logout is RP-initiated, in which case the redirection target is the post\_logout\_redirect\_uri query parameter value used by the initiating RP; otherwise it is not done.

OPs supporting HTTP-based logout and [OpenID Connect Discovery 1.0 (Sakimura, N., Bradley, J., Jones, M., and E. Jay, “OpenID Connect Discovery 1.0,” November 2014.)](#OpenID.Discovery) [OpenID.Discovery] MUST provide this discovery value:

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.

The end\_session\_endpoint is used in exactly the same manner as specified in Sections 2.1 and 5 of OpenID Connect Session Management, including accepting the same query parameters as defined there in Section 5: id\_token\_hint, post\_logout\_redirect\_uri, and state.

|  |
| --- |
| [**TOC**](#toc) |

### 5.  Security Considerations

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

|  |
| --- |
| [**TOC**](#toc) |

### 6.  IANA Considerations

|  |
| --- |
| [**TOC**](#toc) |

### 6.1.  JSON Web Token Claims Registration

This specification registers the following claim in the IANA "JSON Web Token Claims" registry [[IANA.JWT.Claims] (IANA, “JSON Web Token Claims,” .)](" \l "IANA.JWT.Claims) established by [[JWT] (Jones, M., Bradley, J., and N. Sakimura, “JSON Web Token (JWT),” May 2015.)](" \l "JWT).

|  |
| --- |
| **[TOC](" \l "toc)** |

### 6.1.1.  Registry Contents

* 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 (OpenID Provider Logout Functionality)](" \l "OPLogout) of this document

|  |
| --- |
| **[TOC](" \l "toc)** |

### 6.2.  OAuth Dynamic Client Registration Metadata Registration

This specification registers the following client metadata definitions in the IANA "OAuth Dynamic Client Registration Metadata" registry [[IANA.OAuth.Parameters] (IANA, “OAuth Parameters,” .)](" \l "IANA.OAuth.Parameters) established by [[RFC7591] (Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, “OAuth 2.0 Dynamic Client Registration Protocol,” July 2015.)](" \l "RFC7591):

|  |
| --- |
| **[TOC](" \l "toc)** |

### 6.2.1.  Registry Contents

* Client Metadata Name: 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 (Relying Party Logout Functionality)](" \l "RPLogout) of this document
* Client Metadata Name: 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 at the OP when the logout\_uri is used
* Change Controller: OpenID Foundation Artifact Binding Working Group - openid-specs-ab@lists.openid.net
* Specification Document(s): [Section 2 (Relying Party Logout Functionality)](" \l "RPLogout) of this document

|  |
| --- |
| **[TOC](" \l "toc)** |

### 7.  References

|  |
| --- |
| **[TOC](" \l "toc)** |

### 7.1. Normative References

|  |  |
| --- | --- |
| **[IANA.JWT.Claims]** | IANA, “[JSON Web Token Claims](http://www.iana.org/assignments/jwt).” |
| **[IANA.OAuth.Parameters]** | IANA, “[OAuth Parameters](http://www.iana.org/assignments/oauth-parameters).” |
| **[OpenID.Core]** | Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, “[OpenID Connect Core 1.0](http://openid.net/specs/openid-connect-core-1_0.html),” November 2014. |
| **[OpenID.Discovery]** | Sakimura, N., Bradley, J., Jones, M., and E. Jay, “[OpenID Connect Discovery 1.0](http://openid.net/specs/openid-connect-discovery-1_0.html),” November 2014. |
| **[OpenID.Registration]** | Sakimura, N., Bradley, J., and M. Jones, “[OpenID Connect Dynamic Client Registration 1.0](http://openid.net/specs/openid-connect-registration-1_0.html),” November 2014. |
| **[OpenID.Session]** | Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., Mortimore, C., and E. Jay, “[OpenID Connect Session Management 1.0](http://openid.net/specs/openid-connect-session-1_0.html),” August 2015. |
| **[RFC2119]** | Bradner, S., “[Key words for use in RFCs to Indicate Requirement Levels](http://www.rfc-editor.org/info/rfc2119),” BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997. |
| **[RFC3986]** | Berners-Lee, T., Fielding, R., and L. Masinter, “[Uniform Resource Identifier (URI): Generic Syntax](http://www.rfc-editor.org/info/rfc3986),” STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005. |
| **[RFC6749]** | Hardt, D., Ed., “[The OAuth 2.0 Authorization Framework](http://www.rfc-editor.org/info/rfc6749),” 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](http://www.rfc-editor.org/info/rfc7230),” RFC 7230, DOI 10.17487/RFC7230, June 2014. |

|  |
| --- |
| [**TOC**](#toc) |

### 7.2. Informative References

|  |  |
| --- | --- |
| **[JWT]** | Jones, M., Bradley, J., and N. Sakimura, “[JSON Web Token (JWT)](http://tools.ietf.org/html/rfc7519),” RFC 7519, DOI 10.17487/RFC7519, May 2015. |
| **[RFC7591]** | Richer, J., Ed., Jones, M., Bradley, J., Machulak, M., and P. Hunt, “[OAuth 2.0 Dynamic Client Registration Protocol](http://www.rfc-editor.org/info/rfc7591),” RFC 7591, DOI 10.17487/RFC7591, July 2015. |

|  |
| --- |
| **[TOC](" \l "toc)** |

### Appendix A.  Acknowledgements

The OpenID Community would like to thank the following people for their contributions to this specification:

John Bradley (ve7jtb@ve7jtb.com), Ping Identity

Brian Campbell (bcampbell@pingidentity.com), Ping Identity

Michael B. Jones (mbj@microsoft.com), Microsoft

Torsten Lodderstedt (t.lodderstedt@telekom.de), Deutsche Telekom

|  |
| --- |
| [**TOC**](#toc) |

### Appendix B.  Notices

Copyright (c) 2015 The OpenID Foundation.

The OpenID Foundation (OIDF) grants to any Contributor, developer, implementer, or other interested party a non-exclusive, royalty free, worldwide copyright license to reproduce, prepare derivative works from, distribute, perform and display, this Implementers Draft or Final Specification solely for the purposes of (i) developing specifications, and (ii) implementing Implementers Drafts and Final Specifications based on such documents, provided that attribution be made to the OIDF as the source of the material, but that such attribution does not indicate an endorsement by the OIDF.

The technology described in this specification was made available from contributions from various sources, including members of the OpenID Foundation and others. Although the OpenID Foundation has taken steps to help ensure that the technology is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this specification or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. The OpenID Foundation and the contributors to this specification make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this specification, and the entire risk as to implementing this specification is assumed by the implementer. The OpenID Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. The OpenID Foundation invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this specification.

|  |
| --- |
| [**TOC**](#toc) |

### Appendix C.  Document History

[[ To be removed from the final specification ]]

-02

* Tracked terminology changes made in the referenced IETF specs since errata set 1.
* Registered the sid (session ID) claim.
* Registered the logout\_uri and logout\_session\_required client metadata values.
* Stated that the RP's logout response SHOULD include Cache-Control directives keeping the response from being cached.
* Added syntax requirements for logout URIs.

-01

* Simplified to always use iframes, rather than a combination of images and iframes.

-00

* Wrote the initial version based on the proposal circulated as a Word doc.

|  |
| --- |
| [**TOC**](#toc) |

### Author's Address

|  |  |
| --- | --- |
|  | Michael B. Jones |
|  | Microsoft |
| **Email:** | [mbj@microsoft.com](mailto:mbj@microsoft.com) |
| **URI:** | <http://self-issued.info/> |