OpenID Connect Logout using HTTP GET

Michael B. Jones – Microsoft Corporation – February 20, 2015

# Introduction

Several [OpenID Connect](http://openid.net/connect/) implementers have requested a front channel logout mechanism that doesn’t use JavaScript. Other protocols have used HTTP GETs to RP URLs that clear cookies and then return a hidden image or iframe content to achieve this. This proposal does the same thing. It also reuses the RP-initiated logout functionality specified in [Section 5 of OpenID Connect Session Management](http://openid.net/specs/openid-connect-session-1_0.html#RPLogout) (RP-Initiated Logout).

# RP Logout Functionality

RPs supporting logout in this manner need to register a logout URL with the OP as part of their client registration. In the default case, the OP renders an HTML <img src="*logout\_uri*"> tag with the logout URL as the source to request the RP log out. Upon receiving the GET, the RP clears state associated with the logged in session, including any cookies, and then returns an image and a HTTP 200 status code. A single pixel transparent PNG image is suggested. HTTP 4xx or 5xx status codes can be used to indicate that the logout failed. The domain, port, and scheme of this URL MUST be the same as that of a registered redirect\_uri value.

In the case that the RP is an STS 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 can be achieved by having the RP serve content in an iframe that contains logout requests to the downstream sessions. When this is the case, the originating OP MUST instead render an HTML <iframe src="*logout\_uri*"> tag with the logout URL as the source.

An OP MAY use <iframe src="*logout\_uri*"> instead of <img src="*logout\_uri*"> in all cases when requesting logouts. There are two downsides to this. First, multiple iframe loads are less likely to occur in parallel than multiple image loads, decreasing the chances that all logouts occur. Second, the status codes returned by images to indicate whether the logout succeeded or not aren’t available when iframes are used.

If the RP supports Dynamic Client Registration, it uses this metadata value to register the logout URL:

* logout\_uri: OPTIONAL. RP URL that will cause the RP to log itself out and then return an image or iframe contents. An 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 these related metadata values:

* logout\_sid\_required: OPTIONAL. Boolean value specifying whether the RP requires a sid (Session ID) for the RP session at the OP to passed as a sid query parameter when the logout\_uri is used. If omitted, the default value is false.
* logout\_use\_iframe: OPTIONAL. Boolean value specifying whether the RP requires that the logout\_uri be loaded as the target of an iframe. If omitted, the default value is false.

# OP Logout Functionality

OPs supporting GET-based logout need to keep track of the set of logged in RPs so that they know what RPs to contact at their logout URLs to cause them to log out. Some OPs track this state using a “visited sites” cookie. OPs typically will contact them in parallel using a dynamically constructed page with HTML <img …> tags. However, if the RP has declared that its logout URI must be rendered in an iframe, the OP MUST retrieve the logout content using an <iframe …> tag.

If the OP supports Discovery, it uses this metadata value to advertise its support for GET-based logout:

* logout\_supported: OPTIONAL. Boolean value specifying whether the OP supports GET-based logout, with true indicating support. If omitted, the default value is false.

It SHOULD also register this related metadata value:

* sid\_supported: OPTIONAL. Boolean value specifying whether the OP can pass a sid (Session ID) for the RP session at the OP as a sid query parameter when the logout\_uri is used. If supported, the sid claim is also included in ID Tokens. If omitted, the default value is false.

The sid (Session ID) value used in ID Tokens and as a logout\_uri parameter has the following definition:

* sid (Session ID): OPTIONAL. String that identifies an OP to user-agent or device pairing for a logged-in end-user. Its contents are unique to the OP and opaque to the RP. Its syntax is the same as an OAuth client\_id.

# RP-Initiated Logout Functionality

This specification incorporates the RP-initiated logout functionality specified in [Section 5 of OpenID Connect Session Management](http://openid.net/specs/openid-connect-session-1_0.html#RPLogout) by reference. A summary follows.

RPs supporting logout and dynamic client 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 to the RP that initiated the logout action, if it was initiated by an RP; otherwise it isn’t done.

OPs supporting logout and 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.

end\_session\_endpoint is used in exactly the same manner as specified in [Section 2.1](http://openid.net/specs/openid-connect-session-1_0.html#OPMetadata) and [Section 5](http://openid.net/specs/openid-connect-session-1_0.html#RPLogout) of [OpenID Connect Session Management](http://openid.net/specs/openid-connect-session-1_0.html), including accepting the same query parameters as defined there.

# History

20-Feb-15 Replaced the optional id\_token parameter with an optional sid (Session ID) parameter. Enabled the use of iframes with nested images or iframes to achieve downstream logouts.

16-Feb-15 Added an optional id\_token parameter to the logout\_uri to authenticate requests and differentiate between sessions, plus related metadata values. Added that non-200 HTTP status codes can be used when the logout fails. Clarified when post-logout redirection to an RP occurs.

13-Feb-15 Wrote the initial one-pager.