OpenID Connect Logout using HTTP GET

Michael B. Jones – Microsoft Corporation – February 16, 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 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 an https logout URL with the OP as part of their client registration. The OP does an HTTP GET to the logout URL 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 of this URL MUST be the same as the domain of a registered redirect\_uri value.

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

* logout\_uri: OPTIONAL. RP URL using the https scheme that will cause the RP to log itself out and then return an image. An id\_token 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\_id\_token\_required: OPTIONAL. Boolean value specifying whether the RP requires an ID Token for the RP session at the OP to passed as an id\_token query parameter when the logout\_uri is used. If omitted, the default value is false.

It MAY also 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\_redirect\_uris is used in exactly the same manner as specified in [Section 5 of OpenID Connect Session Management](http://openid.net/specs/openid-connect-session-1_0.html#RPLogout) (RP-Initiated Logout). 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.

# OP Logout Functionality

OPs supporting GET-based logout need to keep track of the set of logged in RPs so that it knows 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.

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:

* logout\_id\_token\_supported: OPTIONAL. Boolean value specifying whether the OP can pass an ID Token for the RP session at the OP as an id\_token query parameter when the logout\_uri is used. If omitted, the default value is false.

Also, if the OP supports Discovery, it also 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

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.