OpenID Connect Logout using HTTP GET

Michael B. Jones – Microsoft Corporation – February 13, 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. 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.

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).

# 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.

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.