[MS-OAPX]: OAuth 2.0 Protocol Extensions

This topic lists the Errata found in [MS-OAPX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS

Atom

Errata below are for Protocol Document Version V7.0 – 2017/06/13.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2017/08/07</td><td>
<p>In multiple sections, added revisions for a POST body parameter that is sent from the token broker on the client.</p>
<p>In Section 1.2.1, Normative References, the following references were added:</p>
<p>[IETFDRAFT-OAUTH2TOKBIND] Popov, A., Ed., Nystroem, M., Balfranz,</p>
<p>D., et al., "OAuth 2.0 Token Binding", draft-ietf-oauth-token-binding-04, July 2017, https://tools.ietf.org/html/draft-ietf-oauth-token-binding-04</p>
<p>[IETFDRAFT-TOKBINDPROT] Popov, A., Ed., Nystroem, M., Balfanz, D., et al., "The Token Binding Protocol Version 1.0", draft-ietf-tokbind-protocol-14, April 2017, https://tools.ietf.org/html/draft-ietf-tokbind-protocol-14</p>
<p>[MSKB-4034658] Microsoft Corporation, "August 8, 2017 - KB4034658", https://support.microsoft.com/help/4034658</p>
<p>In Section 2.3.3, Common Data Structures, a new message body parameter, tbidv2, was added to the bottom of the table, along with a new product behavior note.</p>
<p>Changed from:</p>
<table>
<tr><th>Message body parameter</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>x5c</td><td>OPTIONAL. The AD FS server includes this parameter in the successful response to an OAuth logon certificate request. The value is a base64-encoded CMS certificate chain or CMC full PKI response (see [MS-WCCE] section 2.2.2.8).
The AD FS server does not return this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.</td></tr>
</table>
<p>Changed to:</p>
</td></tr>
</table>

Errata Published*	Description

Message body parameter	Description
…	…
x5c	OPTIONAL. The AD FS server includes this parameter in the successful response to an OAuth logon certificate request. The value is a base64-encoded CMS certificate chain or CMC full PKI response (see [MS-WCCE] section 2.2.2.8). The AD FS server does not return this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.
tbidv2	OPTIONAL. The OAuth 2.0 client includes this parameter in the POST body of a request to indicate that the client is providing a referred token-binding ID to the AD FS server for the current request. See [IETFDRAFT-TOKBINDPROT] for details on referred token-bindings. The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.<5>

<5> Section 2.2.3: Even though AD_FS_BEHAVIOR_LEVEL_2 is supported on Windows Server 2016, the tbidv2 parameter is ignored on Windows Server 2016 unless [MSKB-4034658] is applied.

A new section, 2.2.3.8, tbidv2, was added to describe the new message body parameter tbidv2.

Added:

2.2.3.8 tbidv2

```
 POST /token HTTP/1.1
 Host: server.example.com
 Content-Type: application/x-www-form-urlencoded

grant_type={grant_type}&client_id={client_id}&redirect_uri={redirect_uri}&tbid
v2={tbidv2}
```

OPTIONAL

The tbidv2 parameter is optional and can be specified by the client role of the OAuth 2.0 Protocol Extensions in the POST body when the client is providing a referred token-binding ID as part of the request. For details on referred token-binding IDs, see [IETFDRAFT-TOKBINDPROT].

The format for the tbidv2 request parameter is as follows:

```
String = *(%x20-7E)
```

Errata Published*	Description
	`tbidv2 = String` In Section 3.2.5.2.1.1, Request Body, a new message body parameter, tbidv2, was added to the parameter list. Changed from: In addition to the POST body parameters described in [RFC6749] section 4.1.3, the OAuth 2.0 client can choose to send the following additional parameters: ... csr_type: OPTIONAL. See sections 2.2.3 and 2.2.3.6. Changed to: In addition to the POST body parameters described in [RFC6749] section 4.1.3, the OAuth 2.0 client can choose to send the following additional parameters: ... csr_type: OPTIONAL. See sections 2.2.3 and 2.2.3.6. tbidv2: OPTIONAL. See [IETFDRAFT-TOKBINDPROT]. In Section 3.2.5.2.1.3, Processing Details, processing information for the new message body parameter tbidv2 was added. Changed from: • If the AD FS server's ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher and it has not encountered any prior errors in processing, the AD FS server includes an ID token in the response as described in [OIDCCore] section 3.1.3.3. Changed to: • If the AD FS server's ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher and it has not encountered any prior errors in processing, the AD FS server includes an ID token in the response as described in [OIDCCore] section 3.1.3.3. • If the AD FS server's ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher and it has not encountered any prior errors in processing, and a referred token-binding ID was provided on the request using the tbidv2 POST parameter, the AD FS server includes a token-binding claim in the Access Token in the response, as defined in [IETFDRAFT-OAUTH2TOKBIND].

*Date format: YYYY/MM/DD