[MS-OAPXBC]: OAuth 2.0 Protocol Extensions for Broker Clients

This topic lists the Errata found in [MS-OAPXBC] 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 V8.0 – 2021/06/25.

Errata Published*	**Description**
2021/07/13	In Section 3.1.5.1.3.3 Processing Details, updated to support client use of KDFv2 version and specified supporting operating systems. Changed from: "The client derives a signing key from the Session Key ADM element (section 3.1.1), the constant label "AzureAD-SecureConversation", and the ctx value provided in the JWT header of the request by using the process described in [SP800-108]. The client uses this signing key to sign the request." Changed to: "The client derives a signing key from the Session Key ADM element (section 3.1.1), the constant label "AzureAD-SecureConversation", and the ctx value provided in the JWT header of the request by using the process described in [SP800-108]. The client uses this signing key to sign the request.If the capabilities field of the OpenID Provider Metadata ([MS-OIDCE] section 2.2.3.2) from the server includes the value "kdf_ver2", the client can use KDFv2 version<2> for deriving the Session Key. If the client chooses to use KDFv2, the client MUST use SHA256(ctx || assertion payload) instead of ctx as the context for deriving the signing key. The client MUST also add the JWT header field "kdf_ver" with value set to 2 to communicate that KDFv2 was used to create the derived signing key." <2> Section 3.1.5.1.3.3: This protocol now supports KDF Version 2 for creating derived keys, which is used by clients to create a signed JWT. KDF Version 2 is supported on the operating systems specified in [MSFT-CVE-2021-33781], each with its related KB article download installed. Please see Section 3.1.5.1.4.3 Processing Details, which has changed as follows: Changed from: "The client first requests a primary refresh token from the server as defined in sections 3.1.5.1.2 and 3.2.5.1.2. It then uses the Primary Refresh Token ADM element (section 3.1.1) to populate the refresh_token field in this request for the user authentication certificate." Changed to: "The client first requests a primary refresh token from the server as defined in sections 3.1.5.1.2 and 3.2.5.1.2. It then uses the Primary Refresh Token ADM element (section 3.1.1) to populate the refresh_token field in this request for the user authentication certificate.If the capabilities field of the OpenID Provider Metadata ([MS-OIDCE] section 2.2.3.2) from the server includes the value "kdf_ver2", the client can use KDFv2 version for deriving the

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>Session Key. If the client chooses to use KDFv2, the client MUST use SHA256(ctx || assertion payload) instead of ctx as the context for deriving the signing key. The client MUST also add theJWTheader field "kdf_ver" with the value set to 2 to communicate that KDFv2 was used for creating the derived signing key."
Please see Section 3.1.5.2.1.3 Processing Details, which has changed as follows:
Changed from:
"The client derives a signing key from the Session Key ADM element (section 3.1.1), the constant label "AzureAD-SecureConversation", and the ctx value provided in the JWT header of the request by using the process described in [SP800-108]. The client uses this signing key to sign the JWT. "
Changed to:
"The client derives a signing key from the Session Key ADM element (section 3.1.1), the constant label "AzureAD-SecureConversation", and the ctx value provided in the JWT header of the request by using the process described in [SP800-108]. The client uses this signing key to sign the JWT. If the capabilities field of the OpenID Provider Metadata ([MS-OIDCE] section 2.2.3.2) from the server includes the value "kdf_ver2", the client can use KDFv2 version for deriving the Session Key. If the client chooses to use KDFv2, the client MUST use SHA256(ctx || assertion payload) instead of ctx as the context for deriving the signing key. The client MUST also add the JWT header field "kdf_ver" with value set to 2 to communicate that KDFv2 was used for creating the derived signing key."
Please see Section 3.2.5.1.2.1 Request Body, which has changed as follows:
Changed from:
"x5c (REQUIRED): The certificate used to sign the request, following the format described in [RFC7515] section 4.1.6."
Changed to:
"x5c (REQUIRED): The certificate used to sign the request, following the format described in [RFC7515] section 4.1.6.
kdf_ver (OPTIONAL): If the capabilities field of the OpenID Provider Metadata ([MS-OIDCE]section 2.2.3.2) from the server includes the value "kdf_ver2", the client can use KDFv2 version for creating context, which is used in deriving the Session Key. This is used in flows to exchange a Primary Refresh token for another token or user authentication certificate, as defined in sections3.1.5.1.3and 3.1.5.1.4."
Please see Section 3.2.5.1.3.1 Request Body
Changed from:
"ctx (REQUIRED): The base64-encoded bytes used for signature key derivation."
Changed to:
"ctx (REQUIRED): The base64-encoded bytes used for signature key derivation.</td></tr>
</table>

Errata Published*	Description
	kdf_ver (OPTIONAL): If ctx was created using KDFv2, the client MUST include the JWT header with the kdf_ver field set to 2." Please see Section 3.2.5.1.4.1 Request Body Changed from: "ctx (REQUIRED): The base64-encoded bytes used for signature key derivation." Changed to: "ctx (REQUIRED): The base64-encoded bytes used for signature key derivation. kdf_ver (OPTIONAL): If ctx was created using KDFv2, the client MUST include the JWT header with the kdf_ver field set to 2." Please see Section 3.2.5.2.1.1.1 x-ms-RefreshTokenCredential HTTP header format Changed from: "ctx (REQUIRED): The base64-encoded bytes used for signature key derivation." Changed to: "ctx (REQUIRED): The base64-encoded bytes used for signature key derivation. kdf_ver (OPTIONAL): If ctx was created using KDFv2, the client MUST include the JWTheader with this field value set to 2."

*Date format: YYYY/MM/DD