[MS-ADFSPIP]: Active Directory Federation Services and Proxy Integration Protocol

This topic lists the Errata found in the MS-ADFSPIP document 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

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 30, 2015 - Download

July 18, 2016 - Download

Errata below are for Protocol Document Version V5.0 – 2017/06/01.

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td>2017/08/07</td><td>

Several sections were updated to cover the proper handling of certificate errors.

In Section 1.2.1, Normative References, the following reference was added:

[MSKB-4034661] Microsoft Corporation, "August 15, 2017 – KB4034661", https://support.microsoft.com/help/4034661

In Section 2.2.2.11, Serialized Request with Certificate, the key value pairs ErrorType" : "<Error-Type>", and "ErrorCode" : "<Error-Code>" were added to the request object.

Changed from:

```
{
  "Request" :
    {
      ...
    },
  "SerializedClientCertificate" : "<serialized-client-certificate>",
  "CertificateUsage" : "<certificate-usage>",

}
```

Changed to:

```
{
  "Request" :
    {
      ...
    },
  "SerializedClientCertificate" : "<serialized-client-certificate>",
  "CertificateUsage" : "<certificate-usage>",
  "ErrorType" : "<Error-Type>",
  "ErrorCode" : "<Error-Code>"
}
```

</td></tr>
</table>

Errata Published *	Description

	...
	Error-Type: Error Type (section 2.2.2.17).<5>
	Error-Code: Error code, as an integer.<6>
	
	<5> Section 2.2.2.11: The Error-Type field of [Serialized Request with Certificate] is not supported on Windows Server 2012 R2. It is also not supported on Windows Server 2016 unless [MSKB-4034661] is installed.
	<6> Section 2.2.2.11: The Error-Code field of [Serialized Request with Certificate] is not supported on Windows Server 2012 R2. It is also not supported on Windows Server 2016 unless [MSKB-4034661] is installed.
	
	A new section, 2.2.2.17, Error Type, was added to describe the Error Type enumeration:
	
	2.2.2.17 Error Type
	This is an enumeration with the following values:
	`{`
	`  "None"`
	`  "Certificate"`
	`}`
	
	In Section 3.10.5.1.1.3, Processing Details, the content was updated to include rules for success or failure of end-user certificate validation.
	
	Changed from:
	...
	The server MUST process the request as if it was received directly to the endpoint in the server as specified in the request.
	
	Changed to:
	...
	The server MUST process the request as if it was received directly to the endpoint in the server as specified in the request.
	If [Serialized Request with Certificate].ErrorType is set to "Certificate" and [Serialized Request with Certificate].ErrorCode is set to non-zero, then the server SHOULD fail the client's request
	
	In Section 3.11.5, Message Processing Events and Sequencing Rules, steps 3 and 5 were revised and a new step 6 was added.
	
	Changed from:
	...
	3. If CurrentEndpointConfiguration.ClientCertificateQueryMode is "QueryAndRequire", then the client SHOULD attempt to retrieve end-user X509 certificate [RFC4158] using client TLS authentication [RFC2246]. If it obtains a certificate, the client MUST follow the processing in section 3.11.5.1. If it does not obtain a certificate, it SHOULD return a HTTP error code of 204.
	...

Errata Published *	Description
	5. If no certificate was obtained in steps 2 or 3, then the client SHOULD replay the request as follows: 1. The request SHOULD be made to the following URL: ... Changed to: ... 3. If CurrentEndpointConfiguration.ClientCertificateQueryMode is "QueryAndRequire", then the client SHOULD attempt to retrieve end-user X509 certificate [RFC4158] using client TLS authentication [RFC2246]. If it obtains a certificate, the client MUST follow the processing in section 3.11.5.1. ... 5. If no certificate was obtained in step 2, or if a certificate was obtained in steps 2 or 3, but the section 3.11.5.1 validation fails when the CurrentEndpointConfiguration.CertificateValidation value is "IssuedByDrs", then the client SHOULD replay the request as follows: 1. The request SHOULD be made to the following URL: ... 6. If no certificate was obtained in step 3, then the client SHOULD<10> perform the following steps: 1. The client constructs a request as in section 3.10.5.1 with [Serialized Request with Certificate] set to following values: • [Serialized Request with Certificate].ErrorType MUST be set to “Certificate”. • [Serialized Request with Certificate].ErrorCode MUST be set to 1168. 2. The client then performs the common processing defined in section 3.11.5.2. <10> Section 3.11.5: In Windows Server 2012 R2, and in Windows Server 2016 without [MSKB-4034661] installed, the client simply ignores the request if no certificate was obtained. In Section 3.11.5.1, End-user X509 Certificate Success Processing, added "Success" to the section title, and updated the content to include rules for success or failure of end-user certificate validation. Also created a new section (3.11.5.2) and moved part of the content to it. Changed from: If the client obtains a certificate of the end user then the client SHOULD validate the X509 certificate [RFC4158] based on the CurrentEndpointConfiguration.CertificateValidation. If the CurrentEndpointConfiguration.CertificateValidation value is "None" ... If the CurrentEndpointConfiguration.CertificateValidation value is "Ssl" ... If the CurrentEndpointConfiguration.CertificateValidation value is "IssuedByDrs" ... Upon successful validation the client MUST construct a request as in section 3.10.5.1. The [Serialized Request with Certificate].SerializedClientCertificate MUST be set to the base64 string encoded ([RFC4648] section 4) X509 certificate [RFC4158]. If CurrentEndpointConfiguration.CertificateValidation value is "IssuedByDrs" then the [Serialized Request with Certificate].CertificateUsage MUST be set to "Device". If CurrentEndpointConfiguration.CertificateValidation value is "Ssl" then the [Serialized Request with Certificate].CertificateUsage MUST be set to "User". The [Serialized Request with Certificate].Request elements values SHOULD be copied from the incoming HTTP request. The request SHOULD be made to https://[ServiceConfiguration.ServiceHostName]:[ServiceConfiguration.HttpsPort]/adfs/backendproxytls and the client MUST authenticate with client TLS [RFC2246] using [Client State].TrustCertificate.

Errata Published *	Description
	Changed to: If the client obtains a certificate of the end-user then the client SHOULD validate the X509 certificate [RFC4158] based on the CurrentEndpointConfiguration.CertificateValidation. • If the CurrentEndpointConfiguration.CertificateValidation value is "None" ... • If the CurrentEndpointConfiguration.CertificateValidation value is "Ssl" then the whole chain validation [RFC4158] of the certificate SHOULD be performed. • If the CurrentEndpointConfiguration.CertificateValidation value is "IssuedByDrs" then the client SHOULD validate that the end-user certificate was issued by one of ServiceConfiguration.DeviceCertificateIssuers. If the validation of the end-user certificate was successful, or if the validation of the end-user certificate failed and the CurrentEndpointConfiguration.CertificateValidation value is "Ssl", the following processing occurs: • The client MUST construct a request as in section 3.10.5.1. • If the validation of the end-user certificate was successful, then the [Serialized Request with Certificate].SerializedClientCertificate MUST be set to the base64 string encoded ([RFC4648] section 4) X509 certificate [RFC4158]. Otherwise, the [Serialized Request with Certificate].ErrorType SHOULD be set to "Certificate" and the [Serialized Request with Certificate].ErrorCode SHOULD be set to the error value that was encountered while validating the end-user certificate.<11> • The client then performs the common processing defined in section 3.11.5.2. If the validation of the end-user certificate failed and the CurrentEndpointConfiguration.CertificateValidation value is "IssuedByDrs", the client SHOULD replay the request as defined in section 3.11.5 step 5. <11> Section 3.11.5.1: In Windows Server 2012 R2 , and in Windows Server 2016 without [MSKB-4034661] installed, the client simply ignores a request with an invalid certificate. Added a new section: **Section 3.11.5.2 End-user X509 Certificate Common Processing** If CurrentEndpointConfiguration.CertificateValidation value is "IssuedByDrs" then the [Serialized Request with Certificate].CertificateUsage MUST be set to "Device". If CurrentEndpointConfiguration.CertificateValidation value is "Ssl" then the [Serialized Request with Certificate].CertificateUsage MUST be set to "User". The [Serialized Request with Certificate].Request elements values SHOULD be copied from the incoming HTTP request. The request SHOULD be made to https://[ServiceConfiguration.ServiceHostName]:[ServiceConfiguration.HttpsPort]/adfs/backendproxytls and the client MUST authenticate with client TLS [RFC2246] using [Client State].TrustCertificate.

*Date format: YYYY/MM/DD