

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

This topic lists the Errata found in [MS-WCCE] 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.

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

September 29, 2020 - [Download](#)

October 6, 2021 - [Download](#)

October 3, 2022 - [Download](#)

Errata below are for Protocol Document Version [V47.0 - 2021/10/06](#).

| Errata Published* | Description |
|-------------------|---|
| 2023/02/14 | <p>Section 3.2.2.6.3.1.1 PropID=0x0000001D (CR_PROP_TEMPLATES) "Configured Certificate Templates"</p> <p>Description: Updated string definition ("TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2\...") to include a null termination character, to ensure consistent results with calls to the GetCATemplates function.</p> <p>Changed from: "TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2\... " where</p> <p>Changed to: "TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2...\nTemplateNameN\nTemplateOIDN\n\0" where</p> <p>Note: The format and definition of the string cited in section 3.2.1.4.3.2.29 below is correct as is.</p> |
| 2022/12/16 | <p>Section 2.1 Transport</p> <p>Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure that a connection to the CA server is not denied.</p> <p>Changed from: If a CA server has IF_ENFORCEENCRYPTICERTADMIN set (section 3.2.1.1.4) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY (0x06) authentication level is not specified by the client for</p> |

| Errata Published* | Description |
|-------------------|---|
| | <p>certificate administrative operations, the CA MUST deny a connection to the client and return a non-zero error. <7></p> <p>Changed to:</p> <p>If a CA server has IF_ENFORCEENCRYPTICERTADMIN set (section 3.2.1.1.4) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY (0x06) authentication level is not specified by the client for certificate administrative operations, the CA MUST deny a connection to the client and return a non-zero error. <7> <8></p> <p><8> The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTADMIN or IF_ENFORCEENCRYPTICERTREQUEST setting.</p> <p>Section 3.2.1.4.2.1 ICertRequestD::Request (Opnum 3)</p> <p>Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure that a connection to the CA server is not denied.</p> <p>Changed from:</p> <p>If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error.</p> <p>Changed to:</p> <p>If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8), is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <70></p> <p><70>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting.</p> <p>Section 3.2.1.4.2.2 ICertRequestD::GetCACert (Opnum 4)</p> <p>Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure a connection to the CA server is not denied.</p> <p>Changed from:</p> <p>If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error.</p> <p>Changed to:</p> <p>If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <82></p> |

| Errata Published* | Description |
|-------------------|---|
| | <p><82>The operating systems specified in MSFT-CVE-2022-37976, each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting.</p> <p>Section 3.2.1.4.2.3 ICertRequestD::Ping (Opnum 5) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure that a connection to the CA server is not denied.</p> <p>Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error</p> <p>Changed to: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <85></p> <p><85>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting.</p> <p>Section 3.2.1.4.3.2 ICertRequestD2::GetCAProperty (Opnum 7) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure a connection to the CA server is not denied.</p> <p>Changed from: If Config_CA_Interface_Flags contain the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a non-zero error.</p> <p>Changed to: If Config_CA_Interface_Flags contain the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a non-zero error<88></p> <p><88>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting.</p> <p>Section 3.2.1.4.3.3 ICertRequestD2::GetCAPropertyInfo (Opnum 8) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate</p> |

| Errata Published* | Description |
|-------------------|--|
| | <p>administrative operations to ensure a connection to the CA server is not denied. Also specified the operating systems that support this behavior.</p> <p>Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error.</p> <p>Changed to: If Config_CA_Interface_Flags contain the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <108></p> <p><108>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting.</p> |

*Date format: YYYY/MM/DD