[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.

RSS
Atom

September 29, 2020 – Download

Errata below are for Protocol Document Version V46.0 – 2021/06/25.

Errata Published*	Description
2021/09/07	In Section 3.2.1.4.3.2.15.1 Creating a CA Exchange Certificate, provided additional information about creating the certificate: Changed from: 1. For the Subject of the exchange certificate, a common name attribute is used with a value the same as the value of the common name attribute in the subject information of the CA signing certificate (Signing_Cert_Certificate datum) and appending "-Xchg" to the value. The Issuer field is filled with the same value as the Subject field. ... 7. If the CA signing certificate contains an Authority Key Identifier extension, add this extension with the same value as in the CA signing certificate (Signing_Cert_Certificate datum). Authority Key Identifier extension is specified in [RFC3280] section 4.2.1.1. 8. If the CA signing certificate contains a Subject Key Identifier extension, add this extension with the same value as in the CA signing certificate (Signing_Cert_Certificate datum). Subject Key Identifier extension is specified in [RFC3280] section 4.2.1.2. 9. If the CA signing certificate contains an Authority Information Access extension, add this extension with the same value as in the CA signing certificate (Signing_Cert_Certificate datum). Authority Information Access extension is specified in [RFC3280] section 4.2.2.1. 10. If the CA signing certificate contains a CRL Distribution Point extension, add this extension with the same value as in the CA signing certificate (Signing_Cert_Certificate datum). CRL Distribution Point extension is specified in [RFC3280] section 4.2.1.14. 11. The value for Valid From field is the date and time when the request for CA exchange certificate was received minus the value of the Config_CA_Clock_Skew_Minutes data. The Valid To field is set to one week later. Valid From and Valid To are specified in [RFC3280] section 4.1.2.5. Changed to: 1. For the Subject of the exchange certificate, a common name attribute (1) is used with a value the same as the value of the common name attribute (1) in the subject information of the CA signing certificate (Signing_Cert_Certificate datum) and appending "-Xchg" to the value. The Issuer field is filled with the same value as the Subject field of the CA signing certificate (Signing Cert Certificate datum). ...

Errata Published*	Description
	7. The Authority Key Identifier extension is added with the same value as the Subject Key Identifier extension in the CA signing certificate (Signing_Cert_Certificate datum). If Subject Key Identifier extension is not found in CA signing certificate (Signing_Cert_Certificate datum) then SHA1 hash of the public key of CA signing certificate (Signing_Cert_Certificate datum) is used as the value for Authority Key Identifier extension. Authority Key Identifier extension is specified in [RFC3280] section 4.2.1.1. 8. The Subject Key Identifier extension is added with the same value as the SHA1 hash of the public key associated with the exchange certificate. Subject Key Identifier extension is specified in [RFC3280] section 4.2.1.2. 9. The Authority Information Access extension is added with the same value the CA returns when ICertRequestD2::GetCAProperty is called for PropID of CR_PROP_CERTAIAURLS and propIndex of 0xFFFFFFFF. See section 3.2.1.4.3.2.42 for details on how this value is computed. Authority Information Access extension is specified in [RFC3280] section 4.2.2.1. 10. The CRL Distribution Point extension is added with the same value the CA returns when ICertRequestD2::GetCAProperty is called for PropID of CR_PROP_CERTCDPURLS and propIndex of 0xFFFFFFFF. See section 3.2.1.4.3.2.43 for details on how this value is computed. CRL Distribution Point extension is specified in [RFC3280] section 4.2.1.14. 11. The value for Valid From field is the date and time when the request for CA exchange certificate was received minus the value of the Config_CA_Clock_Skew_Minutes data. The Valid To field is set to one week later. Valid From and Valid To are specified in [RFC3280] section 4.1.2.5.
2021/09/07	In a new section 2.2.2.6.5, Null Signature, described the processing and conditions for using a null signature: Changed to: 2.2.2.6.5 Null Signature In CMS and CMC certificate request formats, the PKCS #10 request specified in the TaggedRequest field (see section 3.2.1.4.2.1.4.1.3) can contain only a null signature with the following signature field values: signatureAlgorithm (see section 4.2, [RFC2986]) would be set to a hashing algorithm such as "Sha256" (OID 2.16.840.1.101.3.4.2.1). signature (see section 4.2, [RFC2986]) contains only the unencrypted hash octets computed over the DER encoded certificationRequestInfo component (see section 4.2 of RFC2986) using the hash algorithm specified in the signatureAlgorithm field. Clients can send a PKCS #10 request with a null signature when the PKCS #10 request is specified in the TaggedRequest field in the CMS and CMC request formats as specified in sections 3.1.1.4.3.2.2, section 3.2.1.4.2.1.4.1.1, 3.1.1.4.3.1.3, 3.1.1.4.3.2.2, 3.1.1.4.3.3.3, and 3.1.1.4.3.6.1. If the signature validation fails in section 3.2.1.4.2.1.4.1.1, then the CA MUST also check for a null signature and return a nonzero error to the client only when null signature validation fails as well. CA MUST check for null signature only when the PKCS#10 request is specified in the CMS and CMC request formats as specified in sections 3.2.1.4.2.1.4.1.3, 3.2.1.4.2.1.4.2.2, 3.2.2.6.2.1.2.1.2, and 3.2.2.6.2.1.2.2.
2021/08/10	In Section 3.2.2.6.2.1.4.5.7 msPKI-Private-Key-Flag, removed extra leading zeroes in the following flags in the msPKI-Private-Key-Flag attribute to reduce hex value length from 9 to 8

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>digits in each stated value: 0x00002000 CT_FLAG_ATTEST_REQUIRED *,
0x00001000 CT_FLAG_ATTEST_PREFERRED *,
0x00004000 CT_FLAG_ATTESTATION_WITHOUT_POLICY *,
0x0000020 CT_FLAG_EK_TRUST_ON_USE *, 0x00000400 CT_FLAG_EK_VALIDATE_CERT *,
0x00000800 CT_FLAG_EK_VALIDATE_KEY *

Changed from:

<table>
<tr><th>Flag</th></tr>
<tr><td>0x00000001 CT_FLAG_REQUIRE_PRIVATE_KEY_ARCHIVAL</td></tr>
<tr><td>0x00000080
CT_FLAG_REQUIRE_SAME_KEY_RENEWAL</td></tr>
<tr><td>0x000002000
CT_FLAG_ATTEST_REQUIRED *</td></tr>
<tr><td>0x000001000
CT_FLAG_ATTEST_PREFERRED *</td></tr>
<tr><td>0x00000000
CT_FLAG_ATTEST_NONE *</td></tr>
<tr><td>0x000004000
CT_FLAG_ATTESTATION_WITHOUT_POLICY *</td></tr>
<tr><td>0x000000200
CT_FLAG_EK_TRUST_ON_USE *</td></tr>
<tr><td>0x000000400
CT_FLAG_EK_VALIDATE_CERT *</td></tr>
<tr><td>0x000000800
CT_FLAG_EK_VALIDATE_KEY *</td></tr>
</table>

Changed to:

<table>
<tr><th>Flag</th></tr>
<tr><td>0x00000001 CT_FLAG_REQUIRE_PRIVATE_KEY_ARCHIVAL</td></tr>
<tr><td>0x00000080
CT_FLAG_REQUIRE_SAME_KEY_RENEWAL</td></tr>
<tr><td>0x00002000
CT_FLAG_ATTEST_REQUIRED *</td></tr>
<tr><td>0x00001000
CT_FLAG_ATTEST_PREFERRED *</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description
	0x00000000 CT_FLAG_ATTEST_NONE * 0x00004000 CT_FLAG_ATTESTATION_WITHOUT_POLICY * 0x00000200 CT_FLAG_EK_TRUST_ON_USE * 0x00000400 CT_FLAG_EK_VALIDATE_CERT * 0x00000800 CT_FLAG_EK_VALIDATE_KEY *
2021/07/13	In Section 2.1 Transport, clarified how authentication level configuration impacts client CA connections. Changed from: Authentication level: SHOULD<6> be set to RPC_C_AUTHN_LEVEL_PKT_PRIVACY (6). <6> Section 2.1: "All Windows clients set the authentication level to RPC_C_AUTHN_LEVEL_PKT_PRIVACY. On the server side, if IF_ENFORCEENCRYPTICERTREQUEST or IF_ENFORCEENCRYPTICERTADMIN are set (see section 3.2.1.1.4) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level is not specified from the client, the CA refuses to establish a connection with the client by returning a nonzero error. By default, however, Windows CAs do not require the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level. That is, neither IF_ENFORCEENCRYPTICERTREQUEST nor IF_ENFORCEENCRYPTICERTADMIN are set." Changed to: "Authentication level: SHOULD be set to RPC_C_AUTHN_LEVEL_PKT_PRIVACY (0x06). Windows clients typically set the authentication level to RPC_C_AUTHN_LEVEL_PKT_PRIVACY (0x06).<6> If a CA server has IF_ENFORCEENCRYPTICERTREQUEST set (section 3.2.1.1.4) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY (0x06) authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified by the client for certificate-request operations, the CA MUST deny a connection to the client and return a non-zero error. 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>" <6> Windows XP sets the authentication level to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (0x05). <7> By default, CAs on Windows Server 2012 operating system and later have IF_ENFORCEENCRYPTICERTREQUEST and IF_ENFORCEENCRYPTICERTADMIN set.

*Date format: YYYY/MM/DD