[MS-CRTD]: Certificate Templates Structure

This topic lists the Errata found in [MS-CRTD] 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 V26.0 – 2021/06/25.

Errata Published*	Description
2022/06/28	In Section 2.4 flags Attribute: Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA.
2022/06/14	In Section 2.4 flags Attribute: Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA."
2022/05/10	Section 2.26 msPKI-Enrollment-Flag Attribute

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>Description: "Added the CT_FLAG_NO_SECURITY_EXTENSION (0x00080000) enrollment flag that instructs the CA to not include security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2) in the issued certificate. Also added operating system applicability [MSFT-CVE-2022-26931] for this security update."

Changed From:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00040000
CT_FLAG_SKIP_AUTO_RENEWAL</td><td>This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td></tr>
</table>

Changed To:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00040000
CT_FLAG_SKIP_AUTO_RENEWAL</td><td>This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td></tr>
<tr><td>0x00080000
CT_FLAG_NO_SECURITY_EXTENSION</td><td>This flag[34] instructs the CA to not include the security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2), as specified in [MS-WCCE] sections 2.2.2.7.7.4 and 3.2.2.6.2.1.4.5.9, in the issued certificate.</td></tr>
</table>

[34] This flag is supported by the operating systems specified in [MSFT-CVE-2022-26931], each with its related KB article download installed.</td></tr>
<tr><td>2021/07/27</td><td>In Section 2.27 msPKI-Private-Key-Flag Attribute, replaced normative reference [PKCS12] with [RFC7292].

Changed from:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00000010
CT_FLAG_EXPORTABLE_KEY</td><td>This flag instructs the client to allow other applications to copy the private key to a .pfx file, as specified in [PKCS12], at a later time.</td></tr>
</table>

Changed to:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00000010
CT_FLAG_EXPORTABLE_KEY</td><td>This flag instructs the client to allow other applications to copy the private key to a .pfx file, as specified in [RFC7292], at a later time.</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD