[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

Errata below are for Protocol Document Version V47.0 – 2021/10/06.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/09/03</td><td>
In Section 3.1.1.4.3.8 Certificate Requests in Pre-sign flow
Description: Added new top-level section for new Certificate requests in Pre-sign flow subsections that follow.

In Section 3.1.1.4.3.8.1 New Certificate Request for Pre-sign processing
Description: Added new section describing how a certificate request can be designated for Pre-sign certificate processing at the server. Provided behavior note indicating the OS support for Pre-sign certificate processing.

<pbn> Pre-sign certificate processing is supported by the operating systems specified in [MSKB-5017379] and [MSKB-5017381], each with its related KB article download installed.

In Section 3.1.1.4.3.8.2 New Certificate Request After Pre-sign Processing
Description: Added new section to describe processing at the client after receiving a response for a request with a Pre-sign flag.

Section 3.2.1.1.4 Configuration List
Description: Added a flag to the Configuration List table that determines whether Pre-sign processing is enabled at the server. Also added the dummy private key description to the table.

Changed from:
<table>
<tr><th>Data name</th><th>Data description</th></tr>
<tr><td>Config_CertificateTransparency_Info_Extension_Oid</td><td>A string value that the CA sets for the SignedCertificateTimestampList extension in the issued certificate. The default value is OID szOID_CT_CERT_SCTLIST (1.3.6.1.4.1.11129.2.4.2) [RFC6962].</td></tr>
</table>
Changed to:
<table>
<tr><th>Data name</th><th>Data description</th></tr>
<tr><td>Config_CertificateTransparency_Info_Extension_Oid</td><td>A string value that the CA sets for the SignedCertificateTimestampList extension in the issued certificate. The default value is OID szOID_CT_CERT_SCTLIST (1.3.6.1.4.1.11129.2.4.2) [RFC6962].</td></tr>
<tr><td>Config_PreSignCert_Enabled</td><td>A flag that indicates whether Certificate Pre-sign processing is enabled at the server. The default value is FALSE (not enabled).</td></tr>
<tr><td>Signing_Dummy_Private_Key</td><td>Contains the dummy private key generated with the same public key algorithm and key size as the</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>private key of the current CA signing certificate, as specified in section 3.2.1.1.2.</td></tr>
</table>
In Section 3.2.1.4.2.1.4.10 Processing Rules for Pre-sign Certificate Requests
Description: Added new top-level section for processing rules for Pre-sign certificate requests.
Section 3.2.1.4.2.1.4.10.1 New Certificate Request with Pre-sign flag
Description: Created new section to specify additional processing the CA MUST perform on Certificate Requests containing the Pre-sign flag.
Section 3.2.1.4.2.1.4.10.2 New Certificate Request without Pre-sign flag
Description: Created new section to specify certain processing that the Certificate Authority MUST perform on every new certificate request that does not have the Pre-sign flag set.
Section 3.2.1.4.3.1.1 dwFlags Packed Data Requirements
Description: Added a B bit to define the setting that indicates to the server that it MUST process the request as a new Pre-sign certificate request.
Changed from:
ExtendedFlags: This bit-field defines extended options for the server’s request processing.
<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>A</td><td>0</td><td>0</td></tr>
</table>
Where the bits are defined as follows:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>A</td><td>If this bit is set, the server MUST process the request as a new Certificate Transparency request, in accordance with section 3.2.1.4.2.1.4.3.1.</td></tr>
</table>
Changed to:
ExtendedFlags: This bit-field defines extended options for the server’s request processing.
<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>B</td><td>A</td><td>0</td><td>0</td></tr>
</table>
Where the bits are defined as follows:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>A</td><td>If this bit is set, the server MUST process the request as a new Certificate Transparency request, in accordance with section 3.2.1.4.2.1.4.3.1.</td></tr>
<tr><td>B</td><td>If this bit is set, the server MUST process the request as a new Pre-sign certificate request, in accordance with section 3.2.1.4.2.1.4.10.1.</td></tr>
</table>
</td></tr>
<tr><td>2022/08/09</td><td>In Section 3.2.1.1.1.2 Request Table Optional Data Elements:
Added 'Issuer_Name_Id' data element to the optional data elements request table.
Changed from:</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>".....

▪ Request_Endorsement_Key_Hash
▪ Request_Endorsement_Certificate_Hash"

Changed to:
".....
▪ Request_Endorsement_Key_Hash
▪ Request_Endorsement_Certificate_Hash
▪ Issuer_Name_Id"

In Section 3.2.1.4.2.1.1.4 Storing Request Parameters in the Request Table
Added and defined the Issuer_Name_Id data element to the request parameters in the Request Table.
Changed from:

<table><tr><th>Column name</th><th>Processing rules</th></tr><tr><td>....</td><td>....</td></tr><tr><td>Request_Endorsement_Certificate_Hash</td><td>The CA MUST store the SHA2 hash of the trust module certificate used for attestation
from the certificate request as a hexadecimal string with no spaces.</td></tr></table>
Changed to:
<table><tr><th>Column name</th><th>Processing rules</th></tr><tr><td>....</td><td>....</td></tr><tr><td>Request_Endorsement_Certificate_Hash</td><td>The CA MUST store the SHA2 hash of the trust module certificate used for attestation from the certificate request as a hexadecimal string with no spaces.</td></tr><tr><td>Issuer_Name_Id</td><td>The CA MUST store the version information (section 3.2.1.4.3.2.39) of the current CA signing certificate as stored in the Signing_Cert_Certificate datum.</td></tr></table>

In Section 3.2.1.4.3.2.16, PropID = 0x00000010 (CR_PROP_CAXCHGCERTCHAIN) "CA Exchange Certificate Chain",
"The CA MUST follow the specified processing rule updates to process a client's request for the CA exchange certificate, its complete chain, and all relevant CRLs; which includes updated instructions for constructing a signed CMS message."

Changed from:

▪ If PropIndex parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client.
▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15.
▪ Construct a signed CMS message with the following fields:
  ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData).</td></tr>
</table>

Errata Published*	Description
	▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements: ▪ version: See section [RFC3852], section 5.1. ▪ digestAlgorithms: Same digest algorithm as was used to sign current CA's certificate stored in Signing_Cert_Certificate datum. ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the eContentType set to the OID szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the eContent field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum. ▪ certificates: Contains CA's certificate stored in the Signing_Cert_Certificate datum and its parent certificates. To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1. Changed to: ▪ If PropIndex parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. ▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. ▪ Retrieve the Issuer_Name_Id from the request database by finding the row with the Certificate_Hash equal to the Current_CA_Exchange_Cert hash value. ▪ Find the CA signing certificate corresponding to the Current_CA_Exchange_Cert by looking for an entry in the Signing_Cert table with the certificate index (section 3.2.1.4.3.2.39) matching the lower 16 bits of the Issuer_Name_Id value retrieved in step 3 of this procedure.91 ▪ Construct a signed CMS message with the following fields: ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData). ▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements: ▪ version: See section [RFC3852], section 5.1. ▪ digestAlgorithms: Same digest algorithm as was used by the CA signing certificate retrieved in step 4 of this procedure, to sign the Current_CA_Exchange_Cert. ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the eContentType set to the OID szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the eContent field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum. ▪ certificates: Contains CA's certificate (1), as retrieved in step 4 of this procedure, and its parent certificates (1). To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1. [91] In some cases, the CA signing certificate with "certificate index" zero could be returned instead of the actual signing certificate that issued Current_CA_Exchange_Cert. This behavior can be automatically fixed by restarting certificate service whenever a new exchange certificate is created. In Section 3.2.1.4.3.2.33 PropID = 0x00000021 (CR_PROP_CAXCHGCERTCRLCHAIN) "CA Exchange Certificate Chain and CRL" "The CA MUST follow the specified processing rule updates to process a client's request for the CA exchange certificate, its complete chain, and all relevant CRLs; which includes updated instructions for constructing a signed CMS message." Changed from: ▪ ▪ If *PropIndex* parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. ▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. ▪ Construct a signed **CMS** message with the following fields: ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData).

Errata Published*	Description
	▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements: ▪ version: See section [RFC3852], section 5.1. ▪ digestAlgorithms: Same digest algorithm as was used to sign current CA's **certificate** stored in Signing_Cert_Certificate datum. ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the **eContentType** set to the **OID** szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the **eContent** field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum. ▪ certificates: Contains CA's certificate stored in the Signing_Cert_Certificate datum and its parent certificates. To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1. Changed to: ▪ If *PropIndex* parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. ▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. ▪ Retrieve the **Issuer_Name_Id** from the request database by finding the row with the Certificate_Hash equal to the Current_CA_Exchange_Cert hash value. ▪ Find the CA signing certificate corresponding to the Current_CA_Exchange_Cert by looking for an entry in the Signing_Cert table with the **certificate index** (section 3.2.1.4.3.2.39) matching the lower 16 bits of the **Issuer_Name_Id** value retrieved in step 3 of this procedure.[95] ▪ Construct a signed **CMS** message with the following fields: ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData). ▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements: ▪ version: See section [RFC3852], section 5.1. ▪ digestAlgorithms: Same digest algorithm as was used by the CA signing certificate retrieved in step 4 of this procedure, to sign the Current_CA_Exchange_Cert. ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the **eContentType** set to the **OID** szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the **eContent** field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum. ▪ certificates: Contains **CA's certificate (1)**, as retrieved in step 4 of this procedure, and its parent **certificates (1)**. ~~excluding the **root certificate**~~. To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1. [95] In some cases, the CA signing certificate with "certificate index" zero could be returned instead of the actual signing certificate that issued Current_CA_Exchange_Cert. This behavior can be automatically fixed by restarting certificate service whenever a new exchange certificate is created. In Section 3.2.1.4.3.2.39 PropID = 0x00000027 (CR_PROP_CACERTVERSION) "CA Signing Certificates Revisions" Bolded "version information" Changed from: The CA MUST return the array in a CERTTRANSBLOB (section 2.2.2.2) structure. Each ULONG value in the returned array MUST contain version information for a signing certificate in **little-endian** format. Changed to: The CA MUST return the array in a CERTTRANSBLOB (section 2.2.2.2) structure. Each ULONG value in the returned array MUST contain **version information** for a signing certificate in **little-endian** format.

Errata Published*	Description
2022/07/26	In Section 3.2.1.4.3.2.16 PropID = 0x00000010 (CR_PROP_CAXCHGCERTCHAIN) "CA Exchange Certificate Chain": Removed the statement 'excluding the root certificate' as actual server behavior does not exclude the root certificate in a CMS message. Changed from: "The client has requested the CA exchange certificate and its complete chain. The CA MUST follow these processing rules to process the client's request: 1. If PropIndex parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. 2. Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. 3. Construct a signed CMS message with the following fields: ▪ ContentType: ..... ▪ Content: ..... ▪ version: ..... ▪ digestAlgorithms: ..... ▪ encapContentInfo: ..... ▪ certificates: Contains CA's certificate (1) stored in the Signing_Cert_Certificate datum and its parent certificates (1) excluding the root certificate." Changed to: "The client has requested the CA exchange certificate and its complete chain. The CA MUST follow these processing rules to process the client's request: 1. If PropIndex parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. 2. Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. 3. Construct a signed CMS message with the following fields: ▪ ContentType: ..... ▪ Content: ..... ▪ version: ..... ▪ digestAlgorithms: ..... ▪ encapContentInfo: ..... ▪ certificates: Contains CA's certificate (1) stored in the Signing_Cert_Certificate datum and its parent certificates (1)."~~excluding the root certificate~~
2022/06/28	In Section 3.2.2.6.2.1.4.4.1 Flags Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB

Errata Published*	Description
	If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1."
2022/06/14	In Section 3.2.2.6.2.1.4.4.1 Flags Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1."
2022/05/10	Section 2.2.2.7.7.4 szOID_NTDS_CA_SECURITY_EXT Description: "Created new topic to define the szOID_NTDS_CA_SECURITY_EXT security extension for enhanced security protections. Also added operating system applicability [MSFT-CVE-2022-26931] for this security update." Changed From: "" Changed To: "OID = 1.3.6.1.4.1.311.25.2. Internal Name: szOID_NTDS_CA_SECURITY_EXT[11]. Description: Contains objectSid of the Active Directory object whose information is being used to construct the subject information of an issued certificate. The CA MUST consider this extension from request attributes only when the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is set on the corresponding certificate template object. See section 3.2.2.6.2.1.4.5.9 for specifics on how the CA processes this extension. This extension value MUST be DER-encoded ([X690]). The critical field for this extension SHOULD be set to FALSE. szOID_NTDS_OBJECTSID: 1.3.6.1.4.1.311.25.2.1. Format: The following is the ASN.1 format ([X690]) for this attribute. OtherName ::= SEQUENCE { type-id szOID_NTDS_OBJECTSID,

Errata Published*	Description
	value octet string} [11]This security extension is supported by the operating systems specified in [MSFT-CVE-2022-26931], each with its related KB article download installed." Section 2.3 Directory Service Schema Elements Description: Added 'objectSid' descriptor to the Computer class and User class lists in the Class/Attribute table. Changed From: "Computer cn distinguishedName dNSHostName objectGuid Changed To: "Computer cn distinguishedName dNSHostName objectGuid objectSid Changed From: "User cn distinguishedName objectGuid mail userCertificate userPrincipalName" Changed To: "User cn

Errata Published*	Description
	distinguishedName objectGuid objectSid mail userCertificate userPrincipalName" Section 3.2.2.1.2.1 Search Requests Description: "Added the attribute 'objectSid' to the list of attributes that the CA should use for an LDAP SearchRequest message." Changed From: • mail • objectGUID • userPrincipalName Changed To: • mail • objectGUID • objectSid • userPrincipalName Section 3.2.2.1.3.1 Search Requests Description: Added the attribute 'objectSid' to the list of attributes that the CA should use for an LDAP SearchRequest message. Changed From: • mail • objectGUID • userPrincipalName Changed To: • mail • objectGUID • objectSid • userPrincipalName Section 3.2.2.6.2.1.4.5.9 msPKI-Certificate-Name-Flag

Errata Published*	Description
	Description: "Enhanced the processing instructions to specify that the CA must add the new szOID_NTDS_CA_SECURITY_EXT security extension to the issued certificate when the CT_FLAG_NO_SECURITY_EXTENSION flag is not set; and to do the same when the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is set and CT_FLAG_NO_SECURITY_EXTENSION is not set." Changed From: "4. If CT_FLAG_SUBJECT_REQUIRE_EMAIL is set, the CA MUST set the Subject field of the issued certificate (1) as a DN (1) whose E component value is obtained from the value of the mail attribute (1) of the requestor's user object in the working directory (1). For this, the CA MUST invoke the processing rules in section 3.2.2.1.2 with input parameter EndEntityDistinguishedName set equal to the requester's user object distinguished name (1) and retrieve the mailattribute (1) from the returned EndEntityAttributes output parameter." Changed To: "4. If CT_FLAG_SUBJECT_REQUIRE_EMAIL is set, the CA MUST set the Subject field of the issued certificate (1) as a DN (1) whose E component value is obtained from the value of the mail attribute (1) of the requestor's user object in the working directory (1). For this, the CA MUST invoke the processing rules in section 3.2.2.1.2 with input parameter EndEntityDistinguishedName set equal to the requester's user object distinguished name (1) and retrieve the mail attribute (1) from the returned EndEntityAttributes output parameter. 5. If the CT_FLAG_NO_SECURITY_EXTENSION flag is not set, the CA MUST add the szOID_NTDS_CA_SECURITY_EXT security extension, as specified in section 2.2.2.7.7.4, to the issued certificate with the value set to the string format of the objectSid attribute obtained from the requestor’s user object in the working directory. For this, the CA MUST invoke the processing rules in section 3.2.2.1.2, with input parameter EndEntityDistinguishedName set equal to the requester's user object distinguished name, and retrieve the objectSid attribute from the returned EndEntityAttributes output parameter." Changed From: "3. If CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set, then the CA MUST use the subject and subject alternative name information provided in the certificate (1) request. If no subject name is provided in the request, the CA MUST reject the request." Changed To: "3. If CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set, then the CA MUST use the subject and subject alternative name information provided in the certificate (1) request. If no subject name is provided in the request, the CA MUST reject the request. 4. If CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set and CT_FLAG_NO_SECURITY_EXTENSION is not set, then the CA MUST add the szOID_NTDS_CA_SECURITY_EXT security extension (section 2.2.2.7.7.4) to the issued certificate, that is, if it is provided as an extension in the request."
2022/05/10	In Section 3.2.2.6.2.1.4.5.6 msPKI-Enrollment-Flag

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
Description: Updated client processing instructions to indicate that the CA MUST also enforce the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag when the conditions specified in new section 3.2.2.6.2.1.4.8 are met.
Also revised client processing instructions to specify the conditions under which the subject alternative name (SAN) extension MUST be added to the new certificate being issued.

Changed From:

<table>
<tr><th>Flag</th><th>Client processing</th></tr>
<tr><td>0x00000040
CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT</td><td>The CA MUST enforce this flag only for certificate renewal requests.</td></tr>
</table>
If this flag is set in the template:
● The CA MUST NOT enforce the signature processing rules specified for the following attributes: msPKI-RA-Signature, msPKI-RA-Policies, and msPKI-Application-Policy.
● The CA MUST ignore the CT_FLAG_PEND_ALL_REQUESTS flag.

Changed To:

<table>
<tr><th>Flag</th><th>Client processing</th></tr>
<tr><td>0x00000040
CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT</td><td>The CA MUST enforce this flag only for certificate renewal requests and only when the conditions specified in section 3.2.2.6.2.1.4.8 are met.</td></tr>
</table>
If this flag is set in the template:
● The CA MUST NOT enforce the signature processing rules specified for the following attributes: msPKI-RA-Signature, msPKI-RA-Policies, and msPKI-Application-Policy.
● The CA MUST ignore the CT_FLAG_PEND_ALL_REQUESTS flag.
● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set and the old certificate, based on which reenrollment is occurring, contains the subject alternative name (SAN) extension, then the same SAN extension MUST be added to the new certificate being issued.

In Section 3.2.2.6.2.1.4.8 CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT Enforcement Conditions
Description: Created new topic to specify the conditions that are required to be met before enforcing the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag, that is, if the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag is set in the template.

Changed From:
""

Changed To:
"If the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag is set in the template, the CA MUST verify that all the following conditions are satisfied before enforcing the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag:
</td></tr>
</table>

Errata Published*	Description
	● The old certificate, based on which the reenrollment is occurring, MUST contain the Certificate Template OID extension, as specified in section 2.2.2.7.7.2. ● The TemplateID from the old certificate MUST match the TemplateID of the current template. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is set, then the CA MUST verify that subject name is supplied in the request, and that it matches with the subject of the old certificate. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set, then the old certificate MUST contain the subject alternative name (SubjectAltName) extension. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set, then the SubjectAltName extension from the old certificate MUST contain either an rfc822Name or otherName with OID szOID_NT_PRINCIPAL_NAME (1.3.6.1.4.1.311.20.2.3). ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set and the SubjectAltName contains otherName, then the value of otherName MUST match the value of the userPrincipalName attribute from the requestor's user object in the working directory. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set, and the SubjectAltName contains the rfc822Name, then the value of rfc822Name MUST match the value of the mail attribute from the requestor's user object in the working directory."

*Date format: YYYY/MM/DD