[MS-CRTD]:
Certificate Templates Structure

Revision Summary

Date	Revision History	Revision Class	Comments
03/14/2007	1.0	Major	Updated and revised the technical content.
04/10/2007	1.1	Minor	Updated the technical content.
05/18/2007	2.0	Major	New format; Reorganized as a structure; Moved content to MS-WCCE.
06/08/2007	2.0.1	Editorial	Revised and edited the technical content.
07/10/2007	2.0.2	Editorial	Revised and edited the technical content.
08/17/2007	2.0.3	Editorial	Revised and edited the technical content.
09/21/2007	2.1	Minor	Updated the technical content.
10/26/2007	3.0	Major	Updated and revised the technical content.
01/25/2008	3.0.1	Editorial	Revised and edited the technical content.
03/14/2008	4.0	Major	Updated and revised the technical content.
06/20/2008	5.0	Major	Updated and revised the technical content.
07/25/2008	5.0.1	Editorial	Revised and edited the technical content.
08/29/2008	5.1	Minor	Updated the technical content.
10/24/2008	5.2	Minor	Updated the technical content.
12/05/2008	5.2.1	Editorial	Editorial Update.
01/16/2009	6.0	Major	Updated and revised the technical content.
02/27/2009	7.0	Major	Updated and revised the technical content.
04/10/2009	8.0	Major	Updated and revised the technical content.
05/22/2009	8.1	Minor	Updated the technical content.
07/02/2009	8.1.1	Editorial	Revised and edited the technical content.
08/14/2009	9.0	Major	Updated and revised the technical content.
09/25/2009	10.0	Major	Updated and revised the technical content.
11/06/2009	11.0	Major	Updated and revised the technical content.
12/18/2009	11.0.1	Editorial	Revised and edited the technical content.
01/29/2010	12.0	Major	Updated and revised the technical content.
03/12/2010	13.0	Major	Updated and revised the technical content.

Date	Revision History	Revision Class	Comments
04/23/2010	13.0.1	Editorial	Revised and edited the technical content.
06/04/2010	14.0	Major	Updated and revised the technical content.
07/16/2010	15.0	Major	Significantly changed the technical content.
08/27/2010	15.1	Minor	Clarified the meaning of the technical content.
10/08/2010	15.1	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	16.0	Major	Significantly changed the technical content.
01/07/2011	16.0	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	16.0	No change	No changes to the meaning, language, or formatting of the technical content.
03/25/2011	16.0	No change	No changes to the meaning, language, or formatting of the technical content.
05/06/2011	17.0	Major	Significantly changed the technical content.
06/17/2011	17.1	Minor	Clarified the meaning of the technical content.

Contents

1 Introduction

This document specifies the syntax and interpretation of **certificate templates**. While not strictly a protocol, the templates form the basis of **certificate** management for the Windows Client Certificate Enrollment Protocol. This specification consists of **attributes** that are accessed by using **Lightweight Directory Access Protocol (LDAP)**, as specified in [RFC2251]. These attributes allow clients to define the behavior of a **certificate authority (CA)** when processing certificate requests.

Familiarity with the Windows Client Certificate Enrollment Protocol Specification is required for a complete understanding of this specification.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

access control entry (ACE)
access control list (ACL)
Active Directory
Active Directory Domain Services (AD DS)
attribute
certificate
certification authority (CA)
certificate revocation list (CRL)
certificate template
certification
common name (CN)
cryptographic service provider (CSP)
digital signature
directory
discretionary access control list (DACL)
distinguished name (DN)
Distributed Component Object Model (DCOM)
domain
domain controller (DC)
fully qualified domain name (FQDN)
Domain Name System (DNS)
encryption
enroll/enrollment
enrollment permissions
enterprise certificate authority
key
key archival
key recovery agent (KRA)
Lightweight Directory Access Protocol (LDAP)
NetBIOS name
object
object identifier (OID)
objectGuid
private key
public key
public key algorithm
public key infrastructure (PKI)

registration authority (RA)
revocation
security descriptor
security identifier (SID)
Secure/Multipurpose Internet Mail Extensions (S/MIME)
symmetric algorithm
symmetric key

The following terms are defined in [MS-WCCE]:

certificate renewal request
enroll on behalf of (EOBO)
renewed certificate

The following terms are specific to this document:

asymmetric algorithm: A synonym for **public key algorithm**. For an introduction to these concepts and related terminology, see [PUBKEY] and [RSAFAQ]. See also **public key algorithm**.

autoenrollment: An automated process that performs **certificate enrollment** and renewal. For more information about autoenrollment behavior, see [MS-CAESO].

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as specified in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

References to Microsoft Open Specification documents do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-ADA1] Microsoft Corporation, "Active Directory Schema Attributes A-L".

[MS-ADA2] Microsoft Corporation, "Active Directory Schema Attributes M".

[MS-ADA3] Microsoft Corporation, "Active Directory Schema Attributes N-Z".

[MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification".

[MS-DTYP] Microsoft Corporation, "Windows Data Types".

[MS-WCCE] Microsoft Corporation, "Windows Client Certificate Enrollment Protocol Specification".

[PKCS12] RSA Laboratories, "PKCS #12: Personal Information Exchange Syntax Standard", PKCS #12, Version 1.0, http://www.rsa.com/rsalabs/node.asp?id=2138

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[RFC2251] Wahl, M., Howes, T., and Kille, S., "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997, http://www.ietf.org/rfc/rfc2251.txt

[RFC2560] Myers, M., Ankney, R., Malpani, A., et al., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999, http://www.ietf.org/rfc/rfc2560.txt

[RFC3280] Housley, R., Polk, W., Ford, W., and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002, http://www.ietf.org/rfc/rfc3280.txt

[RFC4262] Santesson, S., "X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities", RFC 4262, December 2005, http://www.ietf.org/rfc/rfc4262.txt

[RFC4523] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates", RFC 4523, June 2006, http://www.ietf.org/rfc/rfc4523.txt

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary".

[MSDN-KEY] Microsoft Corporation, "CERT_KEY_CONTEXT", http://msdn.microsoft.com/en-us/library/aa377205.aspx

[MSFT-AUTOENROLLMENT] Microsoft Corporation, "Certificate Autoenrollment in Windows Server 2003", April 2003, http://technet.microsoft.com/en-us/library/cc778954.aspx

If you have any trouble finding [MSFT-AUTOENROLLMENT], please check here.

[MSFT-CROSSCERT] Microsoft Corporation, "Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003", http://technet.microsoft.com/en-us/library/cc787237.aspx

[PUBKEY] RSA Laboratories, "Crypto FAQ: Chapter 2 Cryptography: 2.1 Cryptographic Tools: 2.1.1 What Is Public-Key Cryptography?", http://www.rsa.com/rsalabs/node.asp?id=2165

[RSAFAQ] RSA Laboratories, "Frequently Asked Questions About Today's Cryptography, Version 4.1", May 2000, http://www.rsa.com/rsalabs/faq/files/rsalabs_faq41.pdf

1.3 Overview

This specification defines the syntax and interpretation of certificate templates. Certificate templates are data structures that specify how certificate requests and certificates are constructed and issued as documented in [MS-WCCE].

Certificate templates are stored as objects in **Active Directory**.

The Windows Client Certificate Enrollment Protocol, as specified in [MS-WCCE], is documented separately. Windows Client Certificate Enrollment Protocol is the protocol by which clients request certificates from the CA and by which any issued certificates are returned to the client. Certificate templates can be thought of as playing a part in that protocol because of their abilities to constrain behaviors of the CAs; otherwise, interactions between templates and the Windows Client Certificate Enrollment Protocol are not limited. A client in the Windows Client Certificate Enrollment Protocol can specify a template for the CA to use in building a certificate, but in that context, a template is

just another complex data structure that is passed as a parameter to a Windows Client Certificate Enrollment Protocol method.

1.4 Relationship to Other Protocols and Other Structures

When used, certificate templates control the behavior of the CA that is accessed by the Windows Client Certificate Enrollment Protocol, as specified in [MS-WCCE], by specifying **enrollment** policies. If templates are not used, the CA behavior and the conduct of the Windows Client Certificate Enrollment Protocol are unconstrained. LDAP, as specified in [MS-ADTS], is the protocol that retrieves the certificate templates. The process of storing templates in the **directory** is an implementation-specific detail and is not specified in this document.

1.5 Applicability Statement

The data structure specified in this protocol specification is applicable to an environment that enables clients to interact with a CA to enroll or manage X.509 certificates. Certificate templates are only appropriate in an Active Directory **domain** configuration, as specified in [MS-ADTS]. The protocol (carrying templates) is only used to communicate from computers in the domain to a **DC** for the domain.

1.6 Versioning and Localization

To determine the certificate template schema version, clients and servers read the msPKI-Template-Schema-Version attribute on the certificate template **object**. For more information, see section 2.16.<1>

1.7 Vendor-Extensible Fields

None.

2 Structures

The PKI-Certificate-Template is the Active Directory schema class that is used for storing template information and attributes. The PKI-Certificate-Template is a container in which all subsequent properties are contained. All attributes defined later in this section are identified by their ldapDisplayName and are case-insensitive.

2.1 cn Attribute

The cn attribute is the **common name (CN)** of the certificate template.<2> For schema details of this attribute, see [MS-ADA1] section 2.110.

2.2 displayName Attribute

The displayName attribute is the display name of a certificate template.<3> For schema details of this attribute, see [MS-ADA1] section 2.175.

2.3 distinguishedName Attribute

The distinguishedName attribute is the **distinguished name (DN)** of the certificate template.<4> For schema details of this attribute, see [MS-ADA1] section 2.177.

2.4 flags Attribute

The flags attribute is the general-enrollment flags attribute. These flags are communicated as an integer value of this attribute.<5> The attribute value can be 0, or it can consist of a bitwise OR of flags from the following table.

Flag	Meaning
0x00000020 CT_FLAG_AUTO_ENROLLMENT	This flag is the same as CT_FLAG_AUTO_ENROLLMENT specified in section 2.26.
0x00000040 CT_FLAG_MACHINE_TYPE	This flag indicates that this certificate template is for an end entity that represents a machine.
0x00000080 CT_FLAG_IS_CA	This flag indicates a certificate request for a CA certificate.
0x00000200 CT_FLAG_ADD_TEMPLATE_NAME	This flag indicates that a certificate based on this section needs to include a template name certificate extension.
0x00000800 CT_FLAG_IS_CROSS_CA	This flag indicates a certificate request for cross-certifying a certificate. Processing rules for this flag are specified in [MS-WCCE] sections 3.1.2.4.2.2.1.1 and 3.2.2.6.2.1.4.4.1.
0x00010000 CT_FLAG_IS_DEFAULT	This flag indicates that the template SHOULD not be modified in any way; it is not used by the client or server in the Windows Client Certificate Enrollment Protocol.
0x00020000 CT_FLAG_IS_MODIFIED	This flag indicates that the template MAY be modified if required; it is not used by the client or server in the Windows Client Certificate Enrollment Protocol.
0x00000400	This flag indicates that the record of a certificate request for a

Flag	Meaning
CT_FLAG_DONOTPERSISTINDB	certificate that is issued need not be persisted by the CA.<6>
0x00000002 CT_FLAG_ADD_EMAIL	Reserved. All protocols MUST ignore this flag.
0x00000008 CT_FLAG_PUBLISH_TO_DS	Reserved. All protocols MUST ignore this flag.
0x00000010 CT_FLAG_EXPORTABLE_KEY	Reserved. All protocols MUST ignore this flag.

For schema details of this attribute, see [MS-ADA1] section 2.231.

2.5 ntSecurityDescriptor Attribute

The ntSecurityDescriptor attribute is a **security descriptor** as specified in [MS-DTYP] section 2.4.6.<7> The **discretionary access control list (DACL)** field of the security descriptor is an access control list (ACL) (as specified in [MS-DTYP] section 2.4.5) that specifies the permission set for this certificate template. Each access control entry (ACE) (as specified in [MS-DTYP] section 2.4.4) in the ACL specifies access rights.

The data structure in this attribute supports all types of ACE. However, the Windows Client Certificate Enrollment Protocol uses only two predefined permissions: Enroll and AutoEnroll. The AutoEnroll permission instructs the Microsoft Windows® autoenrollment client to enroll for that template automatically.

2.5.1 Determining Enrollment Permission of an End Entity for a Template

Following are the processing rules to determine enrollment for end entities on a certificate template. The protocol behavior for these permissions is specified in [MS-WCCE] section 3.2.2.6.2.1.4.3 "Verify End Entity Permissions".

Input Parameters:

- **Template_ntSecurityDescriptor**: The ntSecurityDescriptor attribute of the input template.
- **Requester_SID**: Contains the **SID** ([MS-DTYP] section 2.4.2) of the end entity.

Output Parameter: This parameter can be either True or False.

Processing Rules:

An entity (Active Directory user or group) has **enrollment permission** and output parameter is set to TRUE if the DACL of the security descriptor that is stored in input parameter **Template_ntSecurityDescriptor** contains an ACE that satisfies either one of the following sets of characteristics:

It has an object allowed ACE (see [MS-DTYP] section 2.4.4.3) that satisfies all of the following conditions:

- The **Requester_SID** input parameter is identical to the SID associated with this ACE.

- The **AceType** field of the **ACE_HEADER** structure (as specified in [MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_OBJECT_ACE. This implies that it is an ACCESS_ALLOWED_OBJECT_ACE structure, as specified in [MS-DTYP] section 2.4.4.3.
- The **Mask** field of the ACCESS_ALLOWED_OBJECT_ACE structure MUST have the bits set as specified by the X in the following diagram.

10	1	2	3	4	5	6	7	20	1	2	3	4	5	6	7	30	1	2	3	4	5	6	7	40	1	2	3	4	5	6	7
								X																							

- The **ObjectType** field of the ACCESS_ALLOWED_OBJECT_ACE structure MUST be identical to the Enroll GUID in the following table. GUID is defined in [MS-DTYP] section 2.3.2.

Or,

It has an allowed ACE (see [MS-DTYP] section 2.4.4.2) that satisfies all the following conditions:

- The Requester SID input parameter is identical to the SID associated with this ACE.
- The **AceType** field of the **ACE_HEADER** structure (as specified in [MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE. This implies that it is an **ACCESS_ALLOWED_ACE** structure, as specified in [MS-DTYP] section 2.4.4.2.
- The **Mask** field of the **ACCESS_ALLOWED_ACE** structure MUST have the bits set as specified by the X in the following diagram.

10	1	2	3	4	5	6	7	20	1	2	3	4	5	6	7	30	1	2	3	4	5	6	7	40	1	2	3	4	5	6	7
												X																			

An entity is denied enrollment permissions if the DACL of the security descriptor that is stored in input parameter **Template_ntSecurityDescriptor** has the same **ACE** as previously described, except that the **AceType** field is set to ACCESS_DENIED_OBJECT_ACE_TYPE.

2.5.2 Determining Autoenrollment Permission of an End Entity for a Template

Following are the processing rules to determine enrollment for end entities on a certificate template.

Input Parameters:

- **Template_ntSecurityDescriptor**: The ntSecurityDescriptor attribute of the input template.
- **Requester_SID**: Contains the SID ([MS-DTYP] section 2.4.2) of the end entity.

Output Parameter: This parameter can be either True or False.

Processing Rules:

An entity (Active Directory user or group) has AutoEnroll permission and output parameter is set to TRUE if the DACL of the input parameter **Template_ntSecurityDescriptor** contains an ACE that satisfies either one of the following sets of characteristics:

It has an object allowed ACE **that satisfies all of the following conditions:**

- The **Requester_SID** input parameter is identical to the SID associated with this ACE.
- The **AceType** field of the **ACE_HEADER** structure (as specified in [MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_OBJECT_ACE_TYPE. This implies that it is an **ACCESS_ALLOWED_OBJECT_ACE** structure, as specified in [MS-DTYP] section 2.4.4.3.
- The **Mask** field of the **ACCESS_ALLOWED_OBJECT_ACE** structure MUST have the bits set as specified by the X in the following diagram.

10	1	2	3	4	5	6	7	20	1	2	3	4	5	6	7	30	1	2	3	4	5	6	7	40	1	2	3	4	5	6	7
								X																							

- The **ObjectType** field of the **ACCESS_ALLOWED_OBJECT_ACE** structure MUST be identical to the AutoEnroll GUID in the following table.

Or,

It has an allowed ACE that satisfies all the following conditions:

- The **Requester_SID** input parameter is identical to the SID associated with this ACE.
- The **AceType** field of the **ACE_HEADER** structure (as specified in [MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE. This implies that it is an **ACCESS_ALLOWED_ACE** structure, as specified in [MS-DTYP] section 2.4.4.2.
- The **Mask** field of the **ACCESS_ALLOWED_ACE** structure MUST have the bits set as specified by the X in the following diagram.

10	1	2	3	4	5	6	7	20	1	2	3	4	5	6	7	30	1	2	3	4	5	6	7	40	1	2	3	4	5	6	7
												X																			

An entity is denied AutoEnroll permissions if the DACL of the security descriptor that is stored in input parameter **Template_ntSecurityDescriptor** has the same ACE as previously described except that the **AceType** field is set to ACCESS_DENIED_OBJECT_ACE_TYPE.

The following table lists the predefined GUIDs for the **ObjectType** field of these ACCESS_ALLOWED_OBJECT_ACE structures.

Rights and GUID	Permission
CR; 0e10c968-78fb-11d2-90d4-00c04f79dc55	Enroll
CR; a05b8cc2-17bc-4802-a710-e7c15ab866a2	AutoEnroll

For schema details of this attribute, see [MS-ADA3] section 2.36.

2.5.3 Sets of Permission Bits

If an administrator wants to set permissions for a certificate template, the combined effect of three sets of permission bits can be meaningful: Read, Write, and Full Control.

- Read permission

  An entity (Active Directory user or group) has Read permission if the DACL of the security descriptor that is stored in the ntSecurityDescriptor attribute contains an ACE that has the following characteristics:

  - The entity has a SID (as specified in [MS-DTYP] section 2.4.2) that is identical to the SID associated with this ACE.
  - The **AceType** field of the **ACE_HEADER** structure (as specified in [MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE.
  - The **Mask** field of the **ACCESS_ALLOWED_ACE_TYPE** structure MUST have the following bits set:
    - RC as specified in [MS-DTYP] section 2.4.3
    - LC as specified in [MS-ADTS] section 5.1.3.2
    - RP as specified in [MS-ADTS] section 5.1.3.2

- Write permission

  An entity (Active Directory user or group) has Write permission if the DACL of the security descriptor that is stored in the ntSecurityDescriptor attribute contains an ACE that has the following characteristics:

  - The entity has a SID (as specified in [MS-DTYP] section 2.4.2) that is identical to the SID associated with this ACE.
  - The **AceType** field of the **ACE_HEADER** structure (as specified in [MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE.
  - The **Mask** field of the **ACCESS_ALLOWED_ACE_TYPE** structure MUST have the following bits set:
    - WO as specified in [MS-DTYP] section 2.4.3
    - WD as specified in [MS-DTYP] section 2.4.3
    - WP as specified in [MS-ADTS] section 5.1.3.2

- Full Control permission

  An entity (Active Directory user or group) has Full Control permission if the DACL of the security descriptor that is stored in this attribute contains an ACE that has the following characteristics:

  - The entity has a SID (as specified in [MS-DTYP] section 2.4.2) that is identical to the SID associated with this ACE.

- The **AceType** field of the **ACE_HEADER** structure (as specified in [MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE.
- The **Mask** field of the **ACCESS_ALLOWED_ACE_TYPE** structure MUST have the following bits set:
  - RC as specified in [MS-DTYP] section 2.4.3
  - WO as specified in [MS-DTYP] section 2.4.3
  - WD as specified in [MS-DTYP] section 2.4.3
  - DE as specified in [MS-DTYP] section 2.4.3
  - CC as specified in [MS-ADTS] section 5.1.3.2
  - DC as specified in [MS-ADTS] section 5.1.3.2
  - LC as specified in [MS-ADTS] section 5.1.3.2
  - VW as specified in [MS-ADTS] section 5.1.3.2
  - RP as specified in [MS-ADTS] section 5.1.3.2
  - WP as specified in [MS-ADTS] section 5.1.3.2
  - DT as specified in [MS-ADTS] section 5.1.3.2
  - LO as specified in [MS-ADTS] section 5.1.3.2
  - CR as specified in [MS-ADTS] section 5.1.3.2

2.6 revision Attribute

The revision attribute is the major version of the template.<8>For more information, see [MS-CAESO]. For schema details of this attribute, see [MS-ADA3] section 2.198.

2.7 pKICriticalExtensions Attribute

The pKICriticalExtensions attribute is a list of **OIDs** that identify extensions that MUST have critical flags enabled, if present, in an issued certificate. For more information about critical extensions, see [RFC3280] section 4.2.<9> For schema details of this attribute, see [MS-ADA3] section 2.94.

2.8 pKIDefaultCSPs Attribute

The pKIDefaultCSPs attribute is a list of **cryptographic service providers (CSPs)** that are used to create the **private key** and **public key**.<10>

Each list element MUST be in the following format:

intNum, <strCSP>

where intNum is an integer that specifies the priority order in which the system administrator wants the client to use the CSPs listed, and <strCSP> is the CSP name.

The implication of this list of CSPs is that any one of the listed CSPs is acceptable to the system administrator but that a preference is indicated by the value of intNum if a client has more than one

of those CSPs. The security implications of violating this expressed priority are up to the system administrator who established that priority ranking to determine and to document.

For schema details of this attribute, see section 2.95 of [MS-ADA3].

2.9 pKIDefaultKeySpec Attribute

The following table shows the values that are allowed for the pKIDefaultKeySpec attribute.<11>

Value	Meaning
1	AT_KEYEXCHANGE — **Keys** used to encrypt/decrypt session keys.
2	AT_SIGNATURE — Keys used to create and verify **digital signatures**.

For schema details of this attribute, see section 2.96 of [MS-ADA3].

2.10 pKIEnrollmentAccess Attribute

The pKIEnrollmentAccess attribute is not used by any protocol.<12> For schema details of this attribute, see section 2.97 of [MS-ADA3].

2.11 pKIExpirationPeriod Attribute

The pKIExpirationPeriod attribute represents the maximum validity period of the certificate.<13> The attribute is an 8-byte octet string that initializes the **FILETIME** structure defined in [MS-DTYP] section 2.3.1.

For schema details of this attribute, see section 2.98 of [MS-ADA3].

2.12 pKIExtendedKeyUsage Attribute

The pKIExtendedKeyUsage attribute is a list of OIDs that represent extended key usages, as specified in [RFC3280] section 4.2.1.13.<14> For schema details of this attribute, see section 2.99 of [MS-ADA3].

2.13 pKIKeyUsage Attribute

The pKIKeyUsage attribute is a key usage extension.<15> For schema details of this attribute, see section 2.100 of [MS-ADA3].

2.14 pKIMaxIssuingDepth Attribute

The pKIMaxIssuingDepth attribute is the maximum depth value for the Basic Constraint extension, as specified in [RFC3280] section 4.2.1.10.<16> For schema details of this attribute, see section 2.101 of [MS-ADA3].

2.15 pKIOverlapPeriod Attribute

The pKIOverlapPeriod attribute represents the time before a certificate expires, during which time, clients need to send a **certificate renewal request**[MS-CAESO]. The attribute is an 8-byte octet string that initializes the **FILETIME** structure that is defined in [MS-DTYP] section 2.3.1.

For schema details of this attribute, see [MS-ADA3] section 2.102.

2.16 msPKI-Template-Schema-Version Attribute

The msPKI-Template-Schema-Version attribute specifies the schema version of the templates. The allowed values are 1, 2, and 3.<17> For schema details of this attribute, see section 2.439 of [MS-ADA2].

2.17 msPKI-Template-Minor-Revision Attribute

The msPKI-Template-Minor-Revision attribute specifies the minor version of the templates.<18> Supported values are 0 to 0x7fffffff. For schema details of this attribute, see section 2.438 of [MS-ADA2].

2.18 msPKI-RA-Signature Attribute

The msPKI-RA-Signature attribute specifies the number of recovery agent signatures that are required on a request that references this template.<19> For schema details of this attribute, see section 2.435 of [MS-ADA2].

2.19 msPKI-Minimal-Key-Size Attribute

The msPKI-Minimal-Key-Size attribute specifies the minimum size, in bits, of the public key that the client should create to obtain a certificate based on this template.<20> For schema details of this attribute, see section 2.427 of [MS-ADA2].

2.20 msPKI-Cert-Template-OID Attribute

The msPKI-Cert-Template-OID attribute specifies the object identifier (OID) of this template.<21> For schema details of this attribute, see section 2.420 of [MS-ADA2].

2.21 msPKI-Supersede-Templates Attribute

The msPKI-Supersede-Templates attribute that contains the CNs of all superseded templates.<22>For schema details of this attribute, see [MS-ADA2] section 2.437.

2.22 msPKI-RA-Policies Attribute

The msPKI-RA-Policies attribute is a multistring attribute that specifies a set of certificate policy OIDs, as specified in [RFC3280] section 4.2.1.5, for the **registration authority (RA)** certificates.<23> For schema details of this attribute, see section 2.434 of [MS-ADA2].

2.23 msPKI-RA-Application-Policies Attribute

The msPKI-RA-Application-Policies attribute encapsulates embedded properties for multipurpose use. The syntax for the data that is stored in this attribute is different, depending on the schema version for the template. The schema version of the template is stored in the msPKI-Template-Schema-Version attribute of the certificate template, as described in section 2.16.<24>

2.23.1 Versions 1 and 2

The versions 1 and 2 templates are multistring attributes that specify a set of application policy OIDs for the RA certificates. Application policy OIDs are the same as extended key usage OIDs, as specified in [RFC3280] section 4.2.1.13.

2.23.2 Version 3

For the version 3 templates, the attribute value is a string of property-type-value triplets that are separated by a grave accent (`) character. Each triplet for this attribute has the following format.

```
Name`Type`Value`
```

Where:

Tag	Description
Name	The property name. This value MUST be one of the property names in the following list.
Type	The **Type** MUST be "DWORD" or "PZPWSTR". If "DWORD" is used, the **Value** field contains a Unicode string representation of a positive decimal number. If "PZPWSTR" is used, the **Value** field contains a Unicode string.
Value	The value of the parameter.
`	A delimiter symbol separator.

The property name MUST be one of the following:

- **msPKI-RA-Application-Policies**: A string value that represents a set of application policy OIDs (comma-separated) for the RA certificates. Application policy OIDs are the same as extended key usage OIDs, as specified in [RFC3280] section 4.2.1.13. The type MUST be "PZPWSTR".
- **msPKI-Asymmetric-Algorithm**: A string value that represents the name of the **asymmetric algorithm**. The type MUST be "PZPWSTR".
- **msPKI-Key-Security-Descriptor**: An SDDL string that represents the security descriptor (as specified in [MS-DTYP] section 2.5.1) for the asymmetric key. The type MUST be "PZPWSTR".
- **msPKI-Symmetric-Algorithm**: A string value that represents the name of the **symmetric algorithm** that clients use for key exchanges. The type MUST be "PZPWSTR".
- **msPKI-Symmetric-Key-Length**: An unsigned integer value that represents the length, in bits, of the **symmetric key**. The type MUST be **DWORD**.
- **msPKI-Hash-Algorithm**: A string value that represents the name of the hash algorithm that clients use. The type MUST be "PZPWSTR".
- **msPKI-Key-Usage**: An unsigned integer value that represents how the private key is used (see [MS-WCCE] section 3.1.2.4.2.2.2.5). The type MUST be **DWORD**. A bitwise OR of the following flags is supported for this property.

Name	Value	Meaning
NCRYPT_ALLOW_DECRYPT_FLAG	0x00000001	The private key can be used to perform a decryption operation.
NCRYPT_ALLOW_SIGNING_FLAG	0x00000002	The private key can be used to perform a signature operation.
ALLOW_KEY_AGREEMENT_FLAG	0x00000004	The private key can be used to perform a key-agreement operation.

Name	Value	Meaning
NCRYPT_ALLOW_ALL_USAGES	0x00ffffff	The private key is not restricted to any specific cryptographic operations.

For example:

```
msPKI-Asymmetric-Algorithm`PZPWSTR`RSA`msPKI-Hash-Algorithm`PZPWSTR`SHA1`msPKI-
Key-Usage`DWORD`2`msPKI-RA-Application-Policies`PZPWSTR`1.3.6.1.4.1.311.10.3.8`
```

For schema details of this attribute, see section 2.433 of [MS-ADA2].

2.24 msPKI-Certificate-Policy Attribute

The msPKI-Certificate-Policy attribute specifies each string that represents a policy OID to be added to the certificate policy extension, as specified in [RFC3280] section 4.2.1.5.<25> For schema details of this attribute, see section 2.423 of [MS-ADA2].

2.25 msPKI-Certificate-Application-Policy Attribute

Each string in the msPKI-Certificate-Application-Policy attribute represents an application policy OID to be added to the certificate application policy extension.<26> Application policy OIDs are the same as extended key usage OIDs, as specified in [RFC3280] section 4.2.1.13.

For schema details of this attribute, see section 2.421 of [MS-ADA2].

2.26 msPKI-Enrollment-Flag Attribute

The msPKI-Enrollment-Flag attribute specifies the enrollment flags. The attribute value can be 0, or it can consist of a bitwise OR of flags from the following table.<27>

Flag	Meaning
0x00000001 CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS	This flag instructs the client and server to include a **Secure/Multipurpose Internet Mail Extensions (S/MIME)** certificate extension, as specified in [RFC4262], in the request and in the issued certificate.
0x00000002 CT_FLAG_PEND_ALL_REQUESTS	This flag instructs the CA to put all requests in a pending state.
0x00000004 CT_FLAG_PUBLISH_TO_KRA_CONTAINER	This flag instructs the CA to publish the issued certificate to the **key recovery agent (KRA)** container in Active Directory, as specified in [MS-

Flag	Meaning
	ADTS].
0x00000008 CT_FLAG_PUBLISH_TO_DS	This flag instructs clients and CA servers to append the issued certificate to the **userCertificate** attribute, as specified in [RFC4523], on the user object in Active Directory. The server processing rules for this flag are specified in [MS-WCCE] section 3.2.2.6.2.1.4.5.6.
0x00000010 CT_FLAG_AUTO_ENROLLMENT_CHECK_USER_DS_CERTIFICATE	This flag instructs clients not to do **autoenrollment** for a certificate based on this template if the user's **userCertificate** attribute (specified in [RFC4523]) in Active Directory has a valid certificate based on the same template.
0x00000020 CT_FLAG_AUTO_ENROLLMENT	This flag instructs clients to perform autoenrollment for the specified template.
0x00000040 CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT	This flag instructs clients to sign the renewal request using the private key of the existing certificate. This flag also instructs the CA to process the renewal requests as specified in [MS-WCCE] section 3.2.2.6.2.1.4.5.6.
0x00000100 CT_FLAG_USER_INTERACTION_REQUIRED	This flag instructs the client to obtain user consent before attempting to enroll for a certificate that is based on the specified template.
0x00000400 CT_FLAG_REMOVE_INVALID_CERTIFICATE_FROM_PERSONAL_STORE	This flag instructs the autoenrollment client to delete any certificates that are no longer needed based on the specific template from the local certificate storage.
0x00000800 CT_FLAG_ALLOW_ENROLL_ON_BEHALF_OF	This flag instructs the server to allow **enroll on behalf of (EOBO)** functionality.
0x00001000 CT_FLAG_ADD_OCSP_NOCHECK	This flag instructs the server to not include revocation information and add the id-pkix-ocsp-nocheck extension, as specified in [RFC2560]

Flag	Meaning
	section 4.2.2.2.1, to the certificate that is issued.<28>
0x00002000 CT_FLAG_ENABLE_KEY_REUSE_ON_NT_TOKEN_KEYSET_STORAGE_FULL	This flag instructs the client to reuse the private key for a smart card–based certificate renewal if it is unable to create a new private key on the card.<29>
0x00004000 CT_FLAG_NOREVOCATIONINFOINISSUEDCERTS	This flag instructs the server to not include revocation information in the issued certificate.<30>
0x00008000 CT_FLAG_INCLUDE_BASIC_CONSTRAINTS_FOR_EE_CERTS	This flag instructs the server to include Basic Constraints extension (specified in section 4.2.1.10 of [RFC3280]) in the end entity certificates.<31>

For schema details of this attribute, see [MS-ADA2] section 2.425.

2.27 msPKI-Private-Key-Flag Attribute

The msPKI-Private-Key-Flag attribute specifies the private key flags. Its value can be 0 or can consist of a bitwise OR of flags from the following table.<32>

Flag	Meaning
0x00000001 CT_FLAG_REQUIRE_PRIVATE_KEY_ARCHIVAL	This flag instructs the client to create a **key archival** certificate request, as specified in [MS-WCCE] sections 3.1.2.4.2.2.2.8 and 3.2.2.6.2.1.4.5.7.
0x00000010 CT_FLAG_EXPORTABLE_KEY	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.
0x00000020 CT_FLAG_STRONG_KEY_PROTECTION_REQUIRED	This flag instructs the client to use additional protection for the private key.
0x00000040 CT_FLAG_REQUIRE_ALTERNATE_SIGNATURE_ALGORITHM	This flag instructs the client to use an alternate signature format. For more details, see [MS-WCCE] section 3.1.2.4.2.2.2.8.

For schema details of this attribute, see section 2.432 of [MS-ADA2].

2.28 msPKI-Certificate-Name-Flag Attribute

The msPKI-Certificate-Name-Flag attribute specifies the subject name flags. Its value can be 0, or it can consist of a bitwise OR of flags from the following table.<33> The processing rules for these flags are specified in [MS-WCCE] sections 3.1.2.4.2.2.2.10 and 3.2.2.6.2.1.4.5.9.

Flag	Client processing
0x00000001 CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT	This flag instructs the client to supply subject information in the certificate request.
0x00010000 CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT_ALT_NAME	This flag instructs the client to supply subject alternate name information in the certificate request.
0x00400000 CT_FLAG_SUBJECT_ALT_REQUIRE_DOMAIN_DNS	This flag instructs the CA to add the value of the requester's **FQDN** and **NetBIOS name** to the Subject Alternative Name extension of the issued certificate.
0x01000000 CT_FLAG_SUBJECT_ALT_REQUIRE_DIRECTORY_GUID	This flag instructs the CA to add the value of the **objectGUID** attribute from the requestor's user object in Active Directory to the Subject Alternative Name extension of the issued certificate.
0x02000000 CT_FLAG_SUBJECT_ALT_REQUIRE_UPN	This flag instructs the CA to add the value of the UPN attribute from the requestor's user object in Active Directory to the Subject Alternative Name extension of the issued certificate.
0x04000000 CT_FLAG_SUBJECT_ALT_REQUIRE_EMAIL	This flag instructs the CA to add the value of the e-mail attribute from the requestor's user object in Active Directory to the Subject Alternative Name extension of the issued certificate.
0x08000000 CT_FLAG_SUBJECT_ALT_REQUIRE_DNS	This flag instructs the CA to add the value obtained from the DNS attribute of the requestor's user object in Active Directory to the Subject Alternative Name extension of the issued certificate.
0x10000000 CT_FLAG_SUBJECT_REQUIRE_DNS_AS_CN	This flag instructs the CA to add the value obtained from the DNS attribute of the requestor's user object in Active Directory as the CN in the subject of the issued certificate.
0x20000000 CT_FLAG_SUBJECT_REQUIRE_EMAIL	This flag instructs the CA to add the value of the e-mail attribute from the requestor's user object in Active Directory as the subject of the issued certificate.
0x40000000 CT_FLAG_SUBJECT_REQUIRE_COMMON_NAME	This flag instructs the CA to set the subject name to the requestor's CN from Active Directory, as specified in [MS-ADTS] section 3.1.1.1.7.
0x80000000 CT_FLAG_SUBJECT_REQUIRE_DIRECTORY_PATH	This flag instructs the CA to set the subject name to the requestor's distinguished name (DN) from Active Directory, as specified in [MS-ADTS] section 3.1.1.1.4.

Flag	Client processing
0x00000008 CT_FLAG_OLD_CERT_SUPPLIES_SUBJECT_AND_ALT_NAME	This flag instructs the client to reuse values of subject name and alternative subject name extensions from an existing valid certificate when creating a certificate renewal request.<34>

For schema details of this attribute, see [MS-ADA2] section 2.422.

3 Structure Example

The example in this section is a result of executing the following command on any computer that runs Microsoft Windows® Server operating system.

```
certutil -v -dstemplate administrator
```

The command reads attributes of the "administrator" certificate template.

```
[Administrator]
objectClass = "top", "pKICertificateTemplate"
cn = "Administrator"
distinguishedName =
    "CN=Administrator,CN=Certificate Templates,
     CN=Public Key Services,CN=Services,
     CN=Configuration,DC=contoso, DC=com"
instanceType = "4" not used by the WCCE protocol.
whenCreated = "19990212152445.0Z" 2/12/1999 7:24 AM*
whenChanged = "20060908182747.0Z" 9/8/2006 10:27 AM*
displayName = "Administrator"
uSNCreated = "8221" 0x201d*
uSNChanged = "8221" 0x201d*
showInAdvancedViewOnly = "TRUE"*
name = "Administrator"
objectGUID = "0dbfa8b3-c28f-11d2-91e6-08002ba3ed3b"*
flags = "66106" 0x1023a**

  (CT_FLAG_MACHINE_TYPE -- 40 (64))
(CT_FLAG_IS_CA -- 80 (128))
 (CT_FLAG_IS_CROSS_CA -- 800 (2048))
CT_FLAG_IS_DEFAULT -- 10000 (65536)
(CT_FLAG_IS_MODIFIED -- 20000 (131072))

revision = "4"
objectCategory =
    "CN=PKI-Certificate-Template,CN=Schema,
     CN=Configuration,DC=contoso,DC=com"
not used by the WCCE protocol.
pKIDefaultKeySpec = "1"
pKIKeyUsage = "a0 00"
pKIMaxIssuingDepth = "0"
pKIExpirationPeriod =  "1 Years"
pKIOverlapPeriod =  "6 Weeks"
pKIExtendedKeyUsage =
    "1.3.6.1.4.1.311.10.3.1" Microsoft Trust List Signing,
    "1.3.6.1.4.1.311.10.3.4" Encrypting File System,
    "1.3.6.1.5.5.7.3.4" Secure Email, "1.3.6.1.5.5.7.3.2"
    Client Authentication
pKIDefaultCSPs =
    "2,Microsoft Base Cryptographic Provider v1.0",
    "1,Microsoft Enhanced Cryptographic Provider v1.0"
dSCorePropagationData =
    "16010101000000.0Z" EMPTYnot used by the WCCE protocol.
msPKI-RA-Signature = "0"
msPKI-Enrollment-Flag = "41" 0x29**
```

```
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 1
(CT_FLAG_PEND_ALL_REQUESTS -- 2)
(CT_FLAG_PUBLISH_TO_KRA_CONTAINER -- 4)
CT_FLAG_PUBLISH_TO_DS -- 8
(CT_FLAG_AUTO_ENROLLMENT_CHECK_USER_DS_CERTIFICATE -- 10 (16))
CT_FLAG_AUTO_ENROLLMENT -- 20 (32)
(CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT -- 40 (64))
(CT_FLAG_USER_INTERACTION_REQUIRED -- 100 (256))
    (CT_FLAG_REMOVE_INVALID_CERTIFICATE_FROM_PERSONAL_STORE
      -- 400 (1024))
(CT_FLAG_ALLOW_ENROLL_ON_BEHALF_OF -- 800 (2048))
msPKI-Private-Key-Flag = "16" 0x10**

(CT_FLAG_REQUIRE_PRIVATE_KEY_ARCHIVAL -- 1)
CT_FLAG_EXPORTABLE_KEY -- 10 (16)
(CT_FLAG_STRONG_KEY_PROTECTION_REQUIRED -- 20 (32))
msPKI-Certificate-Name-Flag = "-1509949440" 0xa6000000**

   (CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 1)
   (CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT_ALT_NAME
      -- 10000 (65536))
   (CT_FLAG_SUBJECT_ALT_REQUIRE_DOMAIN_DNS
      -- 400000 (4194304))
   (CT_FLAG_SUBJECT_ALT_REQUIRE_DIRECTORY_GUID
      -- 1000000 (16777216))
    CT_FLAG_SUBJECT_ALT_REQUIRE_UPN
      -- 2000000 (33554432)
    CT_FLAG_SUBJECT_ALT_REQUIRE_EMAIL
      -- 4000000 (67108864)
   (CT_FLAG_SUBJECT_ALT_REQUIRE_DNS
      -- 8000000 (134217728))
   (CT_FLAG_SUBJECT_REQUIRE_DNS_AS_CN
      -- 10000000 (268435456))
   CT_FLAG_SUBJECT_REQUIRE_EMAIL
      -- 20000000 (536870912)
   (CT_FLAG_SUBJECT_REQUIRE_COMMON_NAME
      -- 40000000 (1073741824))
   CT_FLAG_SUBJECT_REQUIRE_DIRECTORY_PATH
      -- 80000000 (-2147483648)
```

*Not used by the Windows Client Certificate Enrollment Protocol.

**The flags in parentheses are optional values for the attributes that are not present in the current template. Some of the possible flags for the attribute have been removed because they are not used by the Windows Client Certificate Enrollment Protocol.<35><36>

4 Security Considerations

4.1 Policy

Certificate templates, including their **access control lists (ACLs)**, express policy by which the **enterprise certificate authority** policy algorithm controls which certificates to issue to end entities in an organization. It is the job of the administrator to translate corporate policy into certificate template contents and ACLs.

4.2 Access Control

The ACL of a certificate template can grant one permission that the default certificate server policy algorithm consults: the enrollment permissions. If an entity has the enrollment permission for a certificate type and requests that certificate, the enterprise certificate authority policy algorithm causes the certificate server to issue that kind of certificate to that entity.

One kind of certificate that can be issued is the Enrollment Agent certificate, which is a particularly powerful certificate. Because an Enrollment Agent is allowed to specify certificates to be issued to any subject, it can bypass corporate security policy. As a result, administrators need to be especially careful when allowing subjects to enroll for Enrollment Agent certificates.

4.3 Auditing

It may be appropriate to use auditing mechanisms provided by the directory storing certificate templates objects in order to monitor important types of access like writing to the certificate templates.

5 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft Windows® 2000 operating system
- Windows® XP operating system
- Windows Server® 2003 operating system
- Windows Server® 2003 R2 operating system
- Windows Vista® operating system
- Windows Server® 2008 operating system
- Windows® 7 operating system
- Windows Server® 2008 R2 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 1.6: Windows defines three template versions: version 1, version 2, and version 3. Version 1 templates are supported by CAs that run on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2. Version 2 templates are supported by Microsoft CAs that run on Windows Server 2003 Enterprise Edition, Windows Server 2003 R2 Datacenter Edition, Windows Server 2008, and Windows Server 2008 R2. Version 3 templates are supported by CAs that run on Windows Server 2008 and Windows Server 2008 R2.

<2> Section 2.1: The cn attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<3> Section 2.2: The displayName attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<4> Section 2.3: The distinguishedName attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<5> Section 2.4: The flags attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<6> Section 2.4: This flag is only supported in Windows Server 2008 R2.

<7> Section 2.5: The ntSecurityDescriptor attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<8> Section 2.6: The revision attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<9> Section 2.7: The pKICriticalExtensions attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<10> Section 2.8: The pKIDefaultCSPs attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<11> Section 2.9: The pKIDefaultKeySpec attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2. For more information about the Microsoft implementation of key types, see [MSDN-KEY].

<12> Section 2.10: The pKIEnrollmentAccess attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<13> Section 2.11: The pKIExpirationPeriod attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<14> Section 2.12: The pKIExtendedKeyUsage attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<15> Section 2.13: The pKIKeyUsage attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<16> Section 2.14: The pKIMaxIssuingDepth attribute is implemented only in Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<17> Section 2.16: The msPKI-Template-Schema-Version attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<18> Section 2.17: The msPKI-Template-Minor-Revision attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<19> Section 2.18: The msPKI-RA-Signature attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<20> Section 2.19: The msPKI-Minimal-Key-Size attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<21> Section 2.20: The msPKI-Cert-Template-OID attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<22> Section 2.21: The msPKI-Supersede-Templates attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<23> Section 2.22: The msPKI-RA-Policies attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<24> Section 2.23: The msPKI-RA-Application-Policies attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<25> Section 2.24: The msPKI-Certificate-Policy attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<26> Section 2.25: The msPKI-Certificate-Application-Policy attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<27> Section 2.26: The msPKI-Enrollment-Flag attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<28> Section 2.26: This flag is supported only in Windows Server 2008 and Windows Server 2008 R2.

<29> Section 2.26: This flag is supported only in Windows Vista, Windows Server 2008, and Windows Server 2008 R2.

<30> Section 2.26: This flag is supported only in Windows Server 2008 R2.

<31> Section 2.26: This flag is supported only in Windows Server 2008 R2.

<32> Section 2.27: The msPKI-Private-Key-Flag attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<33> Section 2.28: The msPKI-Certificate-Name-Flag attribute is implemented only in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2.

<34> Section 2.28: This flag is supported only in Windows Server 2008 R2.

<35> Section 3: The following is the list of the default certificate templates and their attribute values that are installed to Active Directory by Windows Server 2003 and Windows XP.

```
cn: Administrator;
displayName: Administrator;
flags: 66106;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: Administrator;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0;
    1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (4): 1.3.6.1.4.1.311.10.3.1;
    1.3.6.1.4.1.311.10.3.4; 1.3.6.1.5.5.7.3.4; 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xA0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 4;

cn: CA;
```

```
displayName: Root Certification Authority;
flags: 65745;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CA;
pKICriticalExtensions: 2.5.29.19;
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF
pKIKeyUsage: 0x86 0x00
pKIMaxIssuingDepth: -1;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 5;

cn: CAExchange;
displayName: CA Exchange;
flags: 65600;
msPKI-Certificate-Application-Policy: 1.3.6.1.4.1.311.21.5;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 1;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: CAExchange;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0xC0 0x1B 0xD7 0x7F 0xFA 0xFF 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.21.5;
pKIKeyUsage: 0x20 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0xC0 0x1B 0xD7 0x7F 0xFA 0xFF 0xFF
revision: 106;

cn: CEPEncryption;
displayName: CEP Encryption;
flags: 66113;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CEPEncryption;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage:  0x20 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
```

```
revision: 4;

cn: CertificateRequestAgent;
displayName: Certificate Request Agent;
flags: 131616;
msPKI-Certificate-Application-Policy: 1.3.6.1.4.1.311.20.2.1;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 96;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Application-Policies: 1.3.6.1.4.1.311.20.2.1;
msPKI-RA-Signature: 1;
msPKI-Template-Minor-Revision: 4;
msPKI-Template-Schema-Version: 2;
name: CertificateRequestAgent;
pKIDefaultCSPs: 1,Microsoft Base Smart Card Crypto Provider;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 100;

cn: ClientAuth;
displayName: Authenticated Session;
flags: 197152;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: ClientAuth;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 3;

cn: CodeSigning;
displayName: Code Signing;
flags: 66080;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CodeSigning;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
```

```
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.3;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 3;

cn: CrossCA;
displayName: Cross Certification Authority;
flags: 198672;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 512;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Application-Policies: 1.3.6.1.4.1.311.10.3.10;
msPKI-RA-Signature: 1;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: CrossCA;
pKICriticalExtensions: 2.5.29.19;
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF
pKIKeyUsage: 0x86 0x00
pKIMaxIssuingDepth: -1;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 110;

cn: CTLSigning;
displayName: Trust List Signing;
flags: 66080;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CTLSigning;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.10.3.1;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 3;

cn: DirectoryEmailReplication;
displayName: Directory Email Replication;
flags: 196704;
msPKI-Certificate-Application-Policy: 1.3.6.1.4.1.311.21.19;
msPKI-Certificate-Name-Flag: 150994944;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 1024;
```

```
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Supersede-Templates: DomainController;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: DirectoryEmailReplication;
pKICriticalExtensions: 2.5.29.17;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.21.19;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 122;

cn: DomainController;
displayName: Domain Controller;
flags: 197228;
msPKI-Certificate-Name-Flag: 419430400;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: DomainController;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 4;

cn: DomainControllerAuthentication;
displayName: Domain Controller Authentication;
flags: 196704;
msPKI-Certificate-Application-Policy (3): 1.3.6.1.5.5.7.3.2;
   1.3.6.1.5.5.7.3.1; 1.3.6.1.4.1.311.20.2.2;
msPKI-Certificate-Name-Flag: 134217728;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Supersede-Templates: DomainController;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: DomainControllerAuthentication;
pKICriticalExtensions: 2.5.29.17;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (3): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
   1.3.6.1.4.1.311.20.2.2;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
```

```
revision: 119;

cn: EFS;
displayName: Basic EFS;
flags: 197176;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: EFS;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.10.3.4;
pKIKeyUsage:  0x20 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 3;

cn: EFSRecovery;
displayName: EFS Recovery Agent;
flags: 66096;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 33;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: EFSRecovery;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.10.3.4.1;
pKIKeyUsage:  0x20 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 6;

cn: EnrollmentAgent;
displayName: Enrollment Agent;
flags: 197152;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: EnrollmentAgent;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
```

```
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 4;

cn: EnrollmentAgentOffline;
displayName: Exchange Enrollment Agent (Offline request);
flags: 66049;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: EnrollmentAgentOffline;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 4;

cn: ExchangeUser;
displayName: Exchange User;
flags: 66065;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 1;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: ExchangeUser;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.4;
pKIKeyUsage:  0x20 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 7;

cn: ExchangeUserSignature;
displayName: Exchange Signature Only;
flags: 66049;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
```

```
msPKI-Template-Schema-Version: 1;
name: ExchangeUserSignature;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.4;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 6;

cn: IPSECIntermediateOffline;
displayName: IPSEC (Offline request);
flags: 197185;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: IPSECIntermediateOffline;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.8.2.2;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 7;

cn: IPSECIntermediateOnline;
displayName: IPSEC;
flags: 197216;
msPKI-Certificate-Name-Flag: 402653184;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: IPSECIntermediateOnline;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.8.2.2;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 8;

cn: KeyRecoveryAgent;
displayName: Key Recovery Agent;
flags: 196640;
msPKI-Certificate-Application-Policy: 1.3.6.1.4.1.311.21.6;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 39;
```

```
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Application-Policies: 1.3.6.1.4.1.311.21.6;
msPKI-RA-Signature: 1;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 2;
name: KeyRecoveryAgent;
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.21.6;
pKIKeyUsage:  0x20 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 105;

cn: Machine;
displayName: Computer;
flags: 197216;
msPKI-Certificate-Name-Flag: 402653184;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: Machine;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 5;

cn: MachineEnrollmentAgent;
displayName: Enrollment Agent (Computer);
flags: 66144;
msPKI-Certificate-Name-Flag: 402653184;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: MachineEnrollmentAgent;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 5;

cn: OfflineRouter;
```

```
displayName: Router (Offline request);
flags: 66113;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: OfflineRouter;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 4;


cn: RASAndIASServer;
displayName: RAS and IAS Server;
flags: 197216;
msPKI-Certificate-Application-Policy (2):
   1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
msPKI-Certificate-Name-Flag: 1207959552;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Supersede-Templates: NTDEVComputer;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: RASAndIASServer;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 104;

cn: SmartcardLogon;
displayName: Smartcard Logon;
flags: 197120;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 512;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: SmartcardLogon;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (2):
   1.3.6.1.4.1.311.20.2.2; 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xa0 0x00
```

```
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 6;

cn: SmartcardUser;
displayName: Smartcard User;
flags: 197130;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 9;
msPKI-Minimal-Key-Size: 512;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: SmartcardUser;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (3):
   1.3.6.1.4.1.311.20.2.2; 1.3.6.1.5.5.7.3.4; 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 11;

cn: SubCA;
displayName: Subordinate Certification Authority;
flags: 197329;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: SubCA;
pKICriticalExtensions: 2.5.29.19;
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF
pKIKeyUsage: 0x86 0x00
pKIMaxIssuingDepth: -1;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 5;

cn: User;
displayName: User;
flags: 197178;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: User;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
```

```
pKIExtendedKeyUsage (3): 1.3.6.1.4.1.311.10.3.4; 1.3.6.1.5.5.7.3.4;
   1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 3;

cn: UserSignature;
displayName: User Signature Only;
flags: 197154;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: UserSignature;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider;
   2,Microsoft Base Cryptographic Provider v1.0;
   1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.4; 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0x80 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 4;

cn: WebServer;
displayName: Web Server;
flags: 66113;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: WebServer;
pKIDefaultCSPs (2): 2,Microsoft DH SChannel Cryptographic Provider;
   1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 4;

cn: Workstation;
displayName: Workstation Authentication;
flags: 197216;
msPKI-Certificate-Application-Policy: 1.3.6.1.5.5.7.3.2;
msPKI-Certificate-Name-Flag: 134217728;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
```

```
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: Workstation;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xa0 0x00
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF
revision: 104;
```

<36> Section 3: The following is the list of the default certificate templates and their attribute values that are installed to Active Directory by Windows Vista, Windows Server 2008, and Windows Server 2008 R2.

```
cn: Administrator;
displayName: Administrator;
flags: 66106;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.7;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: Administrator;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0; 1,Microsoft Enhanced
Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (4): 1.3.6.1.4.1.311.10.3.1; 1.3.6.1.4.1.311.10.3.4; 1.3.6.1.5.5.7.3.4;
1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 4;

cn: CA;
displayName: Root Certification Authority;
flags: 65745;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.17;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CA;
pKICriticalExtensions (2): 2.5.29.15; 2.5.29.19;
```

```
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF;
pKIKeyUsage: 0x86 0x00;
pKIMaxIssuingDepth: -1;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 5;

cn: CAExchange;
displayName: CA Exchange;
flags: 65600;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.26;
msPKI-Certificate-Application-Policy: 1.3.6.1.4.1.311.21.5;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 1;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: CAExchange;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0; 1,Microsoft Enhanced
Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0xC0 0x1B 0xD7 0x7F 0xFA 0xFF 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.21.5;
pKIKeyUsage: 0x20 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x40 0x96 0xD5 0x36 0xFF 0xFF 0xFF;
revision: 106;

cn: CEPEncryption;
displayName: CEP Encryption;
flags: 66113;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.22;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CEPEncryption;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x20 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 4;

cn: ClientAuth;
displayName: Authenticated Session;
flags: 66080;
```

```
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.4;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: ClientAuth;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 3;

cn: CodeSigning;
displayName: Code Signing;
flags: 66080;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.9;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CodeSigning;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.3;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 3;

cn: CrossCA;
displayName: Cross Certification Authority;
flags: 67600;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.25;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 8;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Application-Policies: 1.3.6.1.4.1.311.10.3.10;
msPKI-RA-Signature: 1;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: CrossCA;
```

```
pKICriticalExtensions (2): 2.5.29.15; 2.5.29.19;
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF;
pKIKeyUsage: 0x86 0x00;
pKIMaxIssuingDepth: -1;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 105;

cn: CTLSigning;
displayName: Trust List Signing;
flags: 66080;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.10;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: CTLSigning;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.10.3.1;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 3;

cn: DirectoryEmailReplication;
displayName: Directory Email Replication;
flags: 65632;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.29;
msPKI-Certificate-Application-Policy: 1.3.6.1.4.1.311.21.19;
msPKI-Certificate-Name-Flag: 150994944;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Supersede-Templates: DomainController;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: DirectoryEmailReplication;
pKICriticalExtensions (2): 2.5.29.15; 2.5.29.17;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.21.19;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 00 80 A6 0A FF DE FF FF;
revision: 115;

cn: DomainController;
```

```
displayName: Domain Controller;
flags: 66156;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.15;
msPKI-Certificate-Name-Flag: 419430400;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: DomainController;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 4;

cn: DomainControllerAuthentication;
displayName: Domain Controller Authentication;
flags: 65632;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.28;
msPKI-Certificate-Application-Policy (3): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
1.3.6.1.4.1.311.20.2.2;
msPKI-Certificate-Name-Flag: 134217728;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Supersede-Templates: DomainController;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: DomainControllerAuthentication;
pKICriticalExtensions (2): 2.5.29.15; 2.5.29.17;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (3): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1; 1.3.6.1.4.1.311.20.2.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 110;

cn: EFS;
displayName: Basic EFS;
flags: 66104;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.6;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
```

```
msPKI-Template-Schema-Version: 1;
name: EFS;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0; 1,Microsoft Enhanced
Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.10.3.4;
pKIKeyUsage: 0x20 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 3;

cn: EFSRecovery;
displayName: EFS Recovery Agent;
flags: 66096;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.8;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 33;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: EFSRecovery;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0; 1,Microsoft Enhanced
Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.10.3.4.1;
pKIKeyUsage: 0x20 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 6;

cn: EnrollmentAgent;
displayName: Enrollment Agent;
flags: 66080;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.11;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: EnrollmentAgent;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
```

```
revision: 4;

cn: EnrollmentAgentOffline;
displayName: Exchange Enrollment Agent (Offline request);
flags: 66049;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.12;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: EnrollmentAgentOffline;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 4;

cn: ExchangeUser;
displayName: Exchange User;
flags: 66065;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.23;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 1;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: ExchangeUser;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0; 1,Microsoft Enhanced
Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.4;
pKIKeyUsage: 0x20 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 7;

cn: ExchangeUserSignature;
displayName: Exchange Signature Only;
flags: 66049;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.24;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
```

```
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: ExchangeUserSignature;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.4;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 6;

cn: IPSECIntermediateOffline;
displayName: IPSec (Offline request);
flags: 66113;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.20;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: IPSECIntermediateOffline;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.8.2.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 7;

cn: IPSECIntermediateOnline;
displayName: IPSec;
flags: 66144;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.19;
msPKI-Certificate-Name-Flag: 402653184;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: IPSECIntermediateOnline;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.8.2.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
```

```
revision: 8;

cn: KerberosAuthentication;
displayName: Kerberos Authentication;
flags: 65632;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.33;
msPKI-Certificate-Application-Policy (4): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
1.3.6.1.4.1.311.20.2.2; 1.3.6.1.5.2.3.5;
msPKI-Certificate-Name-Flag: 138412032;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: KerberosAuthentication;
pKICriticalExtensions (2): 2.5.29.15; 2.5.29.17;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (4): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1; 1.3.6.1.4.1.311.20.2.2;
1.3.6.1.5.2.3.5;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 110;

cn: KeyRecoveryAgent;
displayName: Key Recovery Agent;
flags: 65568;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.27;
msPKI-Certificate-Application-Policy: 1.3.6.1.4.1.311.21.6;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 39;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: KeyRecoveryAgent;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.21.6;
pKIKeyUsage: 0x20 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 105;

cn: Machine;
displayName: Computer;
flags: 66144;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.14;
msPKI-Certificate-Name-Flag: 402653184;
msPKI-Enrollment-Flag: 32;
```

```
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: Machine;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 5;

cn: MachineEnrollmentAgent;
displayName: Enrollment Agent (Computer);
flags: 66144;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.13;
msPKI-Certificate-Name-Flag: 402653184;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: MachineEnrollmentAgent;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.4.1.311.20.2.1;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 5;

cn: OCSPResponseSigning;
displayName: OCSP Response Signing;
flags: 66112;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.32;
msPKI-Certificate-Application-Policy: 1.3.6.1.5.5.7.3.9;
msPKI-Certificate-Name-Flag: 402653184;
msPKI-Enrollment-Flag: 4096;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Application-Policies: msPKI-Asymmetric-Algorithm`PZPWSTR`RSA`msPKI-Hash-
Algorithm`PZPWSTR`SHA1`msPKI-Key-Security-
Descriptor`PZPWSTR`D:(A;;FA;;;BA)(A;;FA;;;SY)(A;;GR;;;S-1-5-80-3804348527-3718992918-
2141599610-3686422417-2726379419)`msPKI-Key-Usage`DWORD`2`;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 3;
name: OCSPResponseSigning;
pKICriticalExtensions: 2.5.29.15;
```

```
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x80 0x37 0xAE 0xFF 0xF4 0xFF 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.9;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0x2C 0xAB 0x6D 0xFE 0xFF 0xFF;
revision: 101;

cn: OfflineRouter;
displayName: Router (Offline request);
flags: 66113;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.21;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: OfflineRouter;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 4;

cn: RASAndIASServer;
displayName: RAS and IAS Server;
flags: 66144;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.31;
msPKI-Certificate-Application-Policy (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
msPKI-Certificate-Name-Flag: 1207959552;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: RASAndIASServer;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 101;

cn: SmartcardLogon;
displayName: Smartcard Logon;
flags: 66048;
```

```
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.5;
msPKI-Certificate-Name-Flag: -2113929216;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 512;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: SmartcardLogon;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.2; 1.3.6.1.4.1.311.20.2.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 6;

cn: SmartcardUser;
displayName: Smartcard User;
flags: 66058;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.3;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 9;
msPKI-Minimal-Key-Size: 512;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: SmartcardUser;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (3): 1.3.6.1.5.5.7.3.4; 1.3.6.1.5.5.7.3.2; 1.3.6.1.4.1.311.20.2.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 11;

cn: SubCA;
displayName: Subordinate Certification Authority;
flags: 66257;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.18;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
msPKI-Minimal-Key-Size: 1024;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: SubCA;
pKICriticalExtensions (2): 2.5.29.15; 2.5.29.19;
pKIDefaultCSPs: 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x1E 0xA4 0xE8 0x65 0xFA 0xFF;
pKIKeyUsage: 0x86 0x00;
```

```
pKIMaxIssuingDepth: -1;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 5;

cn: User;
displayName: User;
flags: 66106;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.1;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 41;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 16;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: User;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (2): 2,Microsoft Base Cryptographic Provider v1.0; 1,Microsoft Enhanced
Cryptographic Provider v1.0;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (3): 1.3.6.1.4.1.311.10.3.4; 1.3.6.1.5.5.7.3.4; 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 3;

cn: UserSignature;
displayName: User Signature Only;
flags: 66082;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.2;
msPKI-Certificate-Name-Flag: -1509949440;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: UserSignature;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (3): 3,Microsoft Base DSS Cryptographic Provider; 2,Microsoft Base
Cryptographic Provider v1.0; 1,Microsoft Enhanced Cryptographic Provider v1.0;
pKIDefaultKeySpec: 2;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage (2): 1.3.6.1.5.5.7.3.4; 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0x80 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 4;

cn: WebServer;
displayName: Web Server;
flags: 66113;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.16;
msPKI-Certificate-Name-Flag: 1;
msPKI-Enrollment-Flag: 0;
```

```
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 1;
msPKI-Template-Schema-Version: 1;
name: WebServer;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs (2): 2,Microsoft DH SChannel Cryptographic Provider; 1,Microsoft RSA SChannel
Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x80 0x72 0x0E 0x5D 0xC2 0xFD 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.1;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 4;

cn: Workstation;
displayName: Workstation Authentication;
flags: 66144;
msPKI-Cert-Template-OID:
1.3.6.1.4.1.311.21.8.11034890.834619.12601478.16236816.7255827.176.1.30;
msPKI-Certificate-Application-Policy: 1.3.6.1.5.5.7.3.2;
msPKI-Certificate-Name-Flag: 134217728;
msPKI-Enrollment-Flag: 32;
msPKI-Minimal-Key-Size: 2048;
msPKI-Private-Key-Flag: 0;
msPKI-RA-Signature: 0;
msPKI-Template-Minor-Revision: 0;
msPKI-Template-Schema-Version: 2;
name: Workstation;
pKICriticalExtensions: 2.5.29.15;
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider;
pKIDefaultKeySpec: 1;
pKIExpirationPeriod: 0x00 0x40 0x39 0x87 0x2E 0xE1 0xFE 0xFF;
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.2;
pKIKeyUsage: 0xA0 0x00;
pKIMaxIssuingDepth: 0;
pKIOverlapPeriod: 0x00 0x80 0xA6 0x0A 0xFF 0xDE 0xFF 0xFF;
revision: 101;
```

6 Change Tracking

This section identifies changes that were made to the [MS-CRTD] protocol document between the May 2011 and June 2011 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.

- New protocol syntax added due to protocol revision.
- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated.**

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
1.2 References	Added explanatory statement regarding the removal of the publishing year from Microsoft Open Specification document references.	N	Content updated.

7 Index