[MS-CRTD]:
Certificate Templates Structure Specification

Revision Summary

Date	Revision History	Revision Class	Comments
12/18/2006	0.1		MCPP Milestone 2 Initial Availability
03/02/2007	1.0		MCPP Milestone 2
04/03/2007	1.1		Monthly release
05/11/2007	1.2		Monthly release
06/01/2007	2.0	Major	Updated and revised the technical content.

Date	Revision History	Revision Class	Comments
07/03/2007	2.0.1	Editorial	Revised and edited the technical content.
07/20/2007	2.0.2	Editorial	Revised and edited the technical content.
08/10/2007	2.0.3	Editorial	Revised and edited the technical content.
09/28/2007	2.1	Minor	Updated the technical content.
10/23/2007	3.0	Major	Updated and revised the technical content.
11/30/2007	3.1	Minor	Updated a normative reference.
01/25/2008	3.1.2	Editorial	Revised and edited the technical content.

Table of 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 **LDAP**, as specified in [RFC2251]. These attributes allow clients to define the behavior of a **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]:

Attribute
Certificate
Certificate Revocation Lists (CRL)
Certificate Services
Certificate Templates
Certification
Certification Authority (CA)
Common Name (CN)
Cryptographic Service Provider (CSP)
Digital Signature
Directory
Distinguished Name (DN)
Distributed Component Object Model (DCOM)
Domain
Domain Controller (DC)
Encryption
Enrollment
Enterprise CA
Key Archival
Key Recovery Agent (KRA)
Lightweight Directory Access Protocol (LDAP)
Object
Object Identifier (OID)
ObjectGUID
Private Key
Public Key
Public Key Algorithm
Public Key Infrastructure (PKI)
Registration Authority (RA)
Revocation
Security Descriptor
Standalone CA
Symmetric Algorithm
Symmetric Key

The following terms are specific to this document:

Active Directory: This refers to **Active Directory**, **Active Directory Domain Services (AD DS)** or **Active Directory Lightweight Directory Services (AD LDS)**. See also, **Active**

Directory Domain Services (AD DS), **Active Directory Lightweight Directory Services (AD LDS)**.

Active Directory Domain Services (AD DS): An operating system **directory** service that is implemented by a **domain controller (DC)**. The **directory** service provides a data store for **objects** that is distributed across multiple **DCs**. The **DCs** interoperate as peers to ensure that a local change to an **object** replicates correctly across **DCs**. **AD DS** first became available as part of Windows 2000 and is available as part of Windows 2000 Server products and Windows Server 2003 products; in these products it is called "Active Directory." It is also available as part of Windows Server 2008 Beta 2 and Beta 3. **AD/DS** is not present in Windows NT 4.0 or in Windows XP. For more information, see [MS-SECO] Section 2.2.2.

Active Directory Lightweight Directory Services (AD LDS): An operating system **directory** service implemented by a **domain controller (DC)**. The most significant difference between **AD LDS** and **AD DS** is that **AD LDS** does not host **domain NCs**. A server can host multiple **AD LDS DCs**. (In Microsoft documentation, **AD LDS** is sometimes called "ADAM".)

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**.

Auto-Enrollment: An automated, policy-driven process that performs **certificate enrollment**, renewal, or **revocation**.<1>

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

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-ADTS] Microsoft Corporation, "Active Directory Technical Specification", June 2007.

[MS-DCOM] Microsoft Corporation, "Distributed Component Object Model (DCOM) Remote Protocol Specification", March 2007.

[MS-DTYP] Microsoft Corporation, "Windows Data Types", January 2007.

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

[MS-WCCE] Microsoft Corporation, "Windows Client Certificate Enrollment Protocol Specification", June 2007.

[PKCS12] RSA Laboratories, "PKCS#12: Personal Information Exchange Syntax Standard", PKCS #12, 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.ietf.org/rfc/rfc2119.txt

[RFC2246] Dierks, T. and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, January 1999, http://www.ietf.org/rfc/rfc2246.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

[RFC2527] Chokhani, S. and Ford, W., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 2527, March 1999, http://www.ietf.org/rfc/rfc2527.txt

[RFC2559] Boeyen, S., Howes, T., and Richard, P., "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2", RFC 2559, April 1999, http://www.ietf.org/rfc/rfc2559.txt

[RFC2797] Myers, M., Liu, X., Schaad, J., and Weinstein, J., "Certificate Management Messages Over CMS", RFC 2797, April 2000, http://www.ietf.org/rfc/rfc2797.txt

[RFC2986] Nystrom, M. and Kaliski, B., "PKCS#10: Certificate Request Syntax Specification", RFC 2986, November 2000, http://www.ietf.org/rfc/rfc2986.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

[RFC3962] Raeburn, K., "Advanced Encryption Standard (AES) Encryption for Kerberos 5", RFC 3962, February 2005, http://www.ietf.org/rfc/rfc3962.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

[CRYPTO] Menezes, A., Vanstone, S., and Oorschot, P., "Handbook of Applied Cryptography", 1997, http://www.cacr.math.uwaterloo.ca/hac/

[MS-ADLS] Microsoft Corporation, "Active Directory Lightweight Directory Services Schema", June 2007.

[MSFT-AUTOENROLLMENT] Microsoft Corporation, "Certificate Autoenrollment in Windows Server 2003", April 2003, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/autoenro.mspx

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://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx

[HOWARD] Howard, M., "Writing Secure Code", Microsoft Press, 2002, ISBN: 0735617228.

[MSDN-KEY] Microsoft Corporation, "CERT_KEY_CONTEXT", http://msdn2.microsoft.com/en-us/library/aa377205.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 Structure Overview (Synopsis)

This document specifies the syntax and interpretation of certificate templates. Certificate Templates is a Microsoft-proprietary data structure that provides the following:

- Examples (templates) for certificates to be issued by a certification authority (CA).
- Certification constraints, which can specify certificate **enrollment** policies.
- Attributes of the **certification** process that serve as instructions to clients that want to succeed in generating a proper certificate request.

Certificate templates are held in a **directory** (**Active Directory**, in Windows implementations) and standard Lightweight Directory Access Protocol (LDAP) can access them.

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, there are limited interactions between templates and the Windows Client Certificate Enrollment Protocol. 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 role, 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

When used, certificate templates control the behavior of the certification authority (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 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 document 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 AD **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 Capability Negotiation

To determine the certificate template schema version, clients and servers MUST read the msPKI-Template-Schema-Version attribute on the certificate template **object**. For more information, see section 2.16.<2>

1.7 Vendor-Extensible Fields

None.

2 Structures

The PKI-Certificate-Template is the AD 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.

2.1 cn Attribute

The **cn** attribute is the **common name** of the certificate template.<3> **Note** attributeId and attributeSyntax are **object identifiers (OIDs)**.

CN: Common-Name

ldapDisplayName: cn

attributeId: 2.5.4.3

attributeSyntax: 2.5.5.12

omSyntax: 64

isSingleValue: TRUE

schemaIdGuid: bf96793f-0de6-11d0-a285-00aa003049e2

systemOnly: FALSE

searchFlags: 1

systemFlags: 12

2.2 displayName Attribute

The **displayName** attribute is the display name of a certificate template.<4>

CN: Display-Name

ldapDisplayName: displayName

attributeId: 1.2.840.113556.1.2.13

syntax: String (Unicode)

isSingleValued: TRUE

schemaIdGuid: bf967953-0de6-11d0-a285-00aa003049e2

systemOnly: FALSE

searchFlags: 5

rangeLower: 0

rangeUpper: 256

attributeSecurityGuid: 59ba2f42-79a2-11d0-9020-00c04fc2d3cf

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

2.3 distinguishedName Attribute

The **distinguishedName** attribute is the **distinguished name (DN)** of the certificate template.<5> The distinguished name (DN) is specified in [MS-ADTS].

CN: Obj-Dist-Name

ldapDisplayName: distinguishedName

attributeId: 2.5.4.49

syntax: Object (DS-DN)

isSingleValued: TRUE

schemaIdGuid: bf9679e4-0de6-11d0-a285-00aa003049e2

systemOnly: TRUE

searchFlags: 8

attributeSecurityGuid: e48d0154-bcf8-11d1-8702-00c04fb96050

mapiID: 32828

isMemberOfPartialAttributeSet: TRUE

systemFlags: 19

2.4 flags Attribute

The **flags** attribute is the general enrollment flags attribute. These flags are communicated as an integer value of this attribute.<6> The attribute value can be 0 or it can consist of a bitwise OR of flags from the following table:

Flag	Meaning
0x00000040	This flag indicates that the entity that requests the certificate should have the characteristic of a machine as opposed to a user.
0x00000080	This flag indicates a certificate request for a CA certificate.
0x00000800	This flag indicates a certificate request for cross-certifying a certificate.<7>
0x00010000	This flag MUST NOT be used.
0x00020000	This flag MUST NOT be used.

CN: flags

ldapDisplayName: flags

attributeId: 1.2.840.113556.1.4.38

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: bf967976-0de6-11d0-a285-00aa003049e2

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

2.5 ntSecurityDescriptor Attribute

The **ntSecurityDescriptor** attribute is a **security descriptor** as specified in [MS-DTYP], section **2.4.6**.<8> The DACL field of the security descriptor is an **ACL** (as specified in [MS-DTYP] section **2.4.5**) that specifies the permission set for this certificate template. Each 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, Windows Client Certificate Enrollment Protocol uses only two predefined permissions: Enroll and AutoEnroll.

An entity (AD user or group) has Enroll permission if the DACL of the security descriptor that is stored in this attribute contains an ACE with the following characteristics:

- The entity has an 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_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 at least one of the bits set that are specified with X in the following diagram.

										1										2									3	
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**
X			X					X																							

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

An entity (AD user or group) has AutoEnroll permission if the DACL of the security descriptor stored in this attribute contains an ACE with the following characteristics:

- The entity has an 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_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 at least one of the bits set that are specified with X in the following diagram.

										1										2										3	
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**
X			X					X																							

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

The protocol behavior with respect to these permissions is specified in [MS-WCCE] sections 3.1.3.4.1.1 and 3.1.2.5.1.2.

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

CN: NT-Security-Descriptor

ldapDisplayName: ntSecurityDescriptor

attributeId: 1.2.840.113556.1.2.281

syntax: String(NT-Sec-Desc)

isSingleValued: TRUE

schemaIdGuid: bf9679e3-0de6-11d0-a285-00aa003049e2

systemOnly: FALSE

searchFlags: 8

rangeLower: 0

rangeUpper: 132096

mapiID: 32787

isMemberOfPartialAttributeSet: TRUE

systemFlags: 26

2.5.1 Sets of Permissions 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.

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

- The entity has an **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 bits marked as X, as in the following diagram.

										1										2									3	
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**
														X													X		X		

An entity (AD user or group) is deemed to have Write permission if the **DACL** of the security descriptor that is stored in this attribute contains an ACE with the following characteristics:

- The entity has an **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 bits marked as X, as in the following diagram.

										1										2									3	
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**
												X	X													X				

An entity (AD user or group) is deemed to have Full Control permission if the DACL of the security descriptor that is stored in this attribute contains an ACE with the following characteristics:

- The entity has an **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 bits marked as X, as in the following diagram.

										1									2									3	
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**
												X	X	X	X								X	X	X	X	X	X	X	X	X

2.6 revision Attribute

The **revision** attribute is the major version of the template.<9>

CN: revision

ldapDisplayName: revision

attributeId: 1.2.840.113556.1.4.145

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: bf967a21-0de6-11d0-a285-00aa003049e2

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.7 pKICriticalExtensions Attribute

The **pKICriticalExtensions** attribute is a list of OIDs identifying extensions that MUST have critical flags enabled, if present, in an issued certificate. For more information about critical extensions, see [RFC3280] section 4.2.<10>

CN: PKI-Critical-Extensions

ldapDisplayName: pKICriticalExtensions

attributeId: 1.2.840.113556.1.4.1330

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: fc5a9106-3b9d-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16i

2.8 pKIDefaultCSPs Attribute

The **pKIDefaultCSPs** attribute is a list of **cryptographic service providers (CSPs)** that MAY be used to create the **private key** and **public key**.<11>

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 Cryptographic Service Provider (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 indicated by 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 document.

CN: PKI-Default-CSPs

ldapDisplayName: pKIDefaultCSPs

attributeId: 1.2.840.113556.1.4.1334

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: 1ef6336e-3b9e-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

2.9 pKIDefaultKeySpec Attribute

The following table shows the values that are allowed for the **pKIDefaultKeySpec** attribute.<12> For more information about the Microsoft implementation of key types, see [MSDN-KEY].

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

CN: PKI-Default-Key-Spec

ldapDisplayName: pKIDefaultKeySpec

attributeId: 1.2.840.113556.1.4.1327

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: 426cae6e-3b9d-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

2.10 pKIEnrollmentAccess Attribute

The **pKIEnrollmentAccess** attribute is not used.<13>

CN: PKI-Enrollment-Access

ldapDisplayName: pKIEnrollmentAccess

attributeId: 1.2.840.113556.1.4.1335

syntax: String(NT-Sec-Desc)

isSingleValued: FALSE

schemaIdGuid: 926be278-56f9-11d2-90d0-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

2.11 pKIExpirationPeriod Attribute

The **pKIExpirationPeriod** attribute represents the maximum validity period of the certificate that is issued.<14> The attribute is a Unicode string representation of a decimal number, little-endian formatted. The integer value is the count of 100 nanosecond intervals that represent the desired maximum validity period of an issued certificate that is based on this certificate template.

CN: PKI-Expiration-Period

ldapDisplayName: pKIExpirationPeriod

attributeId: 1.2.840.113556.1.4.1331

syntax: String(Octet)

isSingleValued: TRUE

schemaIdGuid: 041570d2-3b9e-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

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.<15>

CN: PKI-Extended-Key-Usage

ldapDisplayName: pKIExtendedKeyUsage

attributeId: 1.2.840.113556.1.4.1333

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: 18976af6-3b9e-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

2.13 pKIKeyUsage Attribute

The **pKIKeyUsage** attribute is a key usage extension.<16>

CN: PKI-Key-Usage

ldapDisplayName: pKIKeyUsage

attributeId: 1.2.840.113556.1.4.1328

syntax: String(Octet)

isSingleValued: TRUE

schemaIdGuid: e9b0a87e-3b9d-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

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.<17>

CN: PKI-Max-Issuing-Depth

ldapDisplayName: pKIMaxIssuingDepth

attributeId: 1.2.840.113556.1.4.1329

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: f0bfdefa-3b9d-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

2.15 pKIOverlapPeriod Attribute

The **pKIOverlapPeriod** is a Unicode string representation of a decimal number, little-endian formatted.<18> The integer value is the count of 100-nanosecond intervals representing the desired period of time before certificate expiration for clients to send a renewal certificate request that is based on this certificate template.

CN: PKI-Overlap-Period

ldapDisplayName: pKIOverlapPeriod

attributeId: 1.2.840.113556.1.4.1332

syntax: String(Octet)

isSingleValued: TRUE

schemaIdGuid: 1219a3ec-3b9e-11d2-90cc-00c04fd91ab1

systemOnly: FALSE

searchFlags: 0

isMemberOfPartialAttributeSet: TRUE

systemFlags: 16

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.<19>

CN: ms-PKI-Template-Schema-Version

ldapDisplayName: msPKI-Template-Schema-Version

attributeId: 1.2.840.113556.1.4.1434

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: 0c15e9f5-491d-4594-918f-32813a091da9

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.17 msPKI-Template-Minor-Revision Attribute

The **msPKI-Template-Minor-Revision** attribute specifies the minor version of the templates.<20> Supported values are 0 to 0x7fffffff.

CN: ms-PKI-Template-Minor-Revision

ldapDisplayName: msPKI-Template-Minor-Revision

attributeId: 1.2.840.113556.1.4.1435

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: 13f5236c-1884-46b1-b5d0-484e38990d58

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

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.<21>

CN: ms-PKI-RA-Signature

ldapDisplayName: msPKI-RA-Signature

attributeId: 1.2.840.113556.1.4.1429

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: fe17e04b-937d-4f7e-8e0e-9292c8d5683e

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.19 msPKI-Minimal-Key-Size Attribute

The **msPKI-Minimal-Key-Size** attribute specifies the minimum size of the public key (in bits) that the client should create to obtain a certificate based on this template.<22>

CN: ms-PKI-Minimal-Key-Size

ldapDisplayName: msPKI-Minimal-Key-Size

attributeId: 1.2.840.113556.1.4.1433

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: e96a63f5-417f-46d3-be52-db7703c503df

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.20 msPKI-Cert-Template-OID Attribute

The **msPKI-Cert-Template-OID** attribute specifies the object identifier (OID) of this template.<23>

CN: ms-PKI-Cert-Template-OID

ldapDisplayName: msPKI-Cert-Template-OID

attributeId: 1.2.840.113556.1.4.1436

syntax: String(Unicode)

isSingleValued: TRUE

schemaIdGuid: 3164c36a-ba26-468c-8bda-c1e5cc256728

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.21 msPKI-Supersede-Templates Attribute

The **msPKI-Supersede-Templates** attribute specifies each string value that contains the common name of a superseded template.<24>

CN: ms-PKI-Supersede-Templates

ldapDisplayName: msPKI-Supersede-Templates

attributeId: 1.2.840.113556.1.4.1437

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: 9de8ae7d-7a5b-421d-b5e4-061f79dfd5d7

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.22 msPKI-RA-Policies Attribute

The **msPKI-RA-Policies** attribute specifies a set of strings that are the encoded policy OIDs. Each value of this attribute SHOULD be set in the Policy extension of one of the **Registration Authority (RA)** certificates that its corresponding **private key** was used to sign the request, as specified in [RFC3280] section 4.2.1.5.<25>

CN: ms-PKI-RA-Policies

ldapDisplayName: msPKI-RA-Policies

attributeId: 1.2.840.113556.1.4.1438

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: d546ae22-0951-4d47-817e-1c9f96faad46

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.23 msPKI-RA-Application-Policies Attribute

The **msPKI-RA-Application-Policies** attribute encapsulates embedded properties for multipurpose use.<26>

The following property names are allowed:

- **msPKI-RA-Application-Policies**: String value that represents a set of application policy OIDs (comma-separated) required in RA certificates that contain public keys whose corresponding private keys are used to sign a request. Application policy OIDs are the same as extended key usage OIDs, as specified in [RFC3280] section 4.2.1.13. The type MUST be the string 'PZPWSTR'.
- **msPKI-Asymmetric-Algorithm**: String value that represents the name of the **asymmetric algorithm**. Type MUST be the string 'PZPWSTR'.
- **msPKI-SecurityDescriptor**: String value that represents the security descriptor (as specified in [MS-ADLS] section 2.240) for the asymmetric key. Type MUST be the string 'PZPWSTR'.
- **msPKI-Symmetric-Algorithm**: String value that represents the name of the **symmetric algorithm** that clients use for key exchanges. Type MUST be the string 'PZPWSTR'.
- **msPKI-Symmetric-Key-Length**: Unsigned integer value that represents the length of the **symmetric key** in bits. Type MUST be **DWORD**.
- **msPKI-Hash-Algorithm**: String value that represents the name of the hash algorithm that clients use. Type MUST be the string 'PZPWSTR'.
- **msPKI-Key-Usage**: Unsigned integer value that represents the private key KeyUsage (see [MS-WCCE] section 3.1.4.4.4). Type MUST be **DWORD**. A bitwise OR of the following flags are supported for this property:

Name	Value	Meaning
NCRYPT_ALLOW_DECRYPT_FLAG	0x00000001	Private key MUST be allowed to perform Decryption operation.
NCRYPT_ALLOW_SIGNING_FLAG	0x00000002	Private key MUST be allowed to perform signature operation.
ALLOW_KEY_AGREEMENT_FLAG	0x00000004	Private key MUST be allowed to perform key-agreement operation.
NCRYPT_ALLOW_ALL_USAGES	0x00ffffff	Private key MUST not be restricted to any specific cryptographic operations.

Each value for this attribute has the following format:

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

Where:

Tag	Description
Name	The property name. This value should be one of the property names previously listed.
Type	There are two supported values for the **Type** field: DWORD and PZPWSTR. If DWORD is used, the **Value** field contains a Unicode string representation of a decimal positive (or 0) number. If PZPWSTR is used, the **Value** field contains a Unicode string.
Value	The value of the parameter.
'	A delimiter symbol separator.

For example:

```
msPKI-Asymmetric-Algorithm
          'PZPWSTR'ECDH'msPKI-Symmetric-Algorithm'PZPWSTR'AES'
```

CN: ms-PKI-RA-Application-Policies

ldapDisplayName: msPKI-RA-Application-Policies

attributeId: 1.2.840.113556.1.4.1675

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: 3c91fbbf-4773-4ccd-a87b-85d53e7bcf6a

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.24 msPKI-Certificate-Policy Attribute

The **msPKI-Certificate-Policy** attribute specifies each string that represents a policy OID to be added in the issued certificate policy extension, as specified in [RFC3280] section 4.2.1.5.<27>

CN: ms-PKI-Certificate-Policy

dapDisplayName: msPKI-Certificate-Policy

attributeId: 1.2.840.113556.1.4.1439

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: 38942346-cc5b-424b-a7d8-6ffd12029c5f

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.25 msPKI-Certificate-Application-Policy Attribute

Each string in the **msPKI-Certificate-Application-Policy** attribute represents an application policy OID to be added in the issued certificate application policy extension.<28> Application policy OIDs are the same as extended key usage OIDs, as specified in [RFC3280] section 4.2.1.13.

CN: ms-PKI-Certificate-Application-Policy

ldapDisplayName: msPKI-Certificate-Application-Policy

attributeId: 1.2.840.113556.1.4.1674

syntax: String(Unicode)

isSingleValued: FALSE

schemaIdGuid: dbd90548-aa37-4202-9966-8c537ba5ce32

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

2.26 msPKI-Enrollment-Flag Attribute

The **msPKI-Enrollment-Flag** attribute specifies the enrollment flags. The attribute's value can be 0 or it can consist of a bitwise OR of flags from the following table:<29>

Flag	Meaning
0x00000001	This flag instructs the client and server to include an S/MIME extension, as specified in [RFC4262], in the request and in the issued certificate.
0x00000002	This flag instructs the CA to put all requests in a pending state.

Flag	Meaning
0x00000004	This flag instructs the CA to publish the issued certificate to the **key recovery agent (KRA)** container in Active Directory, as specified in [MS-ADTS].
0x00000008	This flag instructs clients and servers to append the issued certificate to the **userCertificate** attribute, as specified in [RFC4523], on the user object in Active Directory.
0x00000010	This flag instructs clients to check the user's **userCertificate** attribute, as specified in [RFC4523], in AD for valid certificates that match the template enrolled for.
0x00000020	This flag instructs clients to perform **auto-enrollment** for the specified template.
0x00000040	This flag instructs clients to use private keys whose public keys have existing certificates to sign the request.
0x00000100	This flag instructs the client to get a user's consent before attempting to enroll for a certificate based on the specified template.
0x00000400	This flag instructs the client to delete any expired, revoked, or renewed certificate from the user's **userCertificate** attribute, as specified in [RFC4523], of the user object in Active Directory.
0x00000800	This flag instructs the server to allow enroll-on-behalf-of functionality.

CN: ms-PKI-Enrollment-Flag

ldapDisplayName: msPKI-Enrollment-Flag

attributeId: 1.2.840.113556.1.4.1430

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: d15ef7d8-f226-46db-ae79-b34e560bd12c

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

The value is a bitwise-OR of the flags in the previous table.

2.27 msPKI-Private-Key-Flag Attribute

The **msPKI-Private-Key-Flag** attribute specifies the private key flags. Its value can be 0 or it can consist of a bitwise OR of flags from the following table:<30>

Flag	Meaning
0x00000001	This flag instructs the client to create a **key archival** certificate request, as specified in [MS-WCCE] section 3.1.4.4.4.
0x00000010	This flag instructs the client to allow other applications to copy the private key to a .pfx file,

Flag	Meaning
	as specified in [PKCS12], at a later time.
0x00000020	This flag instructs the client to use additional protection for the private key.

CN: ms-PKI-Private-Key-Flag

ldapDisplayName: msPKI-Private-Key-Flag

attributeId: 1.2.840.113556.1.4.1431

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: bab04ac2-0435-4709-9307-28380e7c7001

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

The value is a bitwise-OR of the flags in the previous table.

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:<31>

Flag	Client processing
0x00000001	This flag instructs the client to supply subject information in the certificate request. Information about creating certificate requests is specified in [MS-WCCE], section 3.1.4.1.1.
0x00010000	This flag instructs the client to supply subject alternate name information in the certificate request. Information about creating certificate requests is specified in [MS-WCCE], section 3.1.4.1.1.
0x00400000	This flag instructs the CA to add the value of the DNS of the root domain where the user's object is present to the subject alternate name extension of the issued certificate.
0x80000000	This flag instructs the CA to set the subject name to the requestor's distinguished name (DN) from AD, as specified in [MS-ADTS], section 3.1.1.1.4.
0x40000000	This flag instructs the CA to set the subject name to the requestor's common name (CN) from AD, as specified in [MS-ADTS], section 3.1.1.1.7.
0x20000000	This flag instructs the CA to add the value of the e-mail attribute from the requestor's user object in AD as the subject of the issued certificate.
0x10000000	This flag instructs the CA to add the value obtained from the DNS attribute of the requestor's user object in AD as the CN in the subject of the issued certificate.
0x08000000	This flag instructs the CA to add the value obtained from the DNS attribute of the requestor's user object in AD to the subject alternate name extension of the issued

Flag	Client processing
	certificate.
0x04000000	This flag instructs the CA to add the value of the e-mail attribute from the requestor's user object in AD to the subject alternate name extension of the issued certificate.
0x02000000	This flag instructs the CA to add the value of the UPN attribute from the requestor's user object in AD, to the subject alternate name extension of the issued certificate.
0x01000000	This flag instructs the CA to add the value of the **objectGUID** attribute from the requestor's user object in AD, to the subject alternate name extension of the issued certificate.

CN: ms-PKI-Certificate-Name-Flag

ldapDisplayName: msPKI-Certificate-Name-Flag

attributeId: 1.2.840.113556.1.4.1432

syntax: Integer

isSingleValued: TRUE

schemaIdGuid: ea1dddc4-60ff-416e-8cc0-17cee534bce7

systemOnly: FALSE

searchFlags: 0

systemFlags: 16

The value is a bitwise-OR of the flags in the previous table.

3 Structure Example

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

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

It 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.

<32>

4 Security Considerations

Any cryptographic protocol has security considerations that deal with key handling during cryptographic operations and key distribution. A public key certificate is not a protocol by itself. However, a public key certificate has most of the same security considerations that a cryptographic protocol has—in the sense that a public key certificate is a "message" from the CA to the RP—a "message" addressed, in effect, to "to whom it may concern." A cryptographic protocol that deals with the transmission, certification, or other use of a public key certificate has security considerations in two areas: around the protocol itself and around the certificate and its use.

In addition, a certificate binds two or more pieces of information together. In the most common case, that would be a public key and a name. The name in such a certificate has security relevance, and there are security considerations around the use and provisioning of those names. In some certificate forms, there are attributes bound to either a name or a key, and there are security considerations around the use and provisioning of those attributes.

4.1 Template Access Control

A certificate template contains corporate policy, about the certification of certificates, that the CA enforces. Therefore, the party that can edit the templates can alter corporate CA policy. Each template must be access-controlled in the template database, so that only persons explicitly authorized to modify corporate CA policy are allowed that access to the templates.

4.2 Coding Practices

Any implementation of a protocol exposes code to security attacks. Such code must be developed according to secure coding and development practices to avoid buffer overflows, denial-of-service attacks, escalation of privilege, and disclosure of information. For an introduction to these concepts, secure development best practices, and common errors, see [HOWARD].

4.3 Security Consideration Citations

Implementers of this protocol should be aware of the following security considerations:

- A secure communication channel should exist between the client and server, which may require an out-of-band trust initialization process such as **DCOM**, as specified in [MS-DCOM] section 3.1.4.1.1.2, or TLS, as specified in [RFC2246].
- A client or server should follow the generally accepted principles of secure key management, as specified in [RFC3280] section 9. For an introduction to these generally accepted principles, see [CRYPTO] and [HOWARD].
- A client or server should not archive or escrow a signing key, as specified in [RFC2797] section 9.
- Clients should verify the public key of the server prior to submitting it for archival or escrow, as specified in [RFC2797] section 9.
- Clients and servers should validate cryptographic parameters prior to issuing or accepting certificates, as specified in [RFC2797] section 9.
- A CA and RA should validate the binding of a client identity to a public key, as specified in [RFC3280] section 9. The CA practices of binding an identity to a public key are specified in [RFC2527].

- A client and server should validate and verify certificate path information as specified in [RFC3280] section 6. The requirements for certificate path validation are specified in [RFC3280] section 9.
- A client and server should validate and verify the freshness of **revocation** information of all digital certificates prior to usage, trust, or **encryption** as specified in [RFC3280] section 6.3. The requirements for revocation freshness are specified in [RFC3280] section 9.
- A CA must encode the distinguished name (DN) in the **Subject** field of a CA certificate identically to the DN in the **Issuer** field in certificates issued by that CA, as specified in [RFC3280] section 9.
- A client or server should follow all security considerations as specified in [RFC3852] and [RFC2986] because neither normative reference has a specific security section.
- A client and server should use an authentication session between client and server to mitigate denial-of-service attacks. Information about an authenticated DCOM session is specified in [MS-DCOM] section 2.2.1.14.4. For more information about generic denial-of-service mitigation techniques, see [HOWARD].
- A client and server should consider security issues regarding **public key infrastructure (PKI)** and certificate repositories. For example, security considerations regarding LDAP repositories are specified in [RFC2559] section 10.

5 Appendix A: Windows Behavior

The information in this specification is applicable to the following versions of Windows:

- Windows 2000
- Windows Server 2003
- Windows XP

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Windows behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that Windows does not follow the prescription.

<1> Section 1.1: A Windows client may perform certificate auto-enrollment with certificate templates and **enterprise CAs**. Auto-enrollment is an optional client process specific to client implementation. Not all clients support auto-enrollment. For more information, see [MSFT-AUTOENROLLMENT].

<2> 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 all versions of Windows Server 2008, Windows Server 2003, and Windows 2000 Server. Version 2 templates are supported by Microsoft CAs that run on Windows Server 2008, Windows Server 2003, Enterprise Edition, and Windows Server 2003 R2 Datacenter Edition. Version 3 templates are supported by CAs that run on Windows Server 2008.

<3> Section 2.1: The **cn** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<4> Section 2.2: The **displayName** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<5> Section 2.3: The **distinguishedName** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<6> Section 2.4: The **flags** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<7> Section 2.4: For more information about the Microsoft implementation of cross-certification, see [MSFT-CROSSCERT].

<8> Section 2.5: The **ntSecurityDescriptor** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<9> Section 2.6: The **revision** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<10> Section 2.7: The **pKICriticalExtensions** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<11> Section 2.8: The **pKIDefaultCSPs** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<12> Section 2.9: The **pKIDefaultKeySpec** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<13> Section 2.10: The **pKIEnrollmentAccess** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<14> Section 2.11: The **pKIExpirationPeriod** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<15> Section 2.12: The **pKIExtendedKeyUsage** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<16> Section 2.13: The **pKIKeyUsage** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<17> Section 2.14: The **pKIMaxIssuingDepth** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<18> Section 2.15: The **pKIOverlapPeriod** attribute is only implemented on Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<19> Section 2.16: The msPKI-Template-Schema-Version attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<20> Section 2.17: The **msPKI-Template-Minor-Revision** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<21> Section 2.18: The **msPKI-RA-Signature** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<22> Section 2.19: The **msPKI-Minimal-Key-Size** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<23> Section 2.20: The **msPKI-Cert-Template-OID** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<24> Section 2.21: The **msPKI-Supersede-Templates** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<25> Section 2.22: The **msPKI-RA-Policies** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<26> Section 2.23: The **msPKI-RA-Application-Policies** attribute is only implemented on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

The **msPKI-RA-Application-Policies** property is available for Windows Server 2003 and Windows Server 2008. The **msPKI-Asymmetric-Algorithm**, **msPKI-SecurityDescriptor**, **msPKI-Symmetric-Algorithm**, **msPKI-Symmetric-Key-Length**, **msPKI-Hash-Algorithm**, and **msPKI-Key-Usage** properties are available on Windows Server 2008 only.

<27> Section 2.24: The **msPKI-Certificate-Policy** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<28> Section 2.25: The **msPKI-Certificate-Application-Policy** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<29> Section 2.26: The **msPKI-Enrollment-Flag** attribute is only implemented on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<30> Section 2.27: The **msPKI-Private-Key-Flag** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<31> Section 2.28: The **msPKI-Certificate-Name-Flag** attribute is implemented only on Windows Server 2003, Windows Server 2003 R2, and Windows Server 2008.

<32> Section 3: Attribute values of default certificate templates added in AD for Windows Server 2003.

```
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;
```

6 Index