[MS-CRTD]:

Certificate Templates Structure

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
- **Patents**. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **License Programs**. To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.
- **Trademarks**. The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names**. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Support. For questions and support, please contact dochelp@microsoft.com.

Revision Summary

Date	Revision History	Revision Class	Comments
12/18/2006	0.1	New	Version 0.1 release
3/2/2007	1.0	Major	Version 1.0 release
4/3/2007	1.1	Minor	Version 1.1 release
5/11/2007	1.2	Minor	Version 1.2 release
6/1/2007	2.0	Major	Updated and revised the technical content.
7/3/2007	2.0.1	Editorial	Changed language and formatting in the technical content.
7/20/2007	2.0.2	Editorial	Changed language and formatting in the technical content.
8/10/2007	2.0.3	Editorial	Changed language and formatting in the technical content.
9/28/2007	2.1	Minor	Clarified the meaning of 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.
1/25/2008	3.1.1	Editorial	Changed language and formatting in the technical content.
3/14/2008	4.0	Major	Updated and revised the technical content.
5/16/2008	4.0.1	Editorial	Changed language and formatting in the technical content.
6/20/2008	5.0	Major	Updated and revised the technical content.
7/25/2008	5.0.1	Editorial	Changed language and formatting in the technical content.
8/29/2008	5.1	Minor	Clarified the meaning of the technical content.
10/24/2008	5.2	Minor	Clarified the meaning of the technical content.
12/5/2008	5.2.1	Editorial	Editorial Update.
1/16/2009	6.0	Major	Updated and revised the technical content.
2/27/2009	7.0	Major	Updated and revised the technical content.
4/10/2009	8.0	Major	Updated and revised the technical content.
5/22/2009	8.1	Minor	Clarified the meaning of the technical content.
7/2/2009	8.1.1	Editorial	Changed language and formatting in the technical content.
8/14/2009	9.0	Major	Updated and revised the technical content.
9/25/2009	10.0	Major	Updated and revised the technical content.
11/6/2009	11.0	Major	Updated and revised the technical content.
12/18/2009	11.0.1	Editorial	Changed language and formatting in the technical content.
1/29/2010	12.0	Major	Updated and revised the technical content.
3/12/2010	13.0	Major	Updated and revised the technical content.

Date	Revision History	Revision Class	Comments
4/23/2010	13.0.1	Editorial	Changed language and formatting in the technical content.
6/4/2010	14.0	Major	Updated and revised the technical content.
7/16/2010	15.0	Major	Updated and revised the technical content.
8/27/2010	15.1	Minor	Clarified the meaning of the technical content.
10/8/2010	15.1	None	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	16.0	Major	Updated and revised the technical content.
1/7/2011	16.0	None	No changes to the meaning, language, or formatting of the technical content.
2/11/2011	16.0	None	No changes to the meaning, language, or formatting of the technical content.
3/25/2011	16.0	None	No changes to the meaning, language, or formatting of the technical content.
5/6/2011	17.0	Major	Updated and revised the technical content.
6/17/2011	17.1	Minor	Clarified the meaning of the technical content.
9/23/2011	17.1	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	18.0	Major	Updated and revised the technical content.
3/30/2012	18.0	None	No changes to the meaning, language, or formatting of the technical content.
7/12/2012	18.0	None	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	19.0	Major	Updated and revised the technical content.
1/31/2013	19.0	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	20.0	Major	Updated and revised the technical content.
11/14/2013	20.0	None	No changes to the meaning, language, or formatting of the technical content.
2/13/2014	21.0	Major	Updated and revised the technical content.
5/15/2014	21.0	None	No changes to the meaning, language, or formatting of the technical content.
6/30/2015	22.0	Major	Significantly changed the technical content.
10/16/2015	22.0	None	No changes to the meaning, language, or formatting of the technical content.
7/14/2016	22.0	None	No changes to the meaning, language, or formatting of the technical content.
6/1/2017	22.0	None	No changes to the meaning, language, or formatting of the technical content.

Date	Revision History	Revision Class	Comments
9/15/2017	23.0	Major	Significantly changed the technical content.
9/12/2018	24.0	Major	Significantly changed the technical content.
4/7/2021	25.0	Major	Significantly changed the technical content.
6/25/2021	26.0	Major	Significantly changed the technical content.
9/20/2023	27.0	Major	Significantly changed 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 **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.

Sections 1.7 and 2 of this specification are normative. All other sections and examples in this specification are informative.

1.1 Glossary

This document uses the following terms:

access control entry (ACE): An entry in an **access control list (ACL)** that contains a set of user rights and a **security identifier (SID)** that identifies a principal for whom the rights are allowed, denied, or audited.

access control list (ACL): A list of **access control entries (ACEs)** that collectively describe the security rules for authorizing access to some resource; for example, an object or set of objects.

Active Directory: The Windows implementation of a general-purpose directory service, which uses **LDAP** as its primary access protocol. **Active Directory** stores information about a variety of **objects** in the network such as user accounts, computer accounts, groups, and all related credential information used by Kerberos [MS-KILE]. **Active Directory** is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS), which are both described in [MS-ADOD]: Active Directory Protocols Overview.

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

attestation: A process of establishing some property of a computer platform or of a trusted platform module (TPM) key, in part through TPM cryptographic operations.

attribute: An identifier for a single or multivalued data element that is associated with a directory **object**. An **object** consists of its **attributes** and their values. For example, cn (common name), street (street address), and mail (email addresses) can all be **attributes** of a user object. An **attribute's** schema, including the syntax of its values, is defined in an attributeSchema **object**.

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

certificate: A certificate is a collection of attributes and extensions that can be stored persistently. The set of attributes in a certificate can vary depending on the intended usage of the certificate. A certificate securely binds a public key to the entity that holds the corresponding private key. A certificate is commonly used for authentication and secure exchange of information on open networks, such as the Internet, extranets, and intranets. Certificates are digitally signed by the issuing **certification authority (CA)** and can be issued for a user, a computer, or a service. The most widely accepted format for certificates is defined by the ITU-T X.509 version 3 international standards. For more information about attributes and extensions, see [RFC3280] and [X509] sections 7 and 8.

certificate enrollment: The process of acquiring a digital certificate from a **certificate authority (CA)**, which typically requires an end entity to first makes itself known to the CA (either directly, or through a registration authority). This certificate and its associated **private key**

establish a trusted identity for an entity that is using the **public key**–based services and applications. Also referred to as simply "enrollment".

certificate renewal request: An enrollment request for a new certificate where the request is signed using an existing certificate. The renewal request can use the key pair from the existing certificate or a new key pair. After the new certificate has been issued, it is meant (but not required) to replace the older certificate (a renewed certificate).

certificate template: A list of attributes that define a blueprint for creating an X.509 **certificate**. It is often referred to in non-Microsoft documentation as a "certificate profile". A **certificate template** is used to define the content and purpose of a digital certificate, including issuance requirements (certificate policies), implemented X.509 extensions such as application policies, key usage, or extended key usage as specified in [X509], and enrollment permissions. Enrollment permissions define the rules by which a **certification authority (CA)** will issue or deny certificate requests. In Windows environments, **certificate templates** are stored as **objects** in the **Active Directory** and used by Microsoft enterprise **CAs**.

certification authority (CA): A third party that issues **public key certificates**. Certificates serve to bind public keys to a user identity. Each user and certification authority (CA) can decide whether to trust another user or CA for a specific purpose, and whether this trust should be transitive. For more information, see [RFC3280].

common name (CN): A string attribute of a **certificate** that is one component of a distinguished name (DN). In Microsoft Enterprise uses, a CN must be unique within the forest where it is defined and any forests that share trust with the defining forest. The website or email address of the certificate owner is often used as a common name. Client applications often refer to a **certification authority (CA)** by the CN of its signing certificate.

cryptographic service provider (CSP): A software module that implements cryptographic functions for calling applications that generates digital signatures. Multiple **CSPs** may be installed. A **CSP** is identified by a name represented by a NULL-terminated Unicode string.

digital signature: A message authenticator that is typically derived from a cryptographic operation by using an asymmetric algorithm and private key. When a symmetric algorithm is used for this purpose, the authenticator is typically referred to as a Message Authentication Code (MAC).

directory: The database that stores information about objects such as users, groups, computers, printers, and the directory service that makes this information available to users and applications.

discretionary access control list (DACL): An **access control list (ACL)** that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object.

distinguished name (DN): In **Lightweight Directory Access Protocol (LDAP)**, an LDAP Distinguished Name, as described in [RFC2251] section 4.1.3. The DN of an object is the DN of its parent, preceded by the RDN of the object. For example: CN=David Thompson, OU=Users, DC=Microsoft, DC=COM. For definitions of CN and OU, see [RFC2256] sections 5.4 and 5.12, respectively.

domain: A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a **domain controller (DC)** and host a member list that identifies all members of the domain, as well as optionally hosting the **Active Directory** service. The domain controller provides authentication of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [MS-AUTHSOD] section 1.1.1.5 and [MS-ADTS].

domain controller (DC): The service, running on a server, that implements **Active Directory**, or the server hosting this service. The service hosts the data store for **objects** and interoperates

with other **DCs** to ensure that a local change to an **object** replicates correctly across all **DCs**. When **Active Directory** is operating as Active Directory Domain Services (AD DS), the **DC** contains full NC replicas of the configuration naming context (config NC), schema naming context (schema NC), and one of the domain NCs in its forest. If the AD DS **DC** is a global catalog server (GC server), it contains partial NC replicas of the remaining domain NCs in its forest. For more information, see [MS-AUTHSOD] section 1.1.1.5.2 and [MS-ADTS]. When **Active Directory** is operating as Active Directory Lightweight Directory Services (AD LDS), several AD LDS **DCs** can run on one server. When **Active Directory** is operating as AD DS, only one AD DS **DC** can run on one server. However, several AD LDS **DCs** can coexist with one AD DS **DC** on one server. The AD LDS **DC** contains full NC replicas of the config NC and the schema NC in its forest. The domain controller is the server side of Authentication Protocol Domain Support [MS-APDS].

enroll: To request and acquire a digital certificate from a **certificate authority (CA)**. This is typically accomplished through a **certificate enrollment** process.

Enroll On Behalf Of (EOBO): A proxy enrollment process in which one user, typically an administrator, enrolls for a **certificate** for a second user by using the administrator credentials.

enrollment permissions: A list of administrator-defined rights or **access control lists (ACLs)** that define the capability of a given client (user, machine, or device). **Enrollment permissions** can define a client capability to read a **certificate template**, write a **certificate template**, enroll for a **certificate** based on a specified **certificate template**, auto-enroll for a **certificate** based on a specified **certificate template**, or change permissions on a **certificate template**. **Enrollment permissions** are stored on a **certificate template** and are enforced by the **certificate authority (CA)**. For more information, see [MSFT-TEMPLATES].

enterprise certificate authority (enterprise CA): A **certificate authority (CA)** that is a member of a **domain** and that uses the **domain's Active Directory** service to store policy, authentication, and other information related to the operation of the **CA**. Specifically, the enterprise CA is a server implementation of the Windows Client Certificate Enrollment Protocol that uses the certificate template data structure (see [MS-CRTD]) in its CA policy algorithm implementation.

fully qualified domain name (FQDN): In **Active Directory**, a fully qualified domain name (FQDN) that identifies a **domain**.

key: In cryptography, a generic term used to refer to cryptographic data that is used to initialize a cryptographic algorithm. **Keys** are also sometimes referred to as keying material.

key archival: The process by which the entity requesting the **certificate** also submits the **private key** during the process. The **private key** is encrypted such that only a **key recovery agent** can obtain it, preventing accidental disclosure, but preserving a copy in case the entity is unable or unwilling to decrypt data.

key recovery agent (KRA): A user, machine, or registration authority that has enrolled and obtained a key recovery certificate. A **KRA** is any entity that possesses a **KRA private key** and **certificate**. For more information on **KRAs** and the archival process, see [MSFT-ARCHIVE].

Lightweight Directory Access Protocol (LDAP): The primary access protocol for **Active Directory**. Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), which allows users to query and update information in a directory service (DS), as described in [MS-ADTS]. The Lightweight Directory Access Protocol can be either version 2 [RFC1777] or version 3 [RFC3377].

NetBIOS name: A 16-byte address that is used to identify a NetBIOS resource on the network. For more information, see [RFC1001] and [RFC1002].

object: In **Active Directory**, an entity consisting of a set of attributes, each attribute with a set of associated values. For more information, see [MS-ADTS]. See also directory object.

object identifier (OID): In the context of a directory service, a number identifying an object class or **attribute**. Object identifiers are issued by the ITU and form a hierarchy. An OID is represented as a dotted decimal string (for example, "1.2.3.4"). For more information on OIDs, see [X660] and [RFC3280] Appendix A. OIDs are used to uniquely identify certificate templates available to the **certification authority (CA)**. Within a **certificate**, OIDs are used to identify standard extensions, as described in [RFC3280] section 4.2.1.x, as well as non-standard extensions.

private key: One of a pair of keys used in public-key cryptography. The private key is kept secret and is used to decrypt data that has been encrypted with the corresponding public key. For an introduction to this concept, see [CRYPTO] section 1.8 and [IEEE1363] section 3.1.

public key: One of a pair of keys used in public-key cryptography. The public key is distributed freely and published as part of a digital certificate. For an introduction to this concept, see [CRYPTO] section 1.8 and [IEEE1363] section 3.1.

registration authority (RA): The authority in a PKI that verifies user requests for a digital certificate and indicates to the **certificate authority (CA)** that it is acceptable to issue a **certificate**.

revocation: The process of invalidating a certificate. For more details, see [RFC3280] section 3.3.

Secure/Multipurpose Internet Mail Extensions (S/MIME): A standard for encrypted and digitally signed electronic mail that allows users to send encrypted messages and authenticate received messages.

security descriptor: A data structure containing the security information associated with a securable **object**. A **security descriptor** identifies an **object's** owner by its **security identifier (SID)**. If access control is configured for the **object**, its **security descriptor** contains a **discretionary access control list (DACL)** with **SIDs** for the security principals who are allowed or denied access. Applications use this structure to set and query an **object's** security status. The **security descriptor** is used to guard access to an **object** as well as to control which type of auditing takes place when the **object** is accessed. The **security descriptor** format is specified in [MS-DTYP] section 2.4.6; a string representation of **security descriptors**, called SDDL, is specified in [MS-DTYP] section 2.5.1.

security identifier (SID): An identifier for security principals that is used to identify an account or a group. Conceptually, the **SID** is composed of an account authority portion (typically a **domain**) and a smaller integer representing an identity relative to the account authority, termed the relative identifier (RID). The **SID** format is specified in [MS-DTYP] section 2.4.2; a string representation of **SIDs** is specified in [MS-DTYP] section 2.4.2 and [MS-AZOD] section 1.1.1.2.

symmetric algorithm: A cryptographic algorithm that uses one secret key that can be shared between authorized parties. The key must be kept secret between communicating parties. The same key is used for both encryption and decryption. For an introduction to this concept and terminology, see [CRYPTO] section 1.5, [IEEE1363] section 3, and [SP800-56A] section 3.1.

symmetric key: A secret key used with a cryptographic symmetric algorithm. The key needs to be known to all communicating parties. For an introduction to this concept, see [CRYPTO] section 1.5.

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

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents

in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

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.

[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-ADSC] Microsoft Corporation, "Active Directory Schema Classes".

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

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

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

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

[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., Glaperin, S., and Adams, C., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999, http://www.rfc-editor.org/info/rfc2560

[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.rfc-editor.org/info/rfc3280

[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.rfc-editor.org/rfc/rfc4523.txt

[RFC7292] Moriarty, K., Ed., Nystrom, M., Parkinson, S., et al., "PKCS #12: Personal Information Exchange Syntax v1.1", July 2014, https://www.rfc-editor.org/info/rfc7292

1.2.2 Informative References

[MS-CERSOD] Microsoft Corporation, "Certificate Services Protocols Overview".

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

[MSFT-CVE-2022-26931] Microsoft Corporation, "Windows Kerberos Elevation of Privilege Vulnerability", CVE-2022-26931 May 10, 2022, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26931

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]. The structures also provide settings that influence the behavior of the computer certificate **autoenrollment** feature that is described in [MS-CERSOD]. 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 **domain controller (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 class ([MS-ADSC] section 2.221) is the **Active Directory** schema class that is used for storing template information and **attributes**. 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.
0x00001000 CT_FLAG_DONOTPERSISTINDB	This flag indicates that the record of a certificate request for a certificate that is issued need not be persisted by the CA.<6>

Flag	Meaning
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 ([MS-ADA3] section 2.37) 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**) ([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 Windows **autoenrollment** client to **enroll** for that template automatically.

2.5.1 Determining Enrollment Permission of an End Entity for a Template

The following processing rules are to determine the **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 **security identifier (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 ([MS-DTYP] section 2.4.4.3) 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 ([MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_OBJECT_ACE_TYPE (0x05). This implies that it is an **ACCESS_ALLOWED_OBJECT_ACE** structure ([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.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
								X																							

- The **ObjectType** field of the ACCESS_ALLOWED_OBJECT_ACE structure MUST be identical to the Enroll 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 ([MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE. This implies that it is an **ACCESS_ALLOWED_ACE** structure ([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.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
												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 (0x06).

2.5.2 Determining Autoenrollment Permission of an End Entity for a Template

The following processing rules are to determine the **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 ([MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_OBJECT_ACE_TYPE. This implies that it is an **ACCESS_ALLOWED_OBJECT_ACE** structure ([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.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
								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 ([MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE. This implies that it is an **ACCESS_ALLOWED_ACE** structure ([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.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
												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

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** ([MS-DTYP] section 2.4.2) that is identical to the SID associated with this ACE.
  - The **AceType** field of the **ACE_HEADER** structure ([MS-DTYP] section 2.4.4.1) is ACCESS_ALLOWED_ACE_TYPE (0x05).

- The **Mask** field of the **ACCESS_ALLOWED_ACE_TYPE** structure MUST have the following bits set as shown in [MS-DTYP] section 2.4.3:
  - 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 that is identical to the SID associated with this ACE.
  - The **AceType** field of the **ACE_HEADER** structure is ACCESS_ALLOWED_ACE_TYPE (0x00).
  - 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 that is identical to the SID associated with this ACE.
  - The **AceType** field of the **ACE_HEADER** structure 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 and examples regarding usage, see [MS-WCCE] sections 3.1.2.4.2.2.1.9 and 3.2.2.6.2.1.4.2. For schema details of this **attribute**, see [MS-ADA3] section 2.199.

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 2.95.

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 [MS-ADA3] section 2.96.

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 [MS-ADA3] section 2.97.

2.10 pKIEnrollmentAccess Attribute

The pKIEnrollmentAccess attribute is not used by any protocol.<12> For schema details of this **attribute**, see [MS-ADA3] section 2.98.

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 2.3.3.

For schema details of this attribute, see [MS-ADA3] section 2.99.

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 [MS-ADA3] section 2.100.

2.13 pKIKeyUsage Attribute

The pKIKeyUsage attribute is a **key** usage extension.<15> For schema details of this **attribute**, see [MS-ADA3] section 2.101.

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 [MS-ADA3] section 2.102.

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**, as described in [MS-CERSOD] sections 2.5.2, 2.5.3.1, and 3.6. The **attribute** is an 8-byte octet string that initializes the FILETIME structure that is defined in [MS-DTYP] section 2.3.3.

For schema details of this attribute, see [MS-ADA3] section 2.103.

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, 3, and 4.<17> For schema details of this **attribute**, see [MS-ADA2] section 2.617.

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 [MS-ADA2] section 2.616.

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 [MS-ADA2] section 2.613.

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 creates to obtain a **certificate** based on this template.<20> For schema details of this **attribute**, see [MS-ADA2] section 2.605.

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 [MS-ADA2] section 2.598.

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 2.615.

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 [MS-ADA2] section 2.612.

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 Syntax Option 1

Note An alternative scenario for template schema version 4 is defined in section 2.23.2.

If either of the following is true:

- The template version is 1 or 2.
- The template version is 4 and the template has the CT_FLAG_USE_LEGACY_PROVIDER bit of the msPKI-Private-Key-Flag **attribute** set.

Then the msPKI-RA-Application-Policies attribute contains 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 Syntax Option 2

Note An alternative scenario for template schema version 4 is defined in section 2.23.1.

If either of the following is true:

- The template is version 3.
- The template version is 4 and the template does not have the CT_FLAG_USE_LEGACY_PROVIDER bit of the msPKI-Private-Key-Flag **attribute** set.

Then the msPKI-RA-Application-Policies attribute contains 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

Tag	Description
	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**: A Security Descriptor Description Language (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.
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 [MS-ADA2] section 2.611.

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 [MS-ADA2] section 2.601.

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 [MS-ADA2] section 2.599.

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-ADTS].
0x00000008 CT_FLAG_PUBLISH_TO_DS	This flag instructs 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

Flag	Meaning
	existing certificate. For more information, see [MS-WCCE] section 3.2.2.6.2.1.4.5.6.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. For information about autoenrollment and the local certificate storage, see [MS-CERSOD] section 2.1.2.2.2.
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] 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 [RFC3280] section 4.2.1.10) in the end entity certificates.<31>
0x00010000 CT_FLAG_ALLOW_PREVIOUS_APPROVAL_KEYBASEDRENEWAL_VALIDATE_REENROLLMENT	This flag instructs the CA to ignore the requirement for Enroll permissions on the template when processing renewal requests as specified in [MS-WCCE] section

Flag	Meaning
	3.2.2.6.2.1.4.5.6.<32>
0x00020000 CT_FLAG_ISSUANCE_POLICIES_FROM_REQUEST	This flag indicates that the certificate issuance policies to be included in the issued certificate come from the request rather than from the template. The template contains a list of all of the issuance policies that the request is allowed to specify; if the request contains policies that are not listed in the template, then the request is rejected. For the processing rules of this flag, see [MS-WCCE] section 3.2.2.6.2.1.4.5.8.<33>
0x00040000 CT_FLAG_SKIP_AUTO_RENEWAL	This flag indicates that the certificate should not be auto-renewed, although it has a valid template.
0x00080000 CT_FLAG_NO_SECURITY_EXTENSION	This flag<34> instructs the CA to not include the security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2), as specified in [MS-WCCE] sections 2.2.2.7.7.4 and 3.2.2.6.2.1.4.5.9, in the issued certificate.

For schema details of this attribute, see [MS-ADA2] section 2.603.

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.<35>

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 [RFC7292], 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.

Flag	Meaning
0x00000080 CT_FLAG_REQUIRE_SAME_KEY_RENEWAL	This flag instructs the client to use the same **key** when renewing the certificate.<36>
0x00000100 CT_FLAG_USE_LEGACY_PROVIDER	This flag instructs the client to process the msPKI-RA-Application-Policies **attribute** as specified in section 2.23.1.<37>
0x00000000 * CT_FLAG_ATTEST_NONE	This flag indicates that **attestation** data is not required when creating the certificate request. It also instructs the server to not add any attestation **OIDs** to the issued certificate. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.
0x00002000 * CT_FLAG_ATTEST_REQUIRED	This flag informs the client that attestation data is required when creating the certificate request. It also instructs the server that attestation must be completed before any certificates can be issued. For more details, see [MS-WCCE] sections 3.1.2.4.2.2.2.8 and 3.2.2.6.2.1.4.5.7.
0x00001000 * CT_FLAG_ATTEST_PREFERRED	This flag informs the client that it SHOULD include attestation data if it is capable of doing so when creating the certificate request. It also instructs the server that attestation might or might not be completed before any certificates can be issued. For more details, see [MS-WCCE] sections 3.1.2.4.2.2.2.8 and 3.2.2.6.2.1.4.5.7.
0x00004000 * CT_FLAG_ATTESTATION_WITHOUT_POLICY	This flag instructs the server to not add any certificate policy OIDs to the issued certificate even though attestation SHOULD be performed. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.
0x00000200 * CT_FLAG_EK_TRUST_ON_USE	This flag indicates that attestation based on the user's credentials is to be performed. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.
0x00000400 * CT_FLAG_EK_VALIDATE_CERT	This flag indicates that attestation based on the hardware certificate of the Trusted Platform Module (TPM) is to be performed. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.
0x00000800 * CT_FLAG_EK_VALIDATE_KEY	This flag indicates that attestation based on the hardware key of the TPM is to be performed. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.
0x00200000 * CT_FLAG_HELLO_LOGON_KEY	This flag indicates that the key is used for Windows Hello logon. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.

* Support for these flags is specified in the following behavior note.<38>

- The bitwise AND of the value of the msPKI-Private-Key-Flag attribute and 0x000F0000 determines whether the current **CA** can issue a certificate based on this template, as explained in [MS-WCCE] section 3.2.2.6.2.1.4.5.7.
- The bitwise AND of the value of the msPKI-Private-Key-Flag attribute and 0x0F000000 determines whether the current template is supported by the client, as explained in [MS-WCCE] section 3.1.2.4.2.2.2.8.

For schema details of this attribute, see [MS-ADA2] section 2.610.

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.<39> 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.
0x00800000 CT_FLAG_SUBJECT_ALT_REQUIRE_SPN	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.
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 email 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 email 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

Flag	Client processing
	Active Directory, as specified in [MS-ADTS] section 3.1.1.1.4.
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**.<40>

For schema details of this attribute, see [MS-ADA2] section 2.600.

3 Structure Example

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

```
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"*
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"
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" EMPTY*
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.<41><42>

4 Security Considerations

4.1 Policy

Certificate templates, including their **access control lists (ACLs)**, express policy by which the **enterprise certificate authority (enterprise CA)** 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 (enterprise CA)** 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 might 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 updates to those products.

The terms "earlier" and "later", when used with a product version, refer to either all preceding versions or all subsequent versions, respectively. The term "through" refers to the inclusive range of versions. Applicable Microsoft products are listed chronologically in this section.

Windows Client

- Windows 2000 Professional operating system
- Windows XP operating system
- Windows Vista operating system
- Windows 7 operating system
- Windows 8 operating system
- Windows 8.1 operating system
- Windows 10 operating system
- Windows 11 operating system

Windows Server

- Windows 2000 Server operating system
- Windows Server 2003 operating system
- Windows Server 2008 operating system
- Windows Server 2008 R2 operating system
- Windows Server 2012 operating system
- Windows Server 2012 R2 operating system
- Windows Server 2016 operating system
- Windows Server 2019 operating system
- Windows Server 2022 operating system

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates 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 four template versions: version 1, version 2, version 3, and version 4. Version 1 templates are supported by **CAs** that run on Windows 2000 Server and later. Version 2 templates are supported by Microsoft CAs that run on Windows Server 2003 Enterprise Edition operating system, Windows Server 2003 R2 Datacenter Edition operating system, and Windows Server

2008 and later. Version 3 templates are supported by CAs that run on Windows Server 2008 and later. Version 4 templates are supported by CAs that run on Windows Server 2012 and later.

<2> Section 2.1: The cn attribute is implemented in Windows 2000 Server and later.

<3> Section 2.2: The displayName attribute is implemented in Windows 2000 Server and later.

<4> Section 2.3: The distinguishedName attribute is implemented in Windows 2000 Server and later.

<5> Section 2.4: The flags attribute is implemented in Windows 2000 Server and later.

<6> Section 2.4: This flag is supported in applicable Windows Server releases, with exception of Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2 operating system, and Windows Server 2008.

<7> Section 2.5: The ntSecurityDescriptor attribute is implemented in Windows 2000 Server and later.

<8> Section 2.6: The revision attribute is implemented in Windows 2000 Server and later.

<9> Section 2.7: The pKICriticalExtensions attribute is implemented in Windows 2000 Server and later.

<10> Section 2.8: The pKIDefaultCSPs attribute is implemented in Windows 2000 Server and later.

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

<12> Section 2.10: The pKIEnrollmentAccess attribute is implemented in Windows 2000 Server and later.

<13> Section 2.11: The pKIExpirationPeriod attribute is implemented in Windows 2000 Server and later.

<14> Section 2.12: The pKIExtendedKeyUsage attribute is implemented in Windows 2000 Server and later.

<15> Section 2.13: The pKIKeyUsage attribute is implemented in Windows 2000 Server and later.

<16> Section 2.14: The pKIMaxIssuingDepth attribute is implemented in Windows 2000 Server and later.

<17> Section 2.16: The msPKI-Template-Schema-Version attribute is implemented in applicable Windows Server releases, with the exception of Windows 2000 Server.

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

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

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

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

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

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

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

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

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

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

<28> Section 2.26: This flag is supported in applicable Windows Server releases, with the exception of Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2.

<29> Section 2.26: This flag is supported in Windows Vista and later clients and in Windows Server 2008 and later servers.

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

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

<32> Section 2.26: This flag is supported in Windows Server 2012 and later.

<33> Section 2.26: This flag is supported in Windows Server 2012 and later.

<34> Section 2.26: This flag is supported by the operating systems specified in [MSFT-CVE-2022-26931], each with its related KB article download installed.

<35> Section 2.27: The msPKI-Private-Key-Flag attribute is implemented in Windows Server 2003 and later.

<36> Section 2.27: This flag is supported in Windows Server 2012 and later.

<37> Section 2.27: This flag is supported in Windows Server 2012 and later.

<38> Section 2.27: These flags are supported only in Windows Server 2012 R2 and later.

<39> Section 2.28: The msPKI-Certificate-Name-Flag attribute is implemented in Windows Server 2003 and later.

<40> Section 2.28: This flag is supported in Windows Server 2008 R2 and later.

<41> 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;
```

<42> 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 and later clients and by Windows Server 2008 and later servers.

```
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 this document since the last release. Changes are classified as Major, Minor, or None.

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.
- A document revision that captures changes to protocol functionality.

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 **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

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

Section	Description	Revision class
2.4 flags Attribute	11415 : Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000.	Major
2.26 msPKI-Enrollment-Flag Attribute	Added the CT_FLAG_NO_SECURITY_EXTENSION (0x00080000) enrollment flag that instructs the CA to not include security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2) in the issued certificate. Also added behavior note to indicate that the operating systems that support this enrollment flag are specified in [MSFT-CVE-2022-26931], each with its related KB article download installed,.	Major
2.27 msPKI-Private-Key-Flag Attribute	11190 : Replaced normative reference [PKCS12] with [RFC7292].	Minor

7 Index

N

O

P

R

S

T

V