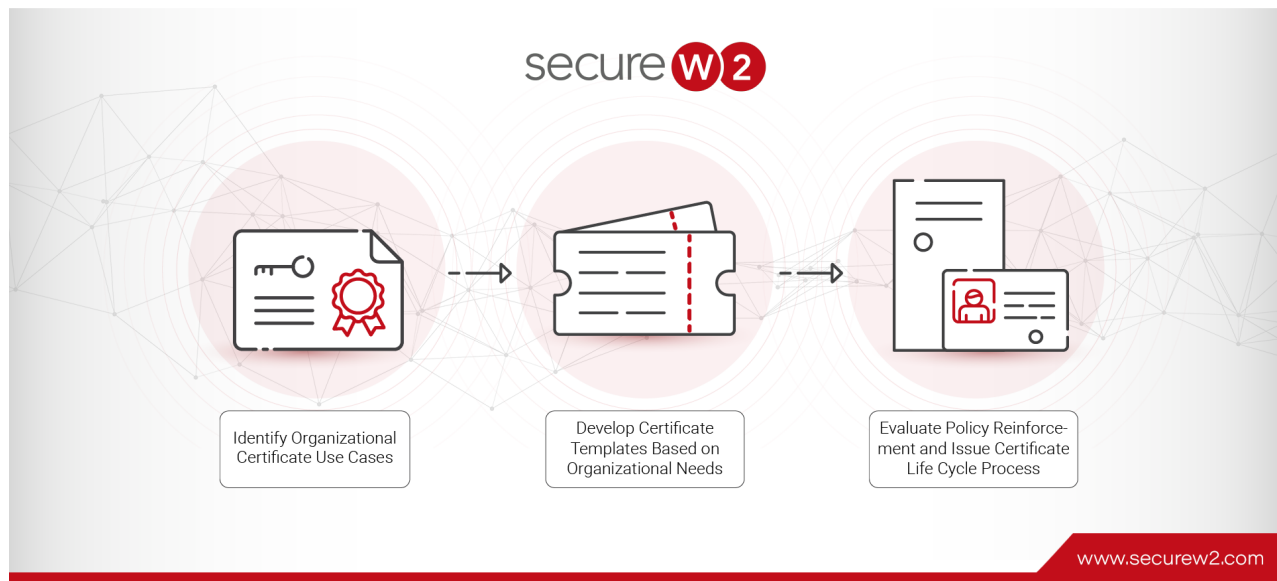


AD CS Certificate Templates: Best Practices

 securew2.com/blog/ad-cs-certificate-templates-security-best-practices

Justin Boone

September 26, 2024



AD CS Certificate Templates: Security Best Practices

Key Points

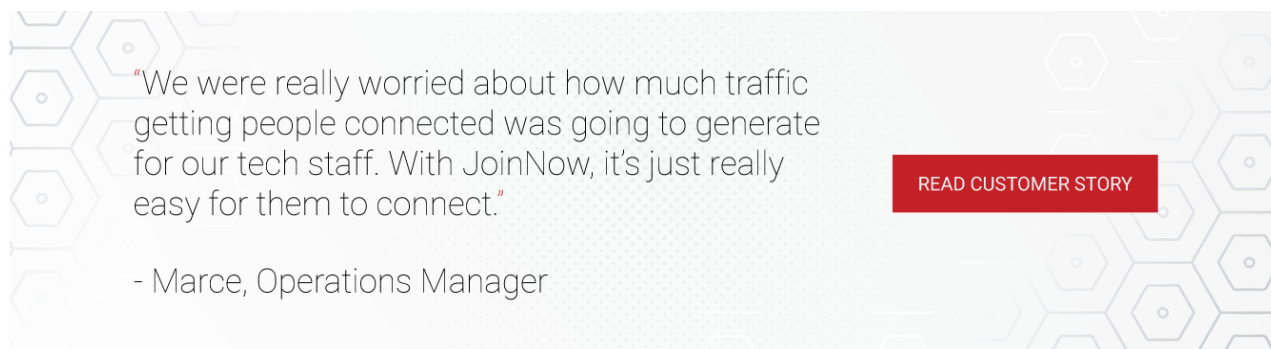
- AD CS certificate templates have different subject types and key usages, such as User, Computer, DirEmailRep, CA, and Key Recovery Agent.
- Be mindful of common weaknesses in certificate templates, such as incorrect EKU settings and ACL permissions, which could jeopardize network security.
- To protect your network, implement best practices for managing certificate templates, such as enforcing strict issuing rules and properly monitoring the certificate lifetime.

Microsoft AD CS allows administrators to establish their domain's CA to deploy a digital certificate with Microsoft PKI Infrastructure. To properly run their PKI infrastructure and after establishing their hierarchy, administrators will look to assign AD CS certificates to specific groups or users depending on their role within the domain. As determined by the *Specterops* article, the certificate templates can be easily misconfigured. They can lead to the organization's domain being compromised through certificate theft, domain escalation, and account and domain persistence attacks.

There is a lot of information to cover, so to understand the best practices, the first four sections will cover the certificate properties, the default certificates, their functions, and the subcategories and key usage the digital certificates belong to. Following that, the article will cover the templates with the most use cases, the certificate's most vulnerable properties, and the best security practices to secure them and the domain.

*Disclaimer: SecureW2 offers a Cloud Managed PKI Service, but this document was vetted by a third party to ensure non-biased best practices were recommended.

Certificate Template Properties



"We were really worried about how much traffic getting people connected was going to generate for our tech staff. With JoinNow, it's just really easy for them to connect."

- Marce, Operations Manager

[READ CUSTOMER STORY](#)

Many certificate properties are essential for determining the certificate functionality for the specific template. Below is a review of these properties and why they are crucial.

General

This section provides an overview of the template, including its display name, template name, and description.

Compatibility

It outlines the compatibility settings for the template, indicating the operating system or application versions that can work with this template.

Request Handling

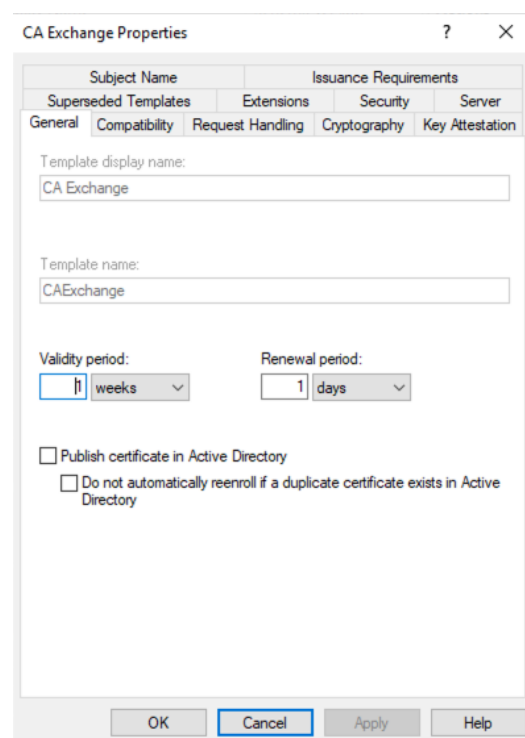
The handling of certificate requests is specified, including options such as whether the Private Key can be exported, if requesters can provide their subject name, and the choice of the service provider (CSP) to be used.

Subject Name

It determines how the subject name (which contains identity information for the certified entity) is constructed. This includes settings for attributes like common name, organization, locality, and other relevant details.

Superseded Templates

The template indicates whether it can be used to renew or update certificates based on templates. It defines which templates can be replaced by using this one.



The screenshot shows the 'CA Exchange Properties' dialog box with the 'Compatibility' tab selected. The 'General' tab is also visible. The 'Compatibility' tab contains the following fields and options:

- Subject Name**: A text box containing 'CA Exchange'.
- Issuance Requirements**: A section with tabs for 'Superseded Templates', 'Extensions', 'Security', and 'Server'.
- Template display name**: A text box containing 'CA Exchange'.
- Template name**: A text box containing 'CAExchange'.
- Validity period**: A dropdown menu set to '11 weeks'.
- Renewal period**: A dropdown menu set to '1 days'.
- ☐ Publish certificate in Active Directory
- ☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

At the bottom of the dialog are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Extensions

Extensions in the certificate can be added if necessary. These extensions may include information about Usage, enhanced Usage, and custom extensions. They provide details regarding how the certificate should be used.

Cryptography

The cryptographic properties of the template are defined here. This includes specifying length, algorithm selection, and other cryptographic properties. It also determines which algorithms should be utilized for encryption hashing operations and digital signatures.

Key Attestation

Specifies if the CA needs to validate the Key and provide information about its properties.

Issuance Requirements

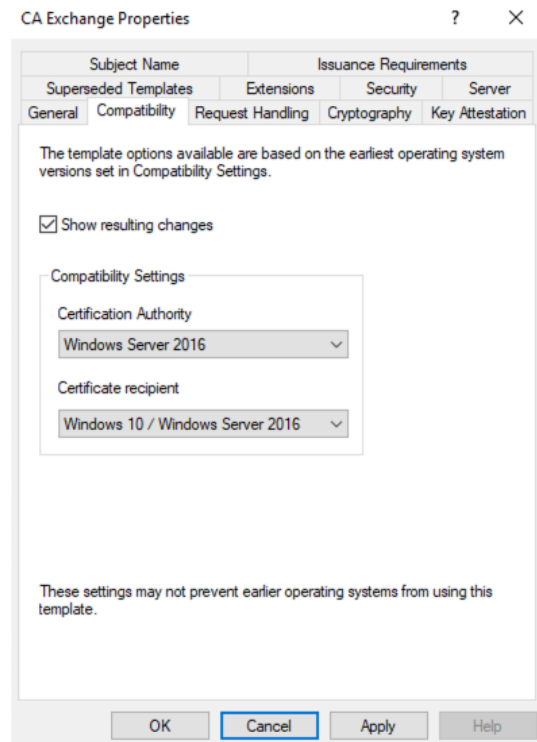
Defines the requirements that must be fulfilled before a certificate can be issued. This might include approval criteria or specific conditions that need to be met.

Security

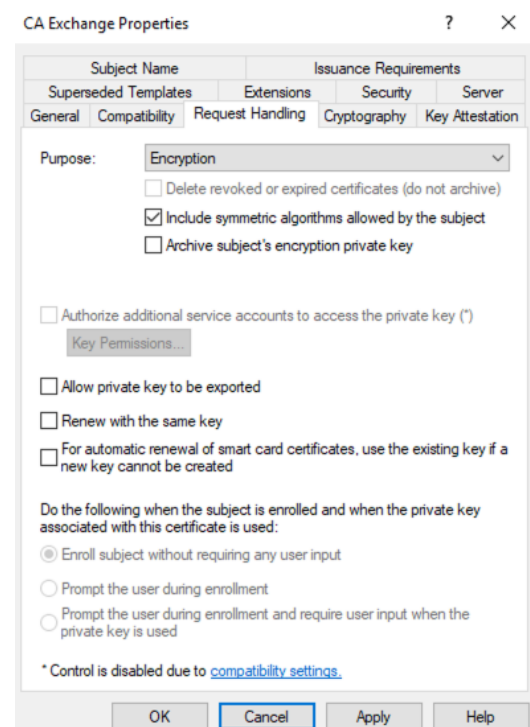
Includes configurations related to the template's security, like whether the Private Key should be stored and whether it should be protected by a hardware security module (HSM).

Server

Relates to settings designed explicitly for server certificates indicating if the template is intended for server authentication



The image shows the 'CA Exchange Properties' dialog box with the 'Compatibility' tab selected. The 'Subject Name' and 'Issuance Requirements' tabs are also visible. The 'Compatibility' tab contains a section for 'Compatibility Settings' with two dropdown menus: 'Certification Authority' set to 'Windows Server 2016' and 'Certificate recipient' set to 'Windows 10 / Windows Server 2016'. There is a checkbox for 'Show resulting changes' which is checked. A note at the bottom states: 'These settings may not prevent earlier operating systems from using this template.' The dialog has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.



The image shows the 'CA Exchange Properties' dialog box with the 'Cryptography' tab selected. The 'Subject Name' and 'Issuance Requirements' tabs are also visible. The 'Cryptography' tab contains a 'Purpose' dropdown set to 'Encryption'. Below it are three checkboxes: 'Delete revoked or expired certificates (do not archive)' (unchecked), 'Include symmetric algorithms allowed by the subject' (checked), and 'Archive subject's encryption private key' (unchecked). There is a checkbox for 'Authorize additional service accounts to access the private key (*)' which is unchecked, with a 'Key Permissions...' button next to it. Below that are three checkboxes: 'Allow private key to be exported' (unchecked), 'Renew with the same key' (unchecked), and 'For automatic renewal of smart card certificates, use the existing key if a new key cannot be created' (unchecked). A section titled 'Do the following when the subject is enrolled and when the private key associated with this certificate is used:' has three radio buttons: 'Enroll subject without requiring any user input' (selected), 'Prompt the user during enrollment' (unchecked), and 'Prompt the user during enrollment and require user input when the private key is used' (unchecked). A note at the bottom states: '* Control is disabled due to [compatibility settings](#).' The dialog has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

CA Exchange Properties ? X

Superseded Templates	Extensions	Security	Server
General	Compatibility	Request Handling	Cryptography
Subject Name		Key Attestation	
Issuance Requirements			

☒ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests

☐ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)

OK Cancel Apply Help

CA Exchange Properties ? X

General	Compatibility	Request Handling	Cryptography	Key Attestation
Subject Name		Issuance Requirements		
Superseded Templates		Extensions	Security	Server

Certificates issued by this template supersede certificates issued by all templates added to this list. Add only those templates whose certificates allow tasks permitted by certificates issued by this template.

Certificate templates:

Template Display Name	Minimum Supported CAs
-----------------------	-----------------------

Add... Remove

OK Cancel Apply Help

CA Exchange Properties



General	Compatibility	Request Handling	Cryptography	Key Attestation
Subject Name		Issuance Requirements		
Superseded Templates		Extensions	Security	Server

To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Edit...

Description of Application Policies:

Private Key Archival

OK Cancel Apply Help

CA Exchange Properties



Superseded Templates		Extensions	Security	Server
Subject Name		Issuance Requirements		
General	Compatibility	Request Handling	Cryptography	Key Attestation

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

☐ Requests can use any provider available on the subject's computer

☒ Requests must use one of the following providers:

Providers:

- ☒ Microsoft Enhanced Cryptographic Provider v1.0
- ☐ Microsoft Base Smart Card Crypto Provider
- ☐ Microsoft DH SChannel Cryptographic Provider
- ☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
- ☐ Microsoft Enhanced RSA and AES Cryptographic Provider

Request hash: Determined by CSP

☐ Use alternate signature format

OK Cancel Apply Help

CA Exchange Properties

? X

Superseded Templates	Extensions	Security	Server
Subject Name		Issuance Requirements	
General	Compatibility	Request Handling	Cryptography
Key Attestation			

Key Attestation

☒ None
☐ Required, if client is capable
☐ Required

Perform attestation based on:

☐ User credentials
☐ Hardware certificate
☐ Hardware key

Issuance policies for key attested certificates

☐ Include issuance policies for enforced attestation types
☐ Perform attestation only (do not include issuance policies)

OK Cancel Apply Help

CA Exchange Properties

? X

Superseded Templates	Extensions	Security	Server
General	Compatibility	Request Handling	Cryptography
Subject Name		Issuance Requirements	

Require the following for enrollment:

☐ CA certificate manager approval

☐ This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

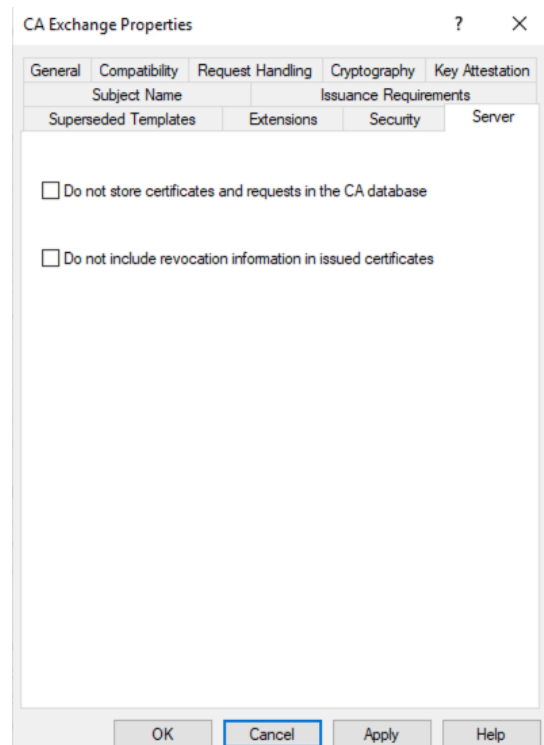
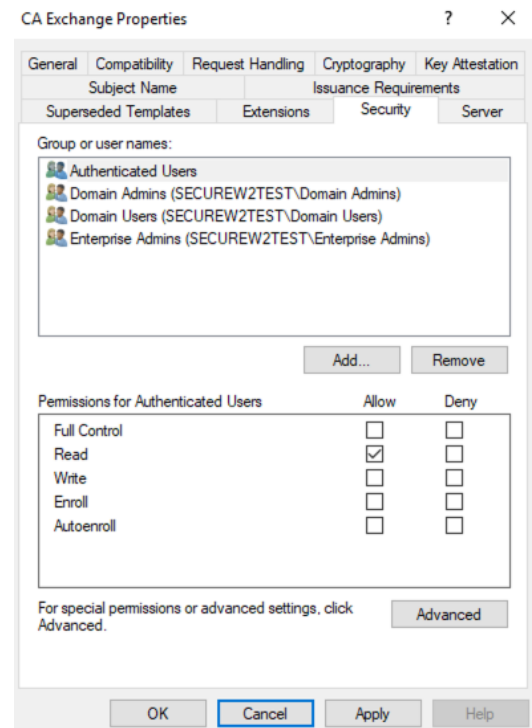
Add... Remove

Require the following for reenrollment:

☒ Same criteria as for enrollment
☐ Valid existing certificate
☐ Allow key based renewal

Requires subject information to be provided within the certificate request.

OK Cancel Apply Help



All Certificate Templates

Certificate templates are an essential part of the PKI environment directed by the CA for what type of certificate a client or user receives with a set of rules based upon its purpose. These certificates are Microsoft AD CS and come with 32 default certificates.

Administrator: Allows trust list signing and user authentication. This certificate template offers signature and encryption services for administrator accounts, facilitating account identification and trust list (CTL) management within the domain. Certificates generated

from this template are stored in Active Directory.

Authenticated Session: This certificate template enables users to authenticate to a web server, providing user credentials for site login without storing information insecurely in a cookie. It is beneficial for remote users to validate their identity without frequent logins.

Basic EFS: Used by Encrypting File System (EFS) to encrypt data. Certificates derived from this template are stored in Active Directory with associated user accounts and are utilized to encrypt data using the Encrypting File System (EFS). The Basic EFS certificate is used for EFS operations exclusively.

CA Exchange: Used to store Keys configured for Private Key archival.

CEP Encryption: Allows the certificate holder to act as a registration authority for Simple Certificate Enrollment Protocol (SCEP) requests.

Code Signing: Used to sign software digitally. These templates allow developers to create certificates for signing application code, ensuring that code management systems and end users can verify the trustworthiness of the software origin.

Computer: Allows a computer to authenticate itself on the network. The Computer template can be used for both workstations and servers.

Cross Certification Authority: Used for cross-certification and qualified subordination.

Directory Email replication: Used to replicate email within AD DS.

Domain Controller: Used by domain controllers as all-purpose certificates. The Domain Controller template is suitable for both client and server authentication, as well as the use of smart card logon support. The most significant difference between it and the Computer template is that the Domain Controller template is designed to help facilitate secure replication between domain controllers.

Domain Controller Authentication: Used to authenticate Active Directory computers and users.

EFS Recovery Agent: The subject can decrypt files previously encrypted with EFS. Certificates of this type permit the decryption of files encrypted with EFS, which is crucial for disaster recovery planning in EFS implementations. This certificate template is also used in conjunction with EFS, but it's used to decrypt data encrypted by EFS. This may be due to someone leaving the company or having been terminated.

Enrollment Agent: Used to request certificates on behalf of another subject. Certificates from this template are used to request and issue other certificates from the enterprise CA on behalf of another entity. For example, web enrollment applications use these certificates to manage certificate requests with the CA.

Enrollment Agent (Computer): Used to request certificates on behalf of another computer subject.

Exchange Enrollment Agent(Offline Request): Used to request certificates on behalf of another subject and supply the subject name in the request. These certificates are utilized within the Exchange to manage enrollment services and provide certificates to other entities within the exchange infrastructure.

Exchange Signature Only: Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for digitally signing email. Certificates derived from this template are user certificates used to sign e: mail messages sent from within the Exchange system.

Exchange User: Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for encrypting email. User certificates are stored in the Active Directory and are specifically used to encrypt email messages within the Exchange system.

IPSec: Used by Internet Protocol security (IPsec) to digitally sign, encrypt, and decrypt network communication.

IPSec (Offline Request): Used by IPsec to digitally sign, encrypt, and decrypt network communication when the subject name is supplied in the request.

Kerberos Authentication: Used to authenticate Active Directory computers and users.

Key Recovery Agent: The Key Recovery Agent certificate is used by an authorized administrator to decrypt Private Keys. It can be used to recover Private Keys, assuming that the CA has been configured to archive and allow recovery of the Private Key associated with the Public Key it was given when a certificate was requested.

OCSP Response Signing: Used by an Online Responder to sign responses to certificate status requests.

RAS and IAS Server: Enables remote access servers and Internet Authentication Service (IAS) servers to authenticate their identity to other computers.

Root Certification Authority: Used to prove the identity of the root CA.

Router (Offline Request): Used by a router when requested through a SCEP request from a CA with a CEP Encryption certificate.

Smart Card Logon: These certificates enable smart card holders to authenticate to Active Directory, providing identity and encryption capabilities as part of a two-factor security system using smart cards.

Smartcard User: Unlike the Smartcard Logon template, these certificates are stored in Active Directory and restrict identity and encryption to email systems.

Subordinate Certification Authority: This is the template used by a root or issuing certificate authority to issue certificates to subordinate certificate authorities.

Trust List Signing: Certificates of this type allow the signing of a trust list to manage certificate security and affirm the signer's identity.

User: This template generates general User Certificates, which are responsible for user activities in the Active Directory, such as authentication, EFS encryption, and interaction with Exchange. This certificate template is used for traditional authentication.

secure **W2**

Never Worry About **Credential Theft** Again

Certificate-based Authentication Renders Networks Virtually Immune to Over-the-air and Phishing Attacks.

[Learn More](#)

User Signature Only: These certificates allow users to sign data, providing identification of the origin of the signed data. It will enable users to sign data digitally.

Web Server: Proves the identity of a Web server. The Web Server template is used for supporting HTTPS on internal websites. This template is typically one that you would want to set up to ask for the common name and any storage area networks (SANs) that you want to use so that users don't get certificate untrusted messages.

Workstation Authentication: Enables client computers to authenticate their identity to servers.

Subject Type

The Subject Type determines the type of identity, object, or attribute to which the certificate would be directed. Below, you'll find the default certificate templates that AD CS offers categorized in their specific subject type. These types are User, Computer, DirEmailRep, CA, and Key Recovery Agent. Below is a list that is separated by their respective subject types:

User

The User subject type plays a role in safeguarding communication and interactions initiated by users. Certificates issued with the User subject type are designed to verify and protect the identity of users within the network. These certificates are used for tasks such as email communication, digital signatures, and user authentication, enhancing the reliability and trustworthiness of transactions involving users in the digital world.

- Administrator
- Authenticated Session
- Basic EFS
- Code Signing
- EFS Recovery Agent
- Enrollment Agent

- Exchange Enrollment Agent
- Exchange Signature
- Exchange User Certificates
- Smart Card Logon
- Smartcard User
- Trust List Signing
- User
- User Signature Only

Computer

The Computer subject type in Active Directory Certificate Services templates addresses the security requirements of machines and devices. Certificates generated from the Computer template validate the identity of computers within the network, bolstering the security posture of IT infrastructure. This subject type is significant in scenarios where secure server communications occur, ensuring that participating computers are legitimate to prevent access and maintain data integrity.

- **CA Exchange**
- **CEP Encryption**
- **Computer**
- **Domain Controller Authentication**
- **Enrollment Agent(Computer)**
- **IPSEC**
- **IPSEC(Offline Request)**
- **Kerberos Authentication**
- **RAS and IAS Server**
- **Router(Offline Request)**
- **Router (Offline Request)**
- **Web Server**
- **Workstation Authentication**

DirEmailRep

The DirEmailRep (Directory Email Replication) subject type in AD CS templates is specifically tailored to meet the needs of directory replication processes in email environments. Certificates issued with the DirEmailRep subject type play a role in securing directory information replication, guaranteeing that sensitive data is transmitted securely between servers. This subject type is vital for maintaining confidentiality and integrity of directory information across email infrastructure.

- **Directory Email Replication**
- **Domain Controller**

Certificate Authority(CA)

The subject type known as Certificate Authority (CA) plays a role in the Active Directory Certificate Services hierarchy. Certificates issued with the CA subject type are used to authenticate and verify the identity of Certificate Authorities within the PKI infrastructure. These certificates are crucial for ensuring trust and maintaining the integrity of the certificate issuance process. They establish a foundation for generating and managing certificates across the network.

- **Cross-Certification Authority**
- **Root Certification Authority**
- **Subordinate Certificate Authority**

Key Recovery Agent

When Key recovery is considered, the Key Recovery Agent subject type becomes essential in Active Directory Certificate Services. Certificates issued with this type enable designated individuals or Entities to recover Private Keys, providing a solution for cases where Key loss or compromise needs to be addressed. This subject type ensures that access to encrypted data remains secure and controlled, allowing authorized parties to recover Keys when required.

Key Recovery Agent

Key Usage

Key Usage is the operation of cryptography that AD CS will use on the pertaining certificate. Operations include Signature, Encryption, and Signature w/ Encryption. Below is the list of certificates that are sorted out by their respective operations:

Signature

A certificate template configured for Signature Key Usage ensures the integrity and authenticity of signatures. This template empowers entities to generate signatures, which validate the origin and unaltered state of content. Applications like code signing and document authentication benefit from certificates created using this template, assuring users that the signed materials are genuine and unaltered.

- **Authenticated Session**
- **Code Signing**
- **Cross: Certification Authority**
- **Enrollment Agent**
- **Enrollment Agent(Computer)**
- **Exchange Enrollment Agent(Offline Request)**
- **Exchange Signature Only**
- **OCSP Response Signing**
- **Root Certification Authority**
- **Subordinate Certification Authority**
- **Trust List Signing**

- **User Signature Only**

The screenshot shows the 'Edit Key Usage Extension' dialog box. The title bar says 'Edit Key Usage Extension' with a close button. The main text says 'Specify the required signature and security options for a key usage extension.' There are two sections: 'Signature' and 'Encryption'. In the 'Signature' section, 'Digital signature' is checked, while 'Signature is proof of origin (nonrepudiation)', 'Certificate signing', and 'CRL signing' are unchecked. In the 'Encryption' section, 'Allow key exchange without key encryption (key agreement)' and 'Allow key exchange only with key encryption (key encipherment)' are both unchecked, and 'Allow encryption of user data' is also unchecked. At the bottom, 'Make this extension critical' is checked. There are 'OK' and 'Cancel' buttons.

Encryption

Within the ecosystem of Active Directory Certificate Services default templates, the Encryption Key Usage template safeguards data confidentiality and privacy. Certificates generated with this template enable encryption and secure communications for files and other information. It is instrumental because data privacy is essential, such as email communication or transmitting data over networks. The Encryption Key Usage template ensures that authorized parties have the means to decrypt and access protected information.

- **Basic EFS**
- **CA Exchange**
- **CEP Encryption**
- **EFS Recovery Agent**
- **Exchange User**
- **Key Recovery Agent**

The screenshot shows the 'Edit Key Usage Extension' dialog box. The title bar says 'Edit Key Usage Extension' with a close button. The main text says 'Specify the required signature and security options for a key usage extension.' There are two sections: 'Signature' and 'Encryption'. In the 'Signature' section, 'Digital signature', 'Signature is proof of origin (nonrepudiation)', 'Certificate signing', and 'CRL signing' are all unchecked. In the 'Encryption' section, 'Allow key exchange without key encryption (key agreement)' is unchecked, 'Allow key exchange only with key encryption (key encipherment)' is selected with a radio button, and 'Allow encryption of user data' is unchecked. At the bottom, 'Make this extension critical' is checked. There are 'OK' and 'Cancel' buttons.

Signature and Encryption

For security measures, in Active Directory Certificate Services, the signature and Encryption Key Usage template provides a solution. Certificates derived from this template can handle both generating signatures and encrypting data. This versatile template is ideal for situations where a certificate is needed to serve as proof of the

legitimacy of content and as a means to protect communication channels by encrypting data. Examples like emails with signatures perfectly demonstrate how these two functions work seamlessly together.

- **Administrator**
- **Computer**
- **Directory Email Replication**
- **Domain Controller**
- **Domain Controller Authentication**
- **IPSEC**
- **IPSec (Offline Request)**
- **Kerberos Authentication**
- **RAS and IAS**
- **Router (Offline Request)**
- **Smart Card Logon**
- **Smartcard User**
- **User**
- **WebServer**
- **Workstation Authentication**

Administrators should look to duplicate these templates and configure their settings to match their domain's needs to promote best security practices tailored to their organization's needs. Next, we will cover the top use cases.

Edit Key Usage Extension

Specify the required signature and security options for a key usage extension.

Signature

- ☒ Digital signature
- ☐ Signature is proof of origin (nonrepudiation)
- ☐ Certificate signing
- ☐ CRL signing

Encryption

- ☐ Allow key exchange without key encryption (key agreement)
- ☒ Allow key exchange only with key encryption (key encipherment)
- ☐ Allow encryption of user data

☒ Make this extension critical

OK Cancel

OK Cancel Apply Help

Most Common Use Cases

Here are some of the most common use cases in which administrators employ AD CS Certificate Templates for their networks.

Code Signing:

A Code Signing Certificate is used to sign digital signatures to apply to software, scripts, or executables. This signature is created using a private key held by the software developer or organization. It is attached to the code before its distribution. When receiving the software, users can verify the signature using the corresponding public key. This ensures that the code hasn't been altered and originates from its claimed source. Code Signing Certificate Templates have a range of applications. They play a role in safeguarding software supply chains by allowing developers to sign their code with these certificates before distributing it. This enables users to verify the authenticity of the software before installing it. Additionally, these templates facilitate code signing at stages of development, allowing seamless collaboration without compromising security.

Computer:

This is often used for VPNs to determine whether a system is authorized, but it can also be used for encryption. By default, the system's name is pulled from Active Directory, though it can be made a manual process. You can always look at the template on the issuing CA, and it will tell you what purposes it's approved for.

Kerberos Authentication:

The Kerberos authentication certificate template is designed explicitly for issuing certificates used in authentication within a Windows environment. These certificates are typically associated with service accounts or users serving as evidence of identity during Kerberos authentication exchanges. Use cases in an enterprise environment include Server Authentication, Single Sign (SSO), Cross Domain Authentication, and secure communications.

User:

This certificate template is used for traditional authentication. It's most commonly used in two-factor authentication (2FA) solutions as the second authentication factor after username and password. This is especially popular with virtual private network (VPN) solutions.

Web Server:

This template is typically one that you would want to set up to ask for the common name and any storage area networks (SANs) that you want to use so that users don't get certificate untrusted messages. When a user is accessing SharePoint to pull off his department documents for the quarterly review, this PC will show their certificate to the RADIUS server. The RADIUS server will check with the CA to ensure the user has the correct certificate to access the Domain Sharepoint server and authenticate access once determined to have the correct certificate.

Knowing these use cases is essential because they're the most used by enterprises. Hackers are aware of these and will look to find any vulnerabilities within the certificate template that can allow them to gain access to compromise the network.

Certificate Templates Most Likely To Be Targeted

Hackers will aim at specific templates to gain administrative privileges to access the network and control domain data fully. Below is the list of certificates that administrators should audit daily to ensure their set configurations are not showing compromising risk or improperly managed with low-privileged users having access to change their settings.

Administrator

Allows trust list signing and user authentication. This certificate template offers signature and encryption services for administrator accounts, facilitating account identification and trust list (CTL) management within the domain. Certificates generated from this template

are stored in Active Directory.

Computer

Allows a computer to authenticate itself on the network. The Computer template can be used for both workstations and servers.

Enrollment

They are used to request certificates on behalf of another computer subject.

Kerberos

It can be used to recover Private Keys, assuming that the CA has been configured to archive and allow recovery of the Private Key associated with the Public Key it was given when a certificate was requested. An authorized administrator uses the Key Recovery Agent certificate to decrypt Private Keys.

User

This template generates general User Certificates responsible for user activities in the Active Directory, such as authentication, EFS encryption, and interaction with Exchange. This certificate template is used for traditional authentication.

Workstation Authentication

Enables client computers to authenticate their identity to servers.

Through Certificate Theft, Domain Escalation, or Account/Domain persistence, attackers will look for opportunities for an overlooked certificate with insecure settings. If the template is insecure, hackers will look for these properties within the settings to complete their attack methods.

Vulnerable Certificate Template Properties

Specific template configurations can cause issues within your set templates. These configurations can lead to attacks such as domain escalation, account persistence, and certificate theft. Please ensure these certificate settings are carefully set before deploying them to end-user accounts or clients. Otherwise, domain administrators will put the enterprise at risk of being compromised.

Authentication Based ECU

Extended Key Usage(EKU) is an X.509 certificate extension that designates the purpose of the Public Key within the certificate. This helps specify the application or service for which a certificate is valid. If not configured correctly, a misconfiguration could result in a certificate meant for server authentication being used for client authentication. This vulnerability can be exploited by attackers who detect this misconfiguration before the

administrator does, giving them an advantage. Another risk associated with EKU settings is the potential for certificate abuse through spoofing or taking advantage of its permissiveness. When EKU settings are not adequately enforced, malicious actors may attempt to use certificates for purposes that can lead to security breaches. Moreover, if EKU settings are overly permissive, it increases the likelihood of access or misuse. For instance, could you give a certificate permission for client and server authentication when it's only needed for one purpose?

Issuance Requirements

Issuance Requirements is a Certificate Setting In a certificate template, issuance requirements outline the conditions that must be met for the Certificate Authority (CA) to issue a certificate based on that template. If the configuration of issuance requirements is appropriate and lenient, it could allow the issuance of certificates with sufficient validation. For instance, if the requirements are set loosely, certificates might be issued without authentication or authorization. Another issue is that if key usage restrictions are not correctly set up, a certificate could be misused for purposes posing security risks.

CA Exchange Properties

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

Require the following for enrollment:

☐ CA certificate manager approval

☐ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Add...

Remove

Require the following for reenrollment:

☒ Same criteria as for enrollment

☐ Valid existing certificate

☐ Allow key based renewal (*)

Requires subject information to be provided within the certificate request.

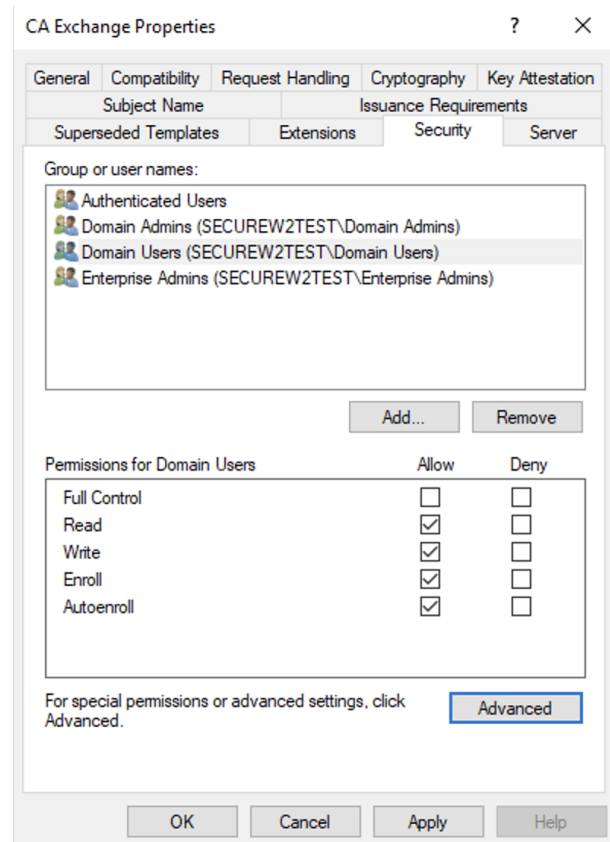
* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

ACL Permissions

Access Control Lists (ACLs) determine who can perform actions on a certificate template. Not having the proper configurations of the ACL permissions on the control list can lead to ACL Permission vulnerabilities. Improper configuration of ACL permissions may grant

users access to certificate templates, potentially leading to the issuance of unauthorized certificates, or it may also grant excessive permissions to users or groups for a certificate template, which can result in unintended or unauthorized issuance of certificates.



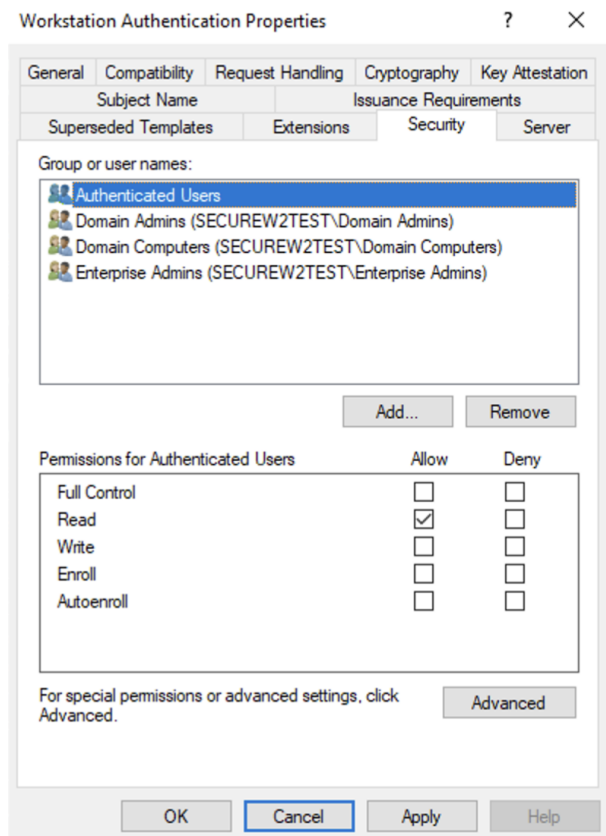
Enrollment Agents

Enrollment agents are accounts with the authority to enroll certificates on behalf of users. If compromised, the Enrollment Agent may give an unauthorized person access to the enrollment agent's credentials; they could misuse this authority to enroll certificates, potentially resulting in access. This can build into a massive problem if routine monitoring or auditing is not implemented because it may make it challenging to identify and respond promptly to malicious certificate enrollments.

Subject Name

The subject name settings in a certificate template determine how the information about the subject(user, device, etc.) is filled out in the issued certificate. Weak Subject Name Constraint settings and Mismatched Subject Names cause security risks in this certificate template setting. Possessing improper subject name constraint settings could allow for certificates with insecure subject information. Mismatched Subject Name settings may cause discrepancies between the name specified in the certificate and the entity it represents, leading to security issues.

After viewing how to look for certificates, the next section will review the best ways to manage certificate templates.

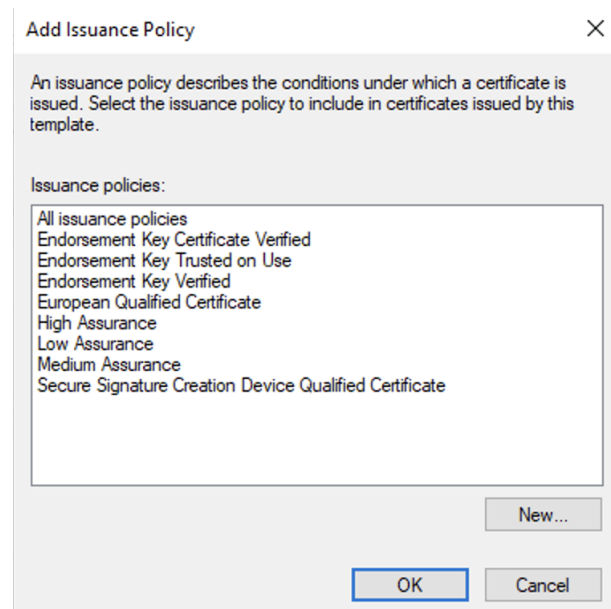


Best Way to Manage Certificate Templates

Administrators should include the following methods to correctly manage certificate templates to prevent attacks and mitigate user error vulnerabilities. These Management Policies include Issuance Requirements, Implementing Certificate Life Cycle, Private Key is Exportable, Extension Key Usages, Digital Signature Encryptions, Validity Period Renewal, and Third Party Management.

Issuance Requirements

To issue a certificate securely and successfully, many requirements must be followed to avoid security breaches. These issue requirements should include certificate management approval, validation requirements, requiring multiple people to sign off on a CA, and the certificate service request (CSR) not requiring the subject name. Having these set policies and settings in place, the Certificate Authority can issue a certificate without the vulnerability of inappropriate permissions for a low-privilege user and proper certificate workflows to ensure management validations.



Certificate Management Approval

Certificate Management Approval is a crucial step in ensuring the integrity and security of the certificate issuance process. This involves obtaining explicit approval from authorized personnel before a certificate is issued. This access control policy can be implemented in three separate ways: Authorization Workflow, Role-Based Access Control, and establishing an approval hierarchy.

To practice authorized workflow within a domain, administrators must define a straightforward workflow that outlines the steps and individuals responsible for approving certificate requests and specify the roles and responsibilities of each approving entity within the organization. The Role-Based Access Control should be used to restrict access to the certificate issuance process to only authorized personnel. To achieve this operating this access control, administrators should assign roles such as Certificate Managers or Approvers to individuals based on their responsibilities. Finally, administrators should establish an approval hierarchy to implement an approval hierarchy, defining the sequence in which approvals must be obtained. They clearly articulate the conditions under which each level of approval is required.

Validation Requirement

Validation plays a role in ensuring that certificates are issued appropriately and legitimately for organizational-based purposes. The validation requirements should include domain ownership verification, organizational or extended validation, and identity verification. A form of validation administrators can implement for organizations is Domain Ownership Verification. Confirming that the entity requesting the certificate owns or has control over the domain for which it is being issued. This will utilize domain validation methods like DNS record verification or email-based validation.

Another form of validation is Organizational Validation or Extended Validation. This can be performed by specifying documentation or verification steps for certificates requiring levels of assurance, such as Organization Validation or Extended Validation certificates. Finally, another valuation policy that can be used is identity validation. This will ensure security and prevent issuing certificates containing identifiable information. It would be best for this verification process to be implemented for individuals or entities requesting these certificates.

Require Multiple People to Sign Off A CR

Consider implementing a step approval system to enhance security measures and minimize risks. Dual/Multiple Authorization processes will be mandatory for certificate requests to undergo multiple authorization levels. This will clearly define the roles and responsibilities of each approver, ensuring that no single individual possesses unilateral authority. You can also implement Threshold-Based Approvals to explore the possibility of implementing a threshold-based system where specific types of certificates or requests exceed a defined risk threshold approvals.

CSR Not Requiring The Subject Name

As a security measure, excluding the Subject Name in Certificate Signing Requests has become increasingly common. You provide reduced exposure to sensitive information by omitting the Subject Name in the Certificate Service Request. The exposure of information during the certificate request process is reduced. You can also improve security by separating the generation of Keys from certificate requests, enhancing the privacy and security of certificate issuance. The Subject Name can be added during the certificate issuance process later on. Finally, implementing the Dynamic Binding of the Subject Name during Issuance will reduce risks associated with exposing the Subject Name.

Life Cycle

The life cycle of certificates is a process that governs the creation, deployment, and maintenance of certificates issued by Active Directory Certificate Services (AD CS). This process plays a role in establishing and maintaining the trustworthiness of identities within an organization.

- Enrollment
 - Devices initiate obtaining a certificate from the Certificate Authority (CA).
- Issuance
 - Once the CA receives a valid enrollment request, it verifies the requestor's identity, generating a certificate. The certificate is then signed using the CA Key to establish a chain of trust between the entity and the CA.
- Distribution
 - Once issued, the certificate must be distributed to its intended recipient, the user, or the device. This can be achieved through email and automated distribution mechanisms such as auto-enrollment or manual distribution.

- **Renewal**

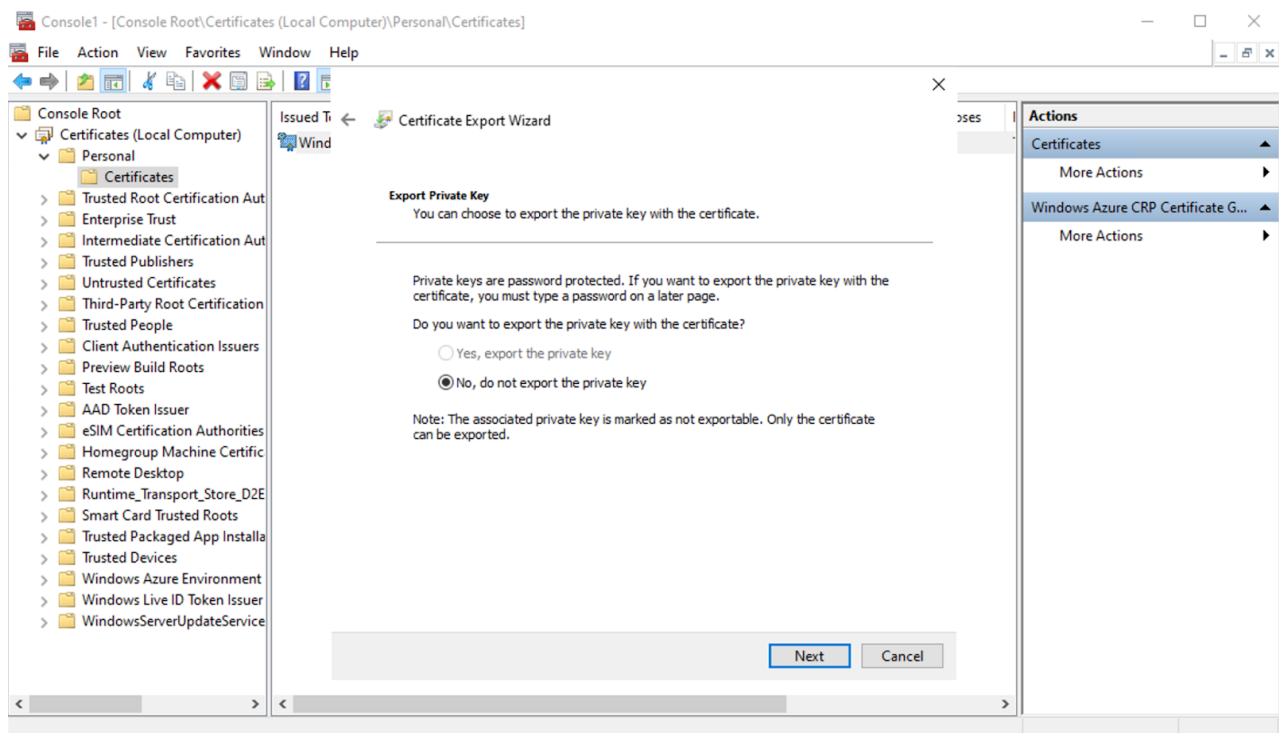
Certificates have an expiration date, after which they become invalid. It is essential to renew them before this deadline to ensure they are valid. Renewal involves extending the validity period to provide secure communication. Automated renewal processes help prevent expiration and potential disruptions.

- **Revocation**

In cases where Keys are compromised, or other security incidents occur, certificates may need revoked. Certificate Revocation List maintained by the Certificate Authority lists no longer valid certificates. This mechanism ensures that entities relying on certificates can check their real-time validity.

Private Key is Exportable

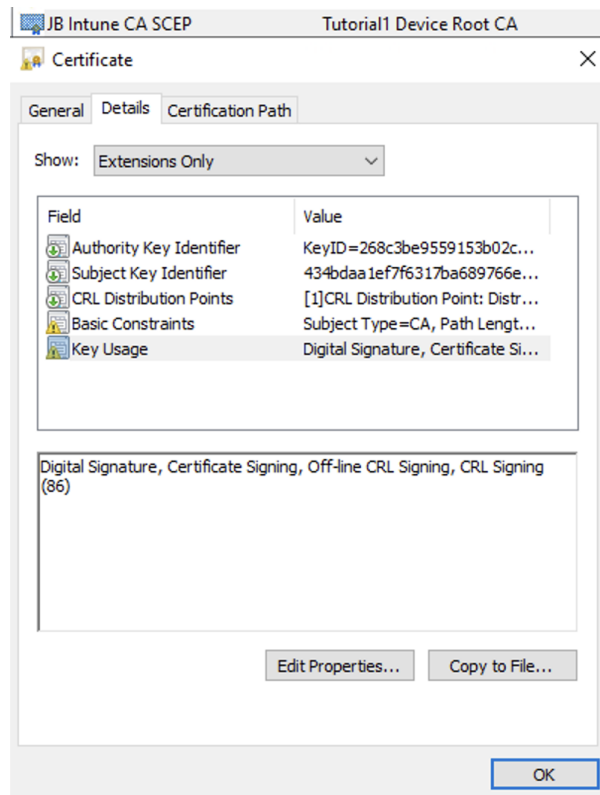
The exportability of Keys brings advantages and security considerations in managing certificates. It enhances flexibility by allowing the same certificate and Private Key to be used across devices to access network and domain resources. Although the security it can provide is precious, it must be warranted that it does come with the risk of the Private Key being compromised if improper access controls are not in place, which can lead to Certificate Theft.



Extension Key Usages

Enabling the following Key usage will significantly assist in managing digital certificates and the cryptographic operations for the key pair associated with the corresponding digital certificate, digital signature, key encipherment, and non-repudiation. Digital Signature Extension Key Usage should be enabled to ensure the trustworthiness and authenticity of domain communications while validating digital signatures. Enabling Key

Encipherment allows the key to perform encryption operations on other keys or perform a key exchange, this is great for establishing encrypted sessions. Finally, the Non-Repudiation Key Usage ensures that the signature on a message can only be generated using the Private Key linked to the Public Key within the certificate, preventing entities from denying involvement in a transaction.



Digital Signature Encryption Options

To validate signatures to ensure the trustworthiness and authenticity of messages and implement excellent certificate practices, the Digital Signature Key should have multiple options to promote versatility with user-friendliness and heightened security. RSA, ECDSA(Elliptic Curve Digital Signature Algorithm), and Secure Hash Algorithm(SHA) are options for Digital Signatures. The RSA is an adopted asymmetric algorithm employed for signatures. It relies on the properties of prime numbers and is renowned for its security and versatility. ECDSA is an alternative to RSA, offering security but with Key lengths. This can be advantageous in environments with resources where more minor Keys are preferred. Secure Hash Algorithms, like SHA 256 or SHA 384, encrypt data before signing it. The choice of which version of the SHA algorithm to use affects the strength of the operation.

Validity Period Renewal

The validity period of a certificate plays a role in security and operational aspects. It is essential to find a ground between security and operational convenience. Shorter validity periods enhance security by minimizing the window for compromise. They also require more frequent renewal efforts. On the other hand, more extended validity periods offer convenience while potentially increasing the risk if a Private Key is compromised during

that ample time. Employing automated renewal processes is considered practice as it reduces the risk of certificate expiration. Computerized systems can proactively handle certificate renewals, ensuring system and user operation without disruptions.

Properties of New Template

Superseded Templates		Extensions	Security
Subject Name	Server	Issuance Requirements	
Compatibility	General	Request Handling	Cryptography
		Key Attestation	

Template display name:
Administrator

Template name:
Administrator

Validity period: 1 years Renewal period: 6 weeks

☒ Publish certificate in Active Directory
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

Third-Party Management

Third-party management is an excellent way for administrators to ensure network security, availability, and increased overall productivity. By working with a company specializing in PKI and network security solutions, administrators will be able to gain more time for other role objectives due to not having to focus on keeping their PKI, saving money overall through both the mitigation of security risk and (if using an on-prem RADIUS Server) cost of maintenance. Finally, this will allow the organization to operate better because of the availability and opportunities to use security protocols such as 802.1x, enabling passwordless authentication.



Upgrading from AD to Azure AD has never been easier

We've helped hundreds of organizations securely transition from on-prem to all-cloud networks.

Disadvantages of AD CS Certificate Templates

There are several disadvantages that administrators should be aware of besides complexities and configuration vulnerabilities. Knowing these disadvantages will better assist in implementing defensive and operational strategies to address the domain's needs better.

Non-windows device and BYOD

Implementing Active Directory Certificate Services (AD CS) in a Bring Your Device (BYOD) environment presents challenges due to the wide range of devices accessing the network. While AD CS is highly effective in managing Windows-based devices, it encounters difficulties when integrating seamlessly with users' platforms and operating systems. This lack of compatibility can result in a security approach that leaves specific devices insufficiently protected and potentially introduces vulnerabilities in the network.

AD CS is primarily designed to function within the Windows ecosystem. However, integration challenges arise when dealing with Windows devices like macOS, Linux, or other operating systems. The deployment and management of certificates become more complex, which may lead to inconsistencies in security policies. This limitation can hinder organizations aiming for an IT environment.

Remote Workers

AD CS faces obstacles in accommodating off-site employees and their diverse array of devices. The need for access to network resources from locations and devices adds complexity to certificate management. Remote workers may encounter difficulties obtaining and renewing certificates, potentially disrupting connectivity and productivity.

Cost for maintenance and running the on-prem servers

Deploying and maintaining AD CS can be demanding regarding costs and ongoing maintenance efforts. The initial setup requires hardware, software licenses, and skilled personnel. Moreover, effectively managing a certificate infrastructure requires attention and expertise. The expenses and maintenance obligations associated with AD CS can present significant obstacles for companies working within resources or without dedicated IT staff.

Conclusion



The **#1 Defense** Against Credential Theft
X.509 digital certificates enable the most secure authentication

[Learn More](#)

Active Directory Certificate Services is a complex feature requiring much understanding and consistent monitoring. Knowing the intricacies of AD CS PKI and the involvement with the Active Directory Environments and Roles are highly acknowledged as necessary to prevent attacks against the domain. Attackers have multiple ways of accomplishing their goal of compromising the network with AD CS. Not knowing about certificate templates can be expensive once exposed by a black hat hacker. One minor misconfiguration of the certificate's validity, maintaining past its expiration date, too many access permissions for non-administrative users, or enabling enrollment of other certificates to low-privileged users can be very detrimental.

We at SecureW2 specialize in raising awareness while ensuring enterprise networks are fully secure and impervious to network-based attacks. We provide cloud-based solutions to ensure availability and versatility integrations with multiple OS or devices to give a more straightforward way to monitor, configure, and automate the certificate lifecycle from enrollment to revocation. If you want more information regarding our PKI solution and the implementation process, visit our homepage to set up a demo and quote today!

Learn about this author

Justin is a Product Marketing Associate from North Carolina. He grew up in Nebraska, where he received his Bachelor's in Cyber Security. He wants to continue to educate himself in the Cyber Security field and use it to bring innovative ideas to fruition. In his free time, he enjoys spending time with his family and friends, reading books, working out in the gym, or playing Rugby.

