Active Directory
Certificate Services
AD CS
Overview
AD CS

Definition

- Active Directory Certificate Services (AD CS) is an Identity and Access Control security technology that provides customizable services for creating and managing public key certificates used in software security systems that employ public key technologies.
Installation

- AD CS comes in many different components, which all can be installed via the Server Manager tool in Windows 2008
Components

- Certification authorities (CAs)
- CA Web enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service
Certification authorities (CAs)

- Root and subordinate CAs are used to issue certificates to users, computers, and services, and to manage certificate validity.
CA Web enrollment

- Web enrollment allows users to connect to a CA by means of a Web browser in order to request certificates and retrieve certificate revocation lists (CRLs).
Online Responder

- The Online Responder service accepts revocation status requests for specific certificates, evaluates the status of these certificates, and sends back a signed response containing the requested certificate status information.
Network Device Enrollment Service

- The Network Device Enrollment Service allows routers and other network devices that do not have domain accounts to obtain certificates.
The Certificate Enrollment Web Service enables users and computers to perform certificate enrollment that uses the HTTPS protocol. Together with the Certificate Enrollment Policy Web Service, this enables policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain.
The Certificate Enrollment Policy Web Service enables users and computers to obtain certificate enrollment policy information. Together with the Certificate Enrollment Web Service, this enables policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain.
Benefits to AD CS

- Organizations can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding private key. AD CS gives organizations a cost-effective, efficient, and secure way to manage the distribution and use of certificates.
- Applications supported by AD CS include Secure/Multipurpose Internet Mail Extensions (S/MIME), secure wireless networks, virtual private network (VPN), Internet Protocol security (IPsec), Encrypting File System (EFS), smart card logon, Secure Socket Layer/Transport Layer Security (SSL/TLS), and digital signatures.
Windows 2008 R2 Enhancements

- Certificate enrollment that uses the HTTPS protocol.
- Certificate enrollment across Active Directory Domain Services (AD DS) forest boundaries.
- Improved support for high-volume certificate issuance.
- Support for CAs on a Server Core installation of Windows Server 2008 R2.
Deployment of AD CS

- Although AD CS can be deployed on a single server, many deployments will include multiple servers configured as CAs, other servers configured as Online Responders, and others serving as Web enrollment portals. Not all operating systems support all features or design requirements, and creating an optimal design will require careful planning and testing before you deploy AD CS in a production environment.
• Used to Manage a CA
• To open the Certification Authority snap-in, click **Start**, click **Run**, type `certsrv.msc`, and click **OK**.
**certmgr.msc**

- Used to Manage Certificates
- To open the Certificates snap-in, click **Start**, click **Run**, type **certmgr.msc**, and click **OK**.
• Used to Manage Certificate Templates
• To open the Certificate Templates snap-in, click Start, click Run, type certtmpl.msc, and click OK.
ocsp.msc

- Used to manage the Online Responder
- To open the Online Responder snap-in, click **Start**, click **Run**, type **ocsp.msc**, and click **OK**.
Implementation and Administration
Certificate Templates

AD CS

http://go.microsoft.com/fwlink/?LinkId=92522
Certificate Templates

- Are used by Enterprise CAs to define the format, content, determine who can enroll and how enrollment can occur
- All templates have a DACL that controls who can read, configure, and to enroll in certificates that were created from this template
- All these templates are defined in Active Directory Domain Services (AD DS)
- AD DS is forest wide and all templates and permissions are shared with other Enterprise CAs
Default Templates in Windows 2008

- Administrator
- Authenticated Session
- Basic EFS
- CA Exchange
- CEP Encryption
- Code Signing
- Computer
- Cross-Certification Authority
- Directory E-mail Replication
- Domain Controller
- Domain Controller Authentication
- EFS Recovery Agent
- Enrollment Agent
- Enrollment Agent (Computer)
- Exchange Enrollment Agent (Offline request)
- Exchange Signature Only
- Exchange User
- IPSec
- IPSec (Offline request)
- Kerberos Authentication
- Key Recovery Agent (KRA)
- OCSP Response Signing
- Remote Access Service (RAS) and Internet Authentication Service (IAS) Server
- Root CA
- Router (Offline request)
- Smart Card Logon
- Smart Card User
- Subordinate CA
- Trust List Signing
- User
- User Signature Only
- Web Server
- Workstation Authentication
Installation Requirements

CA Operating System
- Server 2008 Enterprise
- Server 2003 Enterprise
- Server 2008, 2003 Standard
- Server 2000 (upgrade schema to 2003+)

Template Version
- Version 1, 2, 3
- Version 1, 2
- Version 1
- Version 1
SubjectName – Based on user, computer, program, service, object or anything set as the holder of the public key. SubjectName can be obtained automatically from AD, or added manually in the Certificate Enrollment page

Set Certificate Lifetime

Define Certificate Purpose – Based on function, common group of requirements

Version 3 – Decide to implement advanced cryptographic algorithms

Define CSP (cryptographic service provider). All subjects must use the same one

Determine Key Length

Decide on Smart Card Usage

Set Deployment Method (through Web enrollment, Certificates Snap-In, or API and AutoEnrollment

Archive Private Key if available to do so
Creating a New Template

To create a new version 2 or 3 certificate template

1. Open the Certificate Templates snap-in.

2. In the details pane, right-click an existing certificate that will serve as the starting point for the new certificate, and then click Duplicate Template.


4. On the General tab, enter the Template display name and the Template name, and then click OK.

5. Define any additional attributes for the newly created certificate template.
Acquiring Object Identifiers for Custom Application Policies

To acquire an object identifier

1. Open the Certificate Templates snap-in.
2. In the details pane, right-click the certificate template you want to modify, and then click Properties.
3. On the Extensions tab, click Application Policies, and then click Edit.
4. In the Edit Application Policies Extension dialog box, click Add.
5. In Add Application Policy, ensure that the application you are creating does not exist, and then click New.
6. In the New Application Policy dialog box, provide the name for the new application policy, note the generated object identifier, and then click OK.
To associate the application policy with the certificate template

1. Open the Certificate Templates snap-in.

2. In the details pane, right-click the certificate template you want to change, and then click Properties.

3. On the Extensions tab, click Application Policies, and then click Edit.

4. In Edit Application Policies Extension, click Add.

5. In Add Application Policy, click the desired application policy, and then click OK.
Establishing an Issuance Policy for a Certificate Template

To associate the issuance policy with the certificate template

1. Open the Certificate Templates snap-in.
2. In the details pane, right-click the certificate template you want to change, and then click Properties.
5. In the Add Issuance Policy dialog box, click New.
6. Provide the requested information.
Deploying Certificate Templates
AD CS
Best Practices

- Do not mess with the Certificate Publishers group in AD, this contains the CA computer account and used to publish certificates
- Add all CA computer accounts to all domain Certificate Publisher Groups
- Do not exceed the lifetime of the issuing CA certificate
- Carefully plan certificate templates prior to deployment
- Upgrade Schema if necessary
- Duplicate new templates from existing templates
- Determine which CAs are the most suitable for publishing certificates
- Always keep published certificates to a minimum
Publish Certificate Templates

- Use certificate snap-in (certsrv.msc)
- Published in same place throughout AD Domain
- Certificate templates are objects in AD and have DACLs
Permission Assignments for Certificate Templates

- Assign permissions to global groups (or Universal Groups in the forest)
- Autoenrollment requires Read, Enroll, and Autoenroll permissions
- Enrollment through Certificates Snap-In, Web-Based enrollment then read and enroll permission are required
- For certificate renewal the computer account must have read and enroll
- Write and Full Control permissions to CA managers
Suggestions for Auto Enrollment

- Require user input
- Limit the number of CSP for a template
- Do not allow the creation of a Subject Name, auto enrollment will not work
- Do not require more than one authorized signature in the Issuance Requirements tab of the Certificate
- Be carefully using the option to validate the existing template
Setting Permissions for a Certificate Template

To define permissions to allow a specific security principal to enroll for certificates based on a certificate template

1. Open the Certificate Templates snap-in (Certtmpl.msc).
2. In the details pane, right-click the certificate template you want to change, and then click Properties.
3. On the Security tab, ensure that Authenticated users is assigned Read permissions.
   This ensures that all authenticated users on the network can see the certificate templates.
4. On the Security tab, click Add. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and then click OK.
5. On the Security tab, select the newly added security group, and then assign Allow for the Read and Enroll permissions.
6. Click OK.
Set AutoEnrollment Permissions

To define permissions to allow a specific security principal to autoenroll for certificates based on a certificate template

1. Open the Certificate Templates snap-in.
2. In the details pane, right-click the certificate template you want to change, and then click Properties.
3. On the Security tab, click Add. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and then click OK.
4. On the Security tab, select the newly added security group, and then assign Allow for the Read, Enroll, and Autoenroll permissions.
5. Click Apply.
Publish a Certificate Template

To define which certificate templates are issued by a CA

1. In Administrative Tools, click Certification Authority.
2. In the console tree, expand CAName (where CAName is the name of your enterprise CA).
3. In the console tree, select the Certificate Templates container.
4. Right-click Certificate Templates, and then click New, Certificate Template to Issue.
5. In the Enable Certificate Templates dialog box, select the certificate template or templates that you want the CA to issue, and then click OK.
Remove a Certificate Template

To remove a certificate template from the certificate templates currently issued by a CA

1. In Administrative Tools, click Certification Authority.
2. In the console tree, expand CNAMe (where CNAMe is the name of your enterprise CA).
3. In the console tree, select the Certificate Templates container.
4. In the details pane, right-click the certificate template you want to remove from the CA, and then click Delete.
5. In the Disable Certificate Templates dialog box, click Yes.
Configuring Existing Templates

AD CS
**General**

- **Validity period.** This defines the validity period for an issued certificate. The validity period cannot be greater than the validity period of the CA's certificate. The minimum renewal period is 80 percent of the certificate lifetime or six weeks, whichever is greater.
- **Renewal period.** This is the period of time before the validity period expires when the certificate will be renewed if re-enrollment is supported for the certificate template. (effects autoenrollment)
- **Publish options.** You can choose whether to publish the certificate to AD DS based on the certificate template.
- **Re-enrollment option.** If the certificate template is published in AD DS, you can prevent re-enrollment if a valid certificate of the same certificate template exists for the security principal indicated in the subject.
- **Smart card certificate keys.** For smart card renewal, this option enables the existing key to be used if a new key cannot be created. This helps prevent smart card renewal failures resulting from smart card capacity issues.
Request Handling

• **Use advanced Symmetric algorithm to send the key to the CA.** This option allows the administrator to choose the Advanced Encryption Standard (AES) algorithm to encrypt private keys while they are transferred to the CA for key archival. If this option is selected, the client computer will use AES256 symmetric encryption (along with the CA's exchange certificate for asymmetric encryption) to send the private key to the CA for archival. If this option is not selected, the symmetric algorithm used is Triple Data Encryption Standard (3DES).

• **Add Read permissions to Network Service on the private key.** For computer templates, this option grants Read permission to Network Service for the certificate's private key on the computer to which the certificate is issued. This enables services such as the Online Responder and Internet Information Services (IIS) to use certificates and keys issued to the computer on which they run. In previous versions of Windows, these permissions had to be configured manually.
Cryptography

- **Algorithm name.** This option introduces the ability to select an advanced algorithm for encryption, signing, or both (depending on the template's purpose).

- **Minimum key size.** This option introduces the ability to specify a minimum required size for the keys used with the chosen algorithm.

- **Providers.** Version 2 templates offered a list of CryptoAPI CSPs; version 3 templates offer a dynamically populated list of Cryptography Next Generation (CNG) providers.

- **Hash algorithm.** This option introduces the ability to choose an advanced hash algorithm.

- **Use alternate signature format.** When the RSA algorithm is selected, this check box allows the administrator to specify that certificate requests created for this template include a discrete signature in Public Key Cryptography Standards (PKCS) #1 version 2.1 format.
Subject Name

• The Subject Name must be defined
• Must be unique
• Can be built automatically
• Can be generated during the certificate request
Issuance Requirements

- CA certificate manager approval. All certificates are placed into the pending container for a certificate manager to issue or deny.
- This number of authorized signatures.
- Application policy. This option specifies the application policy that must be included in the signing certificate used to sign the certificate request.
- Issuance policy. This option specifies the issuance policy that must be included in the signing certificate used to sign the certificate request.
Security

- The **Security** tab, shown in the following figure, allows you to define the discretionary access control list (DACL) for a specific certificate template.
Perform Basic Lab