Microsoft

Windows Server Managing and Supporting Active Directory Certificate Services (ADCS)

Module 7: Certificate Templates and Enrollment Methods

Microsoft Services

Module Overview

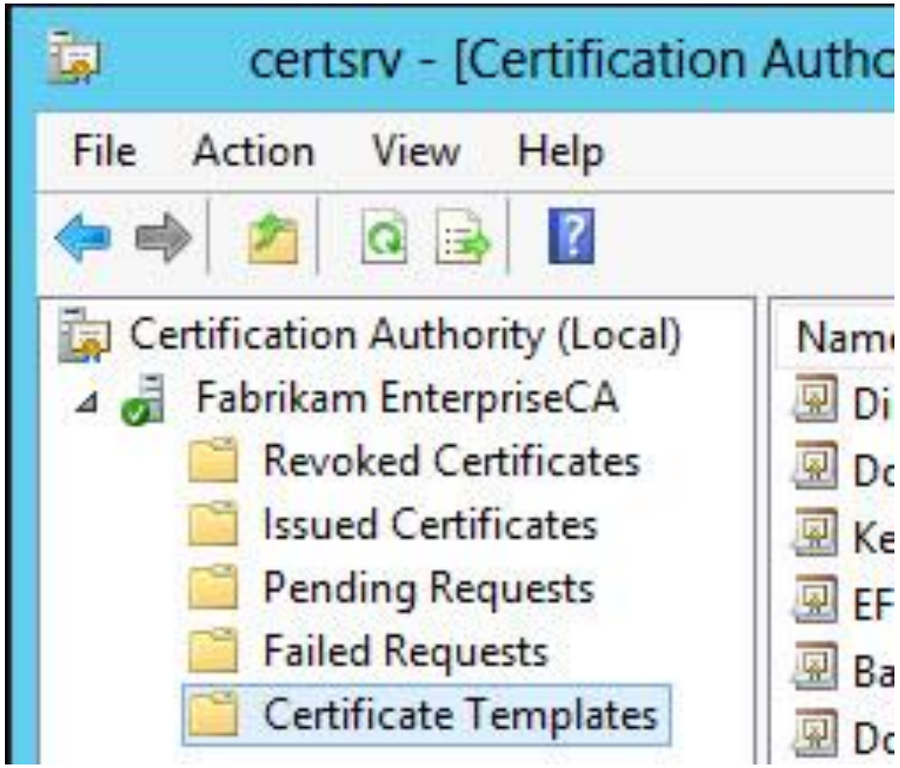
- Certificate Templates
- Template settings
- Enrollment methods
- Certificate file types

Certificate Templates

Certificate Template Terminology

- Enterprise CAs use Certificate Templates to define the format and content of issued certificates
- Certificate Templates define who can enroll for which types of certificates
- Templates and associated permissions are stored in Active Directory under the 'Configuration' partition, available for any Enterprise CA in the forest

Standalone vs. Enterprise CA



Enterprise CAs vs. Standalone CAs

Enterprise CA	Standalone CA
Requires Active Directory	Does not require AD
Can issue certificate for end entities, including Users, Smart Card, Computers	Issue certificate for digital signatures (other CAs)
Certificates Templates are used and shared between all CAs using Active Directory	Certificate Templates are not used
Enforce credential checks on users during enrollment	Certificate requests are set by default to pending for manual approval
Certificate subject name can be generated by requestor or built from Active Directory	Certificate requester must supply all identifying information
Can publish user certificates to AD using Exit Module	

Certificate Templates

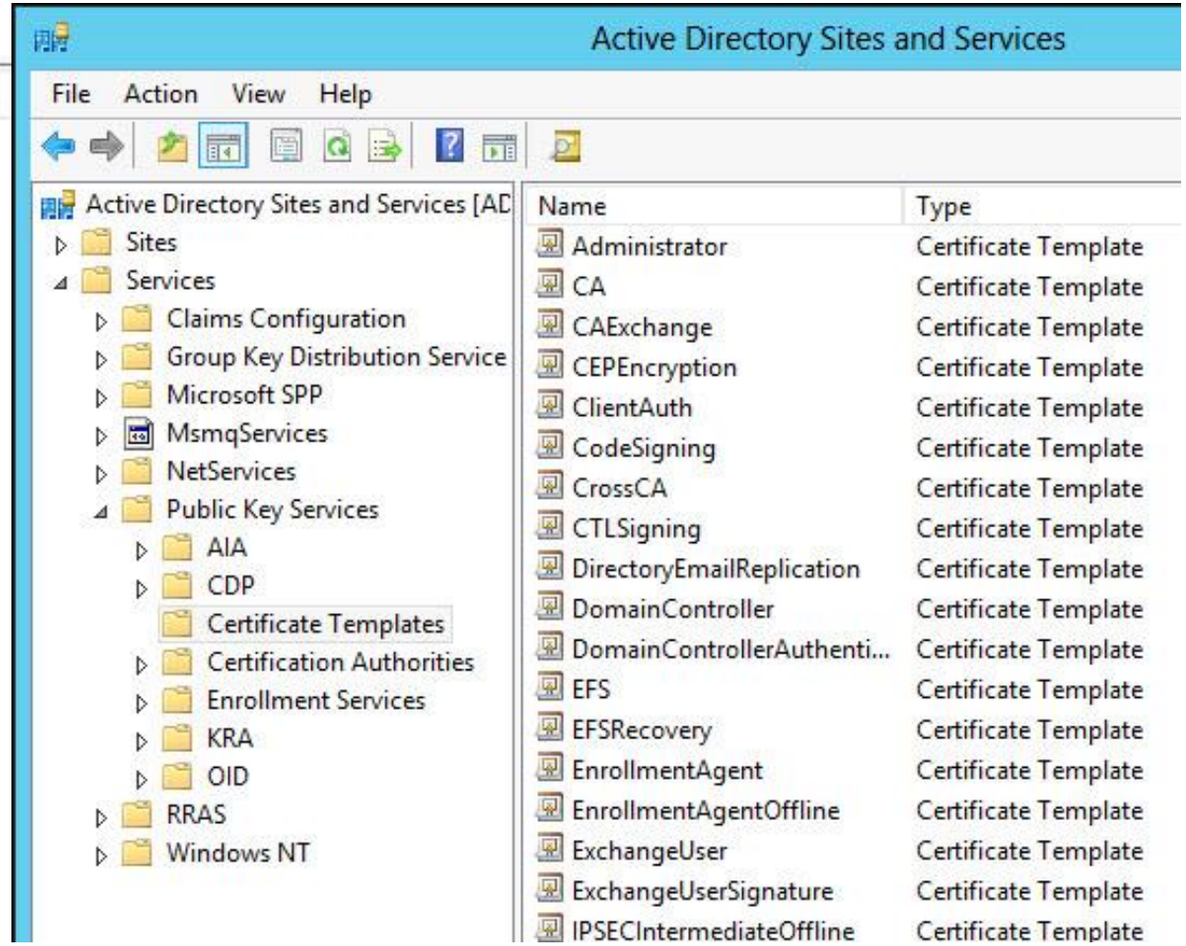
- Enterprise Certification Authorities use templates to:
  - Control the format, purpose and content of certificate
  - Specify which users and computers can enroll
  - Control enrollment method (i.e., enroll and/or auto-enroll)

- Attributes of templates that can be defined:
  - Subject Name
  - Certificate lifetime
  - Usage, Key Length, Key Archival, Key Exportable
  - Cryptographic Service Provider
  - Application and Issuance policies

Mapping of Templates to the AD Object

- Templates are saved in the 'Configuration' naming context (partition) of the Active Directory database

Template Display Name	Schema Versi...	Versi...
Administrator	1	4.1
Authenticated Session	1	3.1
Basic EFS	1	3.1
CA Exchange	2	106.0
CEP Encryption	1	4.1
Code Signing	1	3.1
Computer	1	5.1
Cross Certification Authority	2	105.0
Directory Email Replication	2	115.0
Domain Controller	1	4.1
Domain Controller Authentication	2	110.0
EFS Recovery Agent	1	6.1
Enrollment Agent	1	4.1
Enrollment Agent (Computer)	1	5.1
Exchange Enrollment Agent (Offline requ...	1	4.1



Template Schema Versions

- Template schema versions define the generation of the template
- V1 to V5 is available (depending on CA OS)
- V1 are the default/out-of-the-box certificate templates
- Certification Authority Web Enrollment only supports V1-V2 templates
  Newer version are not supported and won't be displayed by the portal
- Any template version will create an X.509 V3 certificate
- Pay attention that template schema version is different than the template version

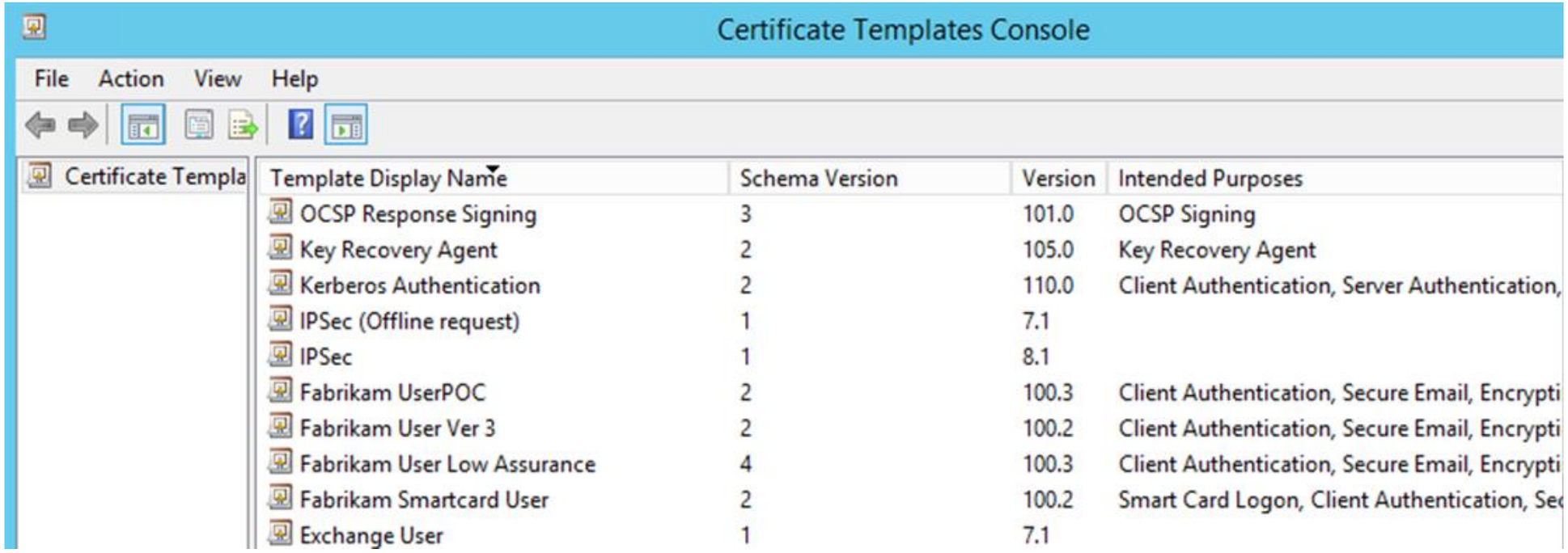
Template Schema Versions

	Version 1	Version 2	Version 3	Version 4	Version 5
Minimum CA OS	Windows Server 2000	Windows Server 2003 Enterprise	Windows Server 2008 Enterprise	Windows Server 2012	Windows Server 2016 and Windows Server 2019
Minimum Client OS	Any	Windows XP	Limited compatibility with Windows XP	Windows Vista and later	Windows Vista and later
Options	Just ACRS, no auto-enrollment	Can be customized	Supports CSP or KSP(CNG)	TPM Key Attestation	Key attestation for SC and BYOD

Managing Certificate Templates

- Templates are managed through the Certificate Templates MMC (certtmpl.msc)
- Version information, settings and Access Control Lists (ACLs) are stored in AD
- If the default templates are missing/deleted:

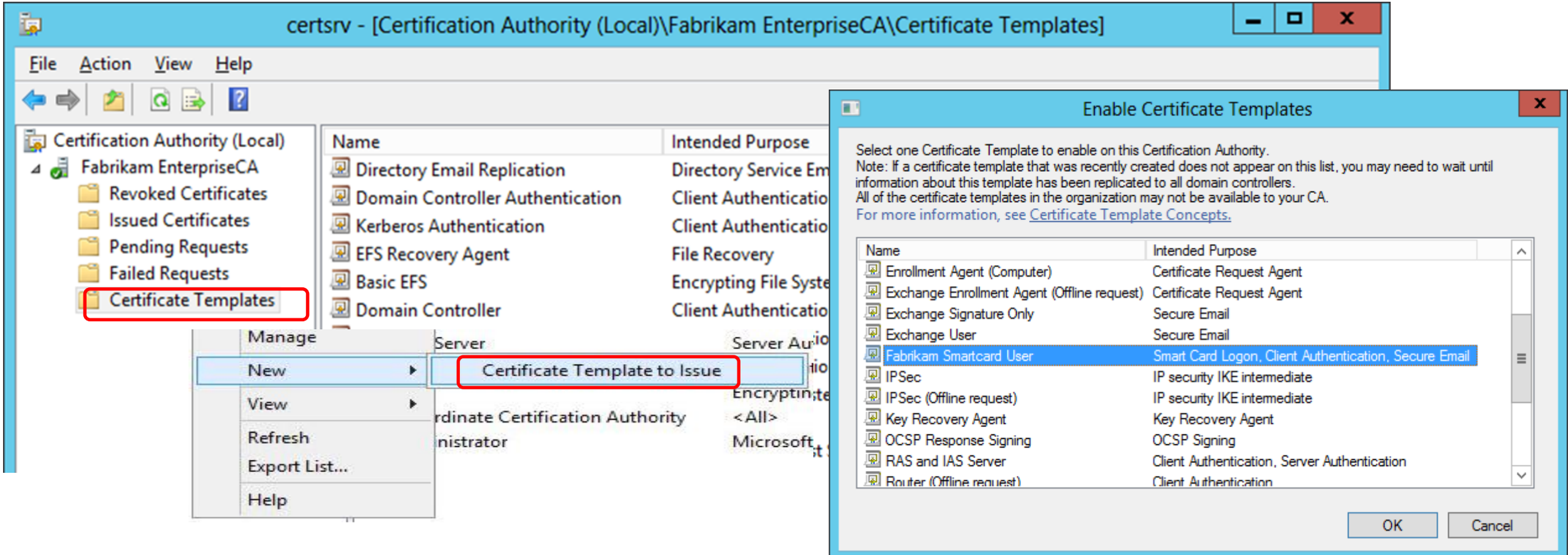
  Certutil -InstallDefaultTemplates



Template Display Name	Schema Version	Version	Intended Purposes
OCSP Response Signing	3	101.0	OCSP Signing
Key Recovery Agent	2	105.0	Key Recovery Agent
Kerberos Authentication	2	110.0	Client Authentication, Server Authentication,
IPSec (Offline request)	1	7.1	
IPSec	1	8.1	
Fabrikam UserPOC	2	100.3	Client Authentication, Secure Email, Encrypti
Fabrikam User Ver 3	2	100.2	Client Authentication, Secure Email, Encrypti
Fabrikam User Low Assurance	4	100.3	Client Authentication, Secure Email, Encrypti
Fabrikam Smartcard User	2	100.2	Smart Card Logon, Client Authentication, Se
Exchange User	1	7.1	

Publishing a Template

- Certificate templates need to be assigned to the CA in order to be available for issuing by users/devices
- After creating/modifying a template, AD replication needs to occur



Managing Templates with PowerShell

- Get-CATemplate
  Gets the list of templates set on the certification authority (CA) for issuance of certificates
- Add-CATemplate
  The Add-CATemplate cmdlet adds a certificate template to the CA for issuing
- Remove-CATemplate
  Removes the templates from the certification authority (CA) which were set for issuance of certificates

Lesson Review

Question 1:

Some of the certificate templates which available using the Certificate Authority, are not available in the Certification Authority Web Enrollment page.

What could be the reason for that (considering security permissions are configured correctly)?

The missing certificate templates are based on schema version 3 or above.
The Web Enrollment service displaying only V1 and V2 certificate templates.

Lesson Review

Question 2:

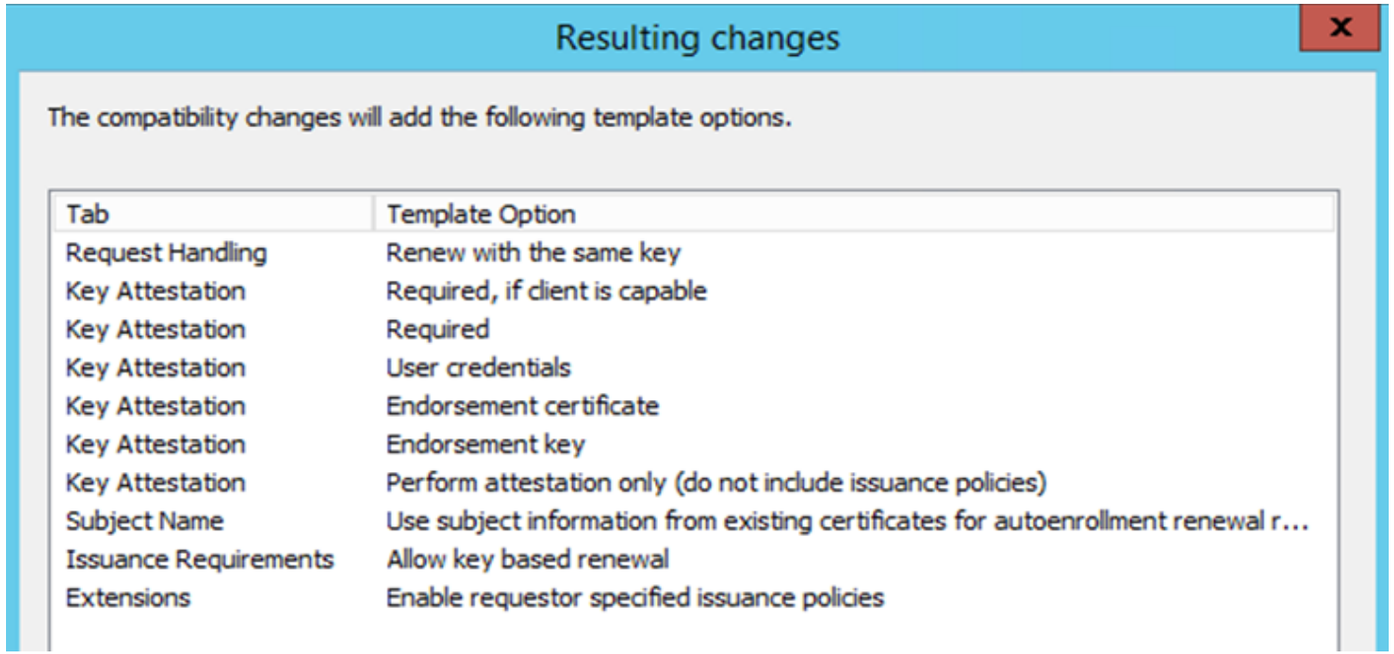
Where certificate templates are stored?
Which Domain Controllers can access the certificate templates?

Certificate templates are stored in the 'Configuration' partition of Active Directory, replicated and available by any Domain Controller in the forest.

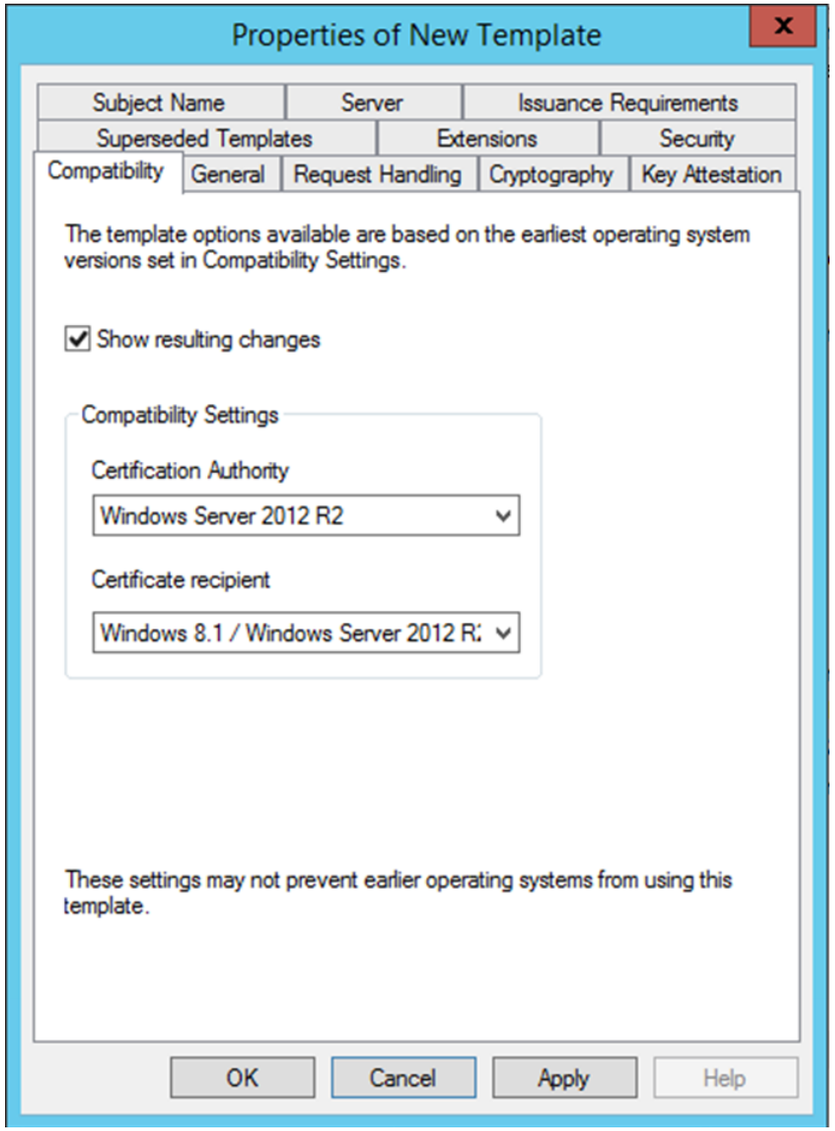
Template Settings

Compatibility Tab

- The Compatibility tab came new in Windows Server 2012
- Helps to determine the differences between capabilities in each OS/template

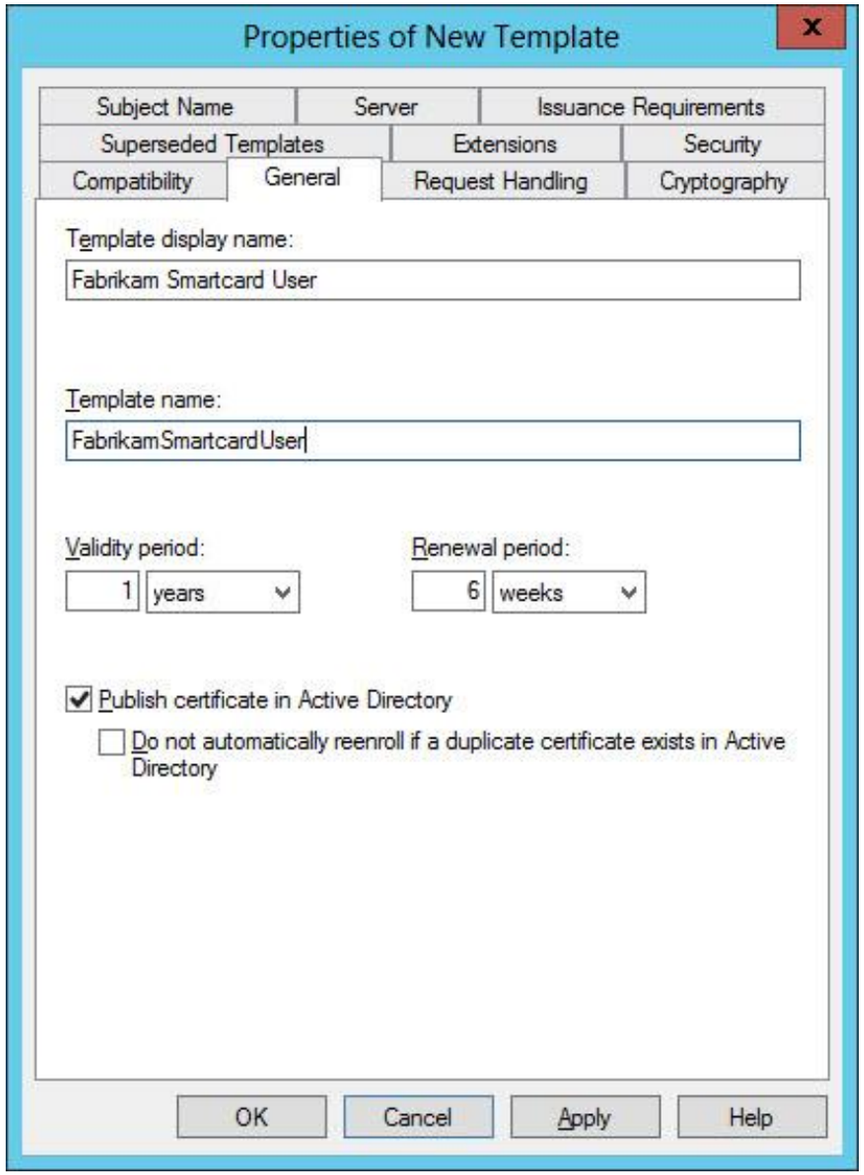


Tab	Template Option
Request Handling	Renew with the same key
Key Attestation	Required, if client is capable
Key Attestation	Required
Key Attestation	User credentials
Key Attestation	Endorsement certificate
Key Attestation	Endorsement key
Key Attestation	Perform attestation only (do not include issuance policies)
Subject Name	Use subject information from existing certificates for autoenrollment renewal r...
Issuance Requirements	Allow key based renewal
Extensions	Enable requestor specified issuance policies



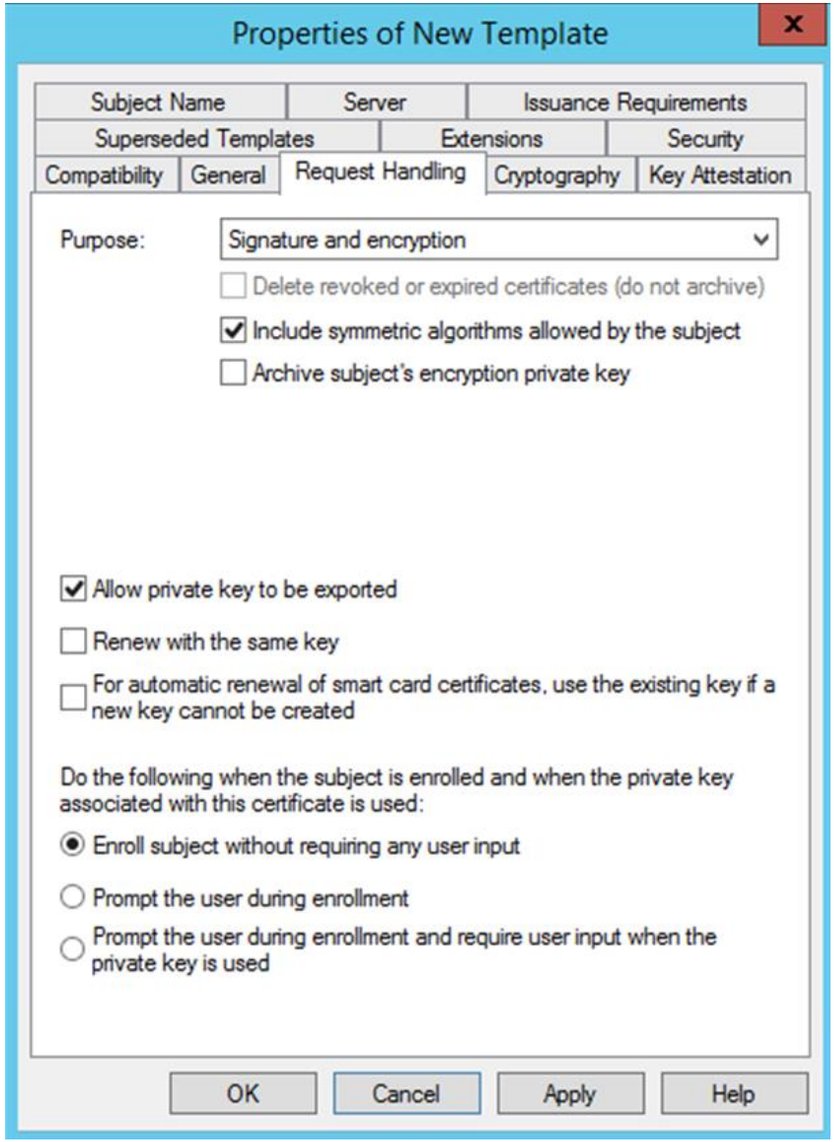
General Tab

- Display name and template name
- Validity period (limited by the the general validty period of the CA)
- Renewal period (For autoenroll certificate templates, minimum renewal period = 80% of certificate or 6 weeks
- Publish certificate in Active Directory (under UserCertificate attribute)



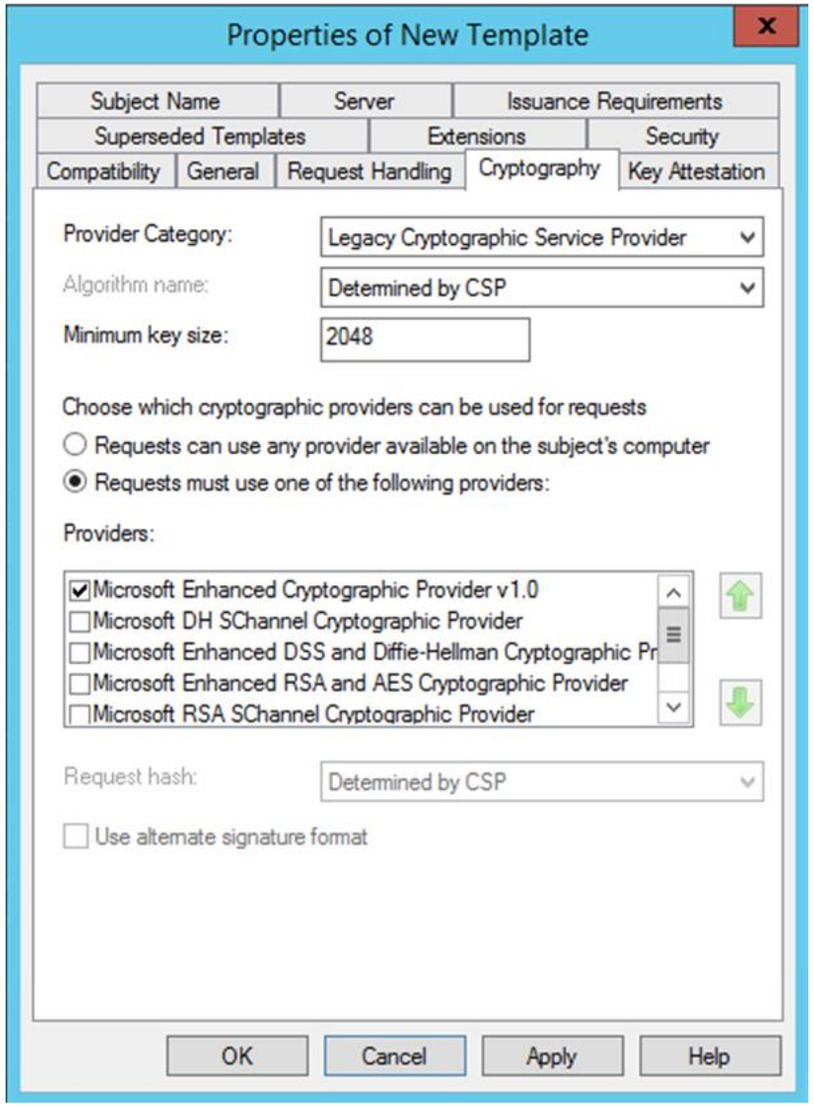
Request Handling Tab

- Purpose
- Private key archival - Enables archival of the certificate's private key in the CA database
- Allow private key to be exported
- Renew with same key



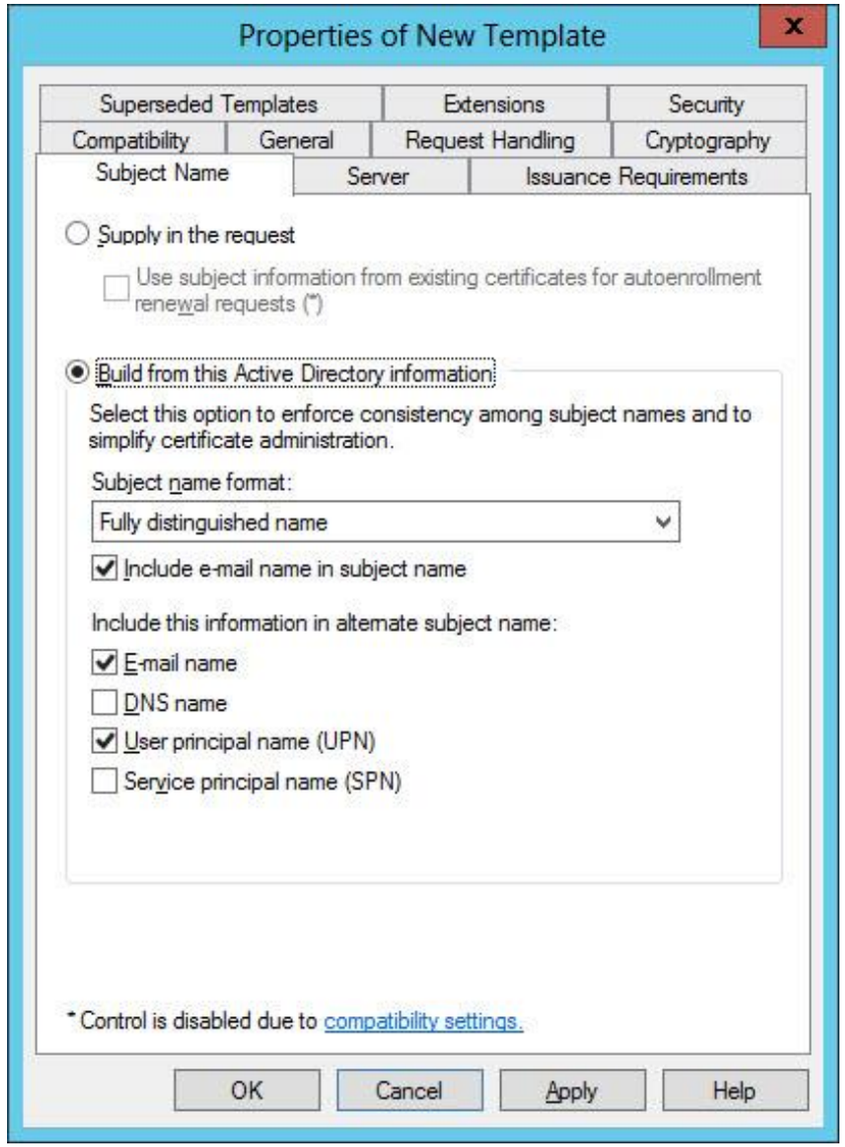
Cryptography Tab

- Decide whether to use Legacy **CSP** (Cryptographic Service Provider) or the newer **KSP** (Key Storage Provider) - and thereby whether to use **CNG** (Cryptography Next Generation) or not
- Minimum key size for the chosen algorithm



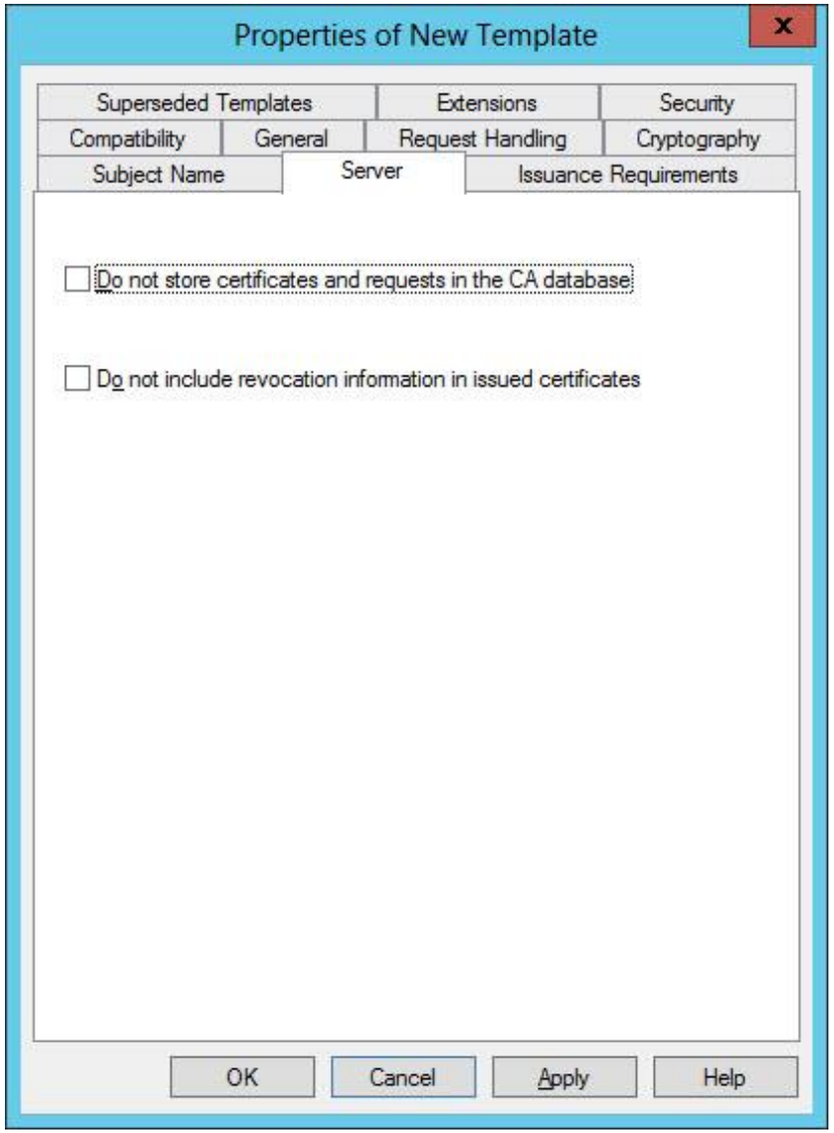
Subject Name Tab

- Where does the Subject come from:
  - Supply in the request
  - Build from this Active Directory information
- Include SAN (Subject Alternative Name)



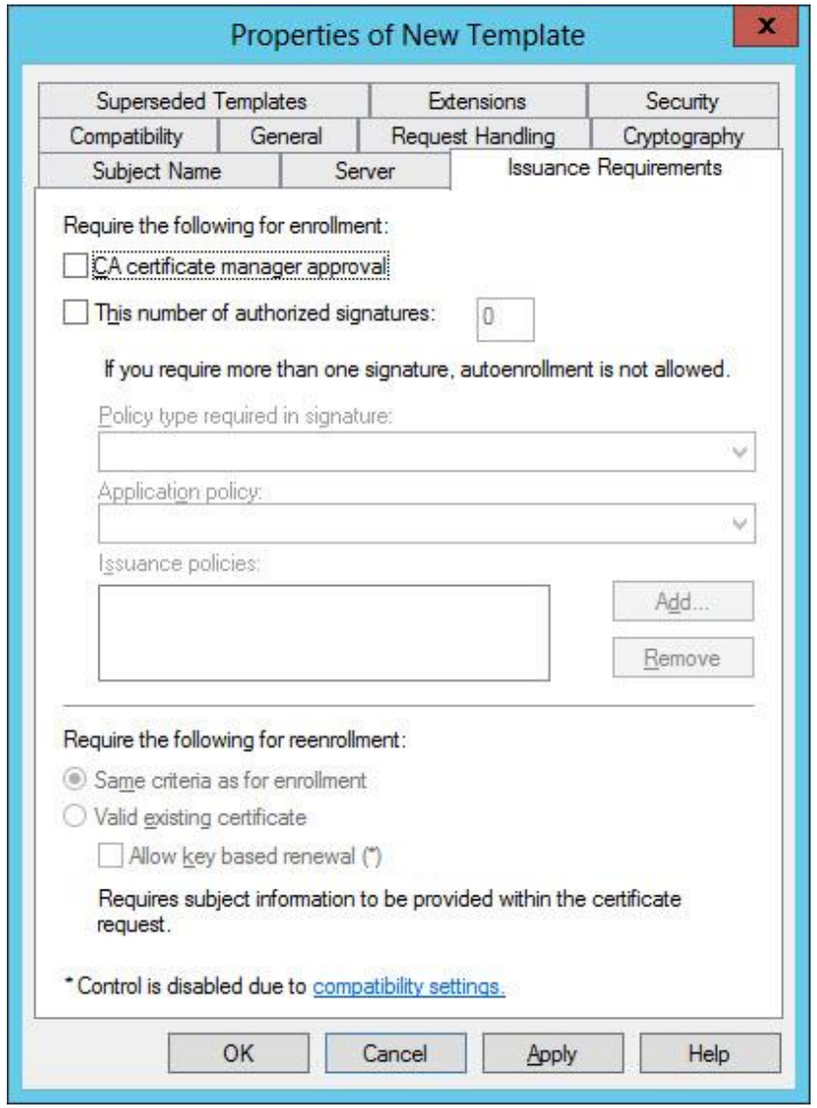
Server Tab

- Do not store certificates in the CA database
- Do not include revocation-info in issued certificates



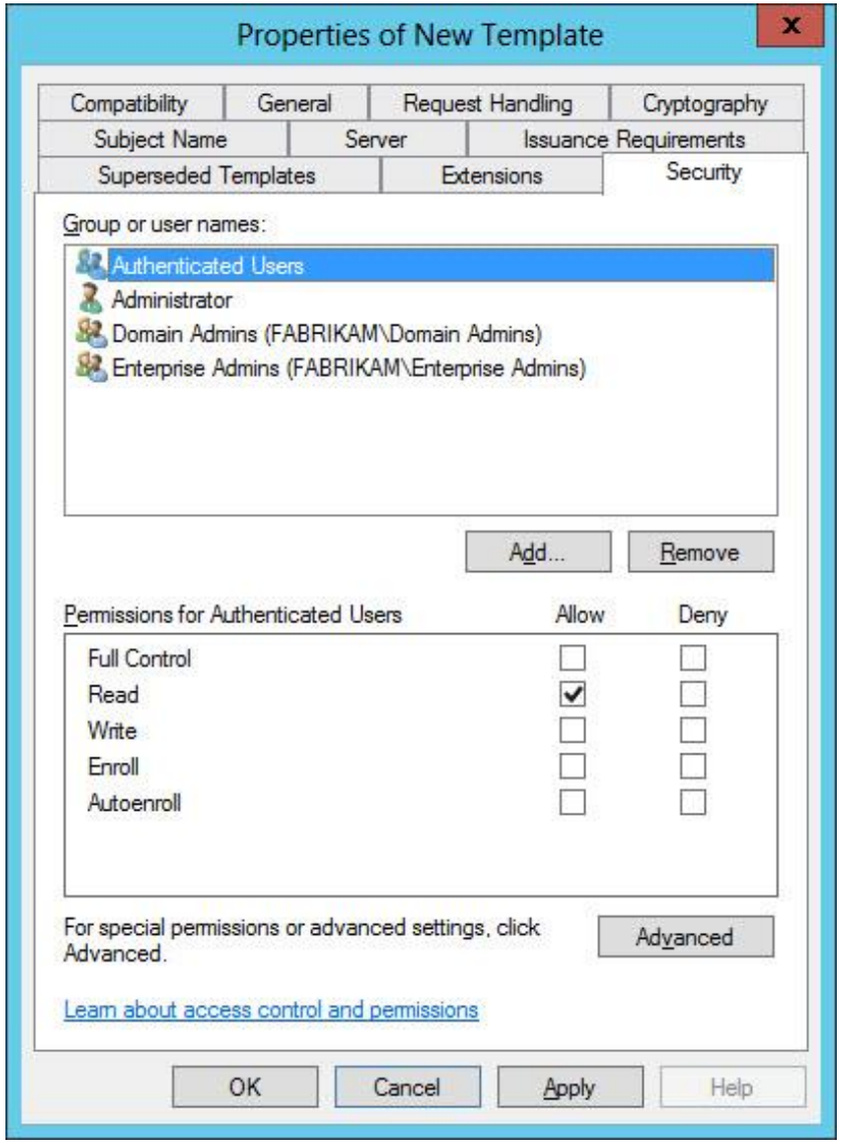
Issuance Requirements Tab

- Decide whether a CA Manager approval is needed for certificate enrollment



Security Tab

- Permissions on the certificate template:
  - **Read**: Authenticated Users need the permission to download the template, otherwise they will not be able to enroll
  - **Enroll**: Allows to enroll manually
  - **Autoenroll**: Allows to receive a certificate through the autoenrollment process
    (Autoenroll required read and enroll permissions as well)



Enrollment Methods

Enrollment Methods

Enrollment using command line or PowerShell

Enrollment using MMC (certlm.msc ,certmgr.msc)

Enrollment Agents

Certificate Authority Web-Enrollment

Auto-Enrollment

Enrollment using Command Line

- Preparing .inf file with relevant information:

```
[NewRequest]
Subject = "CN=MyWebServer.contoso.com"
Exportable = TRUE
KeyLength = 2048
[RequestAttributes]
CertificateTemplate="ContosoWebServer"
```

- Creating a request file (.req) using the .inf file:

  certreq –new config.inf Request.req

- Submit the request to the CA:

  certreq –submit Request.req certnew.cer certnew.pfx

- List Certificate Templates offered by a Certificate Authority:

  certutil -catemplates -config "CASub01\SubCA"

Enrollment using PowerShell

- PowerShell Cmdlet (Get-Certificate):

Administrator: Windows PowerShell

```
PS C:\>
PS C:\> Get-Certificate -Template ContosoCompanyUser -CertStoreLocation cert:\CurrentUser\My

Status Certificate
------ -----------
Issued [Subject]...
```

- Using Get-Certificate and specify required Subject Name and SAN:

Administrator: Windows PowerShell

```
PS C:\>
PS C:\> Get-Certificate -Template ContosoWebServer -SubjectName "CN=Web01" -DnsName "Web01.contoso.com" -CertStoreLocation cert:\LocalMachine\My

Status Certificate
------ -----------
Issued [Subject]...
```

Enrollment with MMC or AutoEnrollment

Client chooses valid certificate template and generates a public-private key pair based on that template

LDAP

Client queries for a list of

- *pKICertificateTemplate* objects
- *pKIEnrollmentService* objects
- *msPKI-Enterprise-Oid* objects

Domain Controller

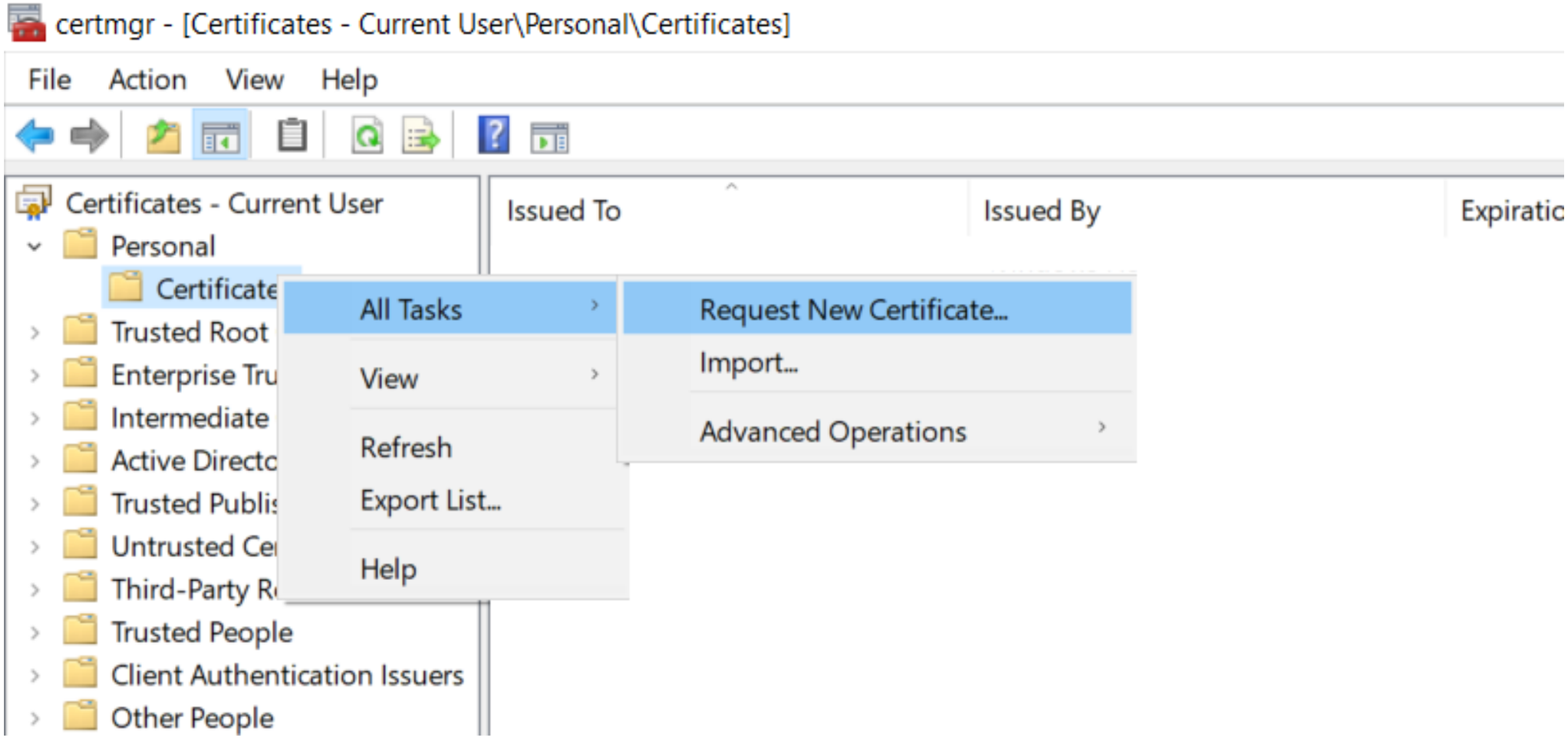
RPC/DCOM

Client sends certificate request and receives certificate

Certificate Authority

Enrollment Using MMC

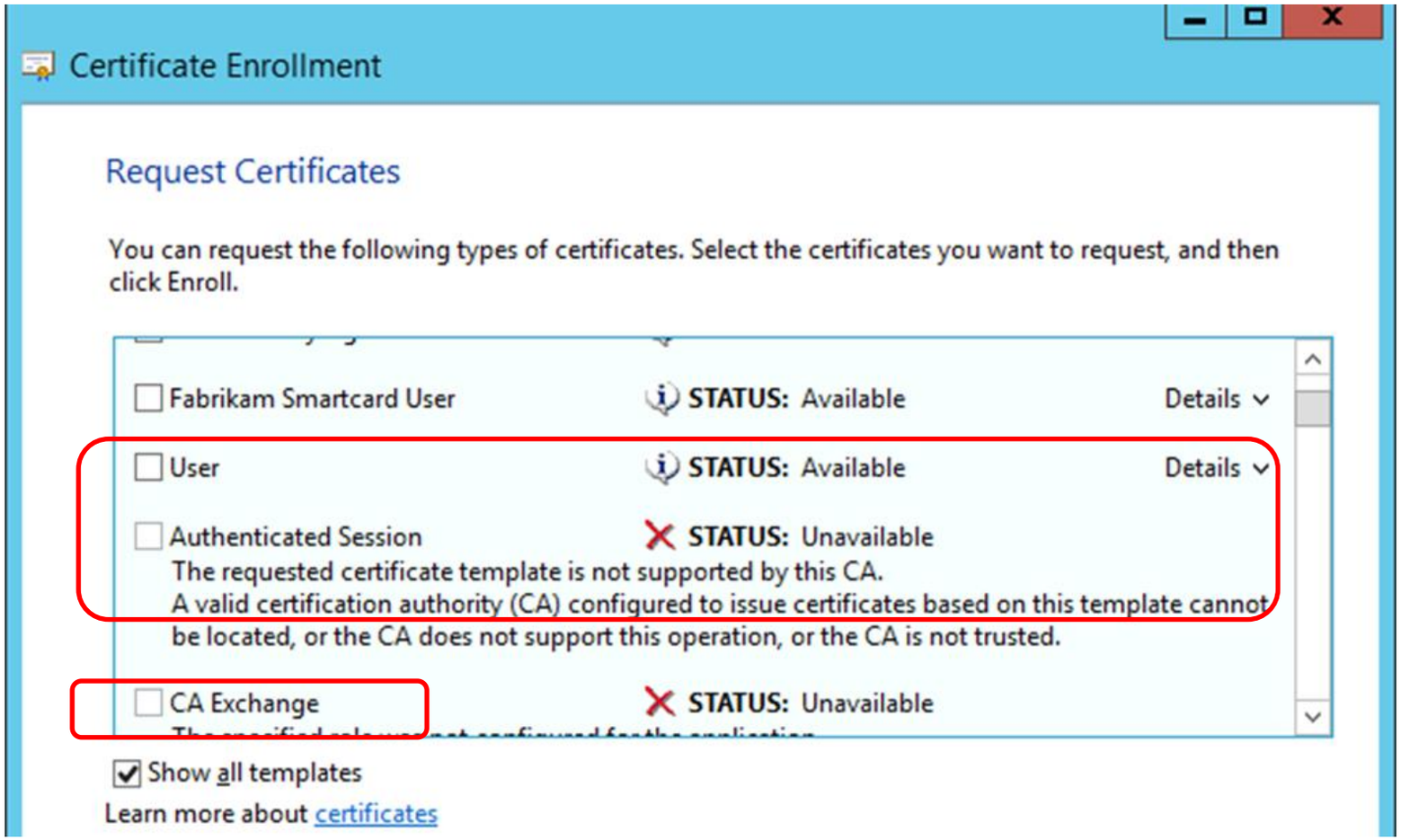
- Personal store > all task > Request New Certificate…



Enrollment Using MMC

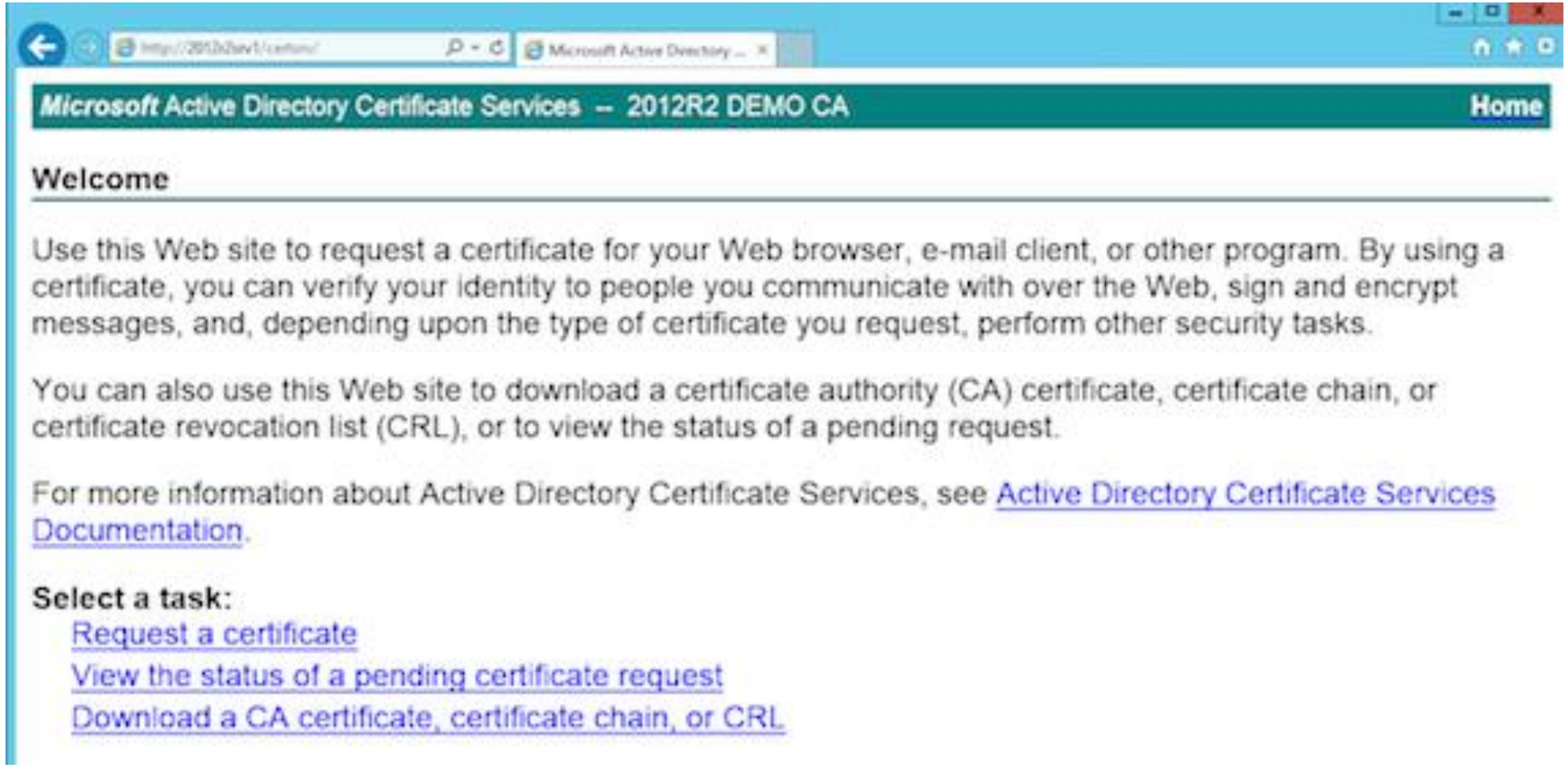
- By default, the list of templates is filtered for those the requestor has Enroll permissions (Read + Enroll security permission)

The **Show all templates** option helps you to troubleshoot permission issues



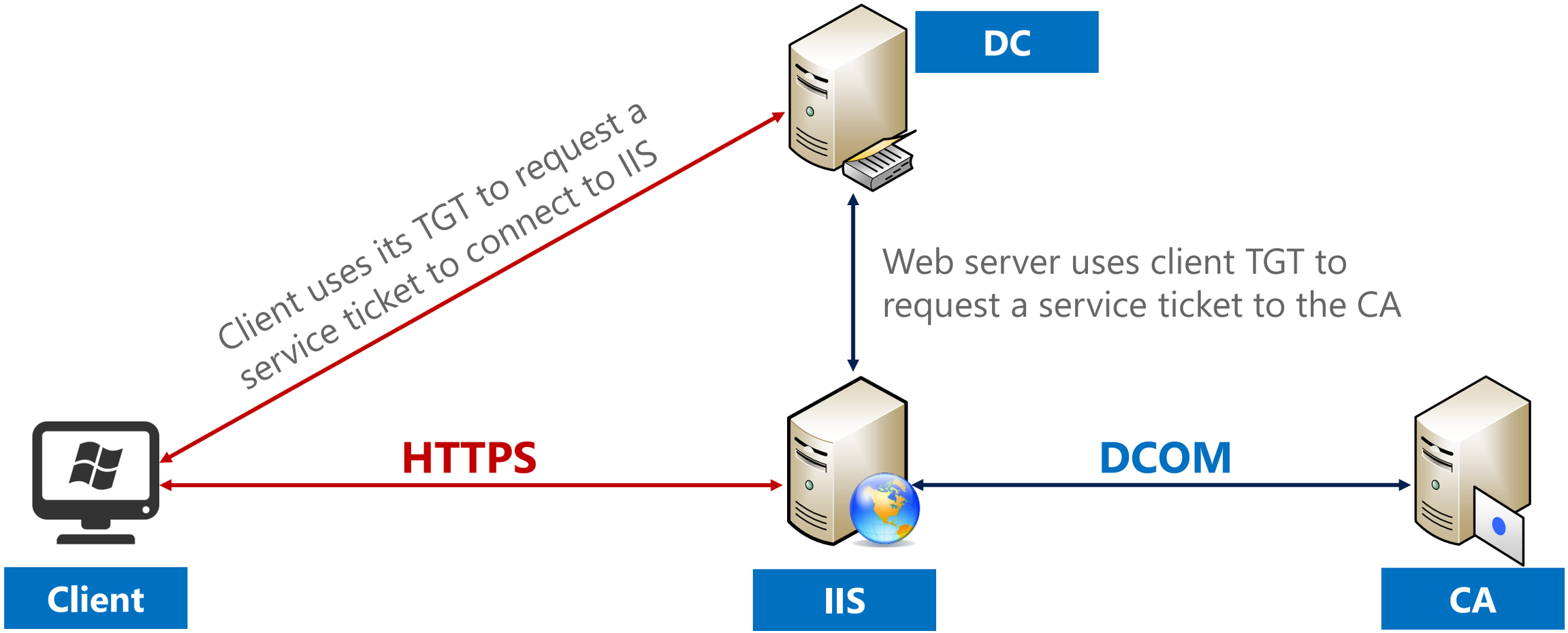
Certificate Authority Web Enrollment Proxy

- The Certificate Authority Web Enrollment role service provides a web portal (based on IIS) that allow to enroll certificates.
- Located at https://<WebServerName>/certsrv



Certificate Authority Web Enrollment Proxy

- When the CA Web Enrollment role service is installed on a different server (other than the CA itself), Kerberos Constrained Delegation is required to allow the web server submitting requests in the user's context



Certificate Authority Web Enrollment

- Install using Server Manager by selecting Active Directory Certificate Services and choosing the role service “Certificate Authority Web Enrollment”
- Don’t get confused with “Certificate Authority Web Service”
- Requires and based on the IIS Server Role
- Supports only V1/V2 Certificate Templates. V3 Certificate Templates and above won’t be available
- Kerberos Constrained Delegation might be required
- Recommended practice: Do no install on a CA server!

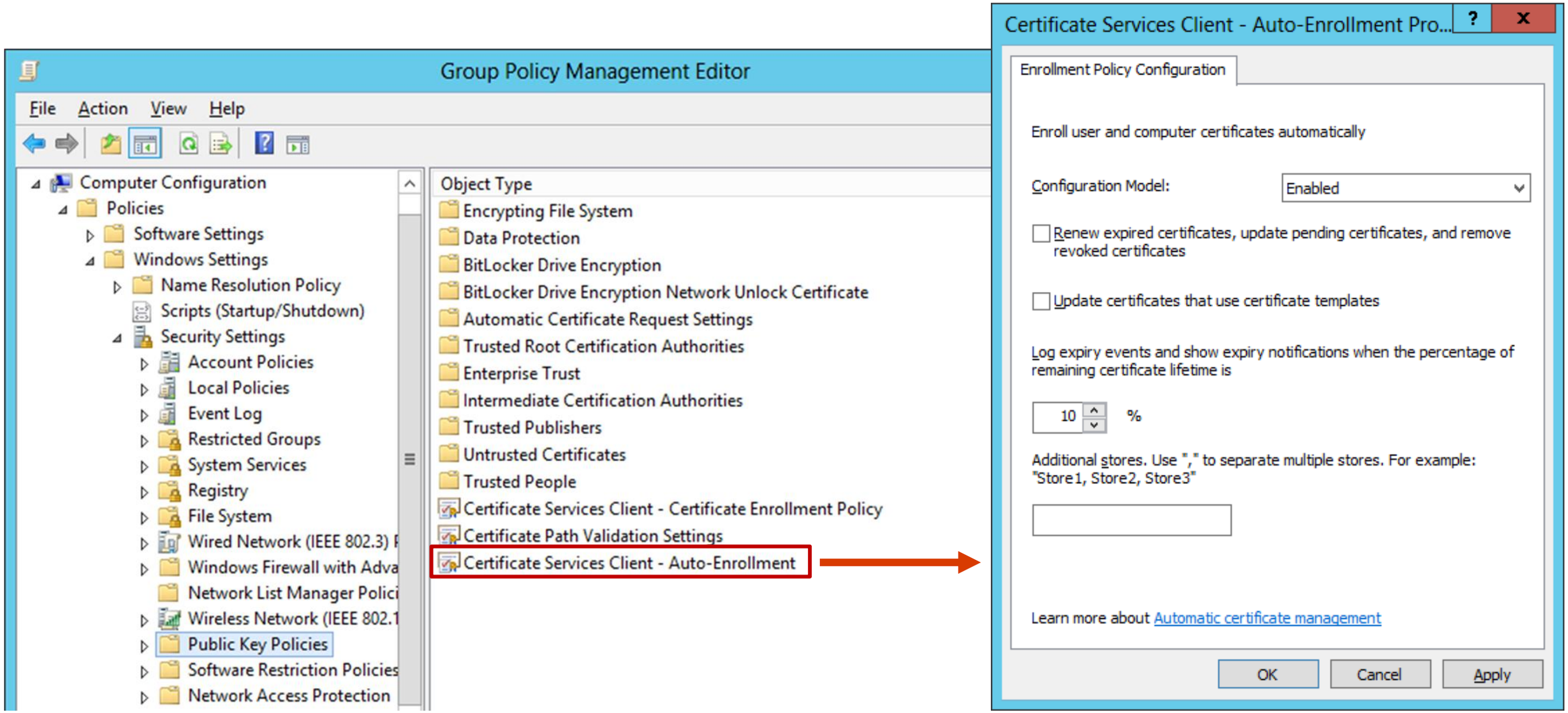
Auto-enrollment

- Allows to receive a certificate automatically through the autoenrollment process, without user interaction
- Covers enrollment, renewal and certificate “housekeeping”
- Certificate autoenrollment is disabled by default

Auto-enrollment (Cont.)

- Enable autoenrollment process by:
  - Configure Windows clients to perform autoenrollment using Group Policy
  - Configure a Version 2 Certificate Template with 'Autoenroll' permission (in addition to the 'Read' and 'Enroll' permissions)
- Group Policy Must be configured for users and computers separately
- Autoenrollment process is triggered by the Winlogon (Certutil -pulse) process or at Group Policy refresh intervals

Auto-Enrollment Group Policy Settings



Lesson Review

Question 1:

Which steps are required in order to deploy a new certificate template for a CA?

- Duplicate an existing certificate template
- Modify the new certificate template as required
- Publish the new certificate template on the CA

Question 2:

What is the major limitation of user enrollment the using MMC?

The MMC enrollment method prevents a user from issuing 'Computer' type certificates.

Module 7 Exercise 1-4

Lab

Duration: 1 Hour

Lesson Review

Question 1:

During the exercise, we installed the Certificate Authority Web Enrollment service role on a dedicated server (adcsweb01).

Why did we not install it on the CA server, although this would be much easier to configure?

We decided to install the Certificate Authority Web Enrollment service role on a dedicated server for security reasons.
It is not recommended to run any service other than the CA service on a CA computer.

Lesson Review

Question 2:

Why do we need to configure Kerberos Constrained Delegation during for Certificate Authority Web Enrollment server?

Configuring Kerberos Constrained Delegation is a requirement because we need to allow the server hosting the Certificate Authority Web Enrollment to access the CA service in the context of the end user.

Certificate File Types

Certificate File Types

- Different file format exists for certificates. Each format:
  - Determines how the certificate is encoded (base64, DER or ASN.1)
  - What information is stored (private key, certificate chain)

File Format	Format Implications	Supported File Extensions
Base 64 Encoded Certificate / DER (Distinguished Encoding Rules) Encoded Certificate	• Supports single certificate • Does not supports storing the private key	• .cer • .crt • .der
PKCS #7 (Cryptographic Message Syntax Standard)	• Supports multiple certificates in a single file • Does not support storing the private key • Based on ASN.1	• .p7b • .p7r
PFX / PKCS #12 (Personal Information Exchange Format)	• Supports multiple certificates in a single file • Containing the private key • Protected with a symmetric key	• .pfx

Certificate File Types used by Unix/Linux

- Linux/Unix using mostly .pem and .key formats in terms of PKI
  - OpenSSL can be used to convert different formats to PEM and KEY files
  - Used mostly by Linux, Java, and 3rd party applications

File Format	Format Implications	Supported File Extensions
PEM (Privacy-Enhanced Electronic Mail)	• Supports multiple certificates in a single file • May contains the private key • Can be protected with a symmetric key	• .pem
KEY (Private Key)	• Contains only the private key of the certificate • Usually protected with a symmetric key	• .key

- Useful commands:
  - Convert .pfx to .key: **openssl.exe pkcs12 -in Certificate.pfx -nocerts -out Certificate.key**
  - Convert .pfx to .pem (including both public and private key): **openssl.exe pkcs12 -in Certificate.pfx -out Certificate.pem**

Certificate Signing Request (CSR)

- Created by the application/OS to submit requests to the CA
  - Usually a base64 encoded (base64, DER or ASN.1)
  - The encoded request enclosed between "-----BEGIN NEW CERTIFICATE REQUEST" and "-----END NEW CERTIFICATE REQUEST----- "
- Containing the requested Common Name (or Subject), as well as other organization information
- Can be easily generated using IIS, OpenSSL and other tools

Creating a CSR using OpenSSL

- OpenSSL can be used to generate a new CSR:
  - Generate a CSR and private key:
    openssl req -new -newkey rsa:4096 -nodes -out Request.csr -keyout Request.key

```
Administrator: Windows PowerShell
PS C:\Program Files\OpenSSL-Win64\bin> .\openssl req -new -newkey rsa:4096 -nodes -out Request.csr -keyout Request.key
Generating a RSA private key
```

  - You will be requested to provide the relevant information, including the requested Subject Name:

```
Country Name (2 letter code) [AU]:IL
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:Haifa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Contoso
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:MyApp.contoso.com
Email Address []:Omer.Eldan@contoso.com
```

Creating a CSR using OpenSSL (Cont.)

- OpenSSL can also be used to decode an existed CSR file:
  - To decode a CSR file:
    openssl req -in Request.csr -noout -text
  - You can now see the request information in plaintext:

Administrator: Windows PowerShell

```
PS C:\Program Files\OpenSSL-Win64\bin> .\openssl req -in Request.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = IL, ST = Some-State, L = Haifa, O = Contoso, OU = IT, CN = MyApp.contoso.com, emailAddress = Omer.E
ldan@contoso.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:b6:5b:0a:f2:6a:d1:8c:3f:8f:29:f4:86:a6:2e:
                    68:62:be:a2:1d:4d:73:80:8e:60:39:3b:45:f1:d4:
```

Module Summary

- Certificate templates are stored in Active Directory
- Different Certificate Templates versions (V1-V4), all issue X.509 v3 certificates
- Different settings (Validity period / Key length / CSP and many more options) defined in the template
- Different enrollment methods available (depending on needs), including MMC, Web Service, and Autoenrollment
- Many certificate file types. Can be converted easily using OpenSSL

Microsoft