Chapter 6

Certificates

Tran Thanh Dien, PhD

August, 2024

Content

- Common certificate types
- Planning your PKI
- Creating a new certificate template
- Issuing your new certificates
- Creating an auto-enrollment policy
- Obtaining a public authority SSL certificate
- Exporting and importing certificates
- OpenSSL for Linux webservers

Do we need a certificate server?

"We need to use certificates to make this work"

For some reason, the use of certificates seems like a daunting task to many of us, even those who have worked in IT for a lot of years.

More and more security is becoming focused on certificates

Do we need a certificate server?

- *The broad term for a certificate environment is public key infrastructure (PKI).*
- *PKI provided by servers in network*
- *The certificate servers known as certification authority (CA) servers*

Common certificate types

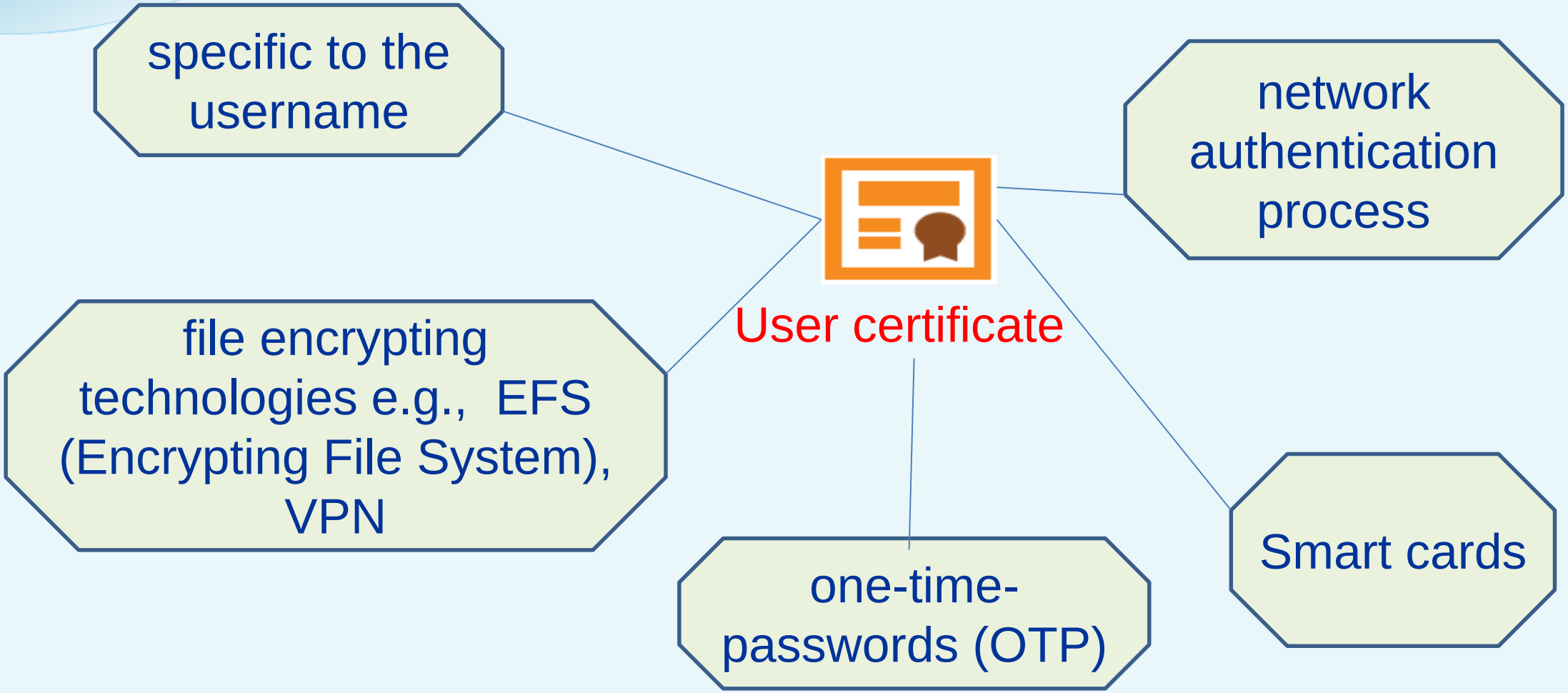
Common certificate types

- There are a number of different types of certificates needing to publish
- When needing a certificate with particular requirements, we build a certificate template to specify it
- Certificate Types:
  - User certificates
  - Computer certificates
  - SSL certificates

- CIA

Common certificate types

User certificates



Common certificate types

Computer certificates

issued to computers

used in the authentication process for a remote access technology, e.g., DirectAccess

Computer certificate

Used in encryption processing between systems on the network

IPsec to encrypt communications between clients and a highly secure file server

SCCM interact with and manage the computer systems

Common certificate types

SSL certificates

Most commonly used to secure website traffic

Common certificate types

SSL certificates

Object

- **Single domain**
  - Protect one domain
    "www" included for free
    ⏭ mysite.nl
- **Multi-domain**
  - Protect several domain under one name
    ⏭ mysite.com
    ⏭ mysite.ch
    ⏭ mysite.fi
- **Wildcard**
  - Protect subdomains of your domain
    ⏭ a.mysite.nl
    ⏭ b.mysite.nl
    ⏭ c.mysite.nl

Validation level

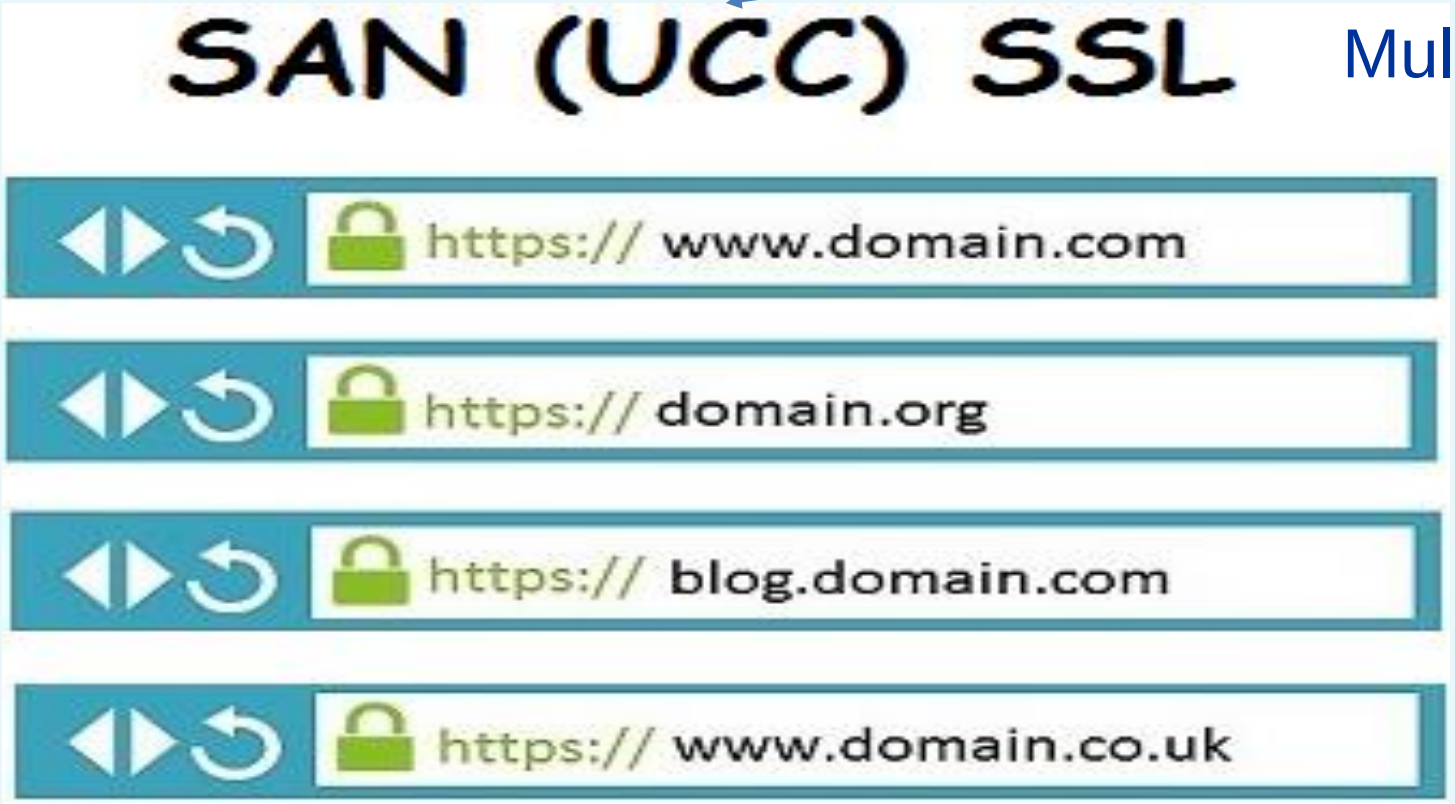
- **DV**
  - ⏭ Verify domain ownership
    ⏭ Low cost
    ⏭ One-day issue
    ⏭ Automated validation
    ⏭ Domain name shown in Certificate
- **OV**
  - ⏭ Verify organization existence
    ⏭ Moderate cost
    ⏭ 1-3 days issue
    ⏭ Manual validation process
    ⏭ Orgname shown in Certificate
- **EV**
  - ⏭ Extensive vetting
    ⏭ High cost
    ⏭ 3-7 days for issue
    ⏭ Extended manual process
    ⏭ Orgname shown in bar

Common certificate types

Multi-domain SSL certificates

Subject Alternative Name

Unified Communications Certificate



Multi-Domain SSL

Common certificate types

Wildcard SSL certificates

Begins with a star (*)

Costs more, significantly more

Common certificate types

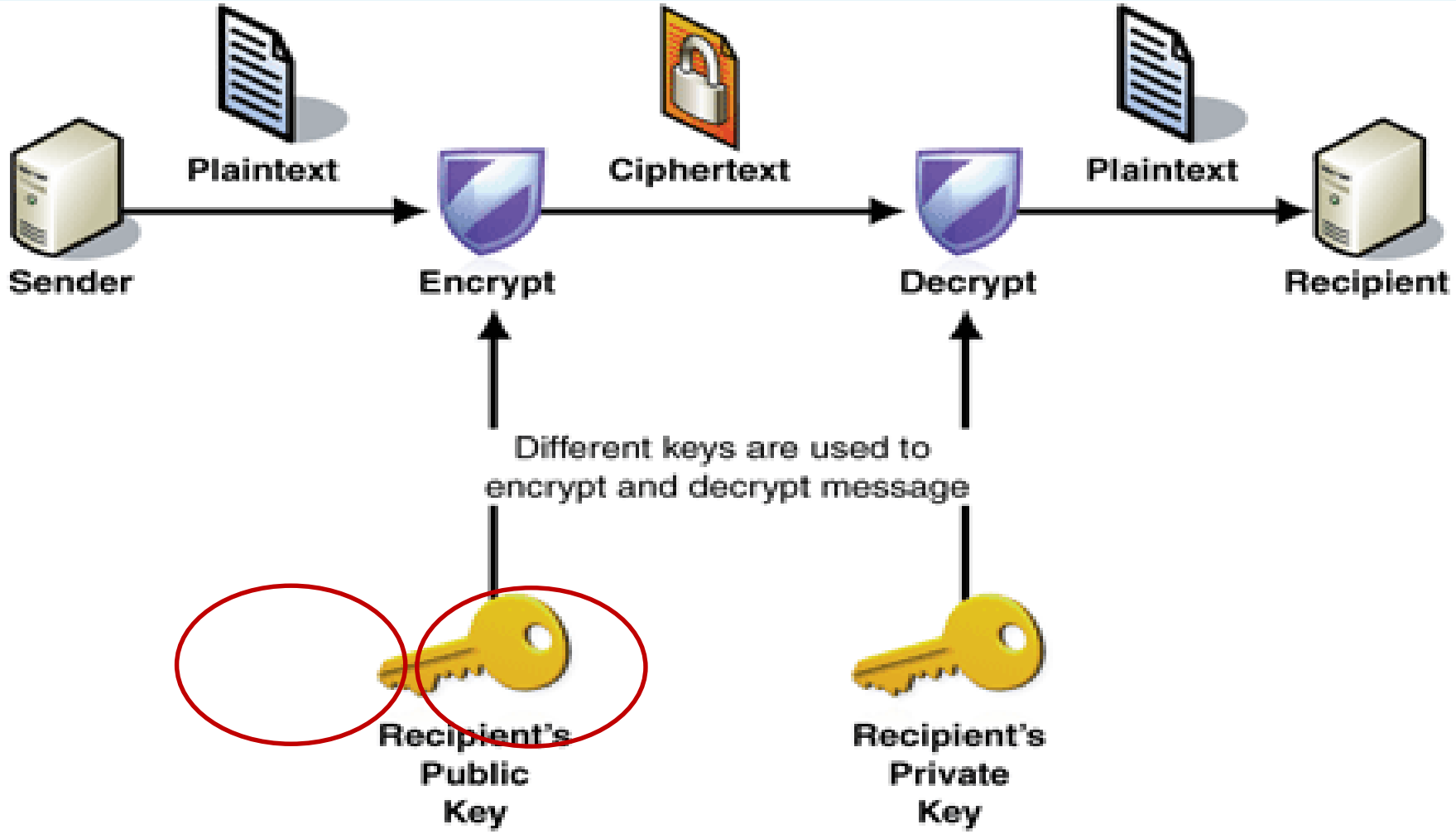
DV, OV and EV SSL certificates

OV also General Purpose SSL Certificates

Public Key Infrastructure (PKI)

PKI process

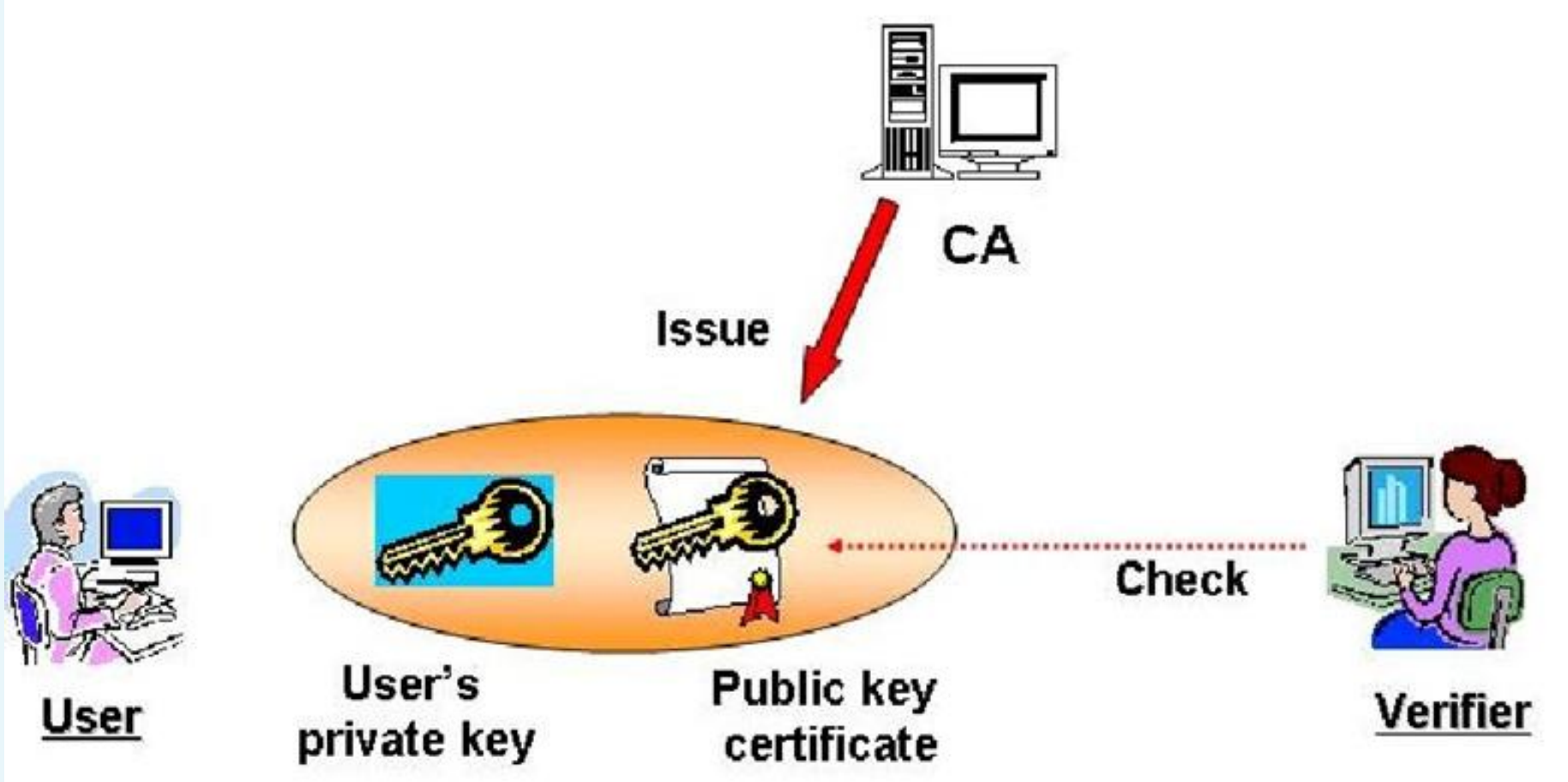
Based on the use of **public and private keys** to provide **confidentiality** and **integrity** of data as it is transmitted over the network.



Public Key Infrastructure (PKI)

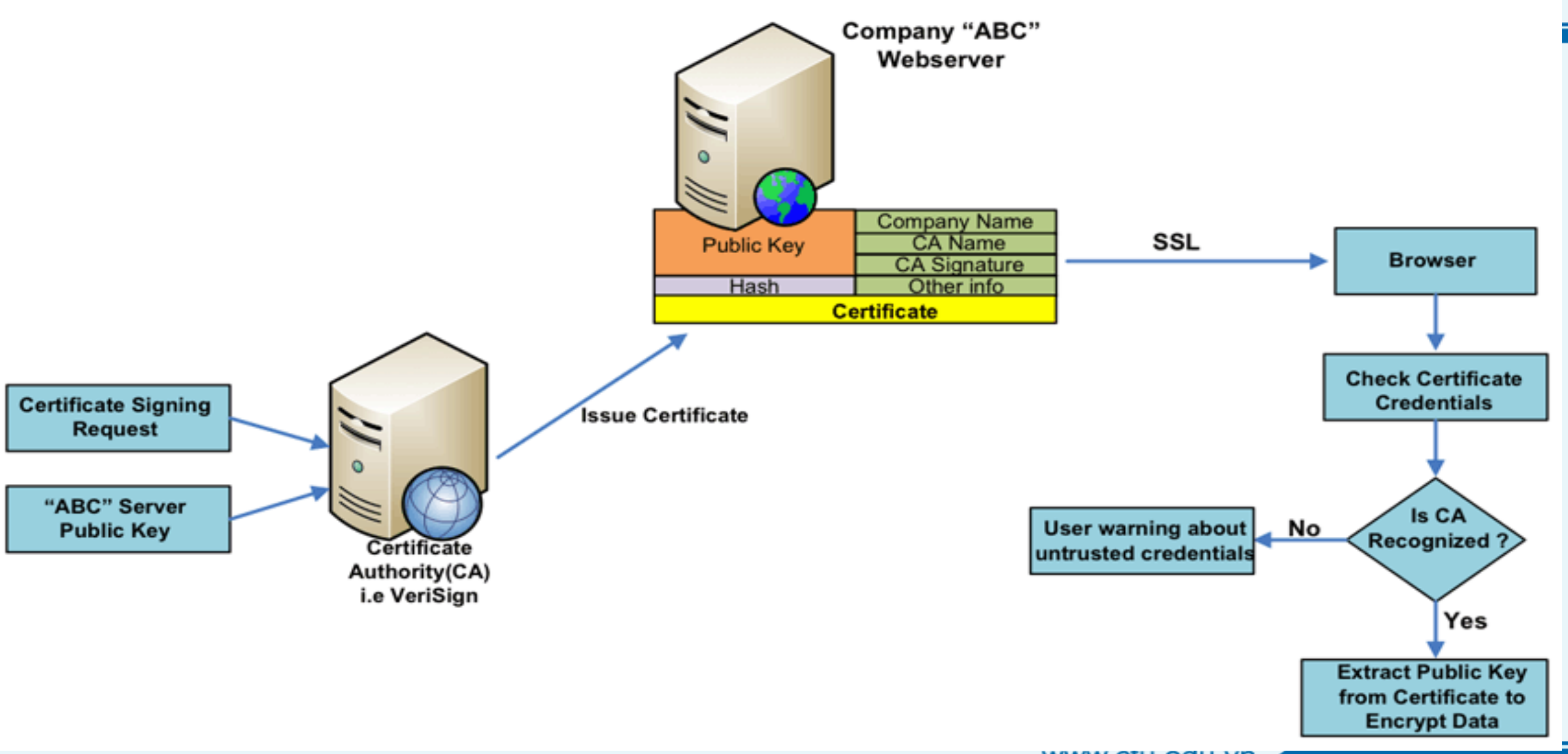
Certification authority (CA) servers

- Servers issued Certificate called certification authority (CA) servers



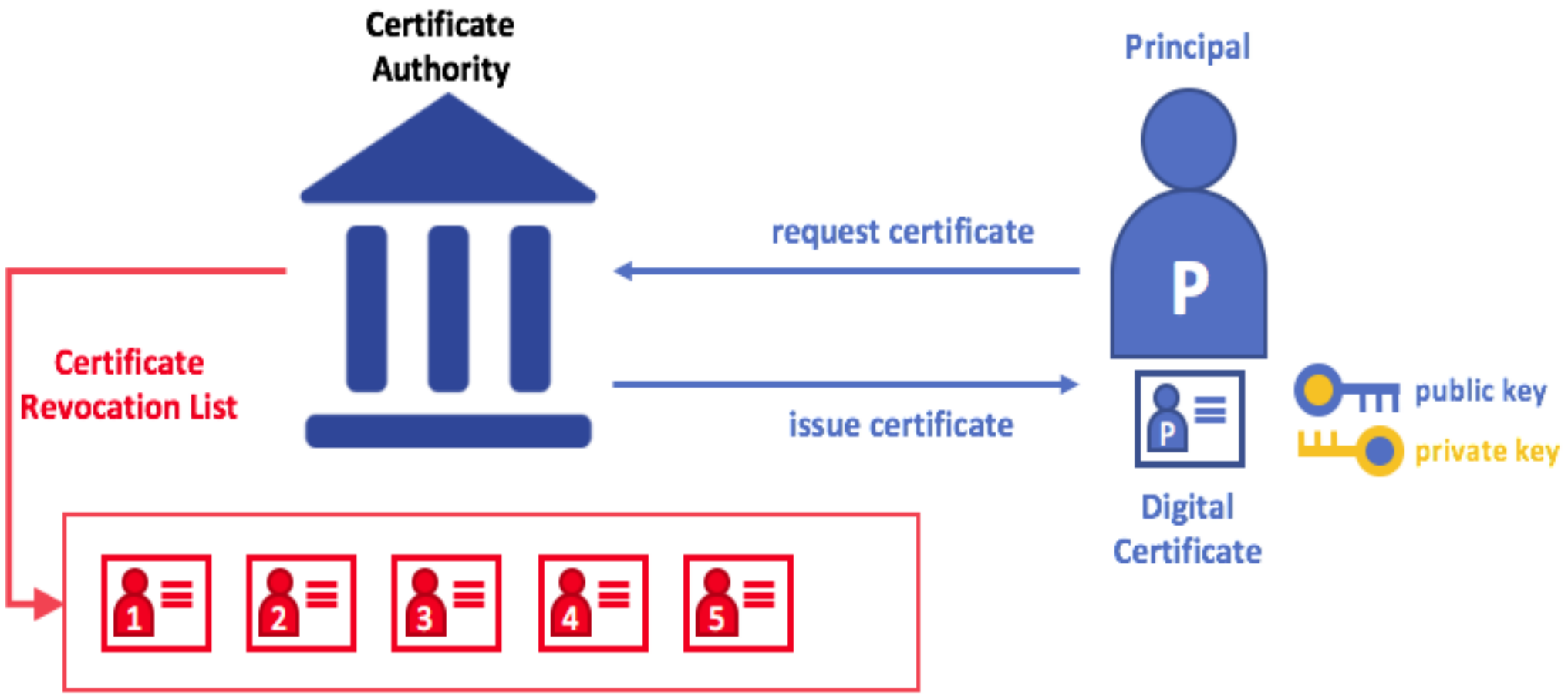
Public Key Infrastructure (PKI)

HTTPS



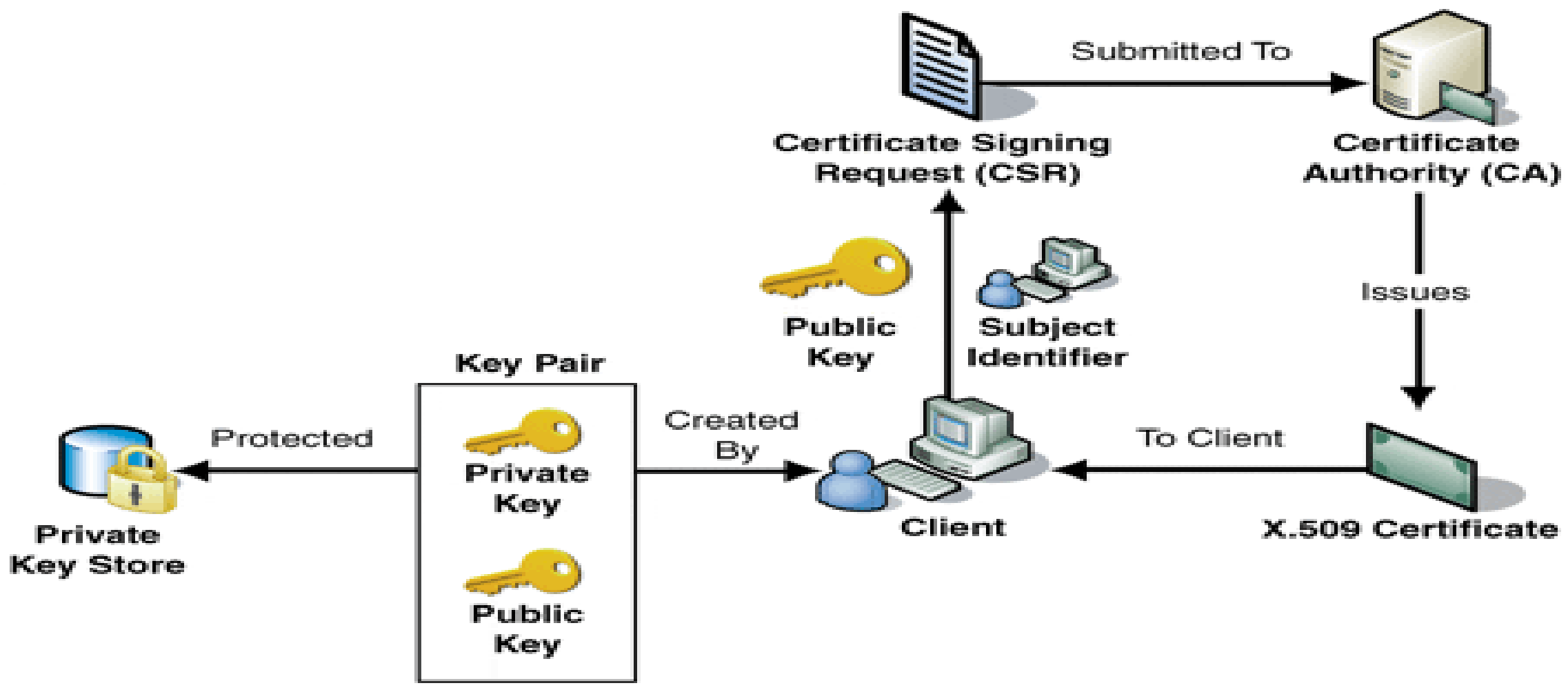
Public Key Infrastructure (PKI)

Certificate signing request



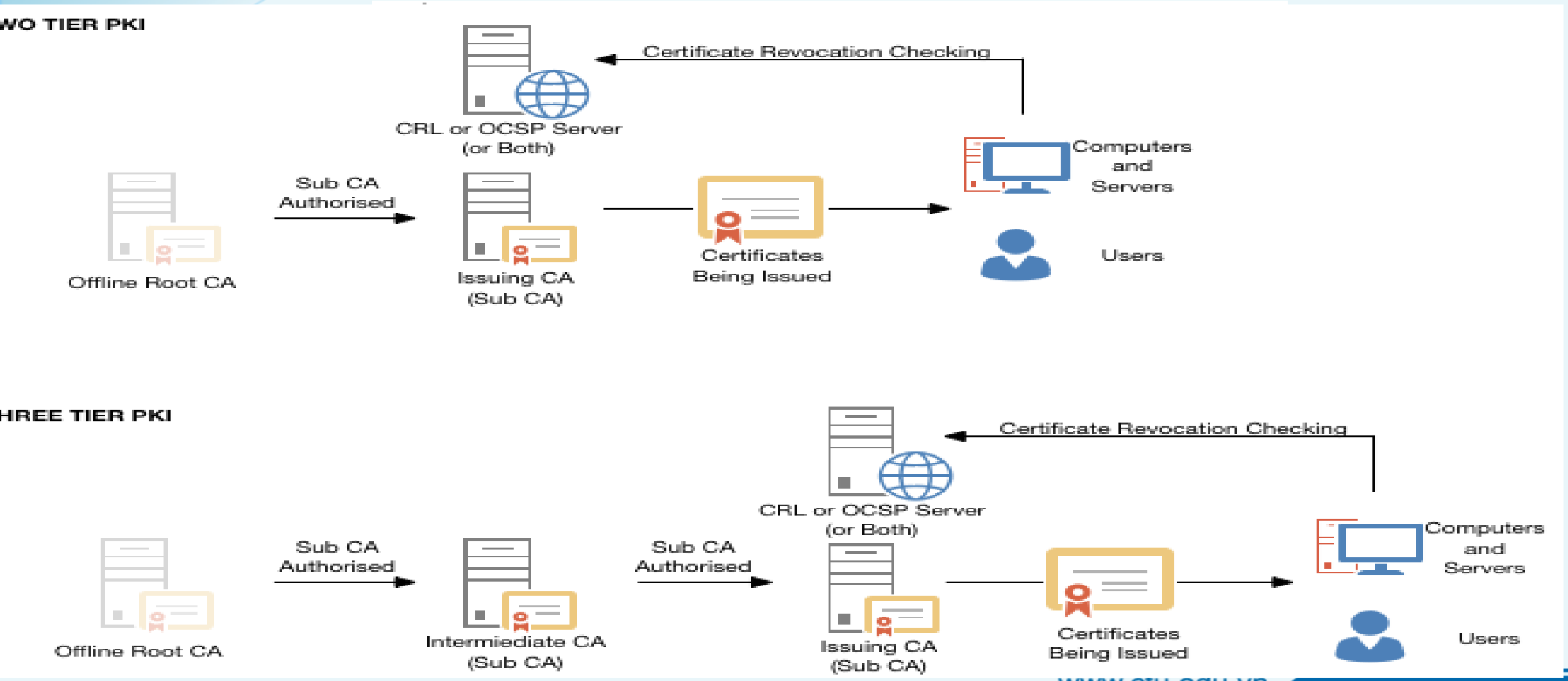
Public Key Infrastructure (PKI)

Certificate signing request



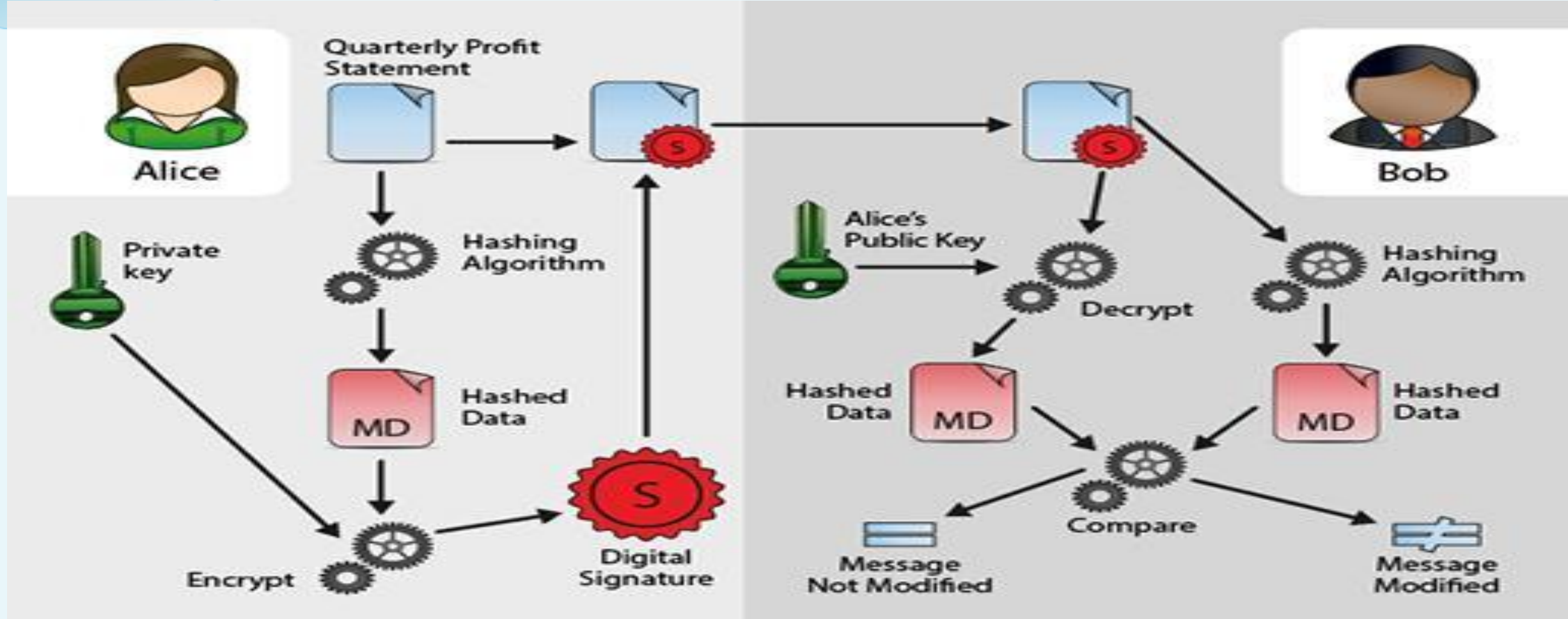
Public Key Infrastructure (PKI)

Certification authority (CA) servers



Public Key Infrastructure (PKI)

Digital Signature



Planning the PKI

Planning the PKI

Active Directory Certificate Services (AD CS)

- Active Directory Certificate Services (AD CS) role provides the functions of a certification authority server
- Should install this role onto one of my domain controller servers?
- No! Unfortunately,
- Technically, it does work. However, it is not a Microsoft-recommended installation path and you should build your CAs on their own servers

Planning the PKI

Add AD CS Role

Add Roles and Features Wizard

Select role services

DESTINATION SERVER
SVR-MBR-B.clc.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD CS
- Role Services
- Confirmation
- Results

Select the role services to install for Active Directory Certificate Services

Role services

- [x] Certification Authority
- [ ] Certificate Enrollment Policy Web Service
- [ ] Certificate Enrollment Web Service
- [x] Certification Authority Web Enrollment
- [ ] Network Device Enrollment Service
- [ ] Online Responder

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

< Previous | Next > | Install | Cancel

Planning the PKI

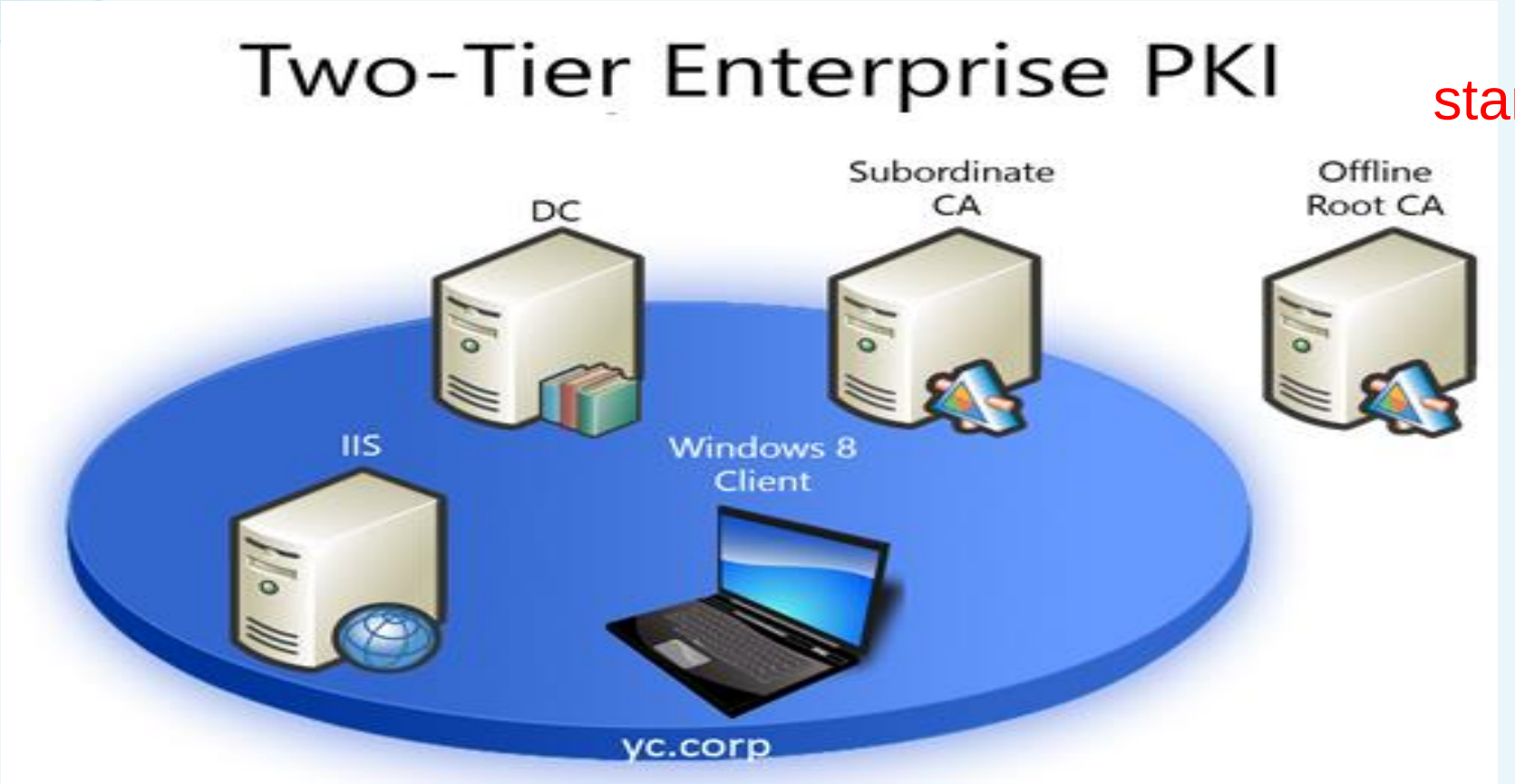
Enterprise versus standalone

Stand-alone vs. Enterprise CAs

Stand-alone CAs		Enterprise CAs	
	Must be used if any CA (root/intermediate/policy) is offline, because a stand-alone CA is not joined to an AD DS domain		Requires the use of AD DS
			Can use Group Policy to propagate certificate to trusted root CA certificate store
	Users provide identifying information and specify type of certificate		Publishes user certificates and CRLs to AD DS
	Does not require certificate templates		Issues certificates based upon a certificate template
	All certificate requests are kept pending until administrator approval		Supports autoenrollment for issuing certificates

Planning the PKI

Enterprise versus standalone

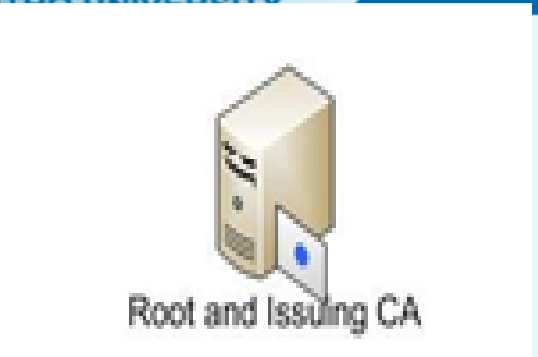


standalone

Subordinate CAs issue the actual certificates, and the root can be safely shut down

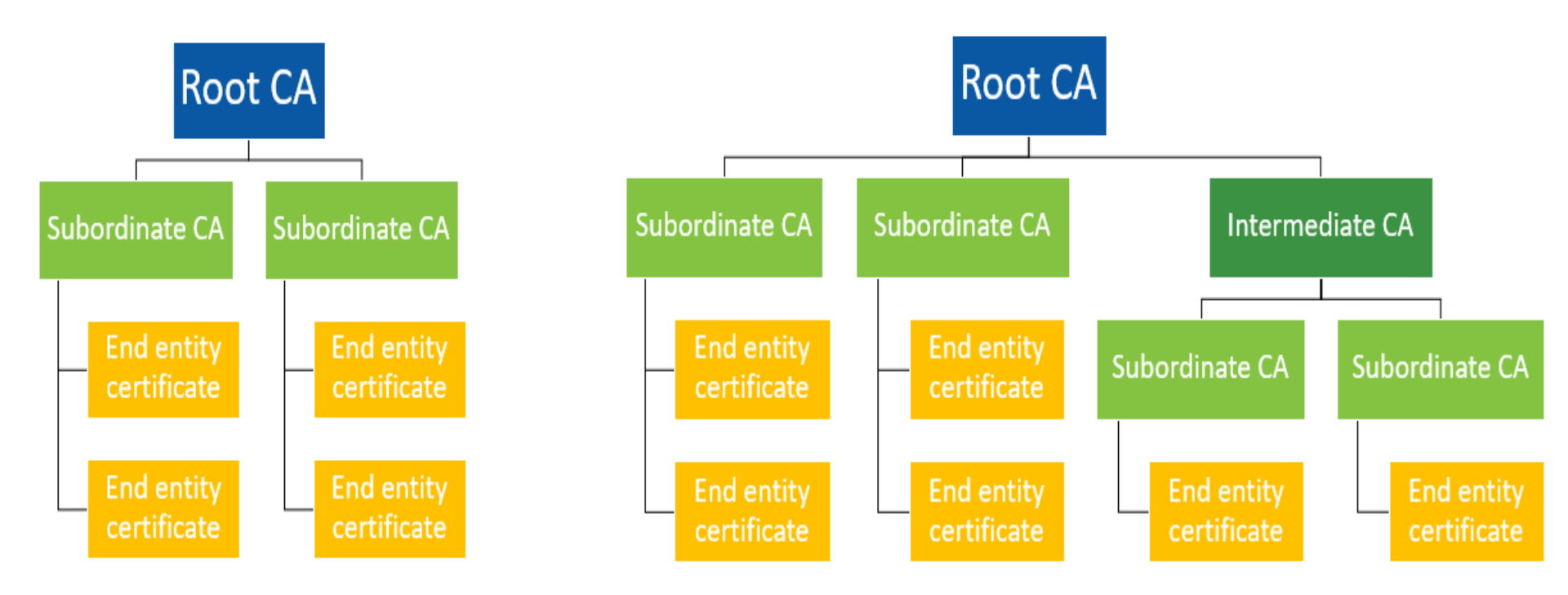
Planning the PKI

Root versus subordinate



a single CA server, then it must be a root

the first CA in your environment needs to be a root, and you can slide subordinates in underneath it



Planning the PKI

Configure Certification Authority

AD CS Configuration

DESTINATION SERVER
SVR-MBR-B.clc.com

Role Services

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Certificate Request
- Certificate Database
- Confirmation
- Progress
- Results

Select Role Services to configure

- [x] Certification Authority
- [x] Certification Authority Web Enrollment
- [ ] Online Responder
- [ ] Network Device Enrollment Service
- [ ] Certificate Enrollment Web Service
- [ ] Certificate Enrollment Policy Web Service

More about AD CS Server Roles

< Previous | Next > | Configure | Cancel

Planning the PKI

Configure Certification Authority

AD CS Configuration

DESTINATION SERVER
SVR-MBR-B.clc.com

Setup Type

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Certificate Request
- Certificate Database
- Confirmation
- Progress
- Results

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

(●) Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

( ) Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

< Previous | Next > | Configure | Cancel

Planning the PKI

Configure Certification Authority

CANTHO UNIVERSITY

DESTINATION SERVER
SVR-MBR-B.clc.com

CA Type

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

(●) Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

( ) Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

More about CA Type

< Previous | Next > | Configure | Cancel

Planning the PKI

Configure Certification Authority

AD CS Configuration

DESTINATION SERVER
SVR-MBR-B.clc.com

Private Key

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

(●) Create a new private key
Use this option if you do not have a private key or want to create a new private key.

( ) Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

- ( ) Select a certificate and use its associated private key
  Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
- ( ) Select an existing private key on this computer
  Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about Private Key

< Previous | Next > | Configure | Cancel

Planning the PKI

Configure Certification Authority

AD CS Configuration

Cryptography for CA

DESTINATION SERVER
SVR-MBR-B.clc.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the cryptographic options

Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider

Key length:
2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography

< Previous | Next > | Configure | Cancel

Planning the PKI

Configure Certification Authority

AD CS Configuration

CA Name

DESTINATION SERVER
SVR-MBR-B.clc.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

CLC-CertServer

Distinguished name suffix:

DC=clc,DC=com

Preview of distinguished name:

CN=CLC-CertServer,DC=clc,DC=com

More about CA Name

< Previous | Next > | Configure | Cancel

Planning the PKI

Configure Certification Authority

- Can I install the CA role onto a domain controller?
- No! Unfortunately
- you should build your CAs on their own servers; try not to co-host them with any other roles whenever possible.

Creating a new certificate template

Creating a new certificate template

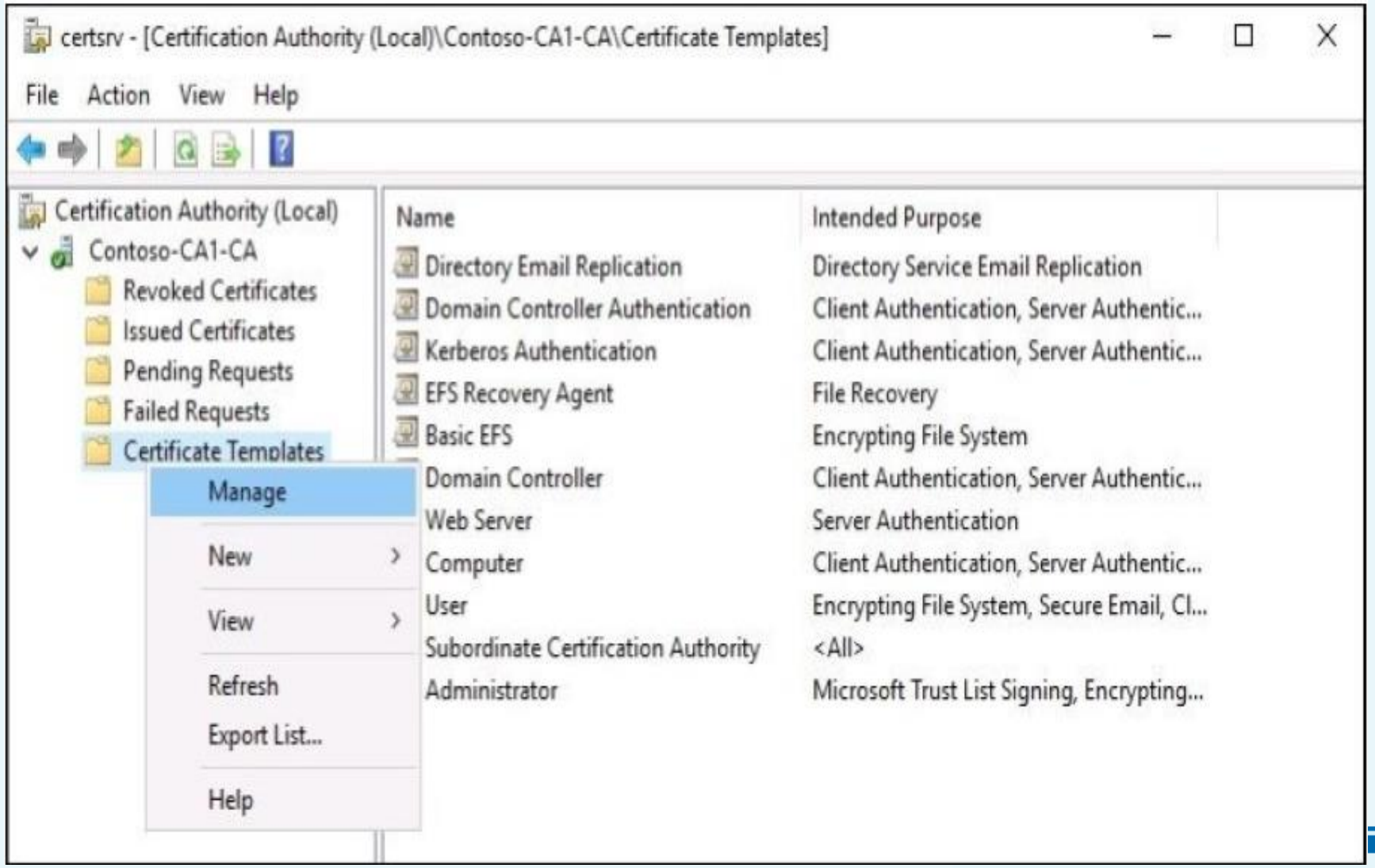
- Enterprise CA server issues a certificate based on a certificate template
- Certificate template include all of the particular settings incorporated into your final certificate
- When issue a certificate from a CA server to a device or user, choosing which certificate template you want to utilize to deploy a certificate based upon the settings configured inside that template

Creating a new certificate template

- Certificate templates are sort of like recipes for cooking.
- On the CA server, you build out your templates and include all of the particular ingredients, or settings, that you want to incorporate into your final certificate.
- When the users request a certificate from the CA server, they tell the CA which template recipe to follow.

Creating a new certificate template

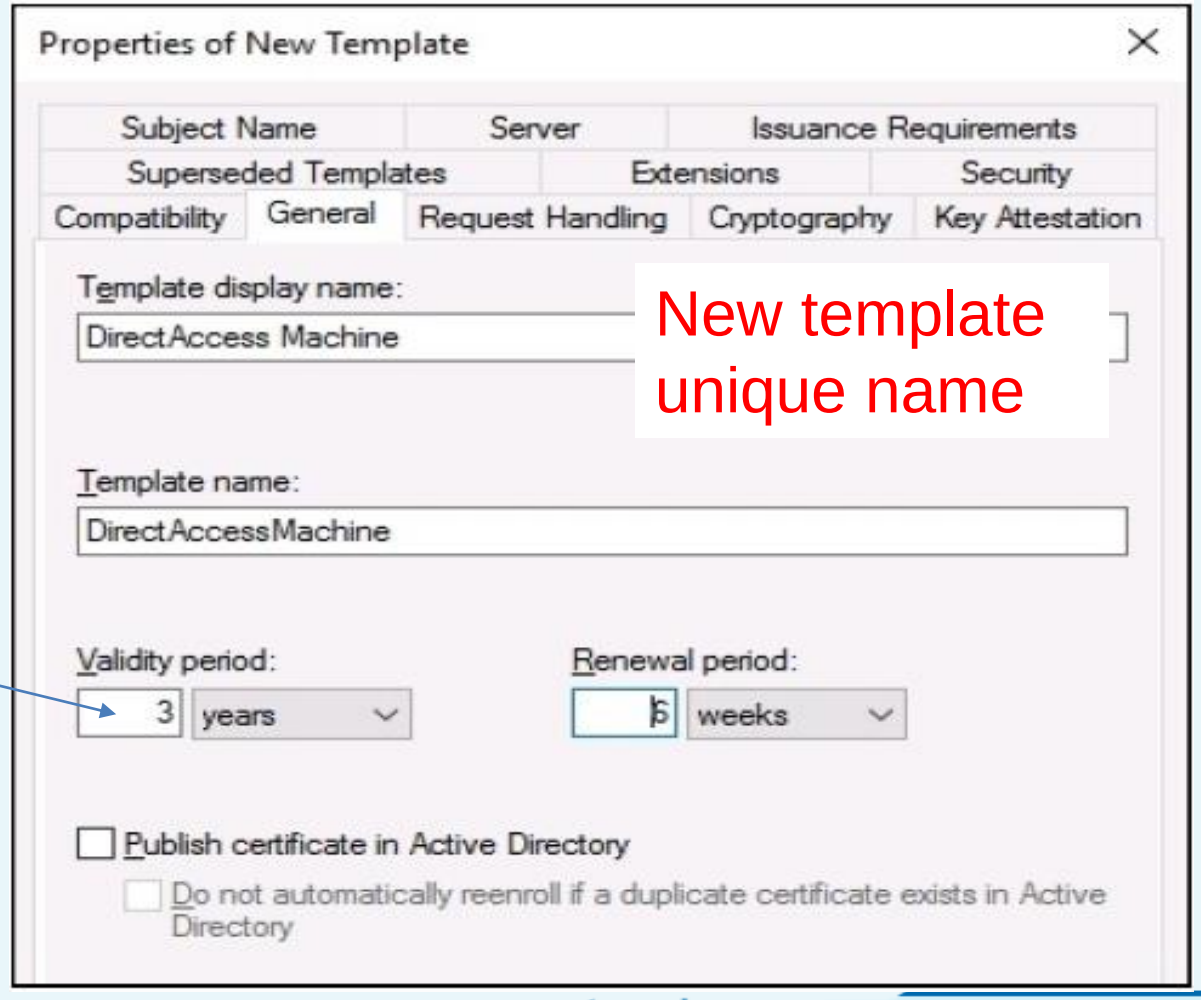
- Launch **Certification Authority**.
- Right-click on **Certificate Templates** folder and choose **Manage**



Creating a new certificate template

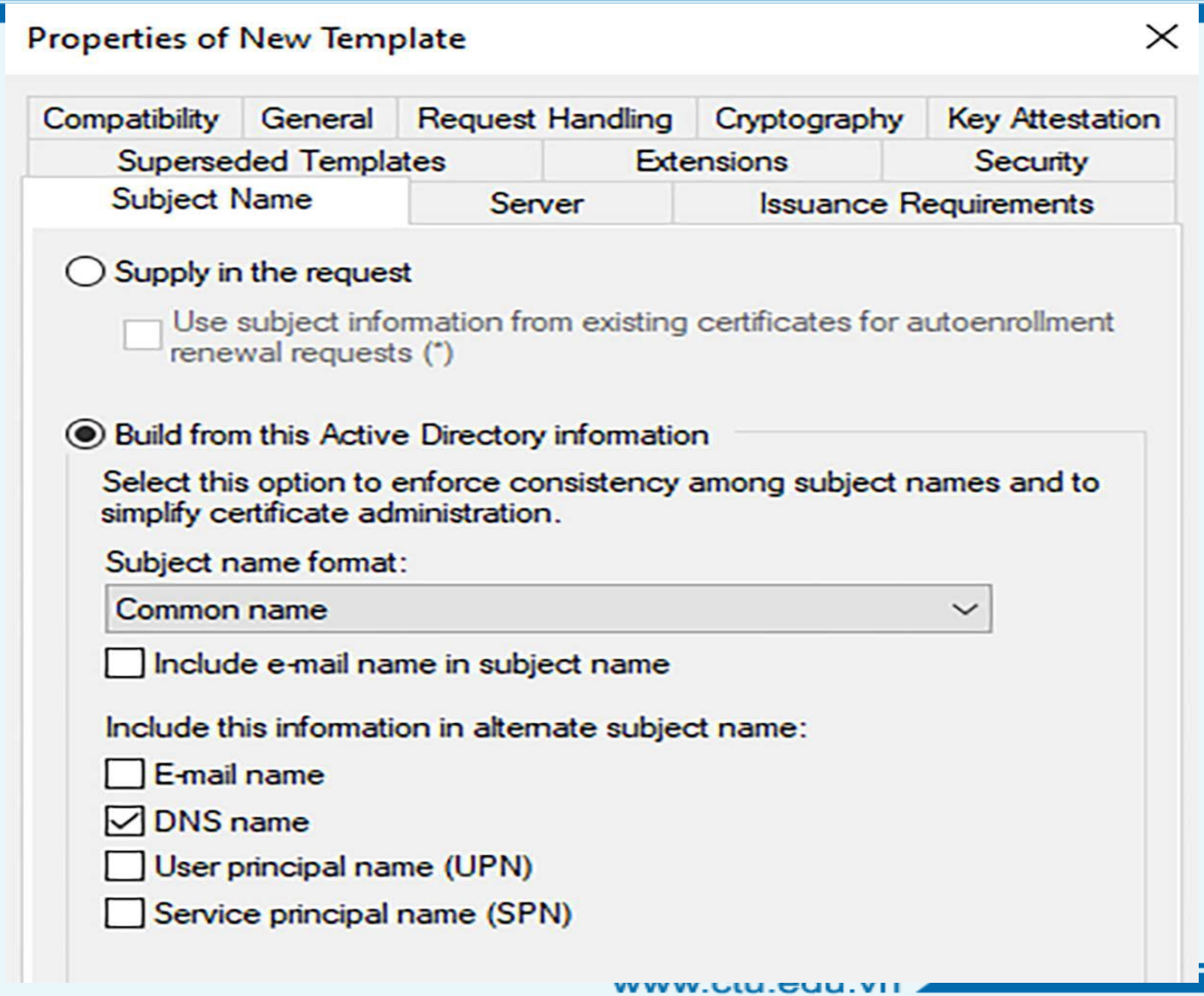
- Find a pre-existing template that we want our new certificate template to serve
- Right-click on the built-in template, and click on **Duplicate Template**

define the validity period for this certificate

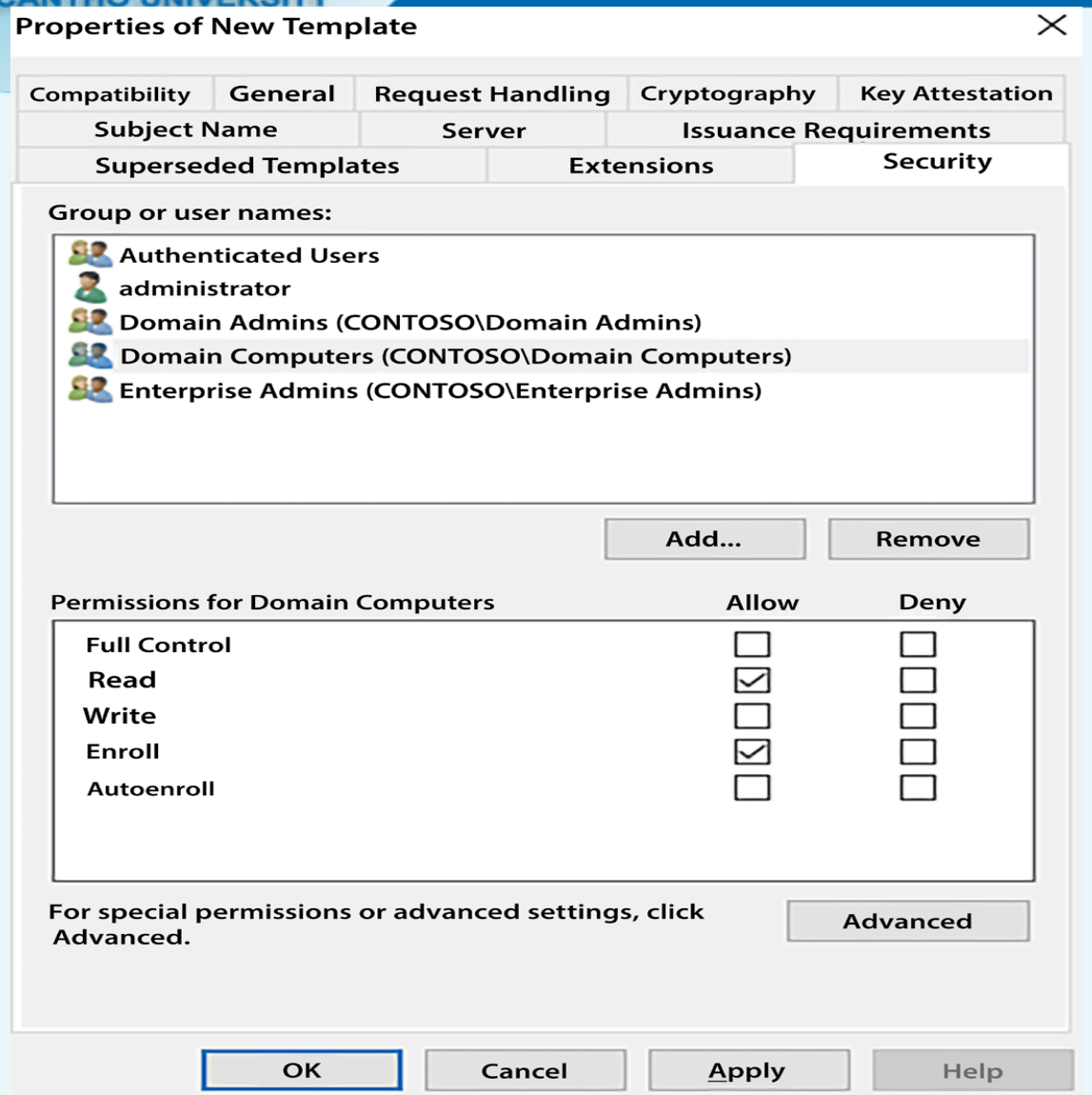


Creating a new certificate template

- Subject Name tab



Creating a new certificate template



Set the security permissions for this template

Enroll permissions: allow any computer joined to the domain have the option of requesting a new certificate

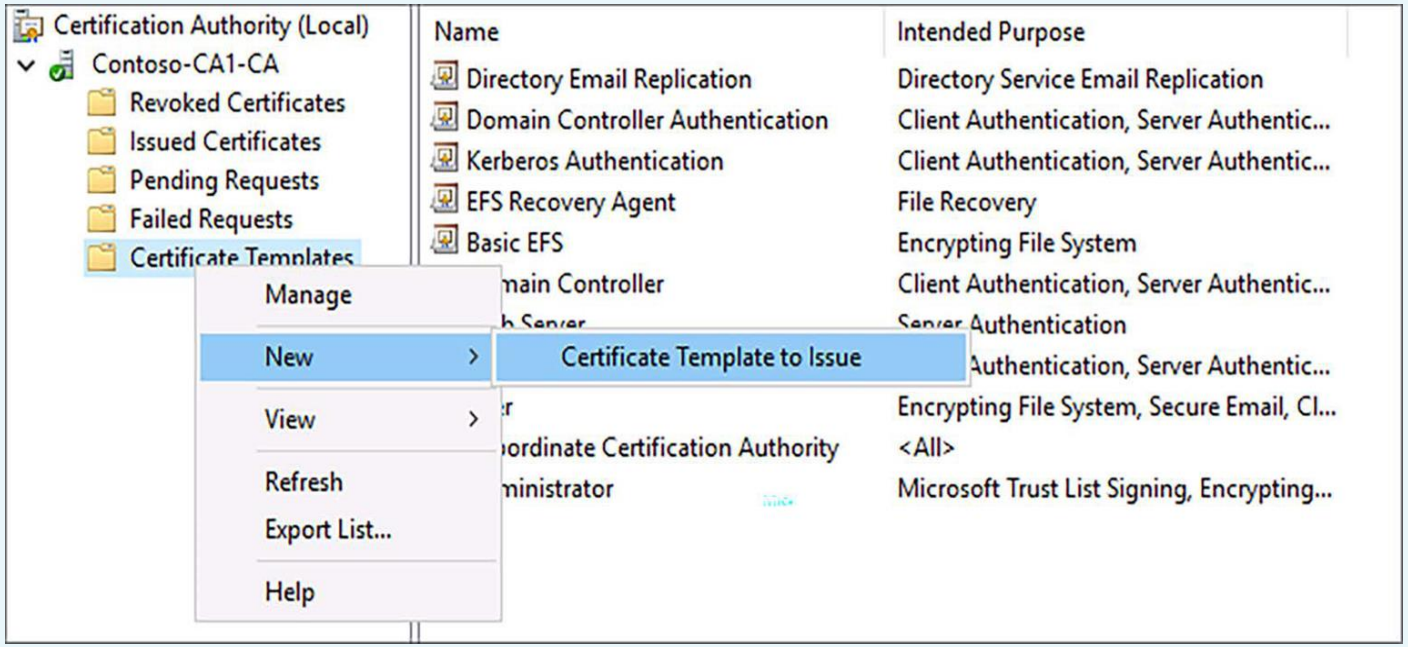
Issuing new certificates

Issuing new certificates

Publishing the template

- After creating the new template, we need to publish it to make it available for issuing new certificates.

- Right-click on the Certificate Templates, then choose **New | Certificate Template to Issue**



- Choose the new template from the list, and click on OK
- The new template is now included in the list of published certificate templates

Issuing new certificates

Requesting a cert from MMC

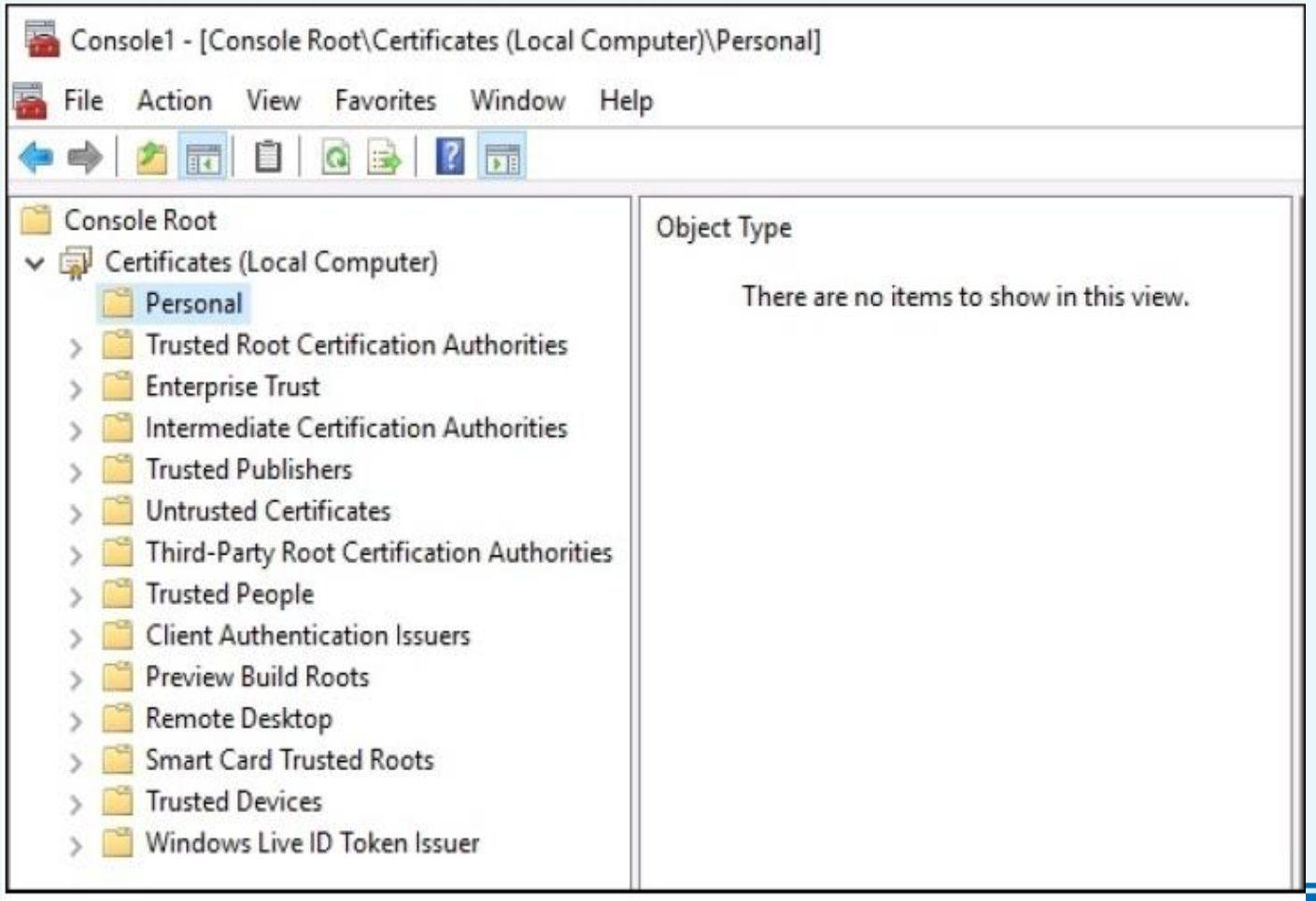
- Log in to a regular client computer on your network to request a certificate
- Launch MMC and add the snap-in for **Certificates**
- When choosing **Certificates** from the list of available snap-ins and click **Add** button; you are presented with some additional options for which certificate store you want to open

Issuing new certificates

Requesting a cert from MMC

- The specific location that we want to install our certificate into is the Personal folder.

- To request a new certificate from our CA server, right-click on the **Personal** folder, and then navigate to **All Tasks | Request New Certificate….**

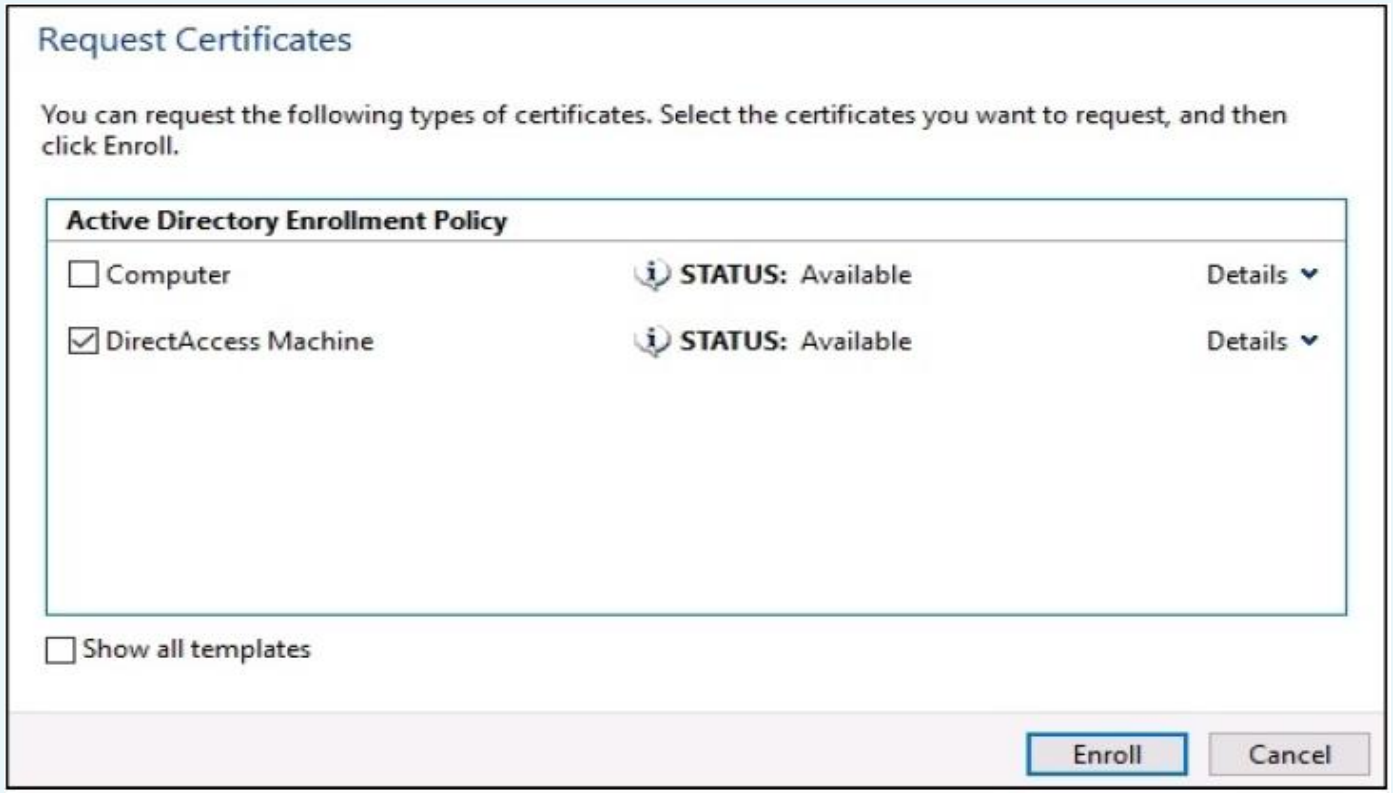


Issuing new certificates

Requesting a cert from MMC

- The Request Certificates screen shows the list of templates that are available to us.

- If you do not see your new template in the list, click on the checkbox **Show all templates**.

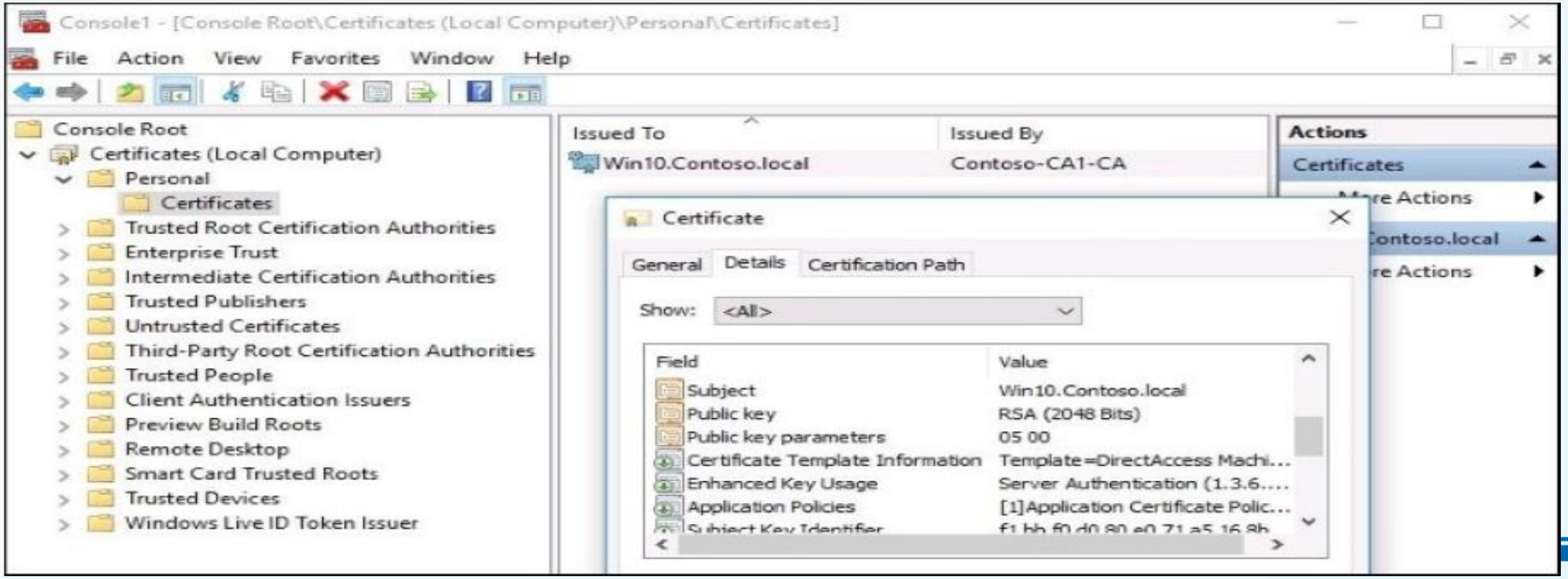


- Put a check mark next to any certificates that you want, and click on Enroll

Issuing new certificates

Requesting a cert from MMC

- Once finished, the new machine certificate is now inside **Personal | Certificates** in the MMC.
- Double-click on the certificate to check its properties



Issuing new certificates

Requesting a cert from the Web interface

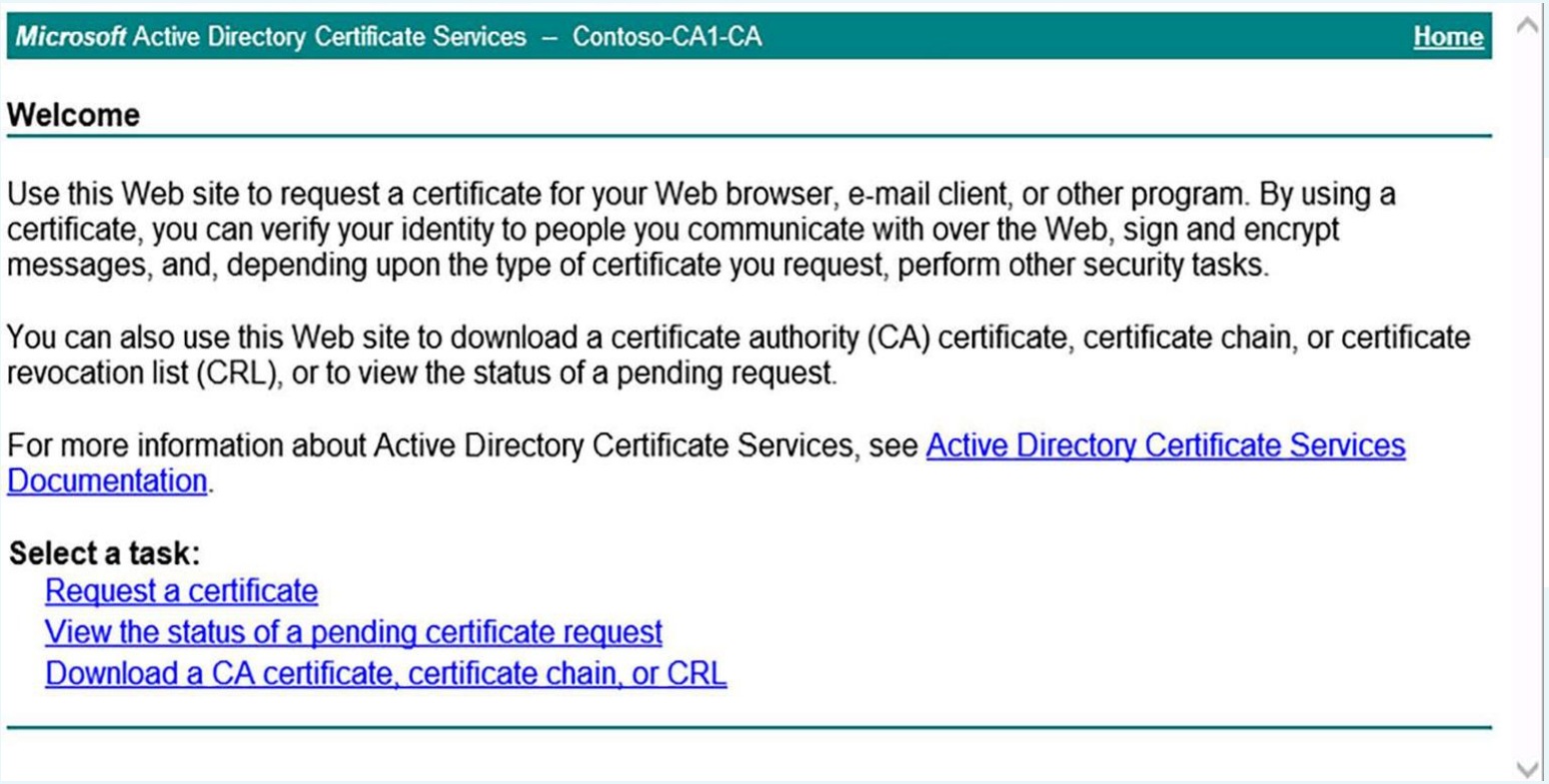
- During installing AD CS role, we have the options to select Certification Authority Web Enrollment

- Once installed on the CA, a website running on that server which you can access via a browser from inside your network.

Issuing new certificates

Requesting a cert from the Web interface

- To request a certificate from a website, launch web browser, and log in to the website running at https://<CASERVER>/certsrv



Microsoft Active Directory Certificate Services – Contoso-CA1-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

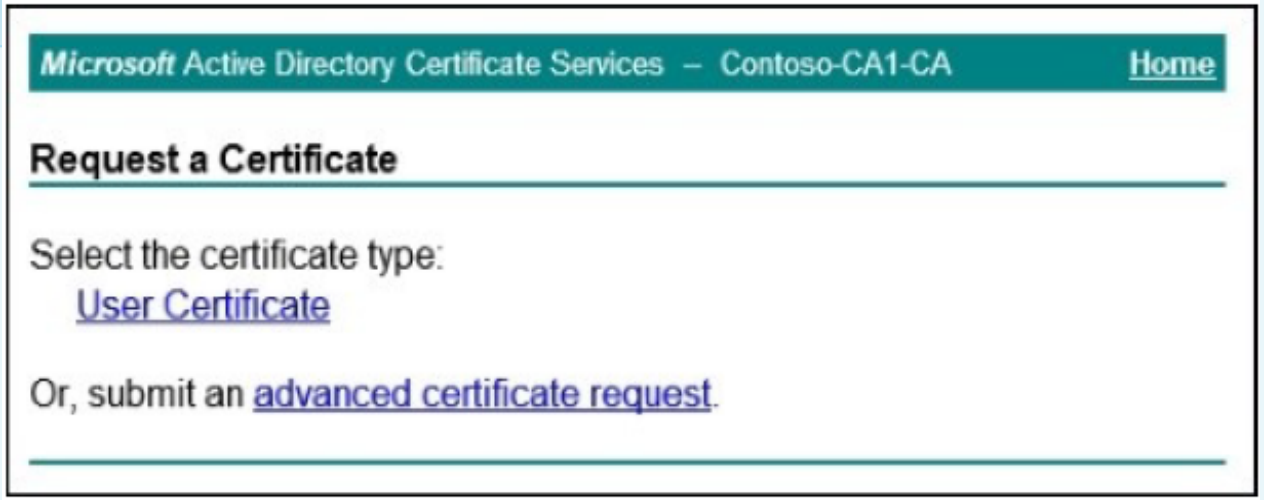
Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Click on **Request a certificate** to request a new certificate from the CA server

Issuing new certificates

Requesting a cert from the Web interface

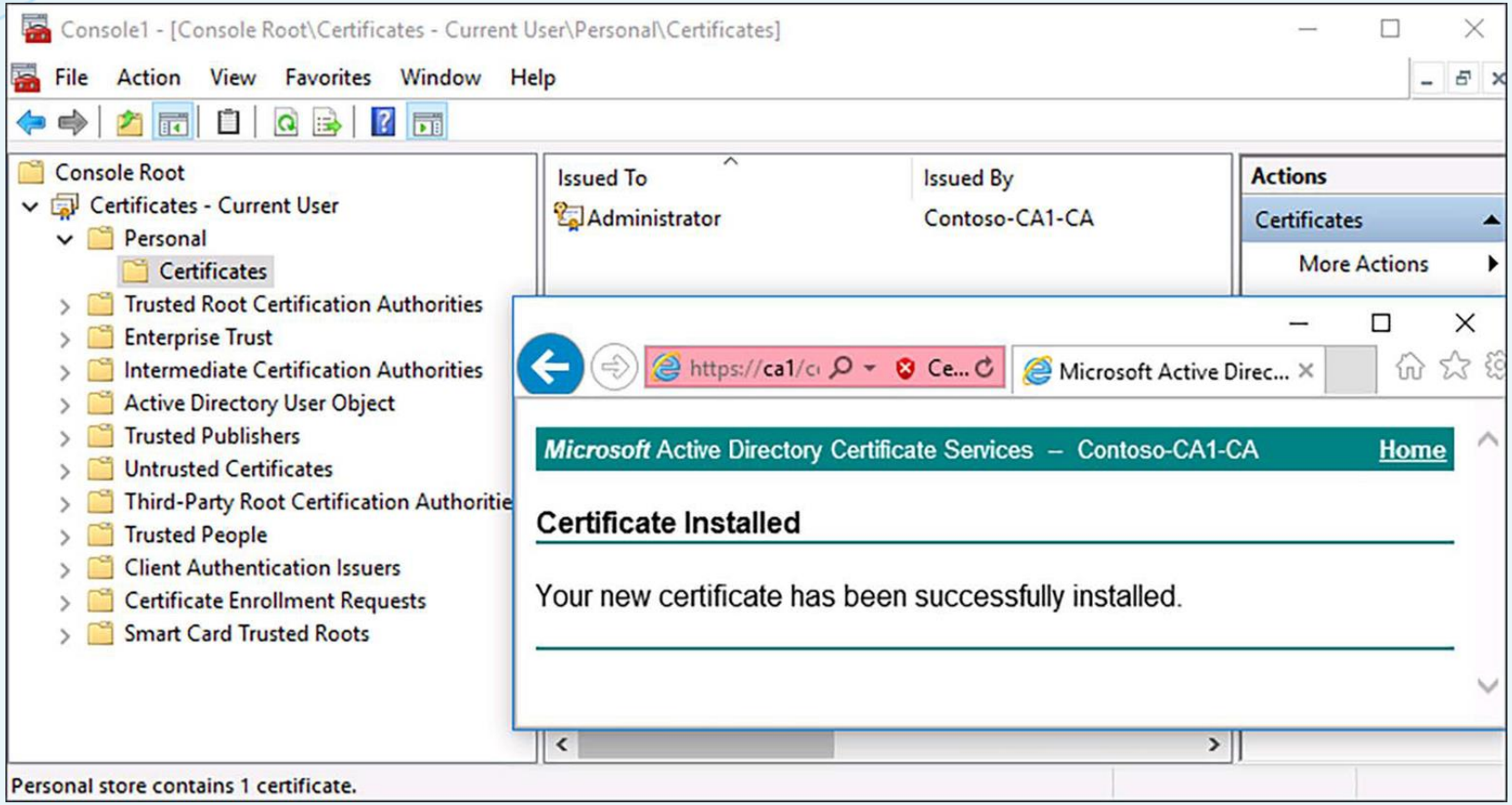


Click on **User Certificate** to request a user-based certificate

- If you need any other kind of certificate, choose the link for **advanced certificate request**
- Next, click the Submit button
- Once the certificate generated you will see a link that allows to Install this certificate
- Click on that link, and the new certificate now installed onto your computer

Issuing new certificates

Requesting a cert from the Web interface



The screenshot shows the response from the website indicating a successful installation

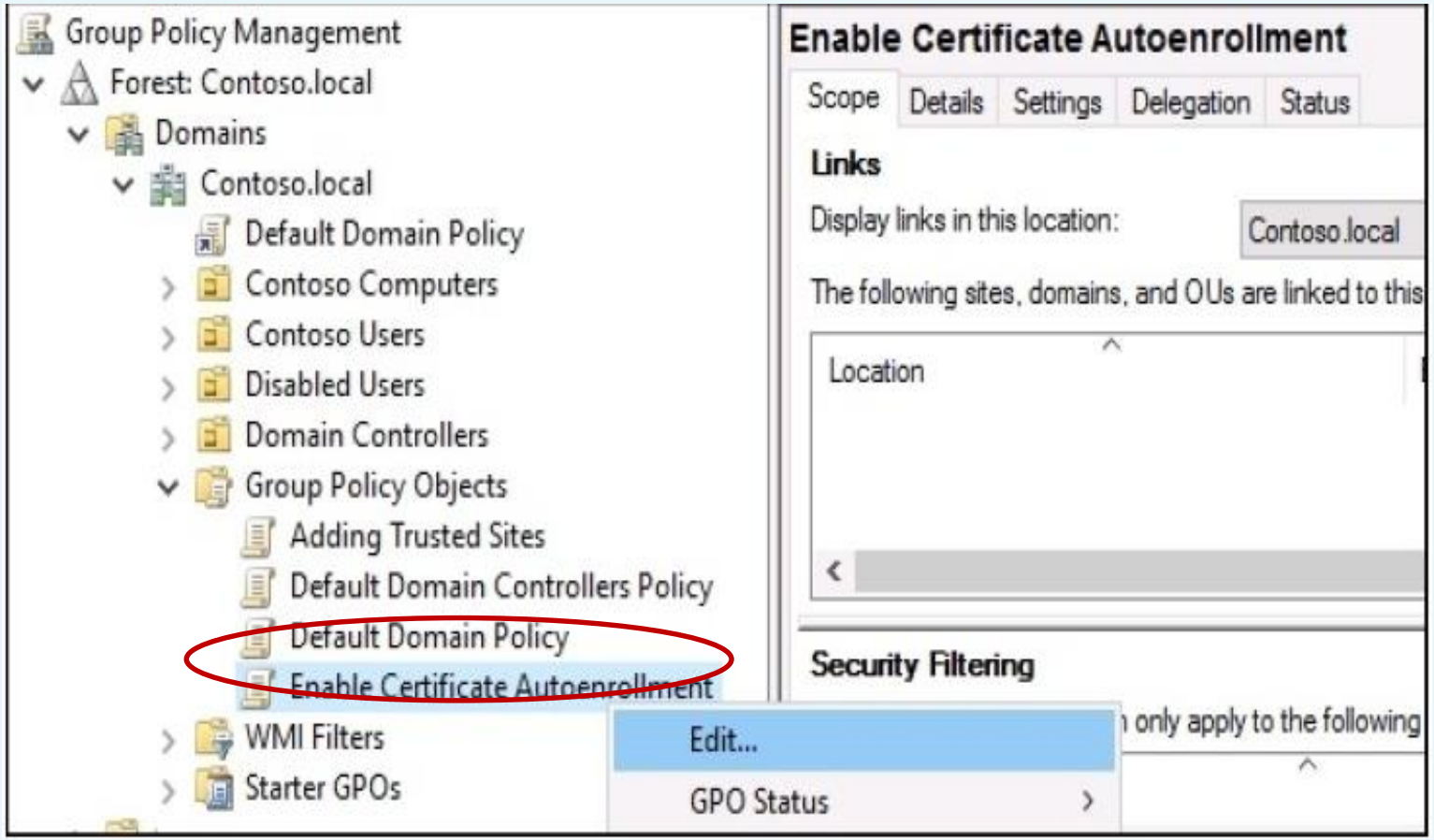
Creating an autoenrollment policy

Creating an autoenrollment policy

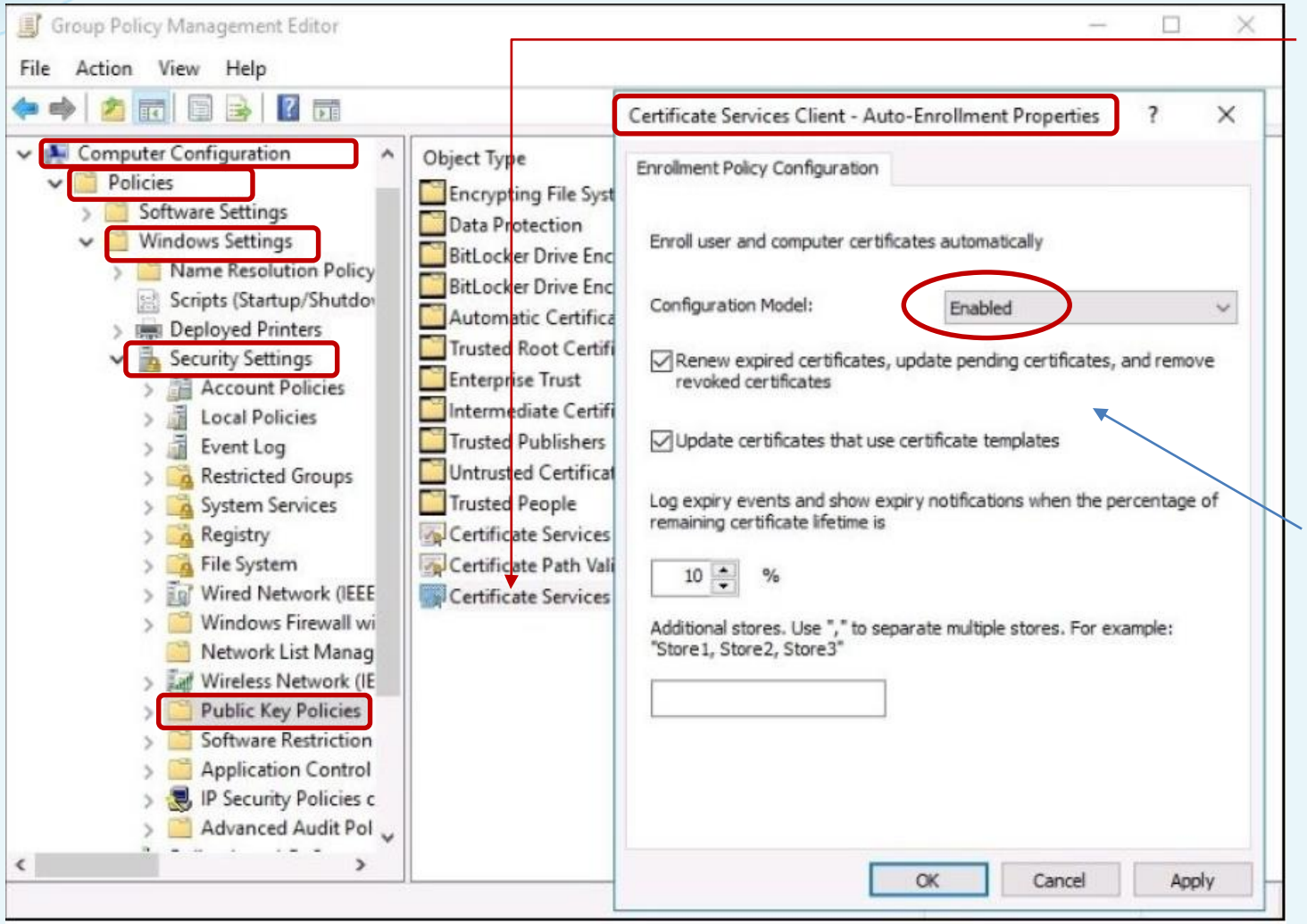
- Requirement: issuing machine certificate to all of the computers in the network
- Uh oh, that sounds like a lot of work
- Group Policy can be utilized to:
  - autoenroll new certificates to all of the machines in the network
  - autorenew at appropriate intervals.

Creating an autoenrollment policy

- Log in to a domain controller server, and open up the Group Policy Management console
- Create a GPO called Enable Certificate Autoenrollment, and editing that GPO to make it do its work



Creating an autoenrollment policy



Double-click on this setting to view its properties

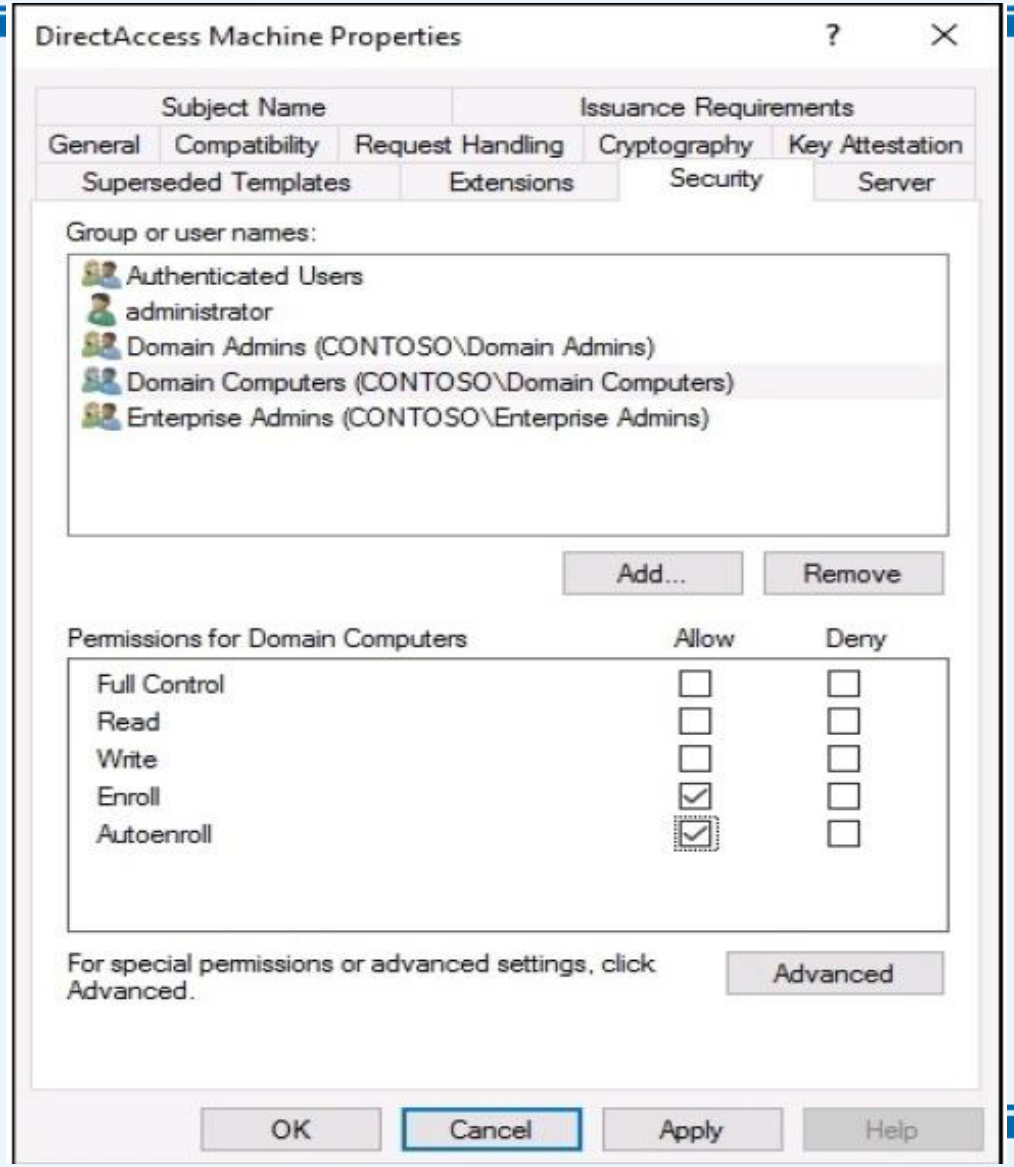
ensure autorenewal happens when the certificates start running into their expiration dates

Creating an autoenrollment policy

- The last thing we need to do on our GPO to make it live: Create a link so that it starts applying!
- Create a specific link to a particular OU that contains machines so that the certificates applied to them
- Autoenrollment has now been enabled on every certificate template published on our CA server.
- Now that the GPO is created and configured to enable autoenrollment, and linked it to an OU, new certificates would be issued. But there are not!!!!

Creating an autoenrollment policy

- We need to adjust the security settings on our new template
- Every certificate template has the **autoenroll** permission identifier, and it is not allowed by default
- Enable the **autoenroll** permission on any template that we want to start distributing itself.



Obtaining a public authority SSL certificate

Obtaining a public authority SSL certificate

- To enable HTTPS to keep the information on the site encrypted: need to install an SSL certificate onto the webservers

  To acquire an SSL certificate from public authority, a three-step process needs to be taken:

  1. Create a certificate request;
  2. Submit the certificate request; and
  3. Install the certificate

Obtaining a public authority SSL certificate

Public/private key pair

- When sending traffic from client to an HTTPS website, the traffic encrypted
- Client uses a key to encrypt the traffic, and the server uses a key to decrypt that traffic
- **Symmetric encryption**:
  - A single key used on both sides
  - Not want it to get into the wrong hands
  - Not generally used for protecting internet website traffic

Obtaining a public authority SSL certificate

Public/private key pair

- **Asymmetric encryption**
  - Utilize two keys: a public key and a private key
  - Public key included inside SSL certificate, and so anyone on the internet can get the public key
  - Client uses public key to encrypt the traffic and sends it over to the webserver
  - Traffic only decrypted by using a corresponding private key, which securely stored on the webserver
  - It is very important to maintain security over your private key and the webservers, ensuring the key doesn’t fall into anyone else’s pocket

Obtaining a public authority SSL certificate

Creating a Certificate Signing Request (CSR)

- Acquired an SSL certificate from public CA entity by logging into their website:
  - Purchasing a certificate
  - And immediately downloading it

  => you've already missed the boat.
- That certificate obviously have no way of knowing about a private key

  => that certificate effectively useless when installed anywhere

Obtaining a public authority SSL certificate

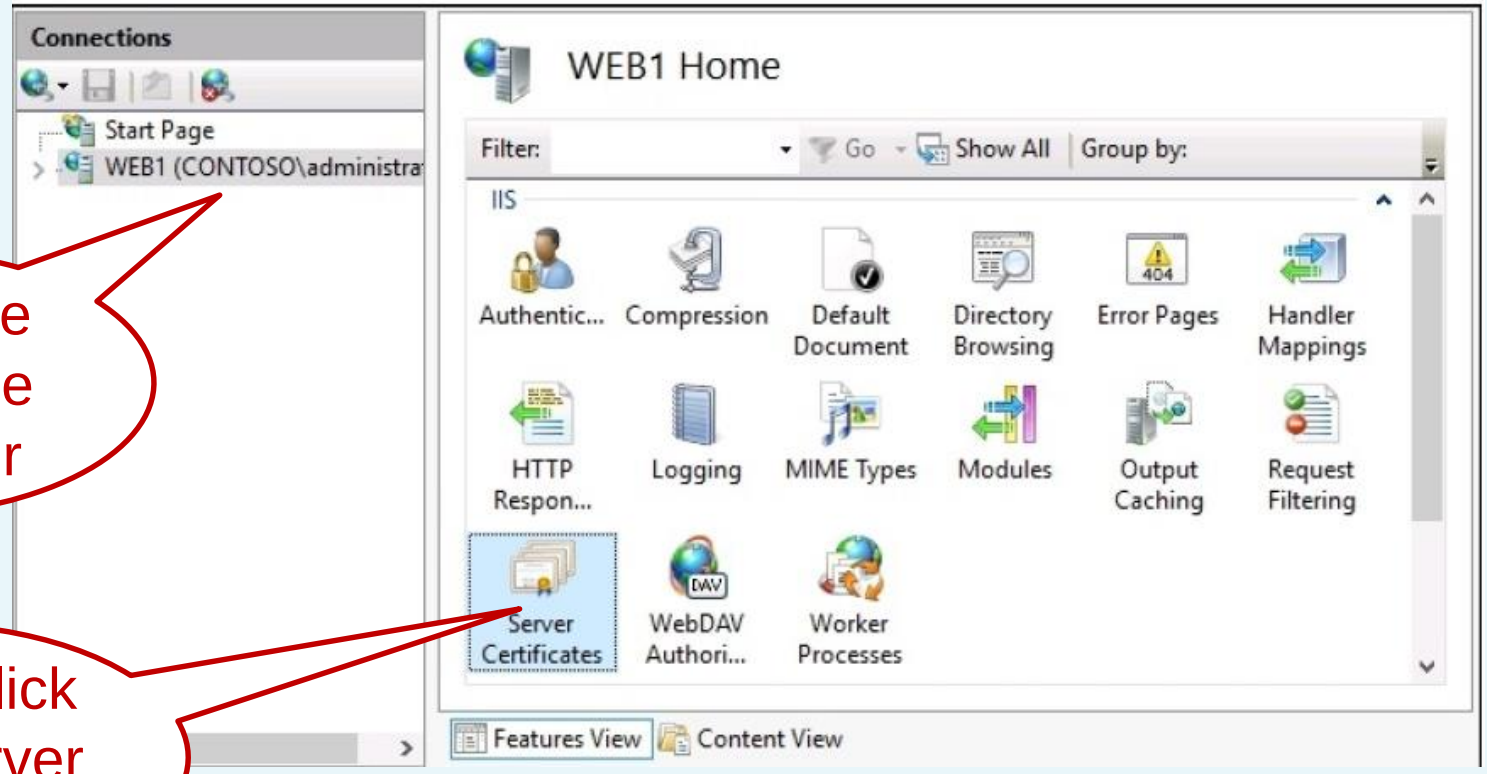
Creating a Certificate Signing Request (CSR)

- SSL certificate onto a web server knows about private key
- Without private key information shared between the server and the cert, SSL certificate good for nothing
- Need to generate a CSR from the local web server to request the certificate from CA
- Webserver platform creates the private key and hides it away on your server
- CSR created in such a way that it knows exactly how to interact with the private key
- Private key not inside the CSR, and your CA vendor never knows it

Obtaining a public authority SSL certificate

Creating a Certificate Signing Request (CSR)

Open up IIS from the **Tools** menu of **Server Manager**



Click on the name of the web server

Double Click on the server Certificates

Obtaining a public authority SSL certificate

Creating a CSR

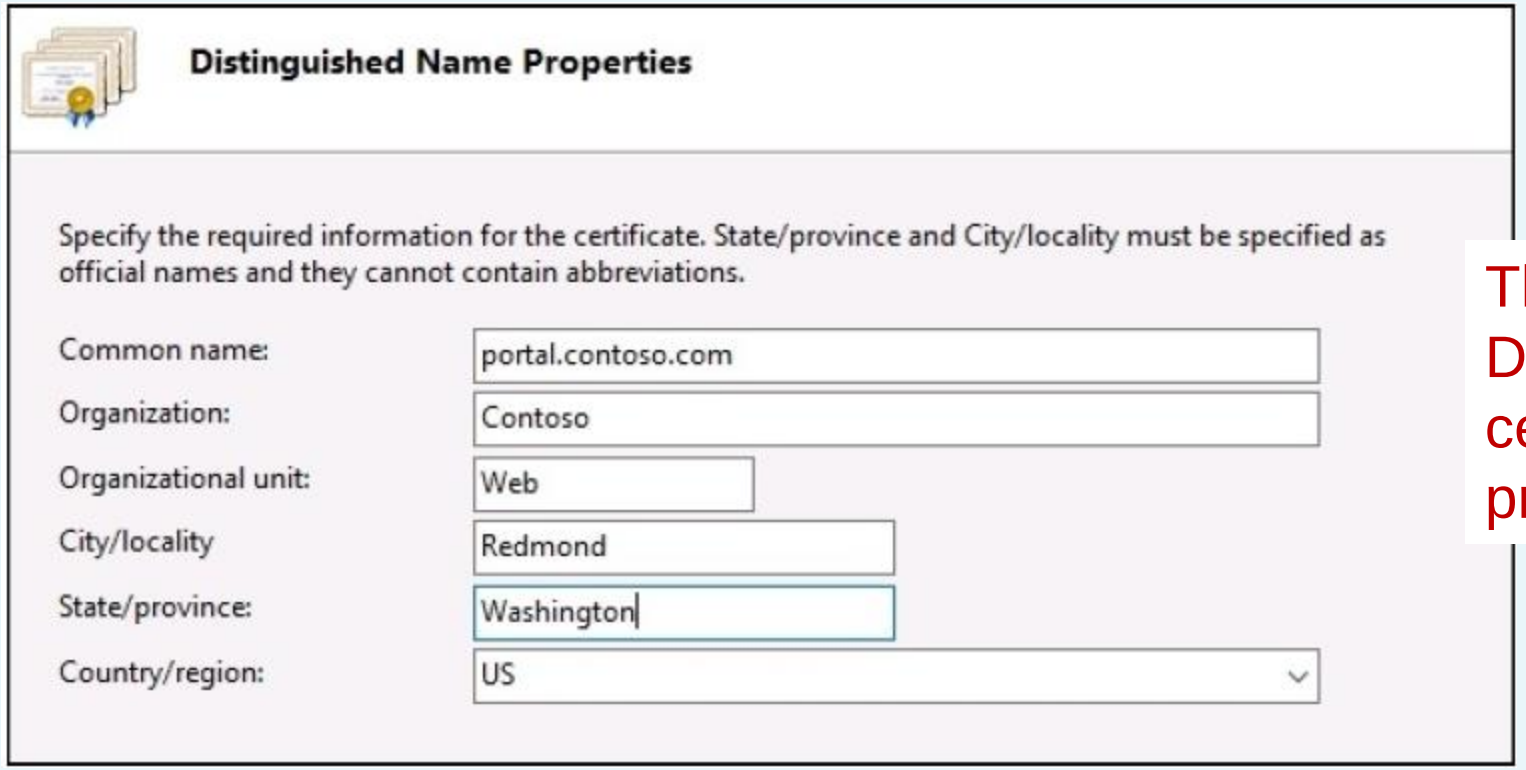
The first step to acquiring our new certificate is creating the certificate request to be used with our CA

Click on Create Certificate Request….

Obtaining a public authority SSL certificate

Creating a CSR

In the resulting wizard, you need to populate the information that will be stored within SSL certificate

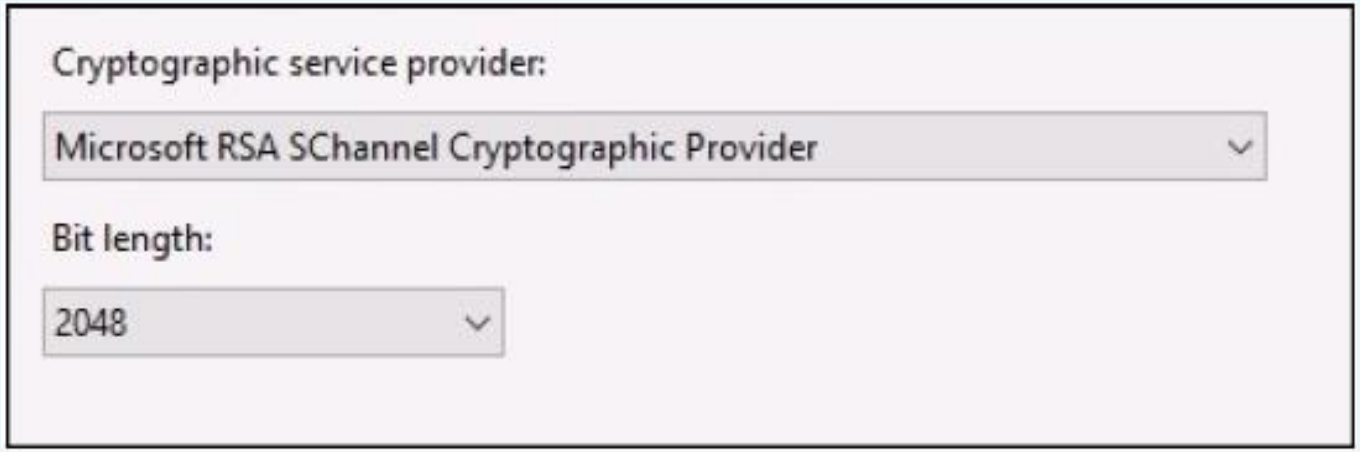


The **Common name:** the DNS name which this certificate is going to protect

Obtaining a public authority SSL certificate

Creating a CSR

- Select suitable Cryptographic service provider
- Bit length: The length of the private encryption key (1024, 2048, 3092,…)



- Saving this CSR as a text file
- Certificate Signing Request (CSR) file created, and we can utilize this file to request the certificate from our public CA

Obtaining a public authority SSL certificate

Submitting the certificate request

- Next step, head on over to the website for your public certification authority
- Once you have an account and log in to the authority's site, you should be able to find an option for purchasing an SSL certificate
- Once you enter the interface for building your new certificate, you will generally be asked for four pieces of information:

1) **Validity period** – How long should this SSL certificate last
2) **Webserver platform** – What type of webserver are you running
3) **Domain ownership validation**: a process to prove that you really own the domain

Obtaining a public authority SSL certificate

Submitting the certificate request

4) The content of CSR file to create new SSL certificate so that it shares private key info with the web server

csr - Notepad

File Edit Format View Help


```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEaDCCA1ACAQAwcTELMAkGA1UEBhMCVVMxEzARBgNVBAgMCldhc2hpbmd0b24x
EDAOBgNVBAcMB1J1ZG1vbmQxEDAOBgNVBAoMB0NvbnRvc28xDDAKBgNVBAsMA1d1
YjEbMBkGA1UEAwwScG9ydGFsLmNvbnRvc28uY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA2OgtBXsiwj1h1AjAdnBPKSHT50vDCY2WbKDiadxpdRDc
D5qSVfNMIuhTWNMSNm06Cy+1MnAc8MpyeS5D4osdG6hetZA96eib2i0S2OM5mLo7
HJBD6TGTBX6OybETTjAB3HdDFu8PbgyESgWLm0fouPjsUNdCQTlrgZ0nlekEK9FE
vHjNryA26zpP05xxBIcLHveSrX+7wwJcaJoyqHQ3TrqqYlHfiEWqCZvkqyCnrRAh
bsCGsJQWCIxjzjhvqvriwipa0DIlx+m+oNcqgixbbLZIm89s02cS61zX2KATgy9Q
H147FzOb5umqM1y7YvtzuXkdaFwqwp3ugCw9el6XRwIDAQABoIIBsDAcBgorBgEE
AYI3DQIDMQ4WDDEwLjAuMTA1ODYuMjBKBgkrBgEEAYI3FRQxPTA7AgEFDBJXRUIx
LkNvbnRvc28ubG9jYWwMFUNPTlRPU09cYWRtaW5pc3RyYXRvcgwLSW5ldE1nci51
eGUwcgYKKwYBBAGCNw0CAjFkMGICAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIA
UwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkA
YwAgAFAAcgBvAHYAaQBkAGUAcgMBADCBzwYJKoZIhvcNAQkOMYHBMIG+MA4GA1Ud
```


Typically, all you need to do is copy the entire contents of the CSR file and paste them into the CA's website.

Obtaining a public authority SSL certificate

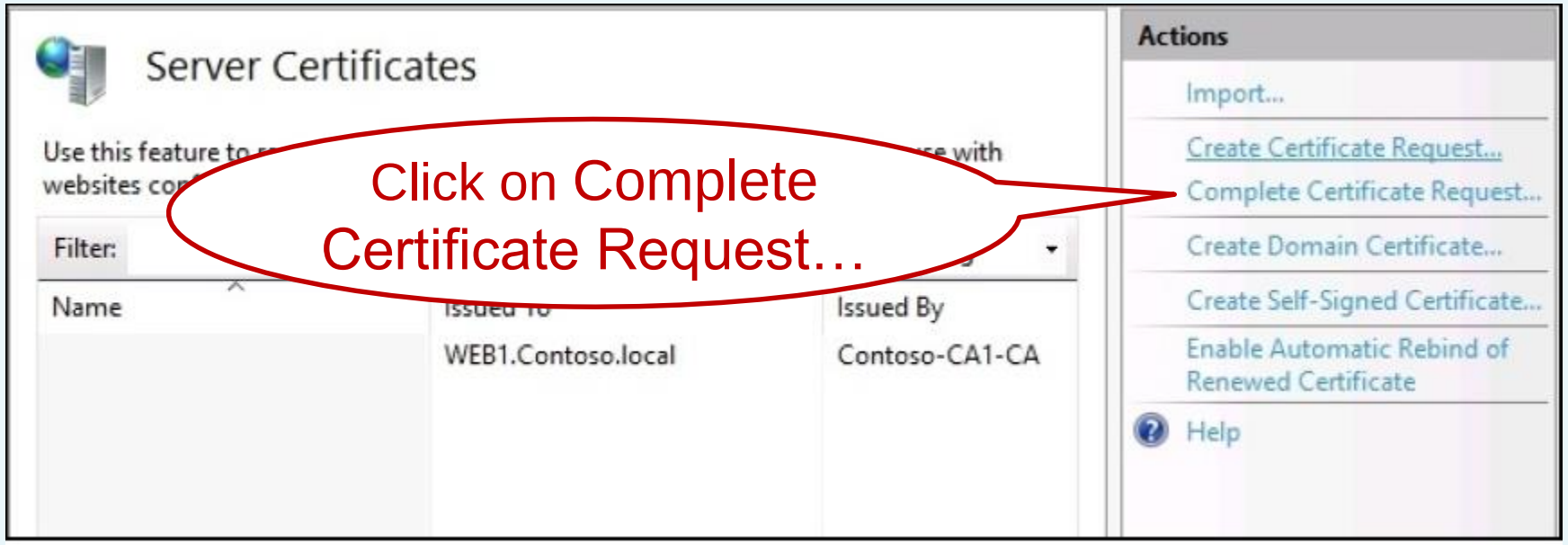
Downloading and installing your certificate

- After requesting, the certificate might be available for download almost immediately, or it could take a few hours
- Once you are able to download the certificate from the CA website, go ahead and copy it over to the web server from which we generated the CSR
- It is critical that you install this new certificate onto the same server.

Obtaining a public authority SSL certificate

Downloading and installing your certificate

Back inside the IIS management console



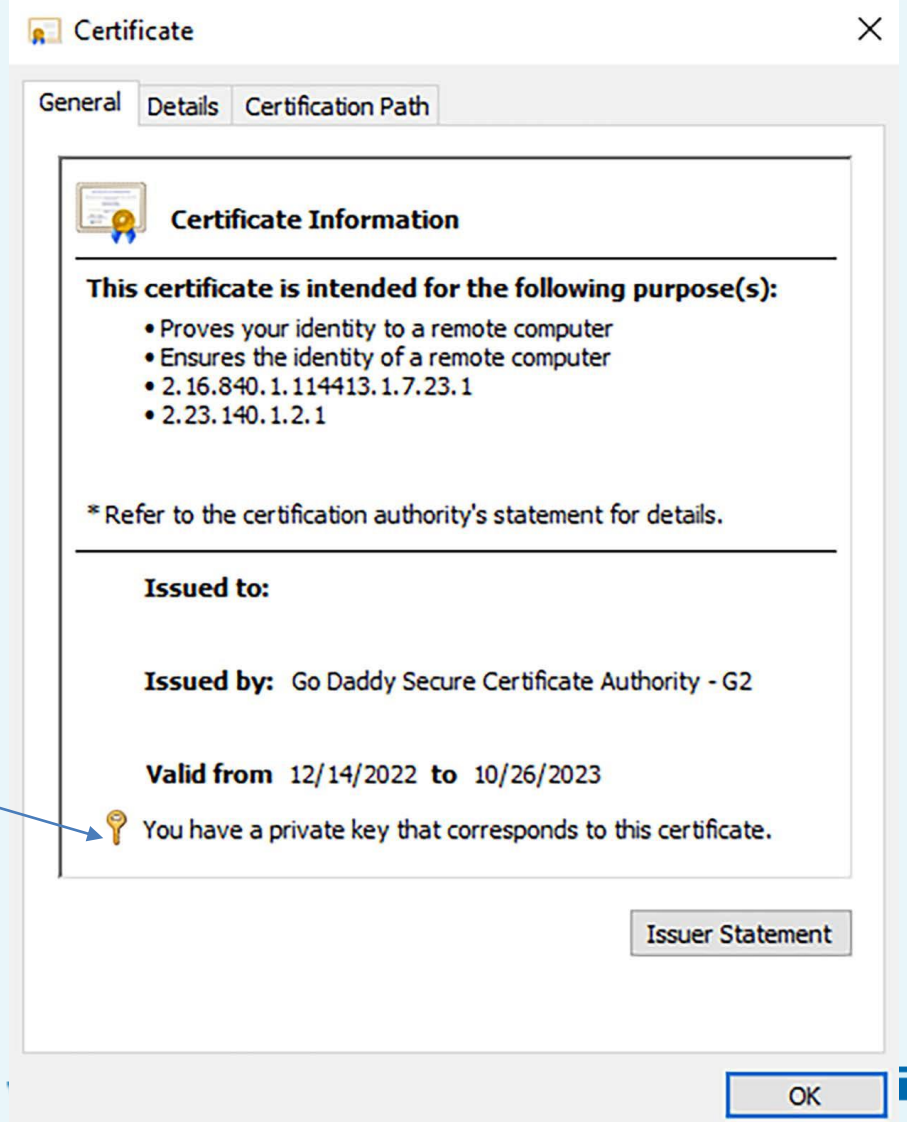
Find the new certificate file that you just downloaded, and import it into our server

Obtaining a public authority SSL certificate

Downloading and installing your certificate

- The new certificate now listed inside IIS, and if double-click on new certificate you will see the properties page for the cert.

The key icon and the text indicates that SSL certificate works properly to protect the website.



Exporting and importing certificates

Exporting and importing certificates

- In some cases, we need to use the same SSL certificate on multiple servers. For example:
  - More than one IIS server serving up the same website
  - Using some form of load balancing
  - Wildcard certificates
- When need for reusing the same SSL certificate on multiple servers, you can simply export it from one and import it on the next.
- Two common places to do this: MMC snap-in for **Certificates**, or from within IIS itself

Exporting and importing certificates

Exporting from MMC

- Launch **Certification Authority** (Server Manager -> tool)
- Click on **Local Computer** certificate store in the MMC, navigate to **Personal** | **Certificates** to show a list of SSL certificates.
- Right-click on the certificate, and then navigate to **All Tasks** | **Export**….
- The first choice you have to make is whether or not to export the private key

Exporting and importing certificates

Exporting from MMC

- If you export without the private key, that certificate will not work on another server.

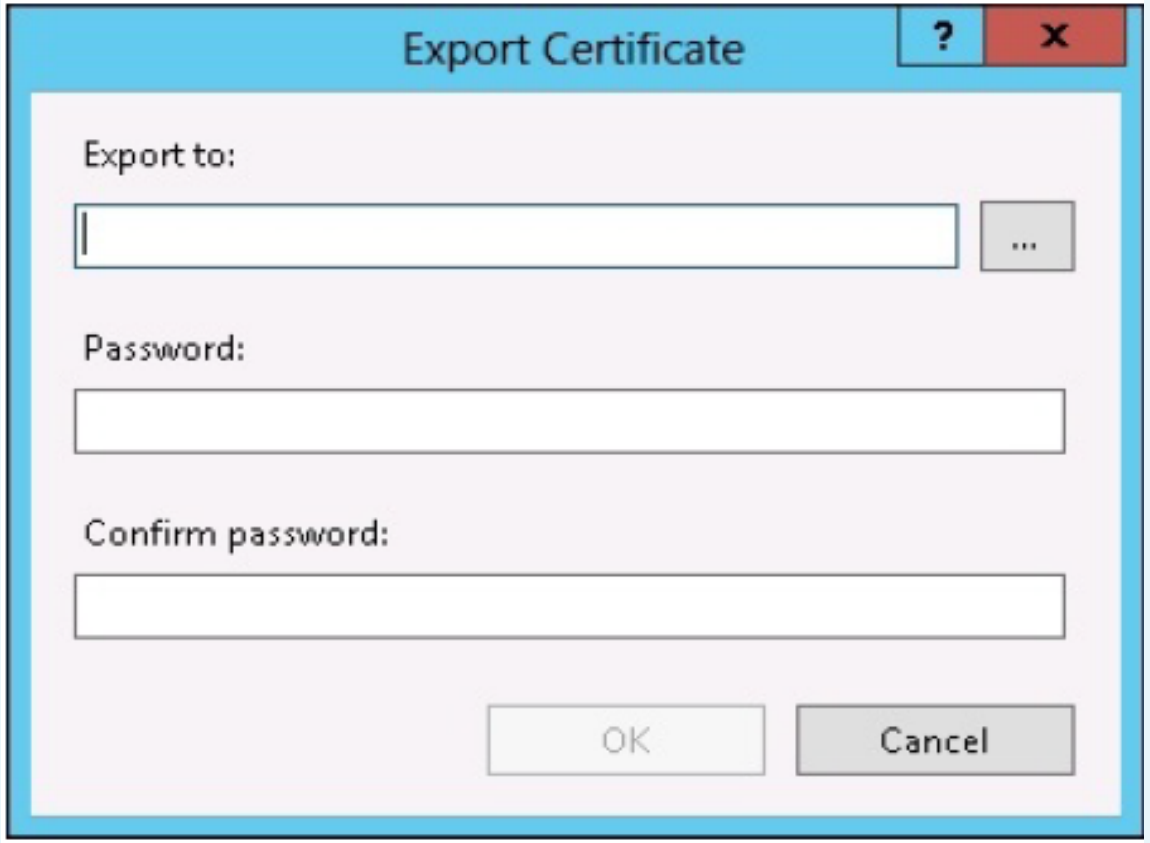
- Select this option to export for validating SSL traffic on second web server

- You are required to supply a password which will be used to protect the exported PFX file

Exporting and importing certificates

Exporting from IIS

- Inside the **Server Certificates** applet for IIS, right-click on the certificate and choose **Export**….
- This launches a single-page wizard that simply asks you for a **location** and **password**
- The private key will be included with the certificate export automatically



Exporting and importing certificates

Importing onto a second server

- From within either console, MMC or IIS, right-click and choose the **Import** action
- Choose the PFX file and then input the password that you used to protect the file.

OpenSSL for Linux webservers

OpenSSL for Linux webservers

- The types of files used for certificates in Linux webservers is difference
- Certificate files for IIS usually CER or CRT
- On most Linux webservers, the certificate file and the private key are each individual files visible right on the server
- Both of these files generally have the PEM file extension
- Three-step process for acquiring and installing a certificate exactly the same
  - Generate a CSR
  - Use the CSR to get a certificate from your CA
  - And install the certificate to your webserver

OpenSSL for Linux webservers

Generate a CSR

- A Certificate Signing Request (CSR): a cryptographic file generated on the server where you plan to install a certificate
- The CSR contains information (such as the common name, organization, country, etc.) that the CA uses to create the certificate
- It also contains the public key that will be included in the certificate, and it is signed with the corresponding private key.

1. Install OpenSSL
2. Log Into Server

OpenSSL for Linux webservers

Generate a CSR

3. Create RSA Private Key and CSR

openssl req -new -newkey rsa:2048 -nodes -keyout [your_domain].key -out your_domain.csr

Replace [your_domain] with the actual domain for which you are generating a CSR.

OpenSSL for Linux webservers

Generate a CSR

4. Enter CSR Information: The system launch a text-based questionnaire. Enter your information in the fields as follows:

- Country Name - a 2-letter country code (US for the United States).
- State - the state in which the domain owner is incorporated.
- Locality - the city in which the domain owner is incorporated.
- Organization name - the legal entity that owns the domain.
- Organizational unit name - the name of the department or group in your organization that deals with certificates.
- Common name - typically, the fully qualified domain name (FQDN), which users type in a web browser to navigate to your website

OpenSSL for Linux webservers

Generate a CSR

4. Enter CSR Information (cont)

- Email address - the webmaster's email address.
- Challenge password - an optional password for your key pair.
- Please take into account that Organization Name and Unit Name must not contain the following characters: < > ~ ! @ # $ % ^ * / \ ( ) ? . , &

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Arizona
Locality Name (eg, city) []:Phoenix
Organization Name (eg, company) [Internet Widgits Pty Ltd]:phoenixNAP
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:phoenixnap.com
Email Address []:example@phoenixnap.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

OpenSSL for Linux webservers

Generate a CSR

5. Locate Certificate Signing Request File

```
bosko@pnap:~$ ls *.csr
phoenixnap.com.csr
```

6. Verify CSR Information

If any information is incorrect, create a new CSR file and fix the errors.

```
bosko@pnap:~$ openssl req -text -in phoenixnap.com.csr -noout -verify
Certificate request self-signature verify OK
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = US, ST = Arizona, L = Phoenix, O = phoenixNAP, CN = phoenix
nap.com, emailAddress = example@phoenixnap.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a0:37:73:bc:a8:48:68:ee:56:70:5e:43:2e:af:
                    e7:45:2d:d3:75:0e:fe:41:3e:96:50:55:03:84:9b:
                    85:09:c7:6c:c1:52:3f:dc:73:23:2b:c7:c2:0d:d6:
```

OpenSSL for Linux webservers

Acquire the certificate

- Now that you have a CSR file, follow through the same series of steps previously discussed to:
  - Submit your CSR to a CA
  - validate yourself as the owner of the domain
  - And download the resulting certificate file
- Use the following syntax to open the file in nano:
  - sudo nano [file_name].csr
  - Copy and paste the text into a submittal form to request your SSL certificate

```
  GNU nano 6.2                    phoenixnap.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICzDCCAbQCAQAwgYYxCzAJBgNVBAYTAlVTMRAwDgYDVQQIDAdBcml6b25hMRAw
DgYDVQQHDAdQaG9lbml4MRMwEQYDVQQKDApwaG9lbml4TkFQMRcwFQYDVQQDDA5w
aG9lbml4bmFwLmNvbTElMCMGCSqGSIb3DQEJARYWZXhhbXBsZUBwaG9lbml4bmFw
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKA3c7yoSGjuVnBe
Qy6v50Ut03UO/kE+llBVA4SbhQnHbMFSP9xzIyvHwg3WgEAik1mZiBRB4zBmir8e
nD9hd3Bj3yk5OB2EnmbnH7pl2HPZaf17WUztl3nwu5GN0pJrEvBEF/11L11SaLuR
Hb9XTb/SXa8aCq3u/DoJRpXJDzzT3OTpf8zc4SUWEZXS/D5L/Wyp6tJrsPQBdMiA
PQFyTWgLI9XOOCjqRaysbTCeVg5I9SymYPGv0wCCLhjjbpGZrdcCeMiD+XrB7e4T
2ZeOY5St0RqBwLbpyrEkmNMsCWv6uT4wCnvmfG/FEAVwfElje7UZUL7RI8dBzbwp
viJ8D2MCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQB7hbwbBbJjgfP8r763MhRr
XD/UbpxN2smPinJTrkJcFEhVVCef6kA2WqS/MwMljZeAmmfb7ItB0l1qcBCT7R0q
TDVHGcFknKnlNCGYmeuvJ7mRrMRZWqj6TbCVSOQRLpUNxlwiuV/x0F/VpriLY9lb
Wc1qR7/QijYyfzFPtOccEkXcugfxqKQFO6iHkfy9uty1earAnQwPQ0eHcr9zaw6j
9OkwDtaGLuyzKNUNgX82yunrRcOBF5dpgcXEtf4kIcfdxR0qKAiBSEEhl6/7Y5oq
28fOPYPHpfpIeXYVd/YwhENNdUS97mtexmph/FuPOq+s+/BgQ+DYKvQ3ngAmC6+Q
-----END CERTIFICATE REQUEST-----
```

OpenSSL for Linux webservers

Install the certificate

- First of all, install the certificate onto the same IIS server (or workstation) from which you generated the CSR file
- This is critically important so that your new certificate successfully pairs up with the private key created when created CSR
- Once the new certificate installed and validated that it looks good, you can now export this certificate (including the private key) to a PFX file
- Newly created PFX file contains both the certificate and the private key.
- The only remaining step is to convert this PFX file into two separate PEM files: the SSL certificate and the private key.

OpenSSL for Linux webservers

Install the certificate

- Download and install OpenSSL
- Put your PFX file in a location that we will reference in our commands. E.g., C:\Cert\Export.pfx
- Open Command Prompt and navigate to the folder where OpenSSL installed. E.g., cd C:\Program Files\OpenSSL-Win64\bin
- Run the following two commands

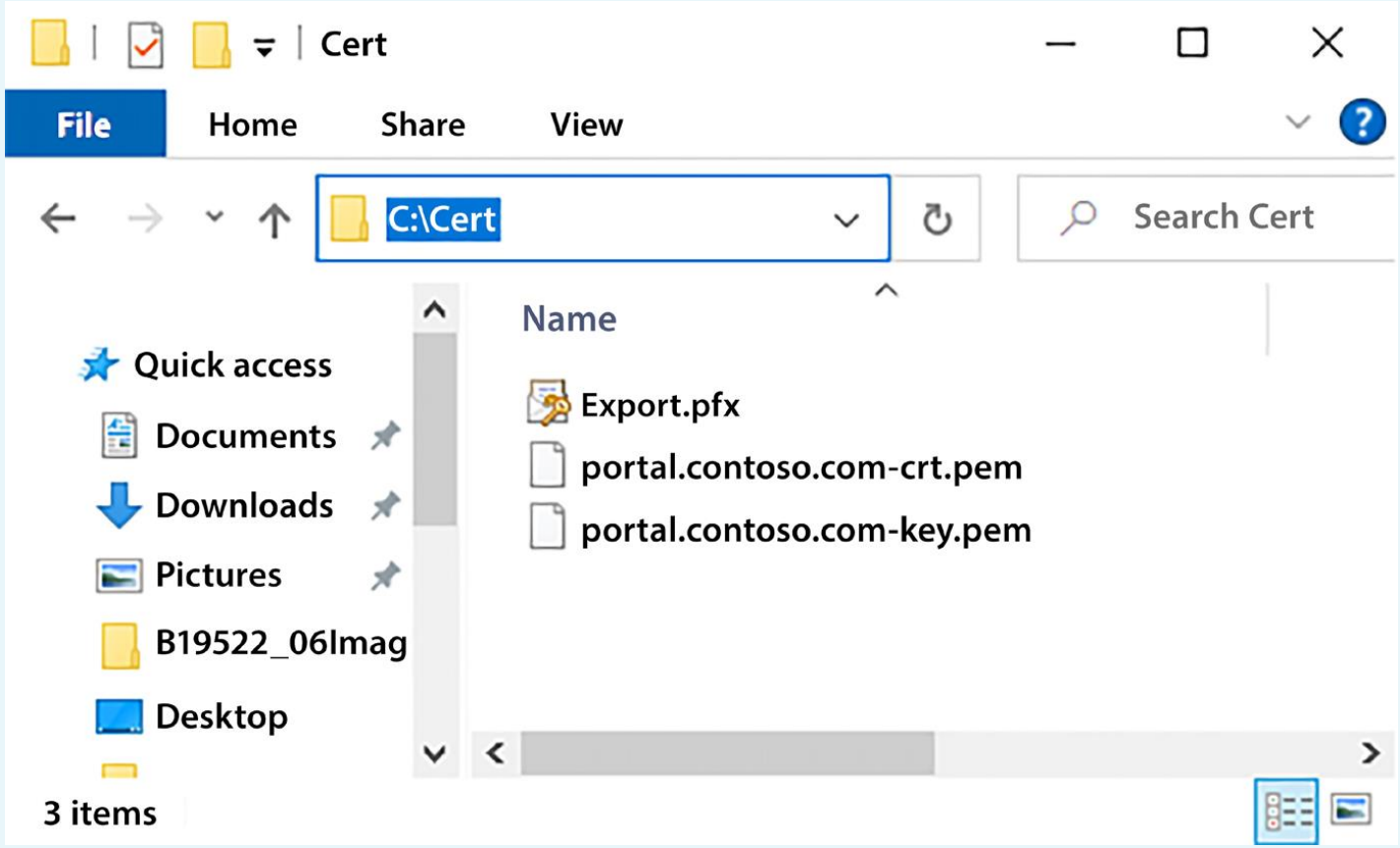
```
openssl pkcs12 -in c:\cert\export.pfx -nokeys -out c:\cert\portal.
contoso.com-crt.pem -nodes

openssl pkcs12 -in c:\cert\export.pfx -nocerts -out c:\cert\portal.
contoso.com-key.pem -nodes
```

OpenSSL for Linux webservers

Install the certificate

- Two new files inside your C:\Cert
- Copy these two files to a particular folder on your Linux webserver to specify the SSL certificate that is going to be used by the site



Summary

- Certificates often get a bad reputation because people think they are a headache to deal with
- The most common certificate related tasks that any server admin will eventually have to tackle within their own networks
- It is clear that building the certificate infrastructure or obtaining and installing certificates on servers is not a big deal