



Implementing SSL for Active Directory LDAP Communication

Author: Renato Pioker

April, 15<sup>th</sup> 2015

# SUMMARY

## Contents

Setting up Active Directory SSL Communication .....	3
Section I – Requesting a Certificate for the Domain Controller .....	4
Section II – Install the Certificate on the Domain Controller .....	9
Section III – Use the Microsoft Certificate Services to Generate a Self-Signed Certificate .....	17

# Setting up Active Directory SSL Communication

The goal of this guide is to enable LDAP communication with AD using a secure and encrypted connection. This configuration is required to allow some CA components to communicate properly with AD, such as CA IDM connector to provide the provisioning operations in AD, and to allow the secure communication between AD and LDAP clients, such as JXplorer and CA SiteMinder Administrative User Interface – as well as other Java LDAP clients.

This guide has three sections:

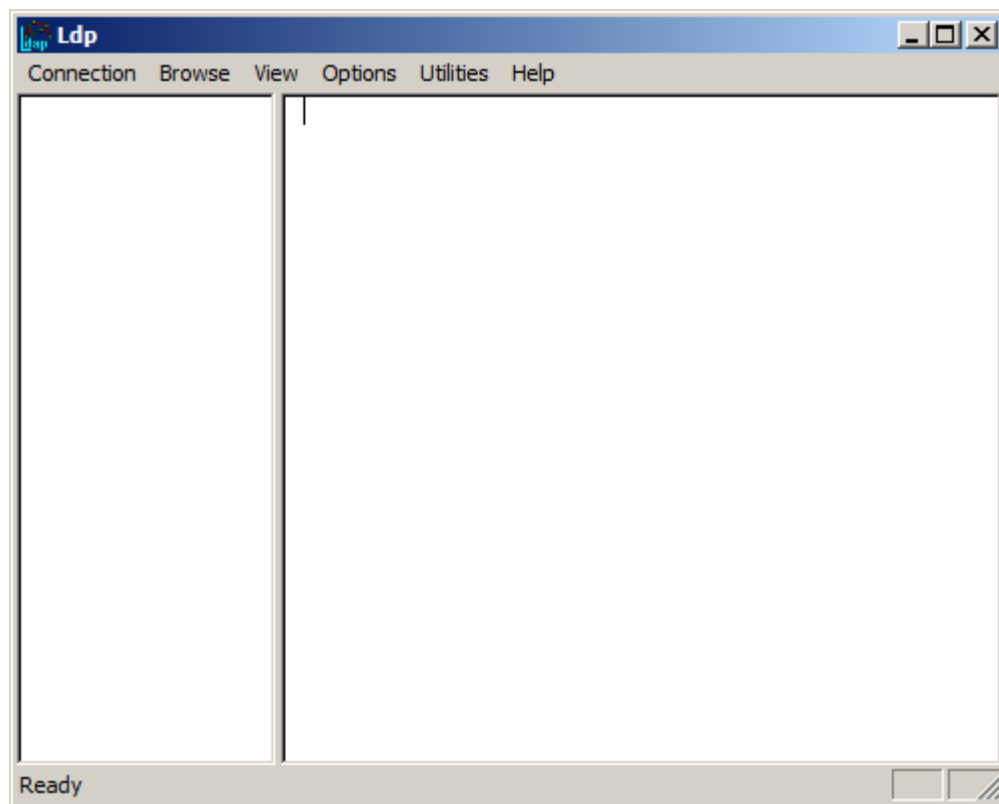
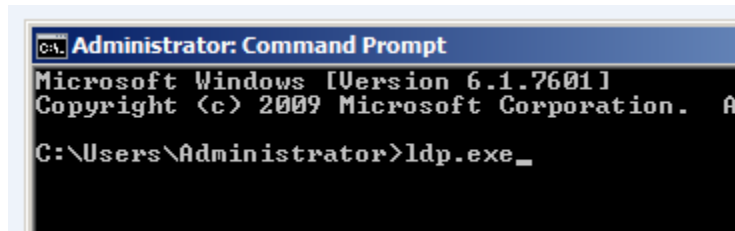
- Section I – Requesting a Certificate for the Domain Controller
- Section II – Install the Certificate on the Domain Controller
- Section III – Use the Microsoft Certificate Services to Generate a Self-Signed Certificate

## Section I – Requesting a Certificate for the Domain Controller

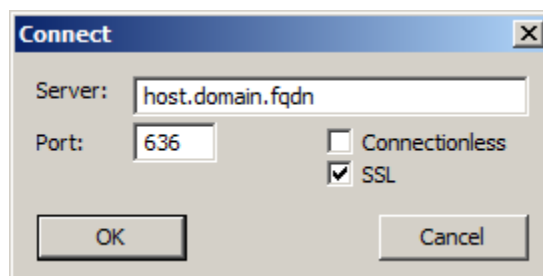
To request a certificate for your domain controller, please follow the steps below:

- 1) Confirm that the SSL communication for AD is not already set:

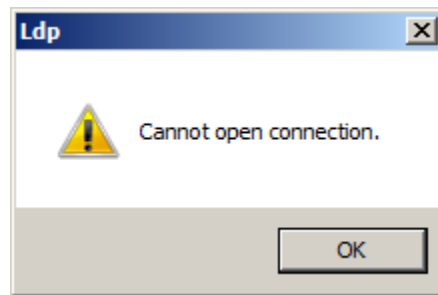
Run the LDP.EXE utility (native from Windows):



At this point, click on the Connection menu and, after, click on Connect. The following window appears:

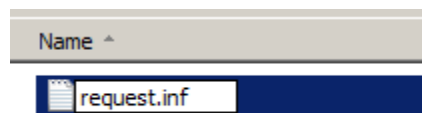
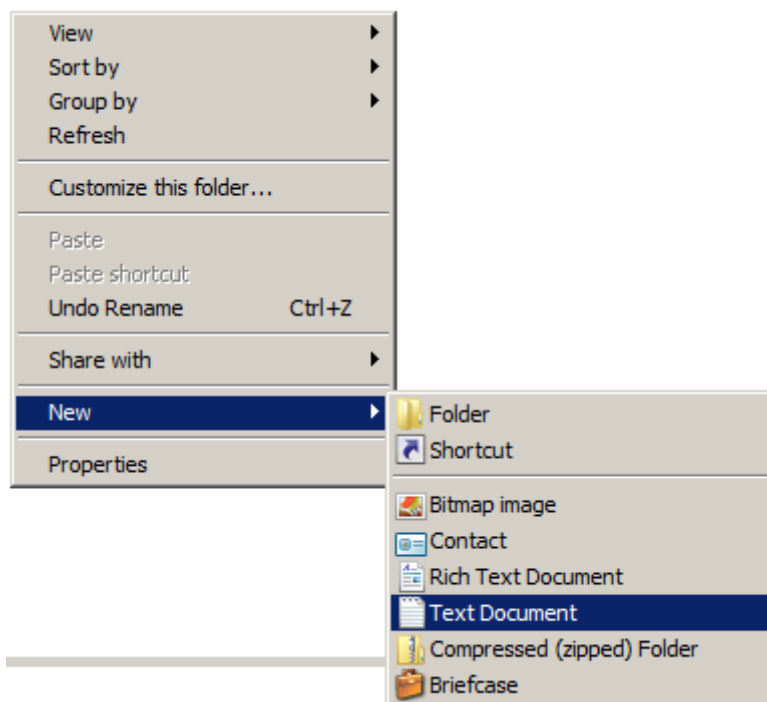


Type the Fully Qualified Domain Name (FQDN) of the domain controller, the communication port (default is 636 for LDAP over SSL) and check the SSL option. Click OK. The LDP utility should return the following error message (if AD is not configured for SSL yet):



2) Create a certificate request:

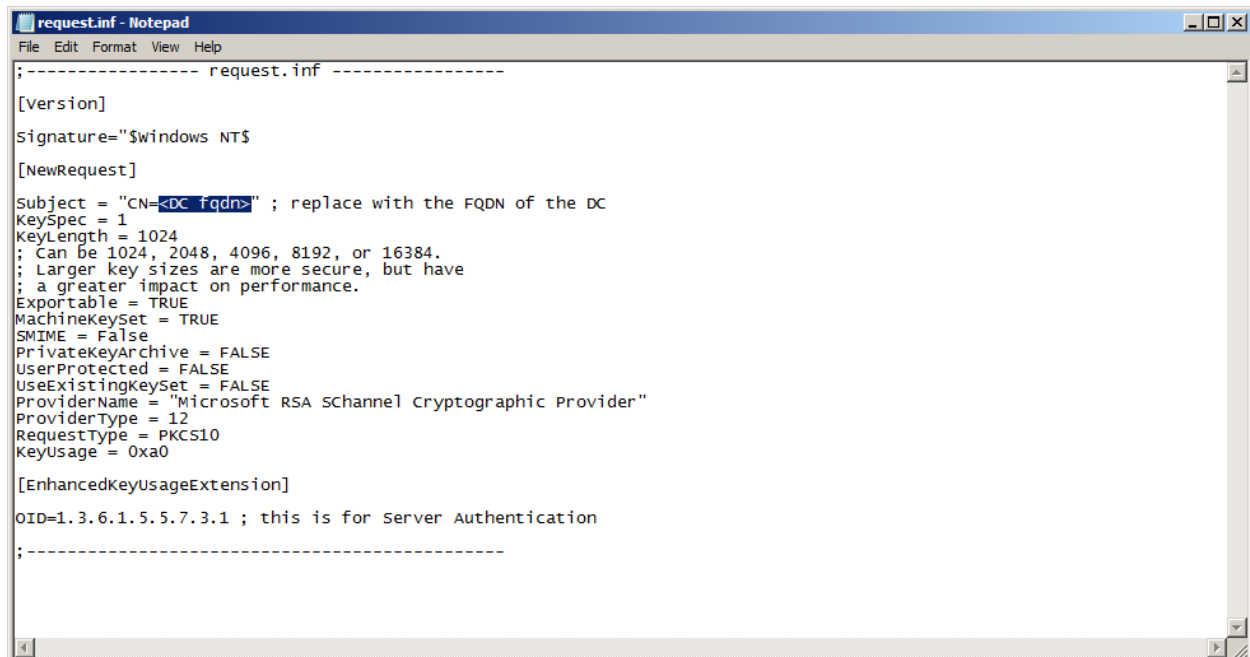
Log in to the domain controller (locally or via Remote Desktop) using a user with administrative rights. After, in a directory that is easy to navigate to via command line, create a file named **request.inf**:



Open the file **request.inf** in notepad and insert the following content:

```
;----- request.inf -----  
  
[Version]  
  
Signature="$Windows NT$  
  
[NewRequest]  
  
Subject = "CN=<DC fqdn>" ; replace with the FQDN of the DC  
KeySpec = 1  
KeyLength = 1024  
; Can be 1024, 2048, 4096, 8192, or 16384.  
; Larger key sizes are more secure, but have  
; a greater impact on performance.  
Exportable = TRUE  
MachineKeySet = TRUE  
SMIME = False  
PrivateKeyArchive = FALSE  
UserProtected = FALSE  
UseExistingKeySet = FALSE  
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"  
ProviderType = 12  
RequestType = PKCS10  
KeyUsage = 0xa0  
  
[EnhancedKeyUsageExtension]  
  
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication  
  
;-----
```

The only parameter that must be changed is "Subject", that must be changed to the domain controller FQDN, as on the following screens:



```
request.inf - Notepad
File Edit Format View Help

;----- request.inf -----
[Version]
Signature="$windows NT$"
[NewRequest]
Subject = "CN=host.domain.fqdn" ; replace with the FQDN of the DC
KeySpec = 1
KeyLength = 1024
; Can be 1024, 2048, 4096, 8192, or 16384.
; Larger key sizes are more secure, but have
; a greater impact on performance.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA Schannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
;-----
```

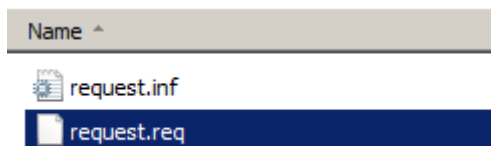
Save and close the file. Now open a command prompt window. To generate the certificate request for the domain controller, navigate to the Directory where you created the request.inf, then execute the command **certreq -new request.inf request.req**

```
Administrator: Command Prompt
C:\Users\Administrator>e:
E:\>cd certificados
E:\certificados>dir
Volume in drive E has no label.
Volume Serial Number is D262-74F8

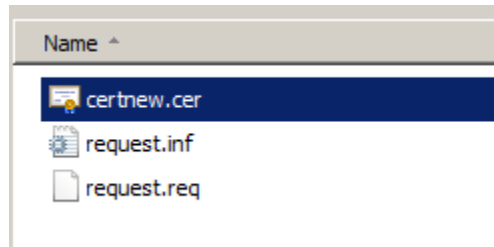
Directory of E:\certificados
10-Apr-15  10:55 AM    <DIR>          .
10-Apr-15  10:55 AM    <DIR>          ..
10-Apr-15  10:57 AM                732 request.inf
               1 File(s)                732 bytes
               2 Dir(s)  64,573,440,000 bytes free

E:\certificados>certreq -new request.inf request.req
```

Press ENTER. A new file will be generated on the same Directory of the file request.inf:



The contents of this new file is the certificate request. Send it to the certification authority, so the new certificate can be generated. Request the certificate using the **Web Server** template and in **Base64**. The certification authority will deliver a file with the .CER extension:



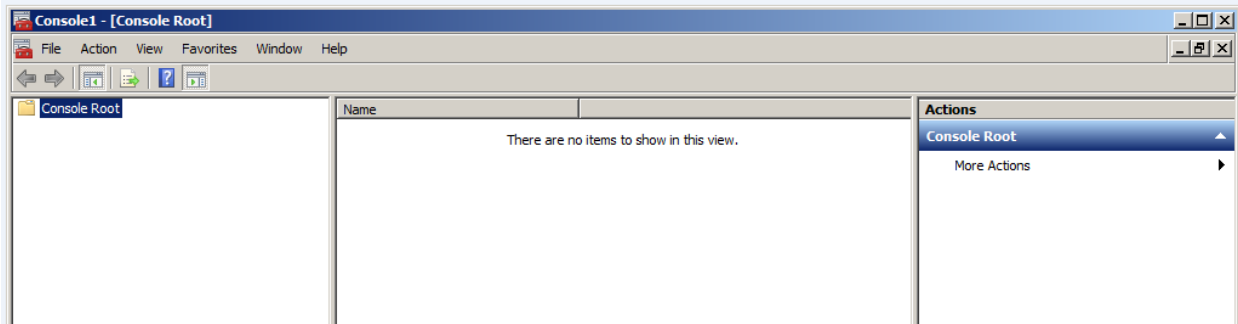
This **certnew.cer** file is the certificate that must be installed in the domain controller. This procedure is covered in the next section.



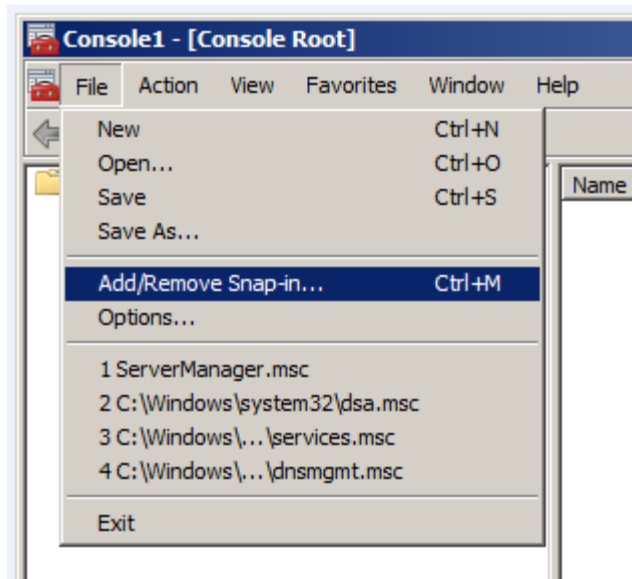
## Section II – Install the Certificate on the Domain Controller

The certificate installation for Active Directory to function in LDAP-S mode is not just a certificate import. It has to be done in a specific way, to enable the Active Directory Domain Services to use the certificate properly. Please follow the steps below:

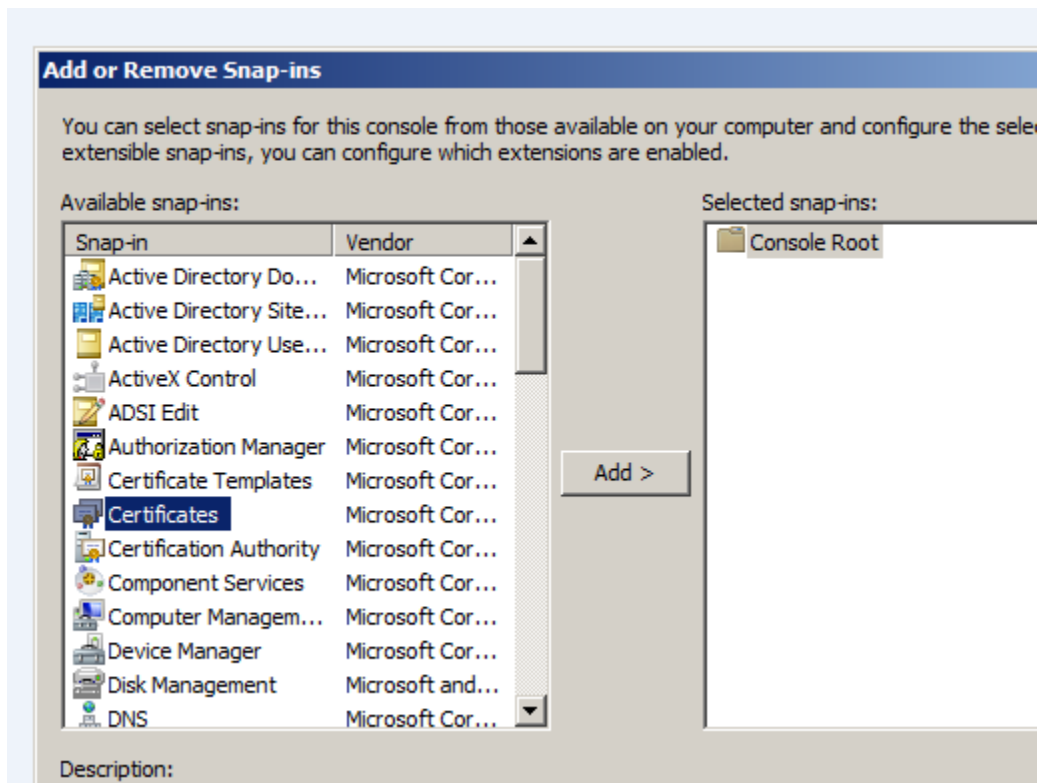
- 1) Open a new MMC (Microsoft Management Console) by clicking on Start / Run / type MMC / click Ok. The following window appears:



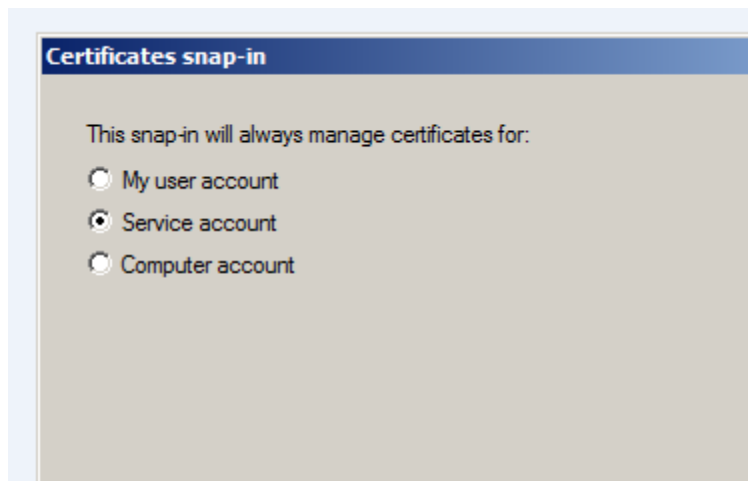
- 2) Click on File menu and then in Add/Remove Snap-in:



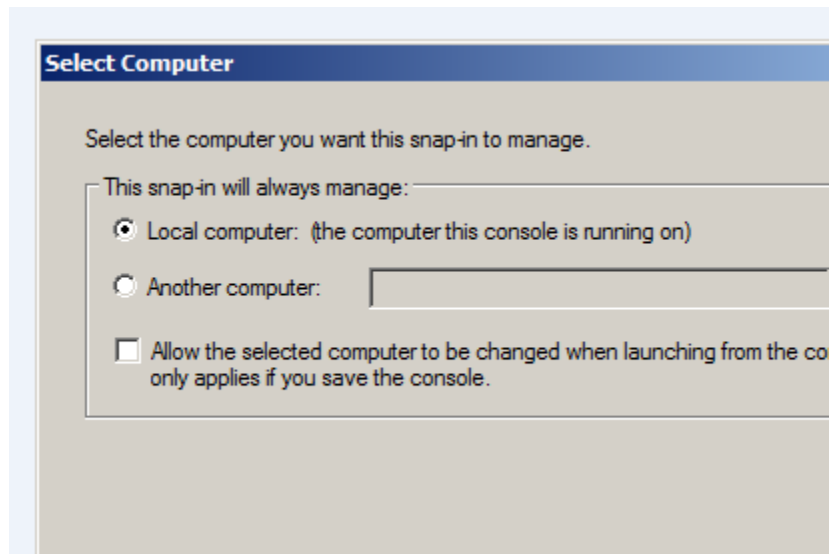
- 3) Select the Certificates snap-in at the left column, and click Add. This will trigger a wizard screen:



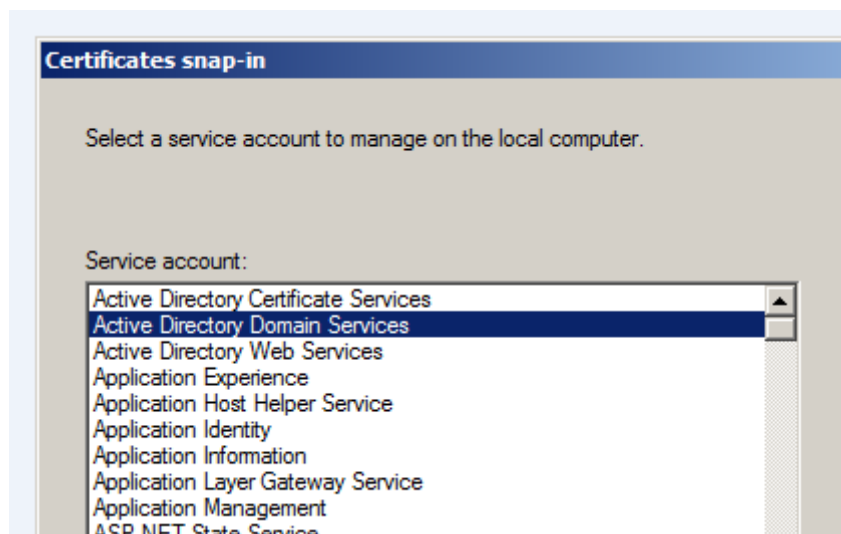
- 4) On the first screen, select Service account and click Next:



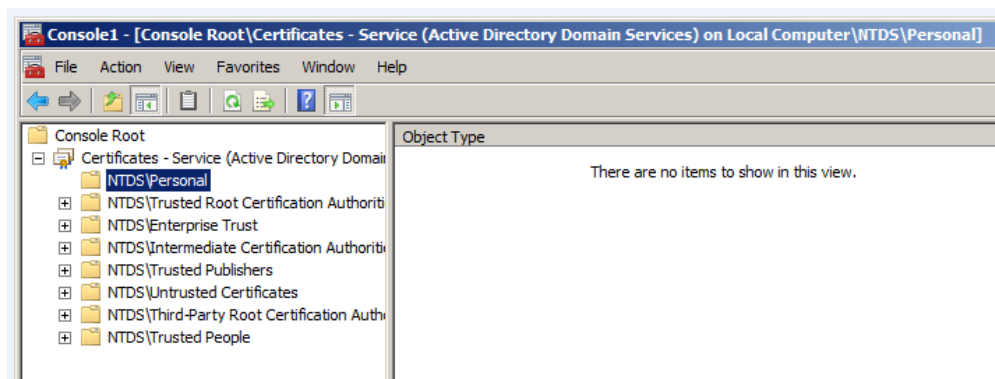
- 5) Select Local computer, and click Next:



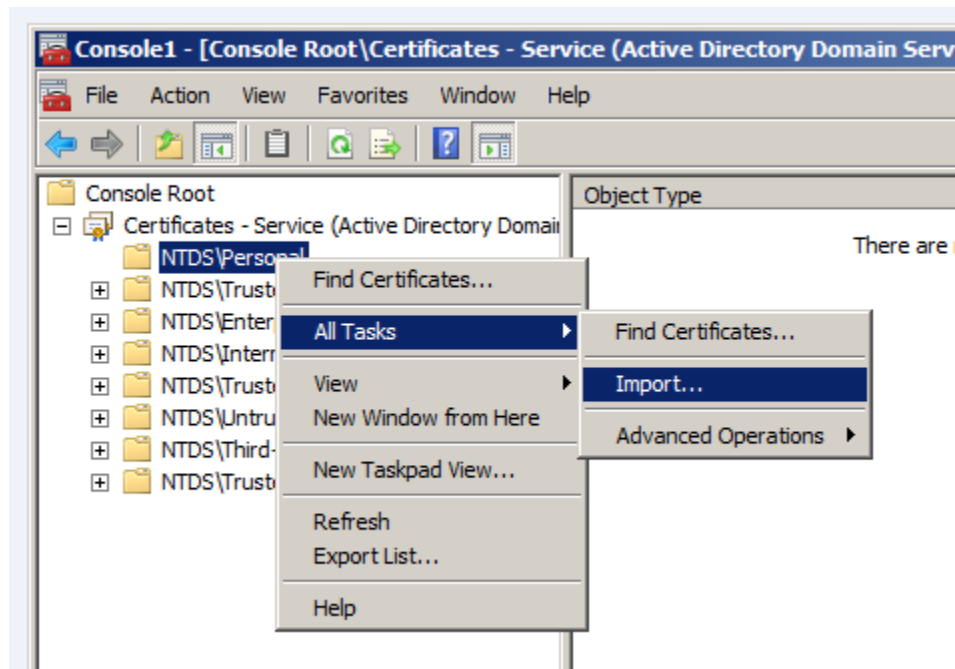
- 6) Select the Active Directory Domain Services option, and click Finish:



- 7) Click OK to close the Add or Remove Snap-ins screen;  
8) Expand the NTDS\Personal folder. It will be empty:

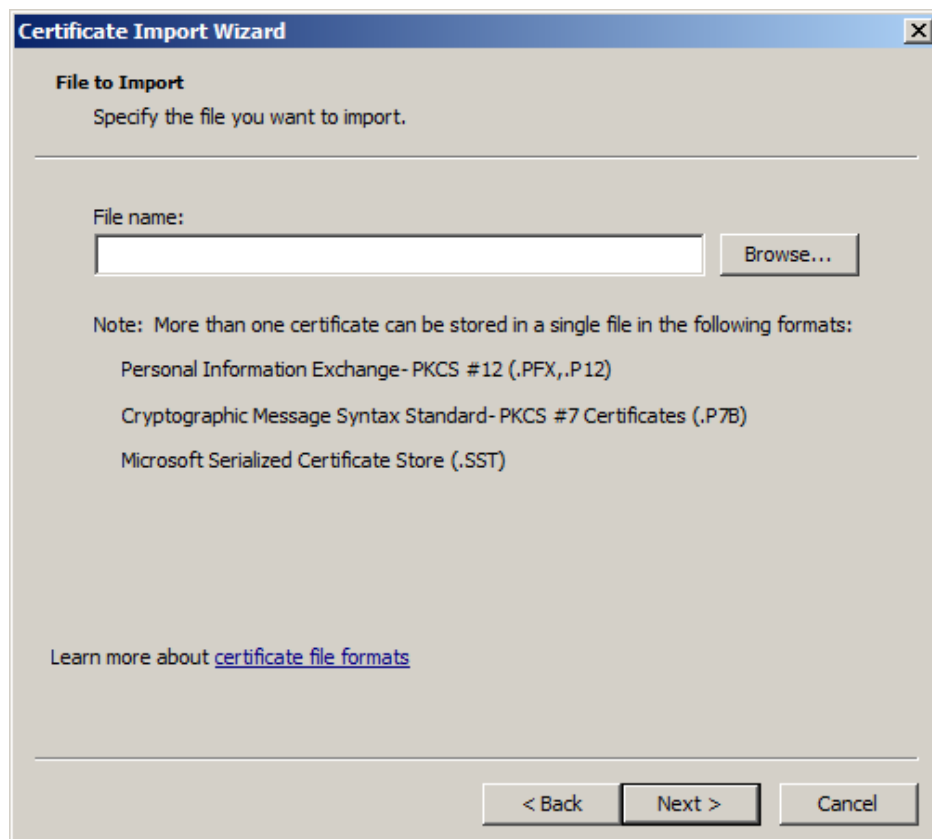


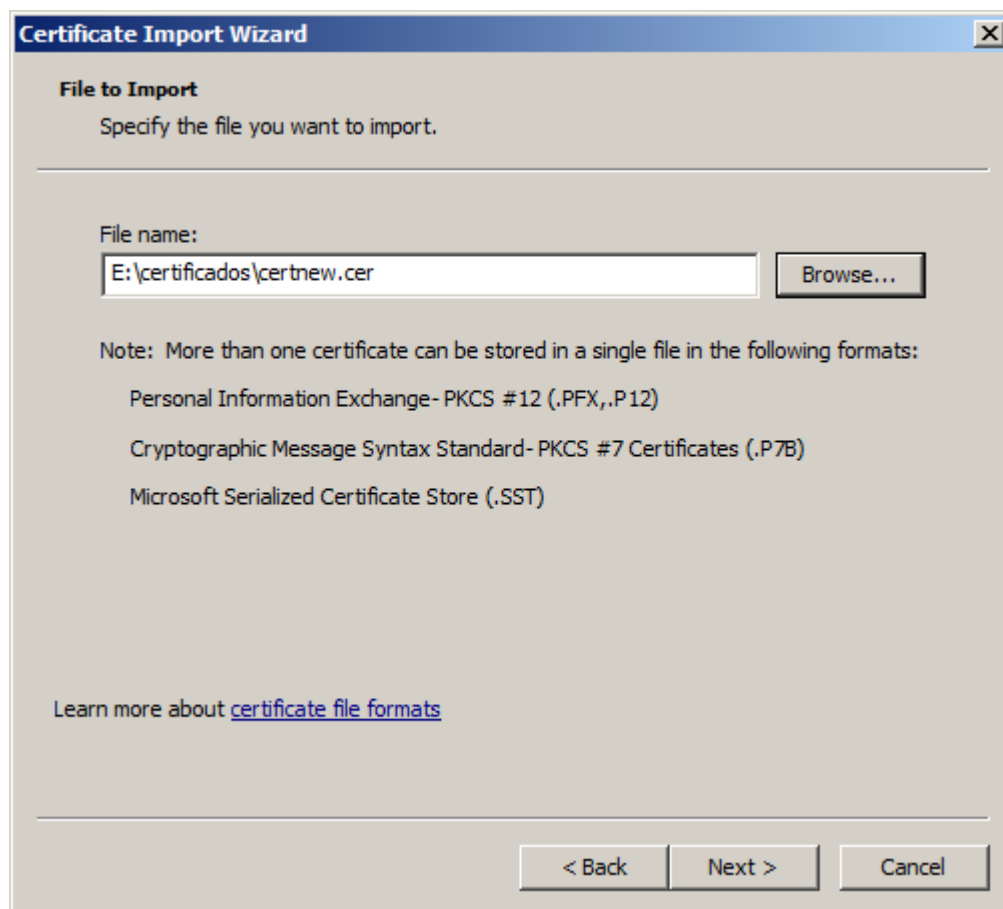
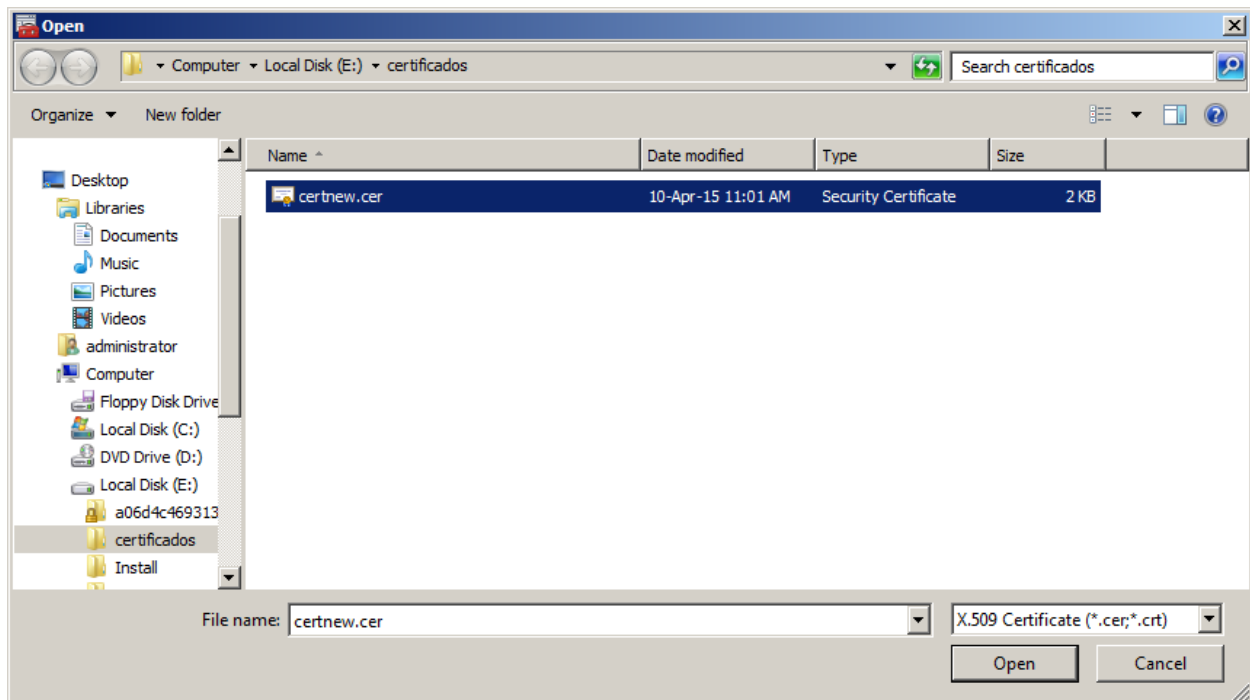
- 9) Right-click the NTDS\Personal folder, point to All Tasks and click Import:



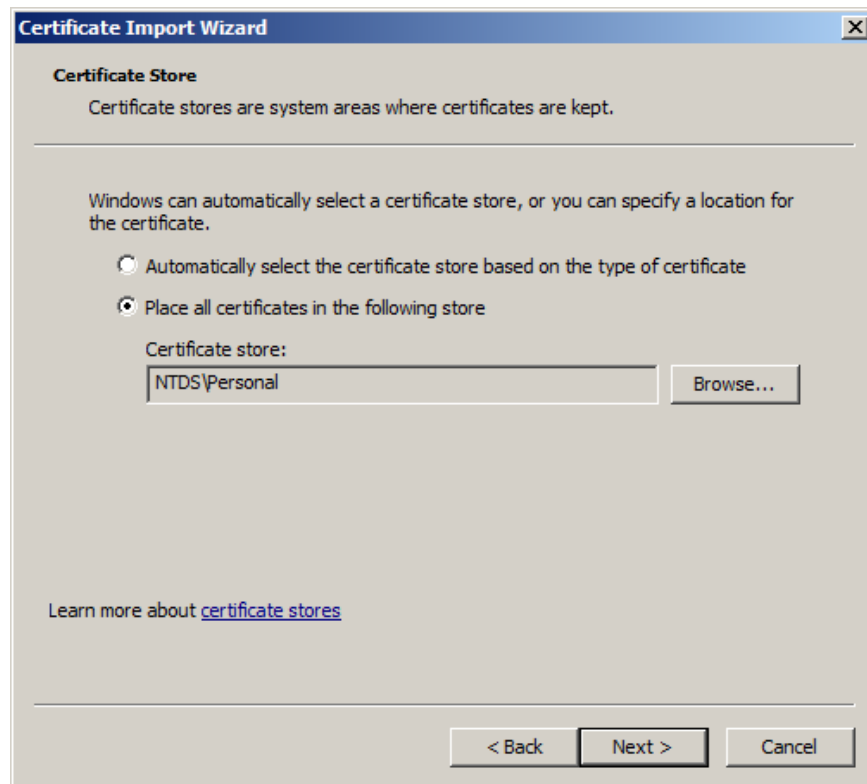
- 10) This will trigger the Certificate Import Wizard. Click Next;

- 11) Click Browse, navigate to the folder where you saved the .CER file, select the .CER file, click Open and click Next:

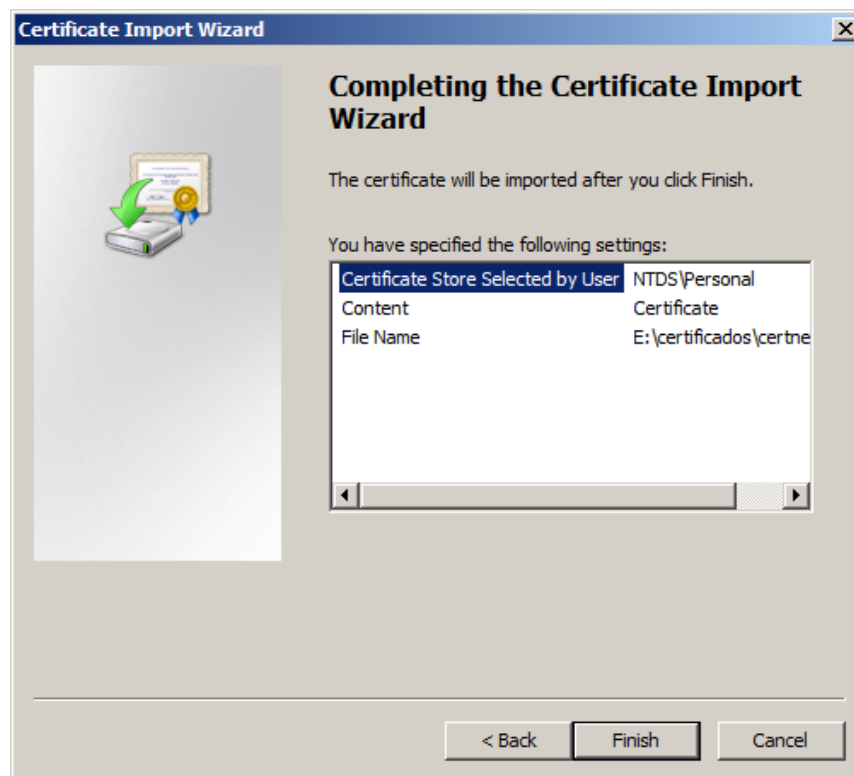




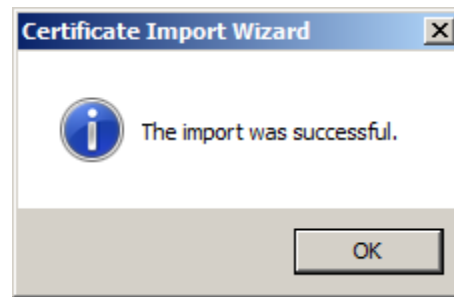
12) Do not change the default selection. Click Next:



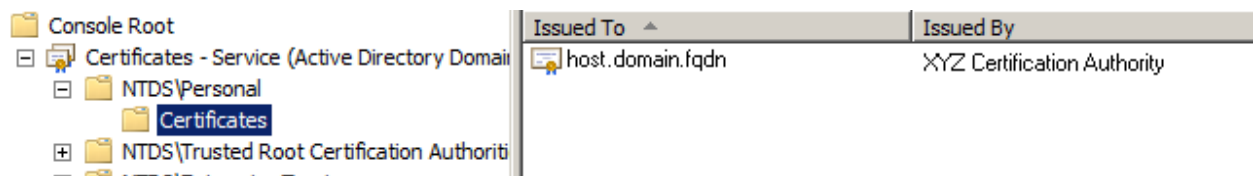
13) Review the import settings and click Finish:



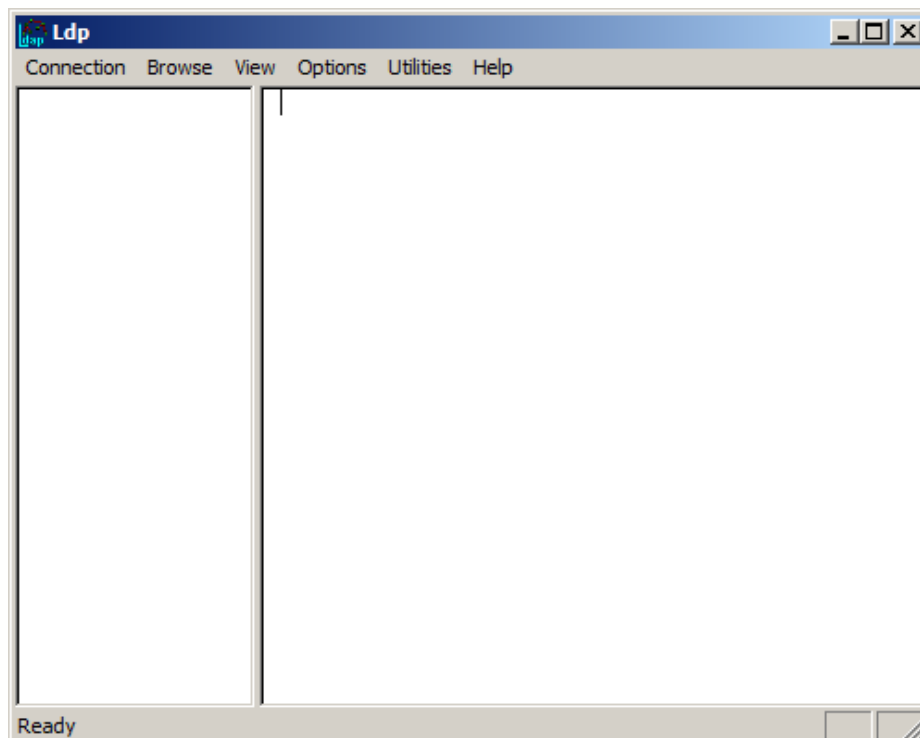
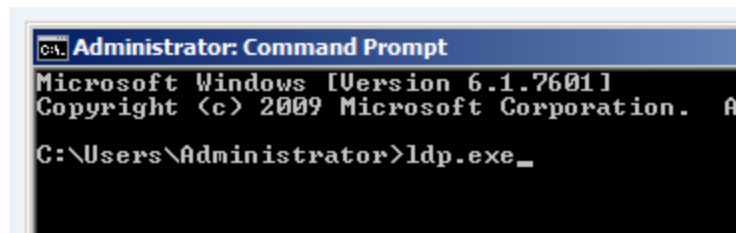
14) The Certificate Import Wizard confirms the success of the import operation. Click OK:



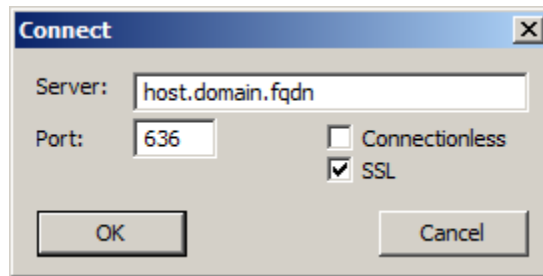
15) Now the MMC Certificates snap-in displays a folder called Certificates under NTDS\Personal and, inside that folder, it shows the imported certificate:



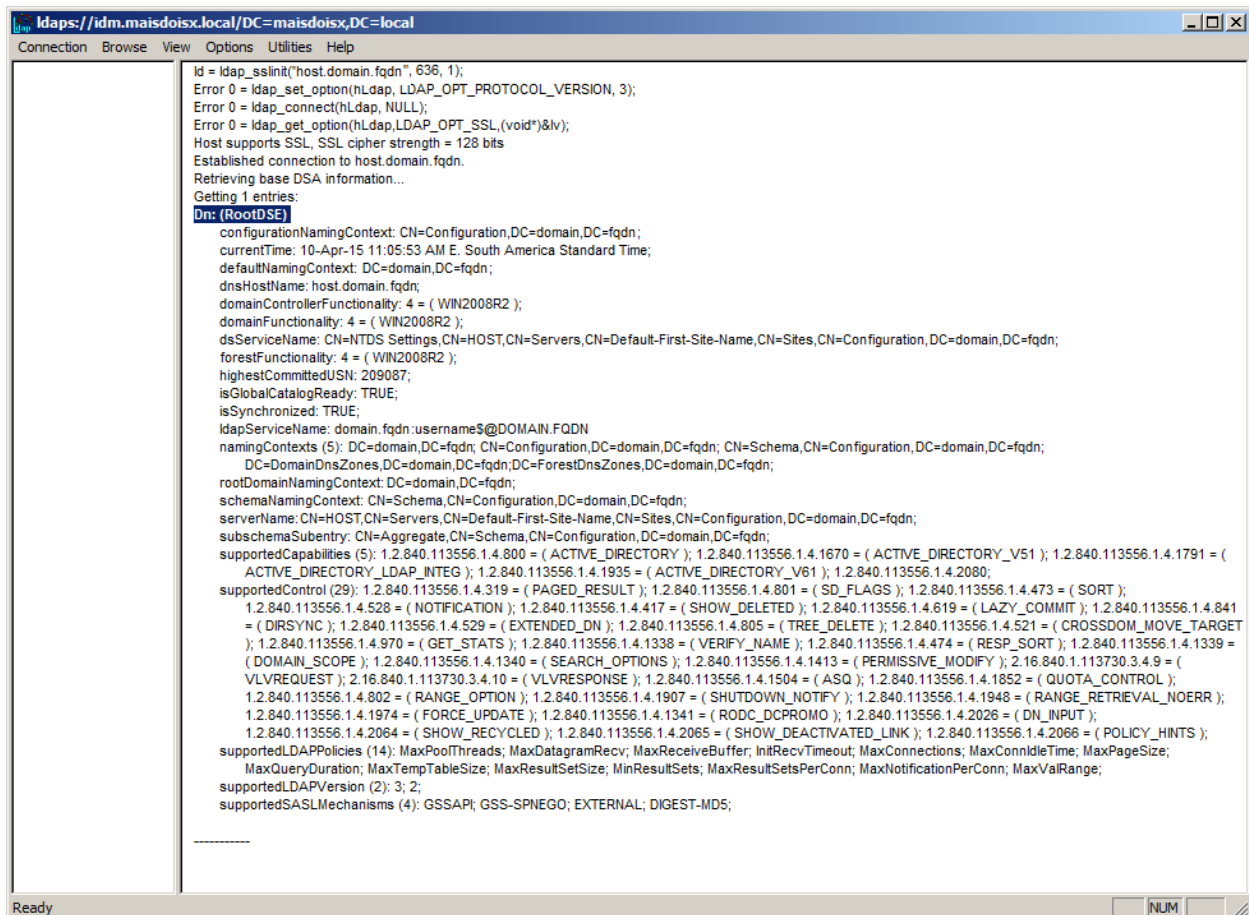
16) Open the LDP.EXE utility once again to validate the certificate installation:



17) At this point, click on the Connection menu and, after, click on Connect. The following window appears:



18) Type the Fully Qualified Domain Name (FQDN) of the domain controller, the communication port (default is 636 for LDAP over SSL) and check the SSL option. Click OK. The LDP utility should return the following:

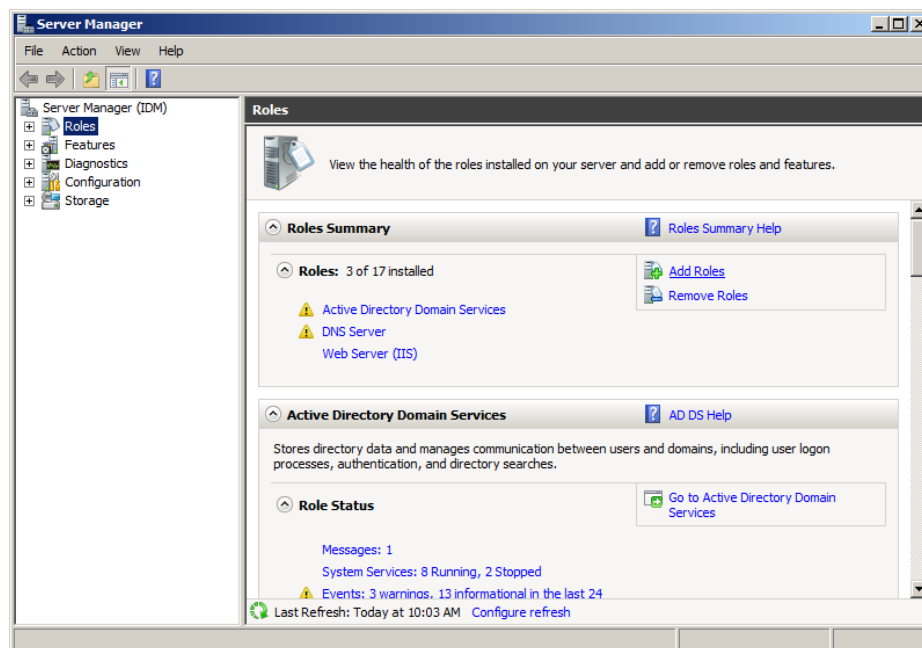




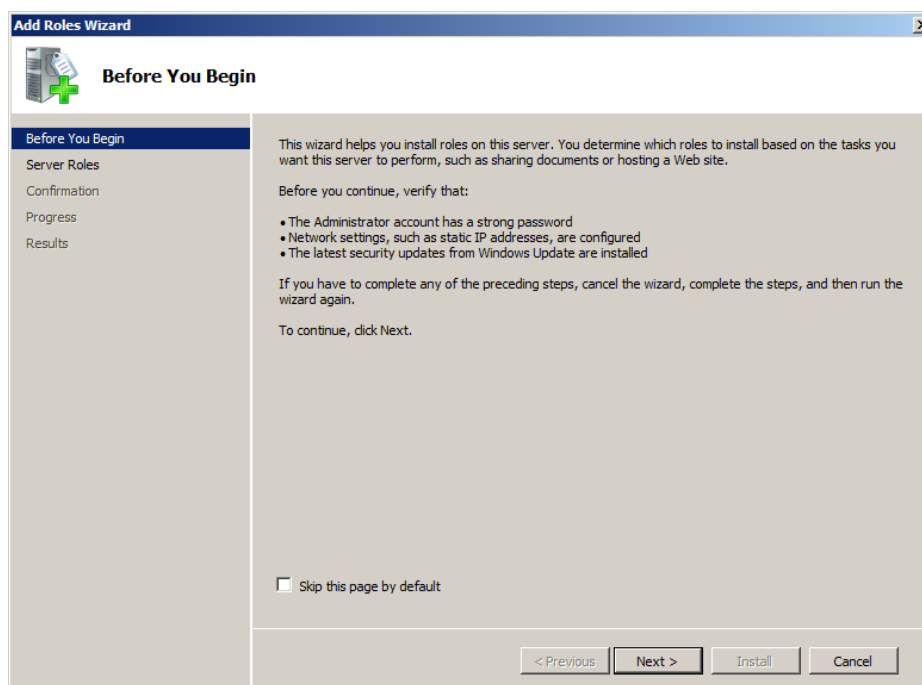
### Section III – Use the Microsoft Certificate Services to Generate a Self-Signed Certificate

If you do not have a certification authority on your environment, and do not have access to a third-party certification authority, you can use Microsoft Certification Services to generate a self-signed certificate. To use it, you must first install it and, after installing, you can submit your certificate request to it and generate the domain controller certificate. Please follow the steps above:

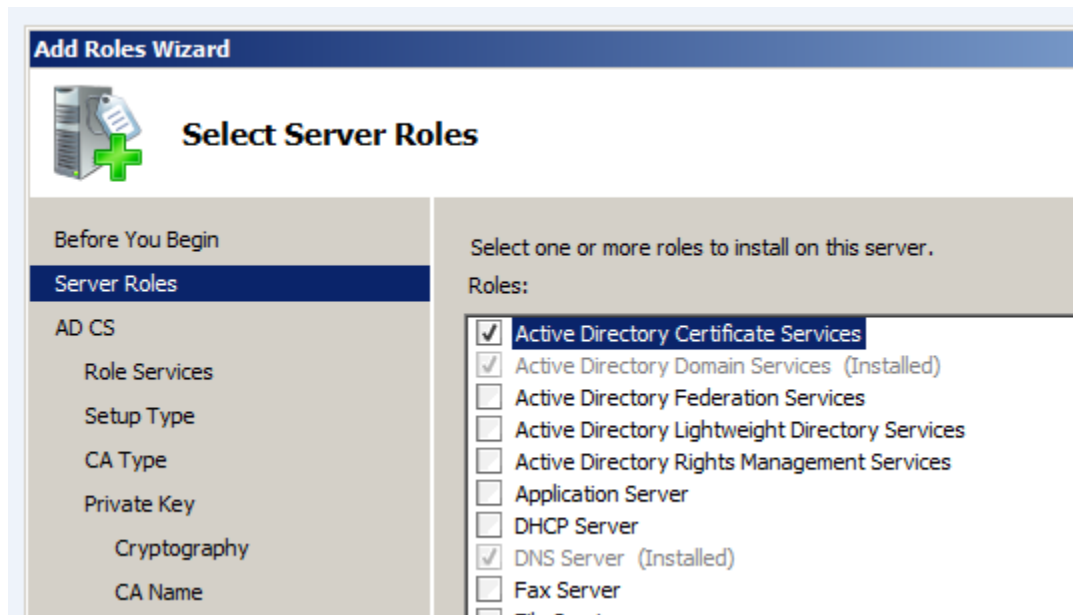
- 1) Open the Server Manager tool in the Domain Controller:



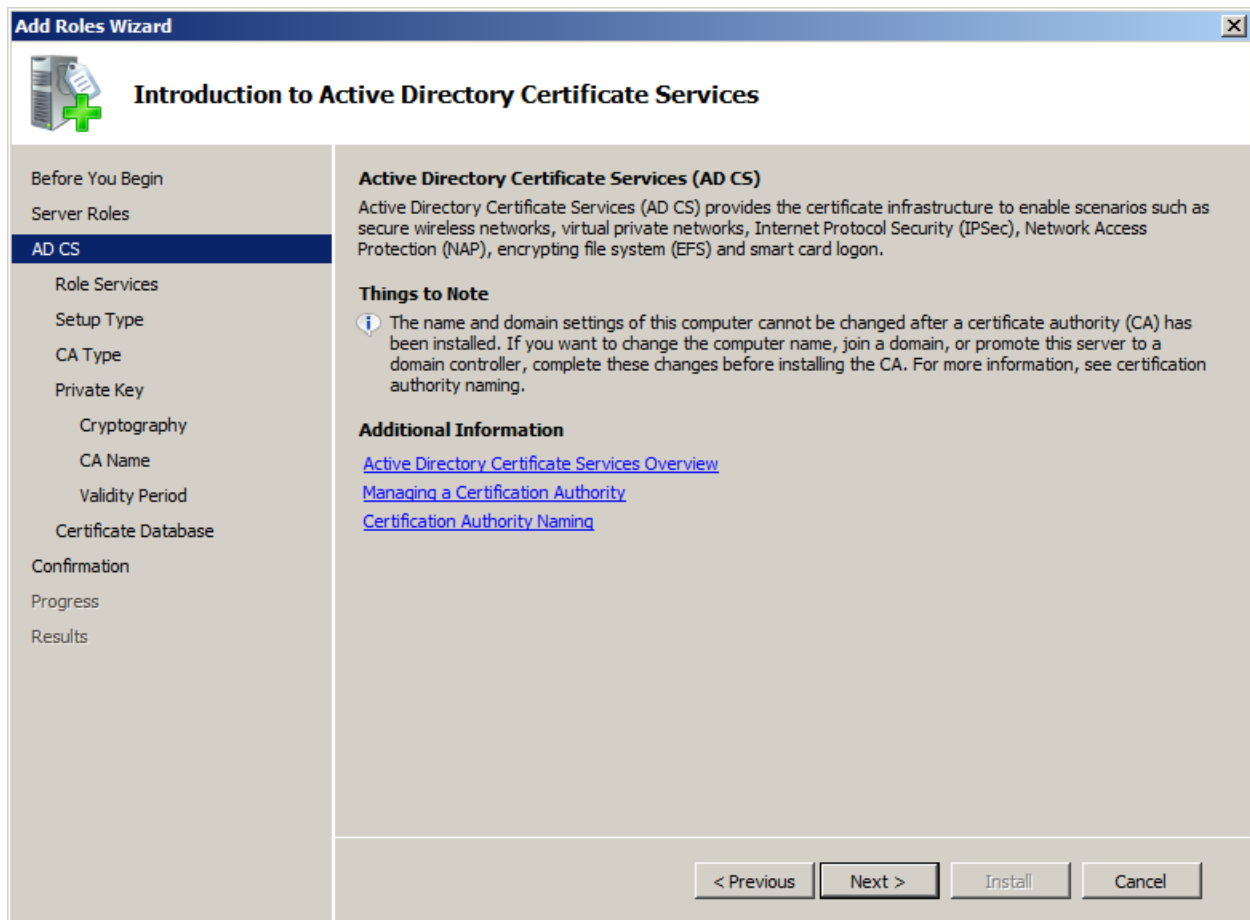
- 2) Click on the Add Roles link. It will trigger the Add Roles Wizard. Click Next:



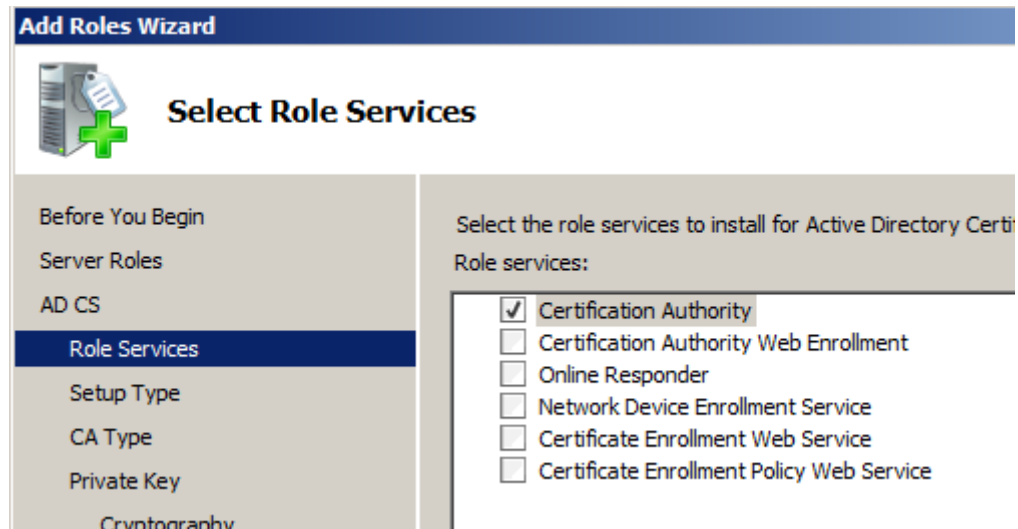
- 3) On the list of roles available, select Active Directory Certificate Services and click Next:



- 4) Review the information on the screen, and click Next:



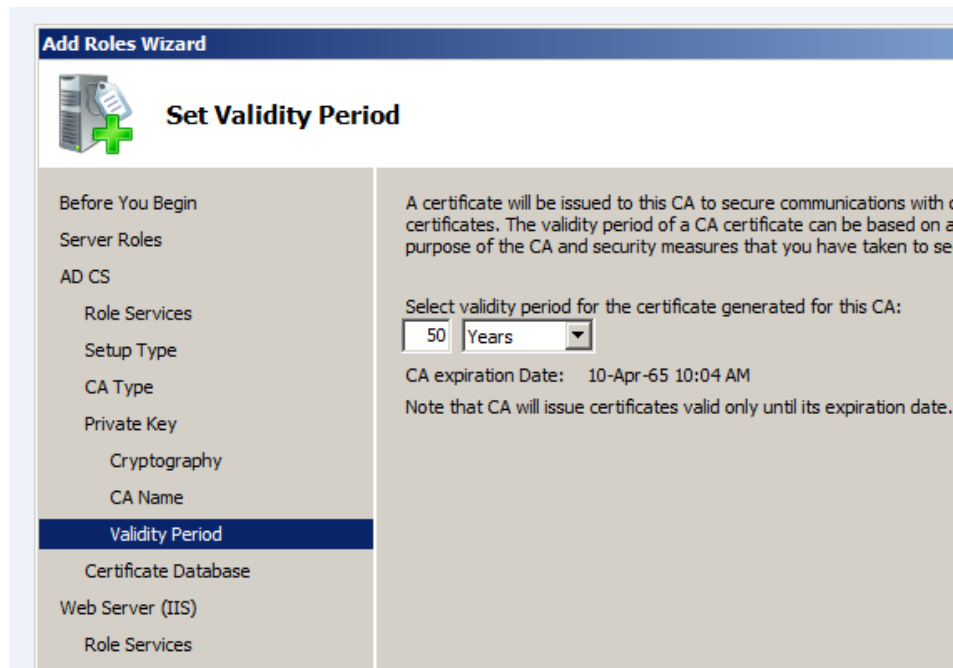
- 5) Leave the default selection, and select the Certification Authority Web Enrollment also:



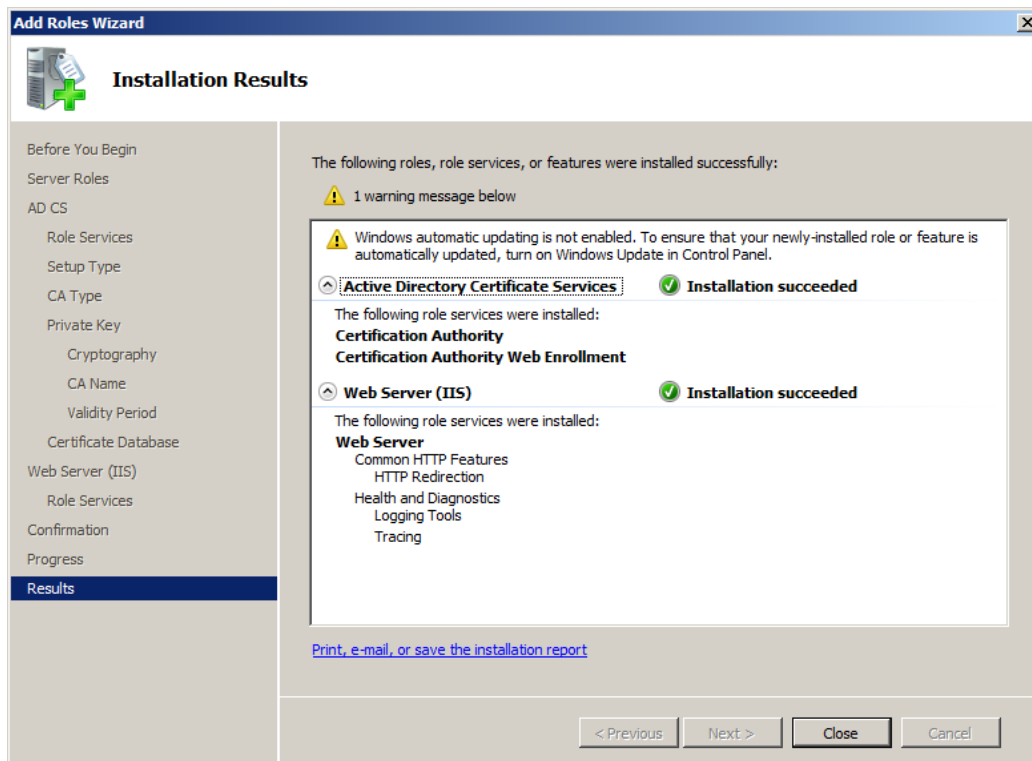
- 6) Accept the default selection by clicking on Add Required Role Services, then click Next:



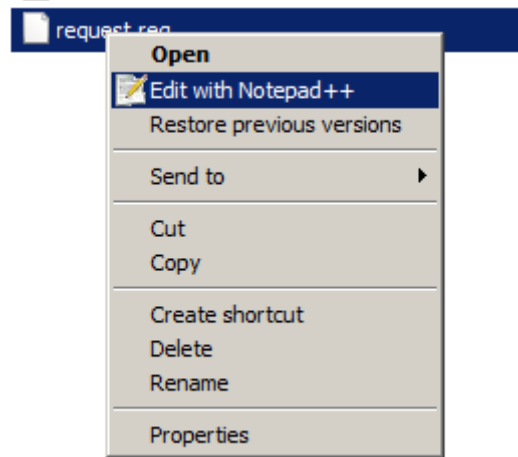
- 7) Accept the default for the next screens, always clicking on Next. On Validity Period, change the default value to 50 years (so your internal Certification Authority will not need to be renewed, unless you want to):



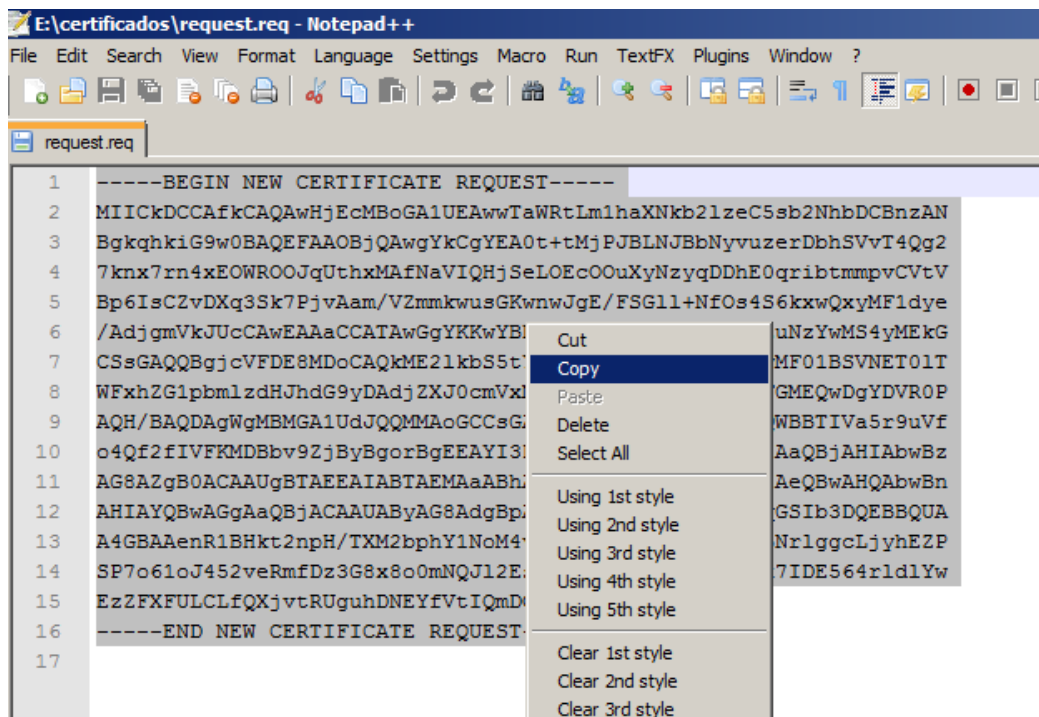
- 8) Accept the default for the next screens, always clicking on Next. On the last screen, review the settings and click Install;
- 9) On the Results screen, click Close:



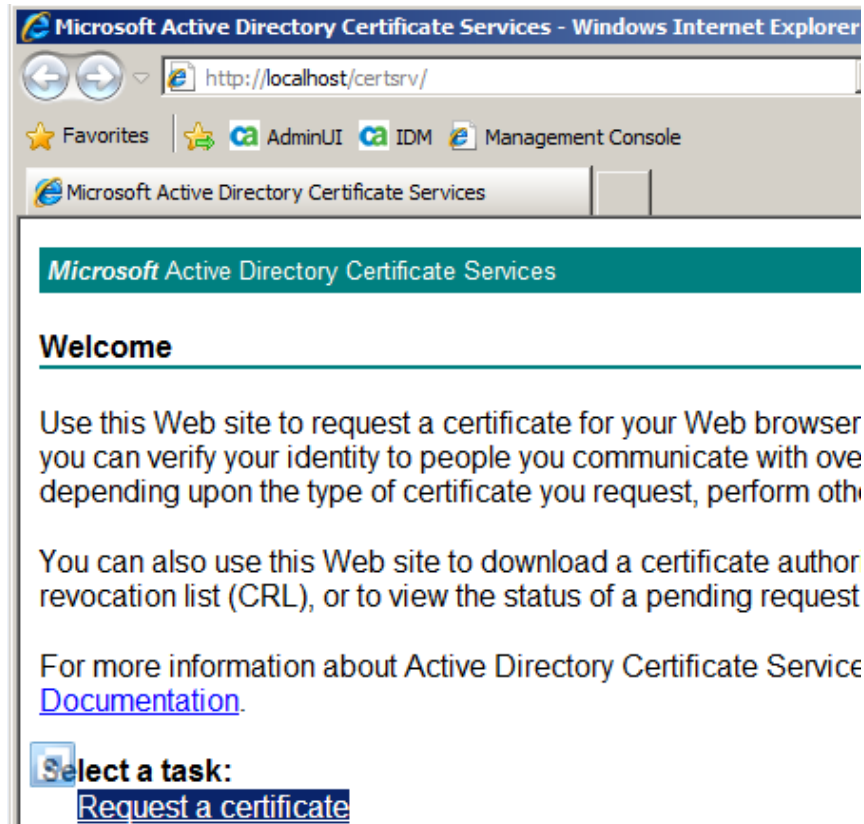
- 10) **Reboot your server.** This reboot is crucial to the Certificate Services consolidate the primary key. If you don't reboot and generate the certificate by the next steps below, your certificate will be **invalid** upon the next reboot of this server;
- 11) Open the **request.req** file you generated on the Section I of this guide using a text editor:



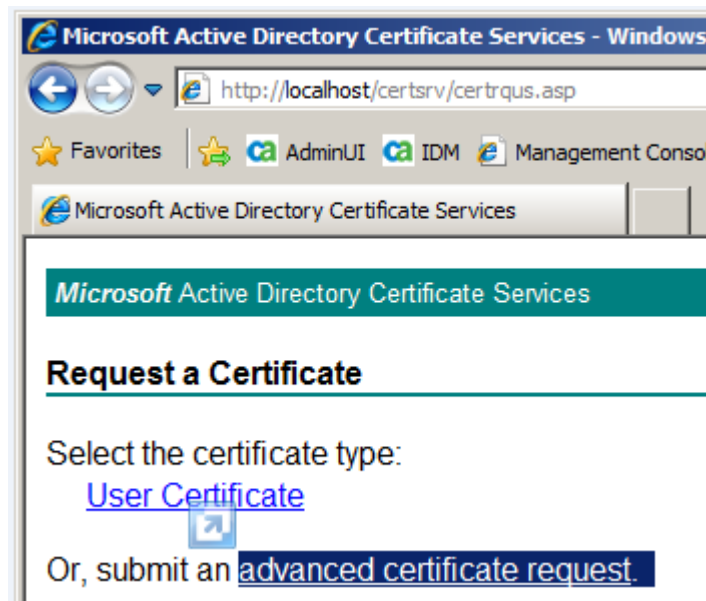
- 12) Select all the content, and copy it:



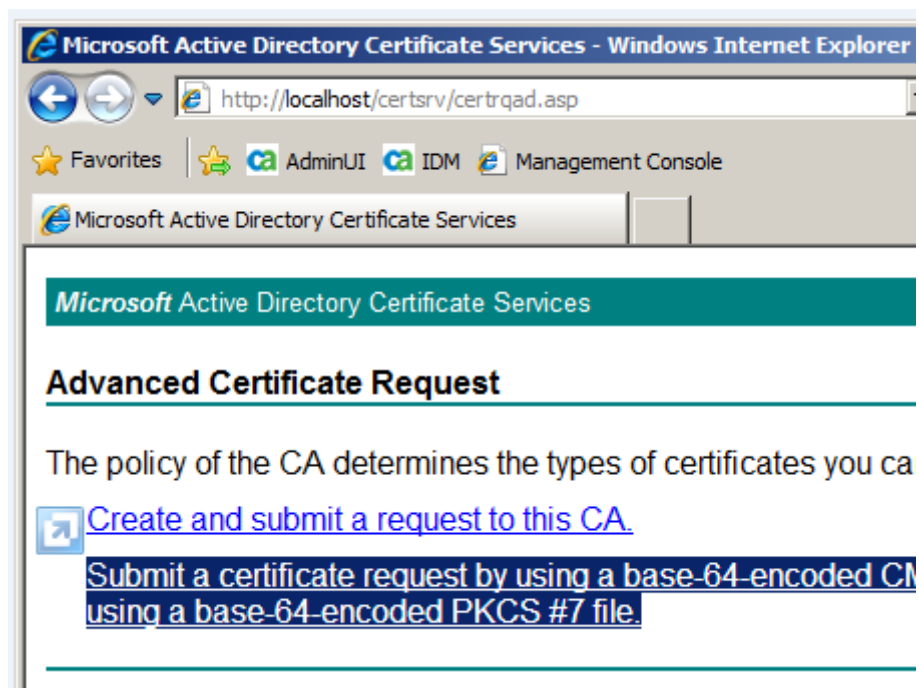
- 13) Access your Certificate Services page by navigating to <http://localhost/certsrv>:



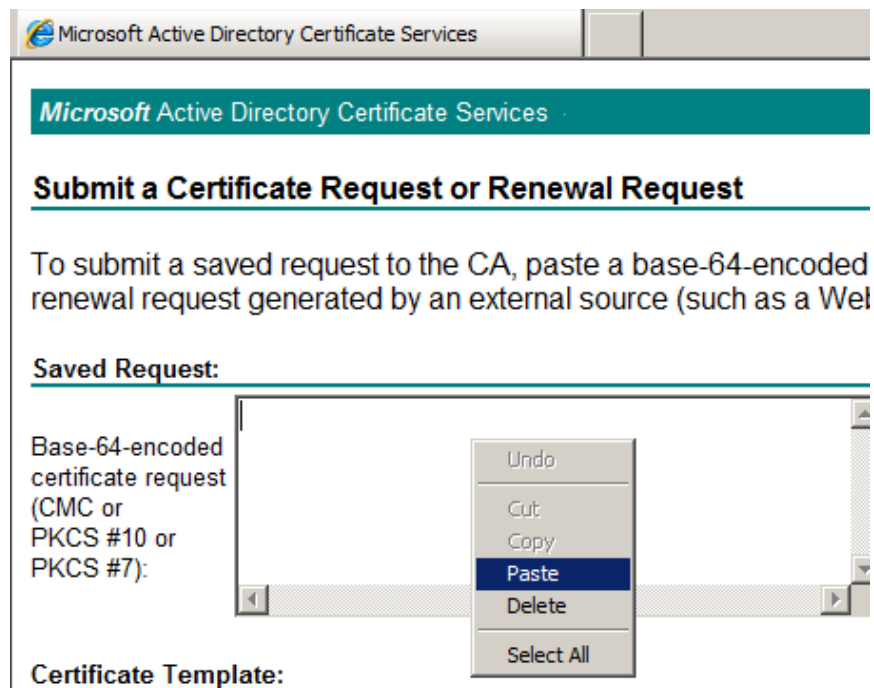
14) Click on Request a certificate link. On the page that opens, click on advanced certificate request:



15) Click on the Submit a certificate request by using a [...] file link:



16) Paste the contents of request.req into the Saved Request field:



17) Select the Web Server certificate template, and click Submit:

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or renewal request generated by an external source (such as a Web server)

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
AHIAYQBwAGgAaQBjACAAUABYAG8AdgBpAGQAZQByA4GBAAenR1BHkt2npH/TXM2bphY1NoM4vY4RfbGsSP7o61oJ452veRmfdz3G8x8o0mNQJl2EsOLBhHKyEz2FXFULCLfQXjvtRUguhDNEYfVtIQmDOShtAXfu-----END NEW CERTIFICATE REQUEST-----
```

### Certificate Template:

Additional Attributes:

Attributes:

User

User

Basic EFS

Administrator

EFS Recovery Agent

Web Server

Subordinate Certification Authority


- 18) Select the Base 64 option and click Download certificate (you can safely ignore the ActiveX error message):



## Certificate Issued

The certificate you requested was issued to you.

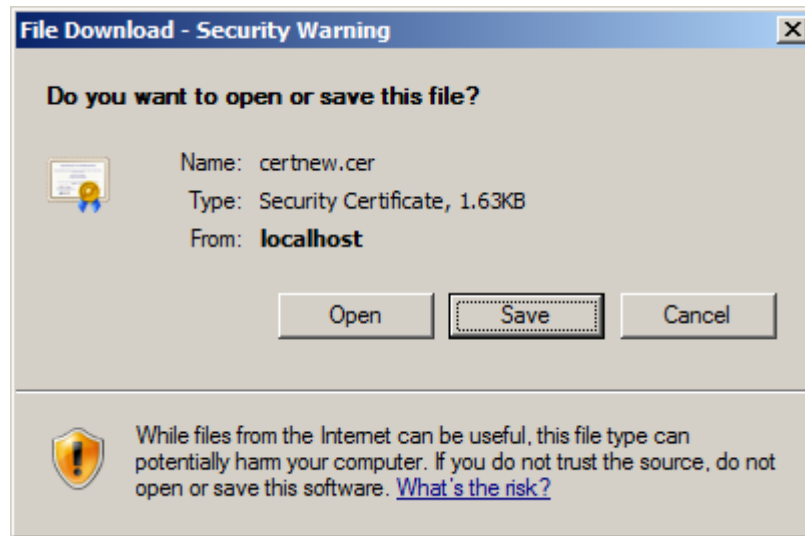
☐ DER encoded or ☒ Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)

- 19) Save the file **certnew.cer** on your local filesystem:





20) Done! Now go back to Section II and install the certificate.