Summary

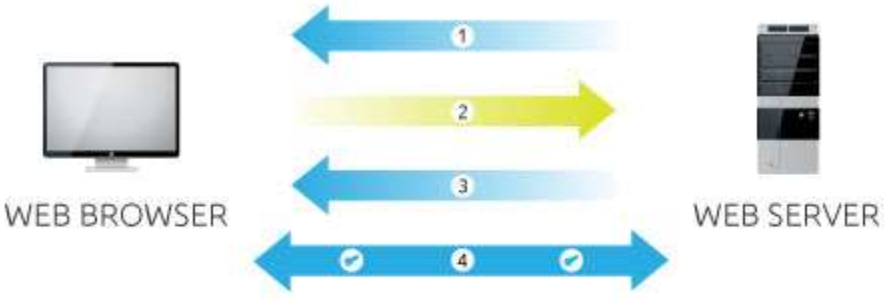
An organization called Hexad0m requires CA (Certification Authority) to issue certifications to the systems and the users. This certification authority gives a sigh of relief to the users as it allows and helps users to verify the communication between systems to make sure that the website they are visiting is completely secured, and encrypted, and no data can be leaked out in under manner ways under the act of validation of binding the data in cryptographic key pairs in the digital world.

The research covers the main issues with the SSL PKI threat model and later on explains its postulates regarding threats that can take place during CA assigning, spoofing, SSL stripping, Encrypted Traffic Threats, and much more, and later on take a look at what are some methods to safe keep under such situations.

Introduction

In internet security, SSL (**Secure Sockets Layer**) is the standard. The data transmitted over the Internet is encrypted between a client and server which prohibits unauthorized users or attackers to read or use encrypted data without a secret decryption key. SSL encryptions are used in several websites for securing data against theft, modification, or spoofing.

Public Key Infrastructure (PKI) is a set of hardware, software, people, rules, and procedures that are required for digital certificates to be created, managed, distributed, used, stored, and revoked. PKI also connects keys using the certificate authority with user IDs (CA). With the use of PKI, a hybrid encryption method can be used for both forms of encryption. The SSL certificate of the server includes an asymmetric public and private key pair in SSL interactions used to create a secure communication layer and this entire session of user and server creates a symmetric session key for the SSL Handshake which can be described as:



However, no security is perfectly secured so we will be looking at some of the ways to exploit security issues within the SSL PKI route and define what are some ethical measurements to be taken under such circumstances [1].

SSL PKI Design & Implementation

Offline Root Certification Authority

Basic Setup

The research is based on 2 servers (Domain Server and Subordinate CA Server), and 1 client computer (User 2) to demonstrate the connectivity and tests. DNS is already configured on **Domain Controller** for creating a connection between networks. Following IP configuration is used in the network:

Domain Controller (Server 1)

- 192.168.150.254 = IP Address
- 255.255.255.0 = Sub Net Mask
- 192.168.150.2 = Gateway
- 127.0.0.1 = DNS

Subordinate CA (Server 2)

- 192.168.150.124 = IP Address
- 255.255.255.0 = Sub Net Mask
- 192.168.150.2 = Gateway
- 192.168.150.254 = DNS

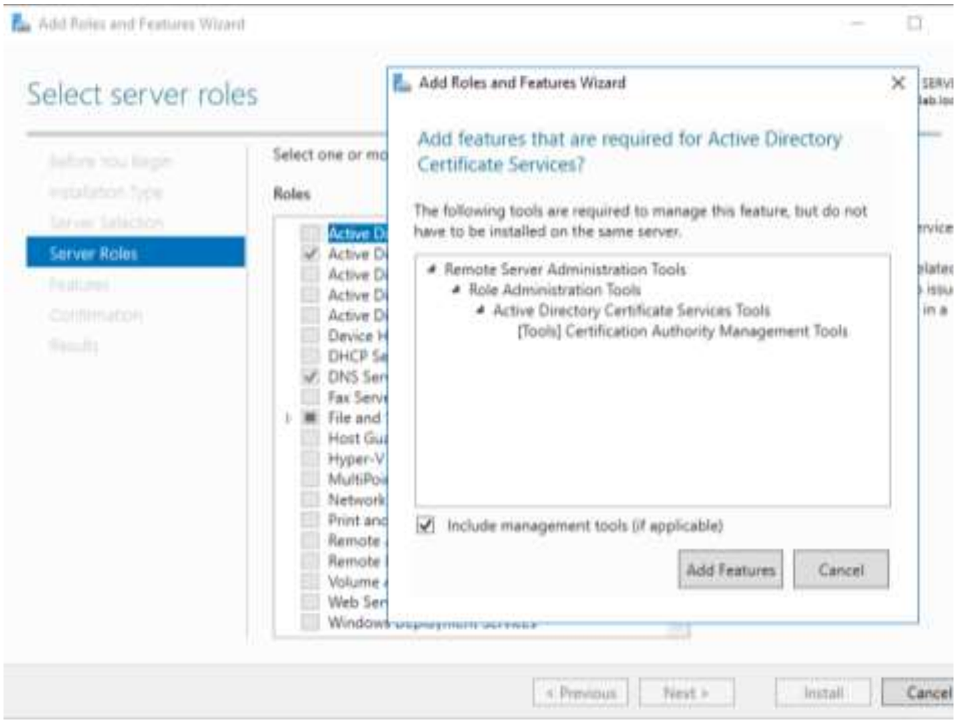
User2 (Client)

- 192.168.150.123 = IP Address
- 255.255.255.0 = Sub Net Mask
- 192.168.150.2 = Gateway
- 192.168.150.254 = DNS

Considering that each client computer is connected under a network and a domain called **testlab.local**, the study will go deep into how the certification Authority will be configured for the firm called Hexad0m.

AD CS Setup

In this stage, Active Directory Certificate Service or **AD CS** will be installed on Subordinate CA.



Add Roles and Features Wizard

Select server roles

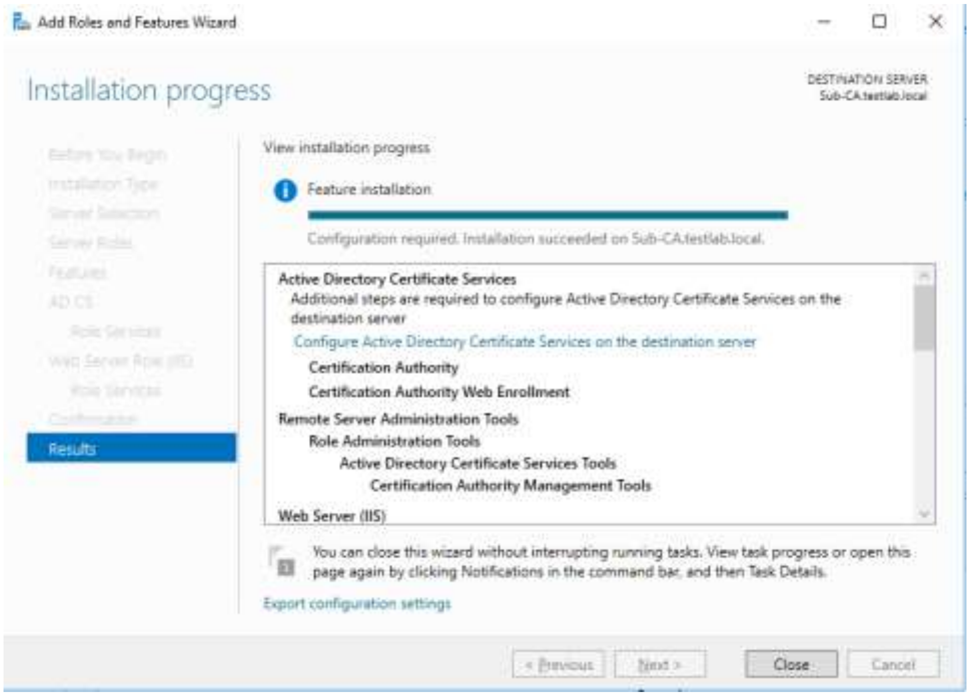
Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)

Two features will be installed for AD CS setup called **Certification Authority** and **Web Enrolment**. Note, we will also be installing **DNS** and **IIS** on our **Subordinate CA** for the assignment of data through online means, and only default options are selected in the upcoming areas. For **role services**, **Certification Authority** and **Web Enrolment** will be chosen. Once all the configurations are added, and the feature is installed, AD CS will be started.



Installation progress

DESTINATION SERVER
Sub-CA.testlab.local

View installation progress

Feature installation

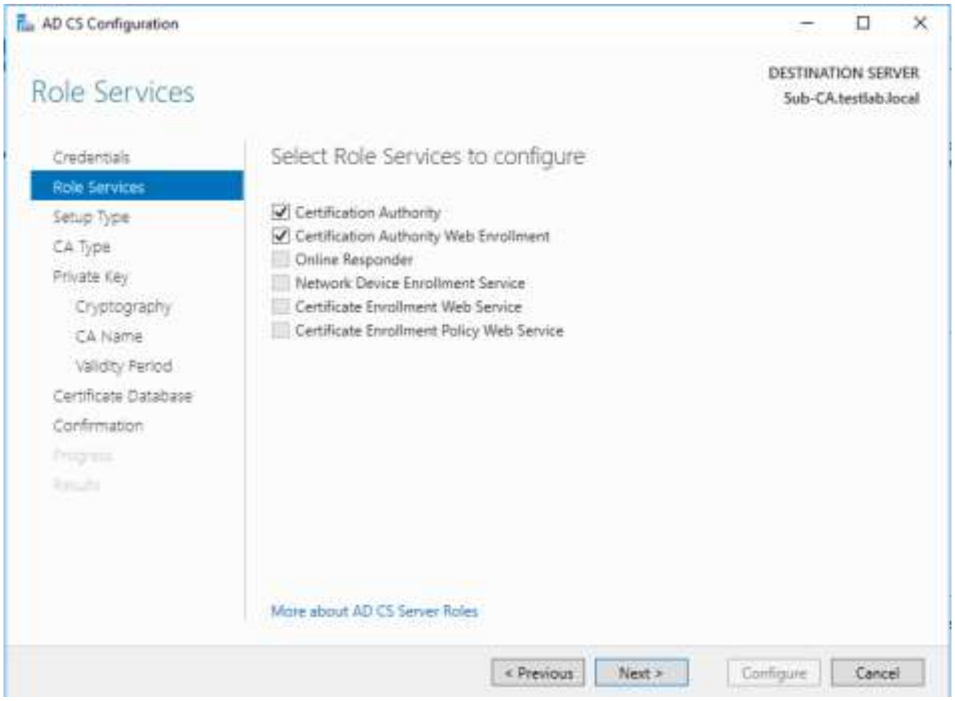
Configuration required. Installation succeeded on Sub-CA.testlab.local.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Certification Authority Web Enrollment
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools
Web Server (IIS)

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

In this stage, **Certification Authority** and **Web Enrolment** will be chosen to be able to provide the certificates to the user in a virtual interface using Web Enrolment.



Role Services

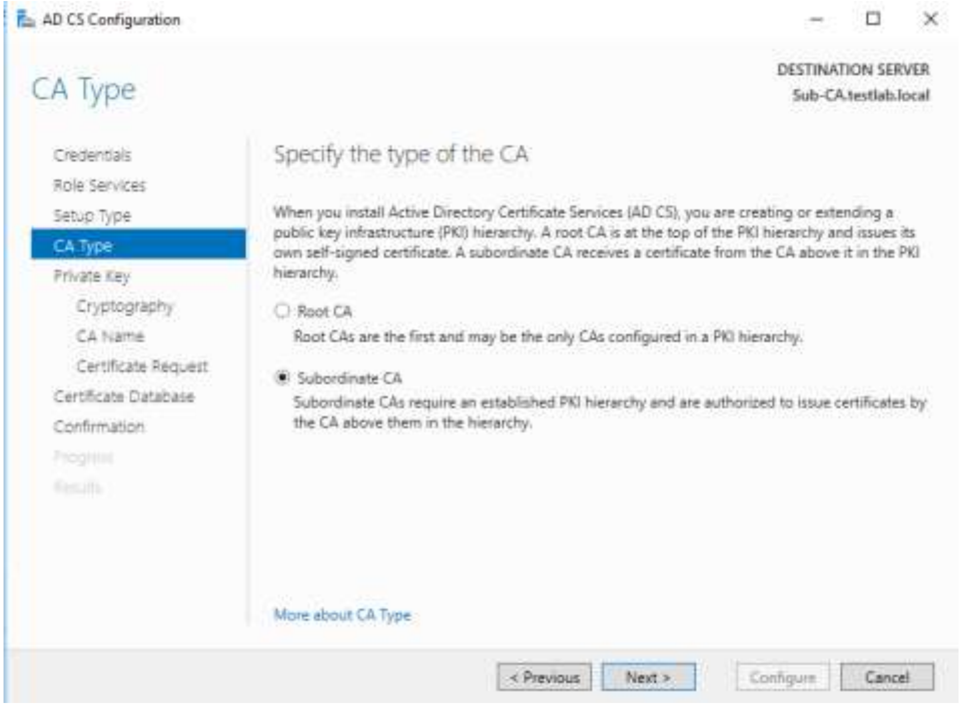
DESTINATION SERVER
Sub-CA.testlab.local

Select Role Services to configure

☑ Certification Authority
☑ 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

In the next step, **Enterprise CA** will be chosen to issue the certificates and **subordinate CA** will be selected after that.



CA Type

DESTINATION SERVER
Sub-CA.testlab.local

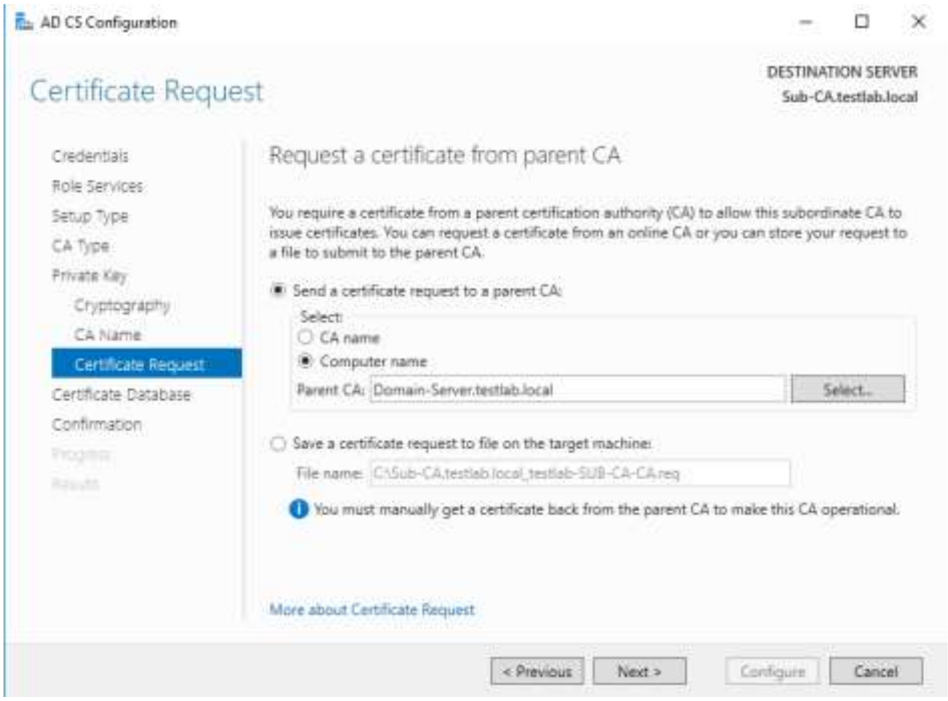
Specify the type of the CA

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.

Since this is a new setup, the new private key will be made and fairly after that, all steps ahead will be the default. While making sure that our domain server is selected in the certificate request as it will be requesting assigning it to the client system.



Certificate Request

DESTINATION SERVER
Sub-CA.testlab.local

Request a certificate from parent CA

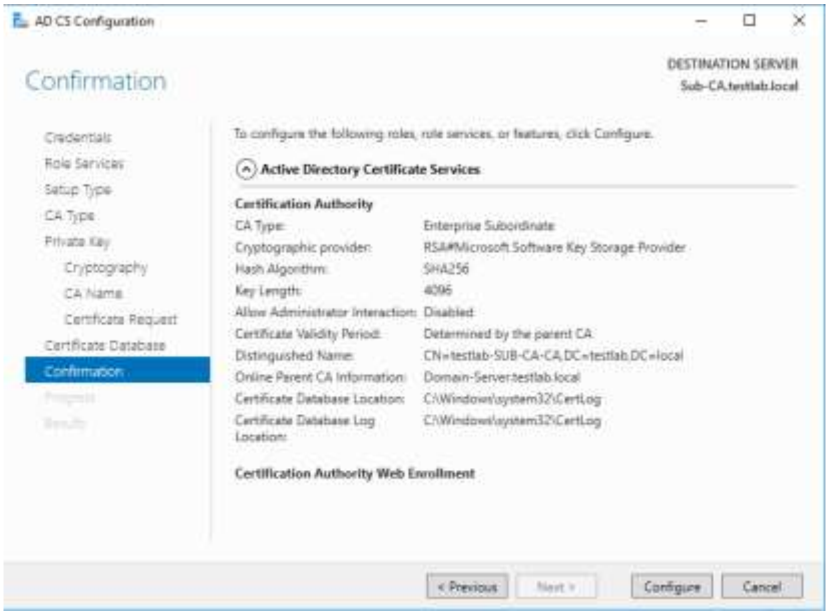
You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.

● Send a certificate request to a parent CA:
Select:
○ CA name
● Computer name
Parent CA: Domain-Server.testlab.local

○ Save a certificate request to file on the target machine:
File name: C:\Sub-CA.testlab.local_testlab-SUB-CA-CA.req

You must manually get a certificate back from the parent CA to make this CA operational.

Once this all is configured, the confirmation section will list out all the options that were selected during the configuration of AD CS.



Confirmation

DESTINATION SERVER
Sub-CA.testlab.local

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

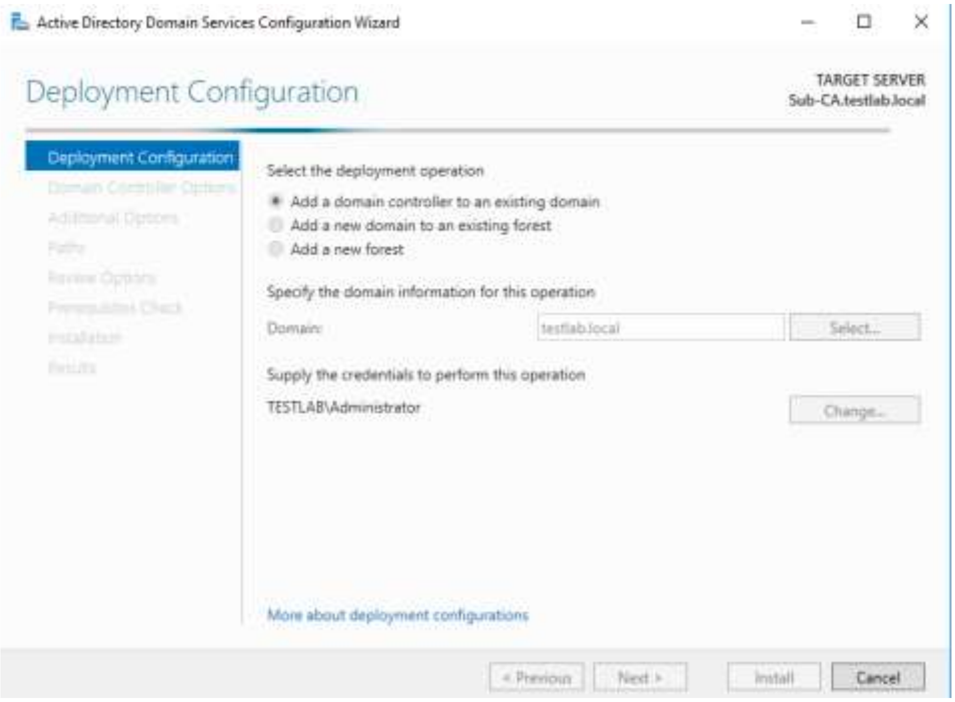
Certification Authority

CA Type: Enterprise Subordinate
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 4096
Allow Administrator Interaction: Disabled
Certificate Validity Period: Determined by the parent CA
Distinguished Name: CN=testlab-SUB-CA-CA,DC=testlab,DC=local
Online Parent CA Information: Domain-Server.testlab.local
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog

Certification Authority Web Enrollment

DNS Configuration

In this step, DNS will be configured for leading it to the already existing domain called **testlab.local**. Additionally, administer account will be used to log in over the server as:



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
Sub-CA.testlab.local

Select the deployment operation

● Add a domain controller to an existing domain
○ Add a new domain to an existing forest
○ Add a new forest

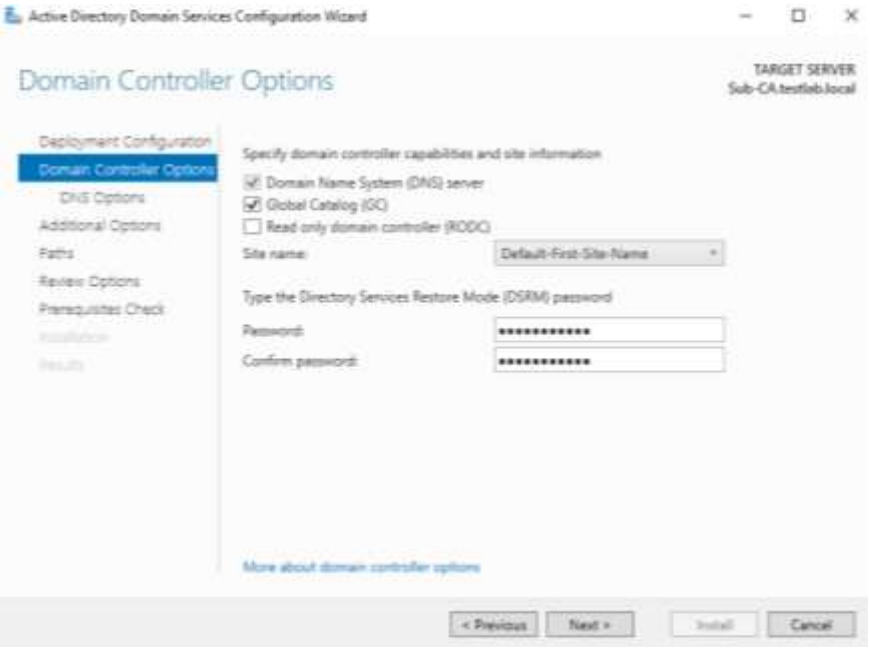
Specify the domain information for this operation

Domain: testlab.local

Supply the credentials to perform this operation

TESTLAB\Administrator

Upon completion, the password will be used to protect the domain during sign-up when accessing the domain which can be seen configured as:



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
Sub-CA.testlab.local

Specify domain controller capabilities and site information

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
□ Read only domain controller (RODC)

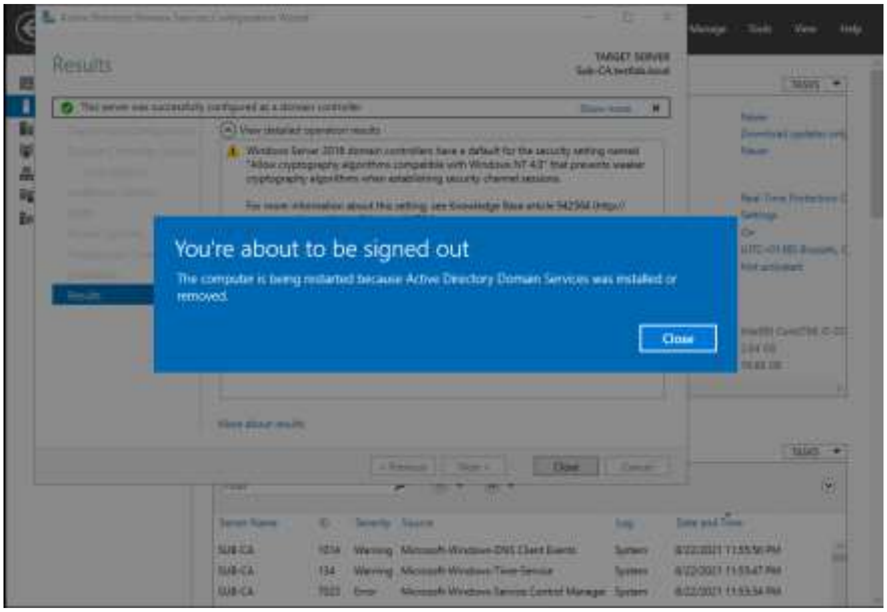
Site name: Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

Password: ************

Confirm password: ************

Upon configuring while keeping all the chosen options default for the rest, the server subordinate CA will restart.



Results

TARGET SERVER
Sub-CA.testlab.local

This server was successfully configured as a domain controller

View detailed operation results

Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://

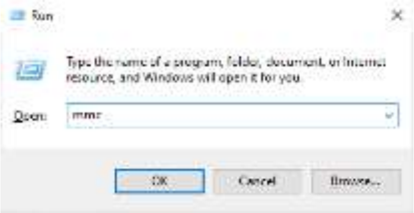
You're about to be signed out

The computer is being restarted because Active Directory Domain Services was installed or removed.

Server Name	ID	Severity	Source	Log	Date and Time
SUB-CA	1014	Warning	Microsoft-Windows-DNS Client Events	System	8/22/2021 11:55:50 PM
SUB-CA	134	Warning	Microsoft-Windows-Time-Service	System	8/22/2021 11:55:47 PM
SUB-CA	7023	Error	Microsoft-Windows-Service Control Manager	System	8/22/2021 11:53:34 PM

Issuing Certificates

The study here will explain how the certificates can be issued to provide users with the certificates. We will use the command **Ctrl + Win** to open the **run** tab and write **MMC** to open Console.

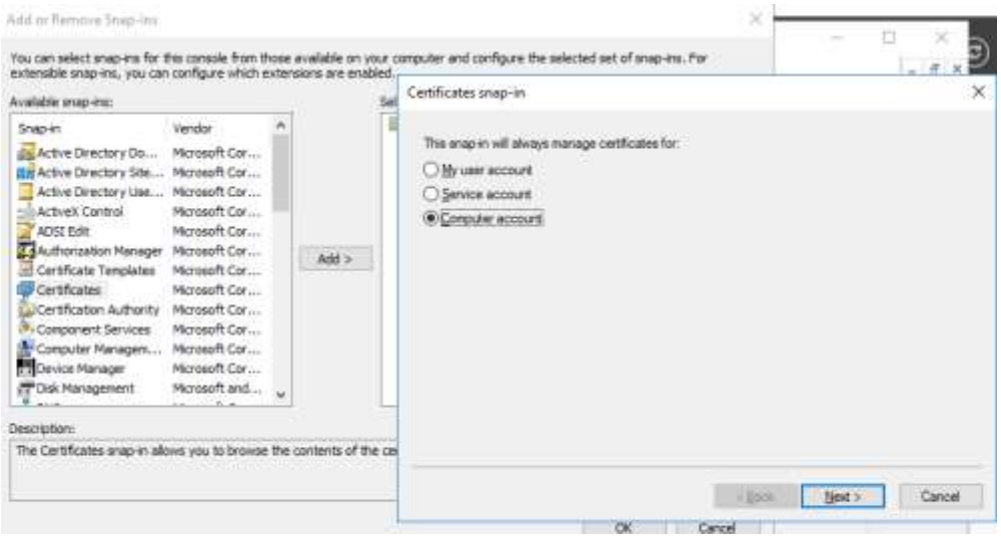


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

From **File → snap-in**, certificates option will be added such that the certificates can be assigned in the later step, and the following lookup is obtained:



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Description:

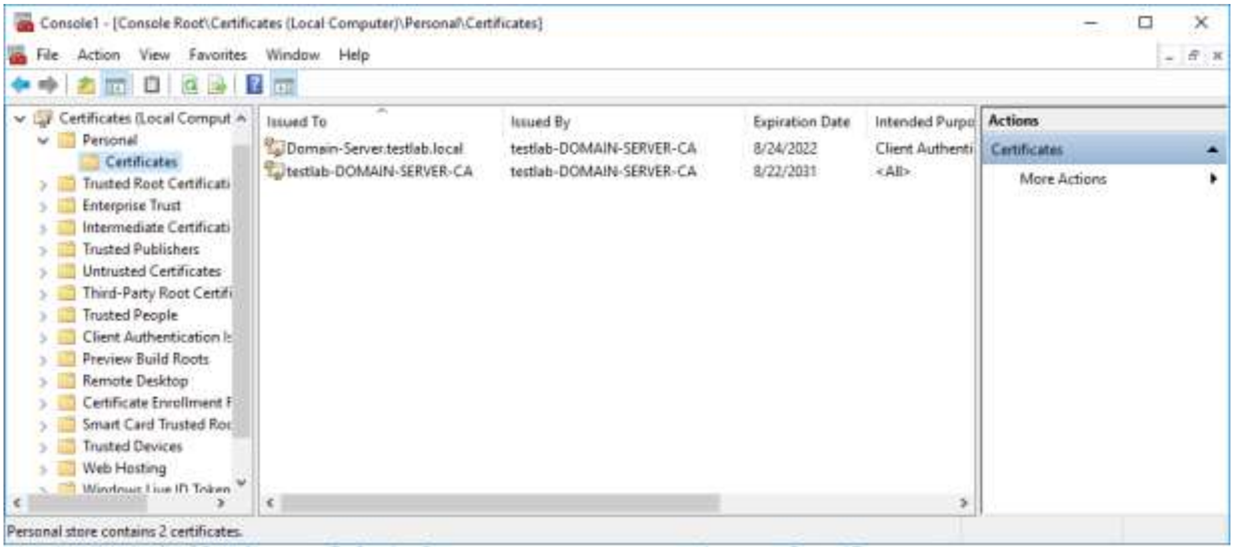
The Certificates snap-in allows you to browse the contents of the ce

Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

In this, the local account will be selected:



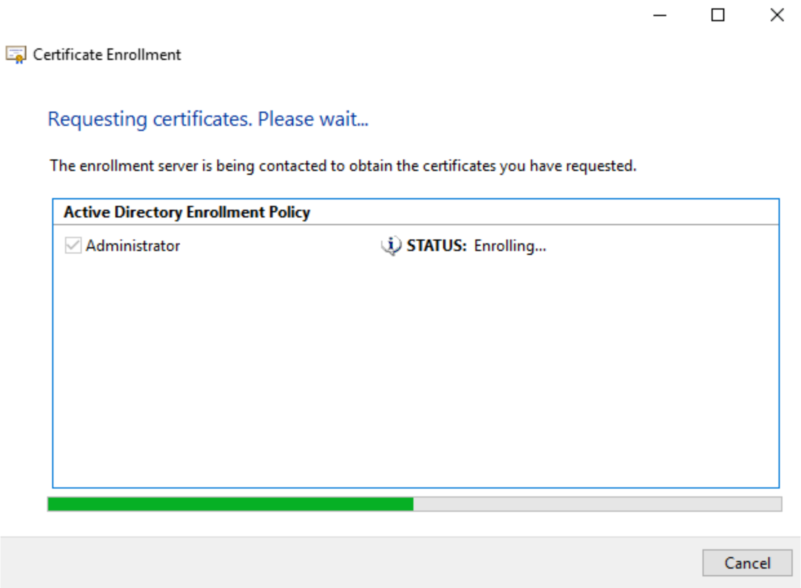
Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

- Certificates (Local Comput
  - Personal
    - Certificates
  - Trusted Root Certificati
  - Enterprise Trust
  - Intermediate Certificati
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certifi
  - Trusted People
  - Client Authentication Is
  - Preview Build Roots
  - Remote Desktop
  - Certificate Enrollment F
  - Smart Card Trusted Roo
  - Trusted Devices
  - Web Hosting
  - Windows Live ID Token

Issued To	Issued By	Expiration Date	Intended Purpo
Domain-Server.testlab.local	testlab-DOMAIN-SERVER-CA	8/24/2022	Client Authenti
testlab-DOMAIN-SERVER-CA	testlab-DOMAIN-SERVER-CA	8/22/2031	<All>

Personal store contains 2 certificates.

Here, a new certificate will be issued using a right-click to our **Domain Server** (Server 1). The server will enrol the administrator certificate and during enrolment, the following screen is to be expected:



Certificate Enrollment

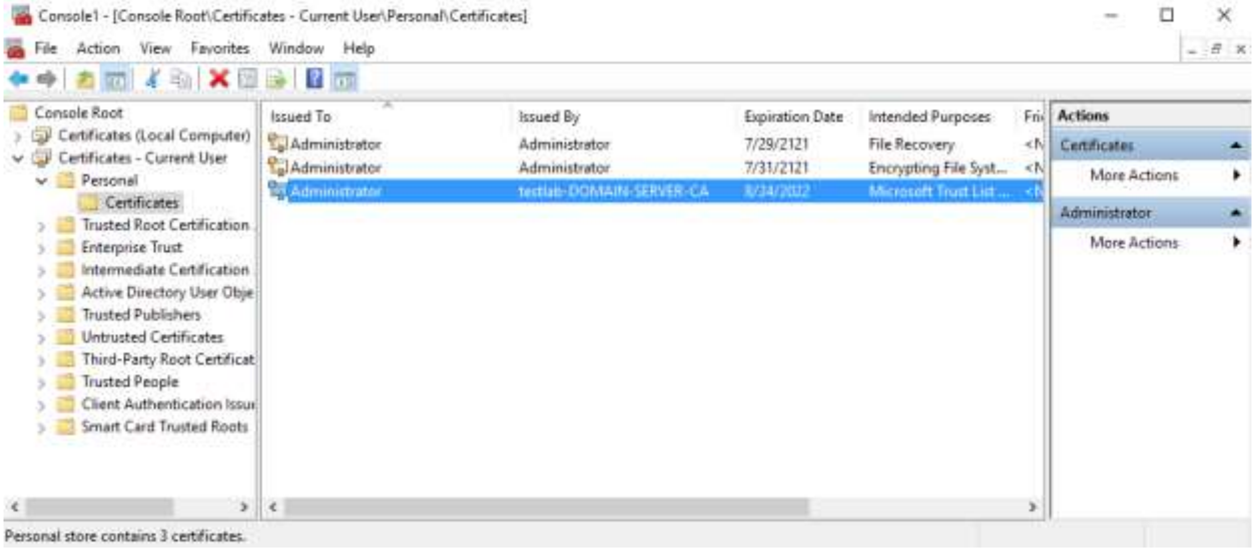
Requesting certificates. Please wait...

The enrollment server is being contacted to obtain the certificates you have requested.

Active Directory Enrollment Policy

☑ Administrator — STATUS: Enrolling...

Upon the completion of this, a new certificate can be seen issued in our console issued by our Domain Server for itself.



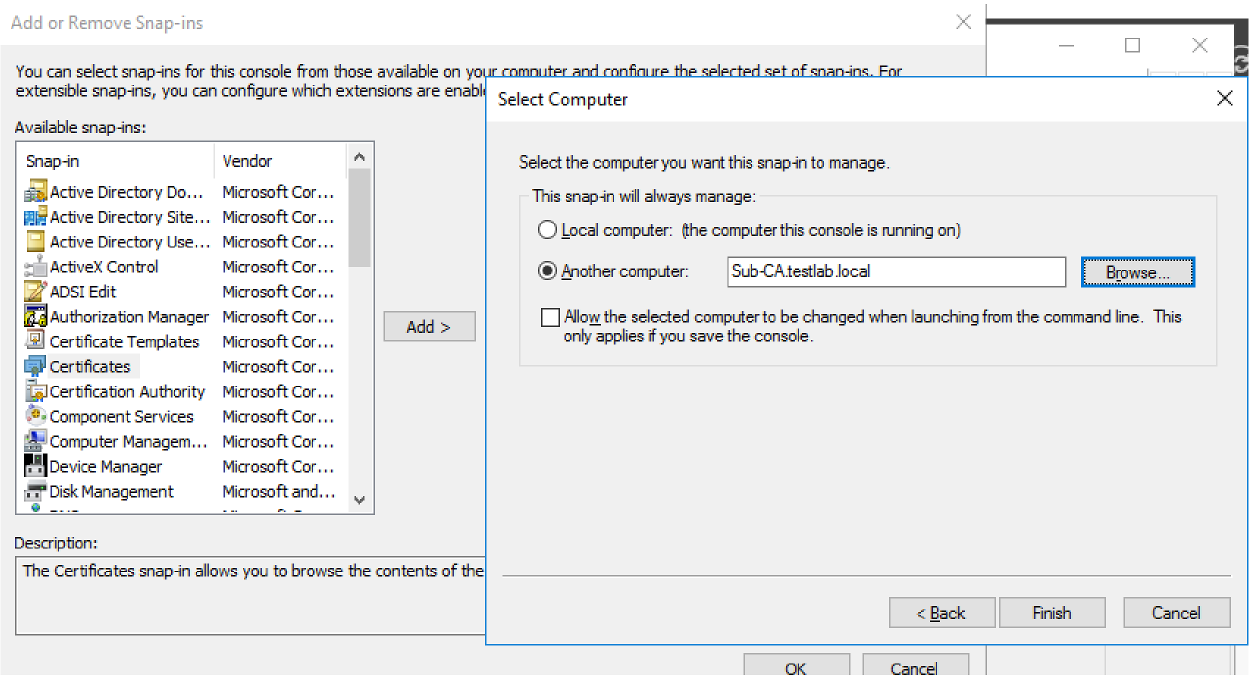
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Fri
Administrator	Administrator	7/29/2121	File Recovery	<N
Administrator	Administrator	7/31/2121	Encrypting File Syst...	<N
Administrator	testlab-DOMAIN-SERVER-CA	8/24/2022	Microsoft Trust List ...	<N

Personal store contains 3 certificates.

Issue Other Users

Other Users or Servers can be assigned by going into the **Snap-in** section and adding the location of the Server/User which, according to this research will look like this:



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabl

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Description:

The Certificates snap-in allows you to browse the contents of the

Select Computer

Select the computer you want this snap-in to manage.

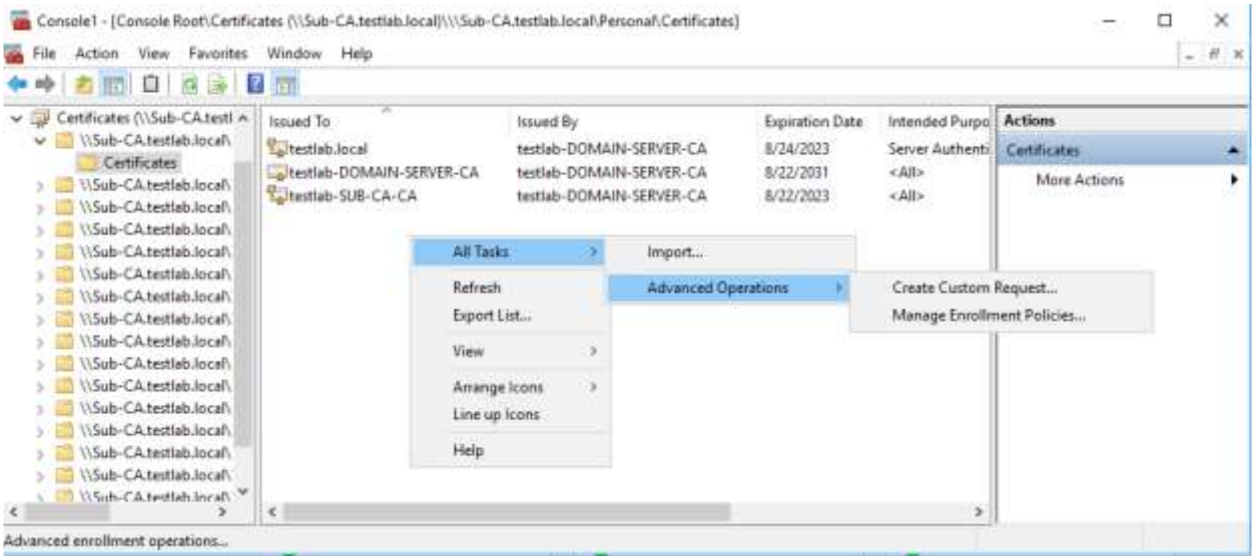
This snap-in will always manage:

○ Local computer: (the computer this console is running on)

● Another computer: Sub-CA.testlab.local

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Now, the certificates can be assigned in the same way as we did with the **Domain Server**:



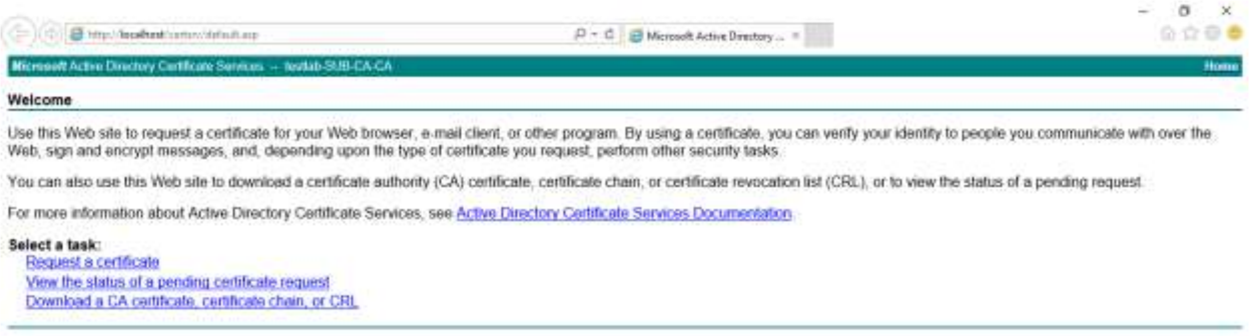
Console1 - [Console Root\Certificates (\\Sub-CA.testlab.local)\\\Sub-CA.testlab.local\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purpo
testlab.local	testlab-DOMAIN-SERVER-CA	8/24/2023	Server Authenti
testlab-DOMAIN-SERVER-CA	testlab-DOMAIN-SERVER-CA	8/22/2031	<All>
testlab-SUB-CA-CA	testlab-DOMAIN-SERVER-CA	8/22/2023	<All>

Advanced enrollment operations...

Requesting Certificates

In the previous step, we installed a feature called IIS that provides an internet service that will be used to connect to the network during setup of AD CS setup. A user or server can also request a certificate by going to the following address http://testlab.local/cert/default.asp.



http://localhost/certsrv/default.asp
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- testlab-SUB-CA-CA
Home

Welcome

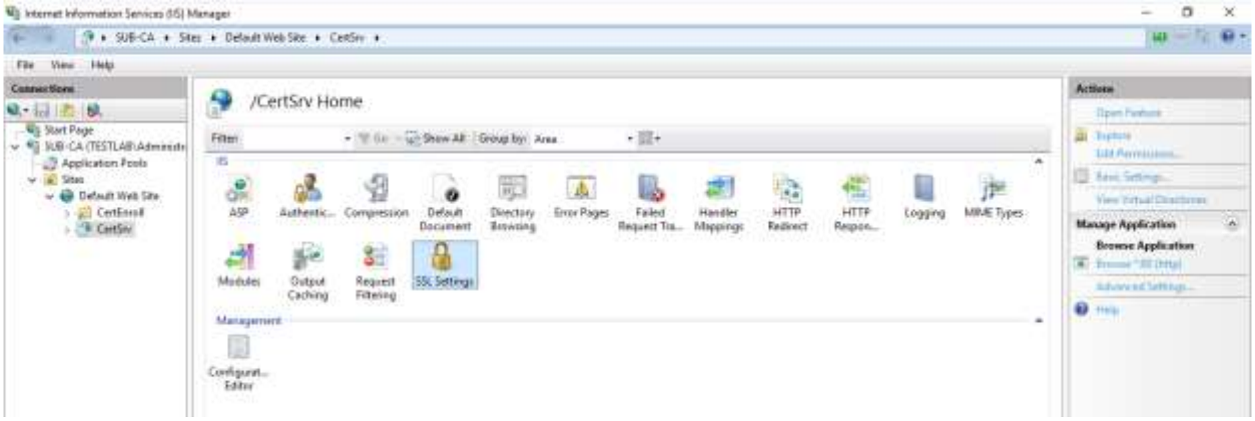
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security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

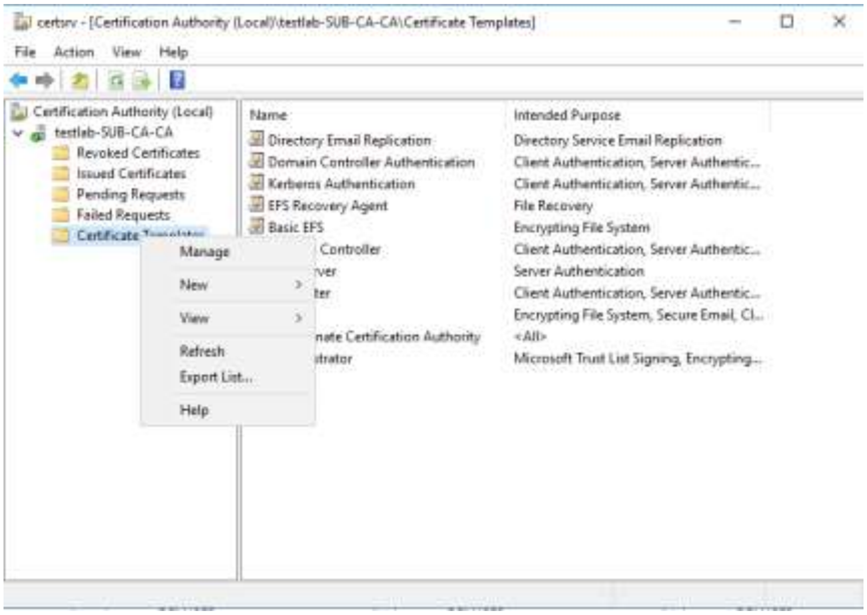
We can also open the IIS (Internet Information Services) to show the website status and ways to configure it to the requirements of the firm.



Later on in the research, TLS and SSL encryption will be made by a certificate that will be generated to create a secure interface for the network of the organization.

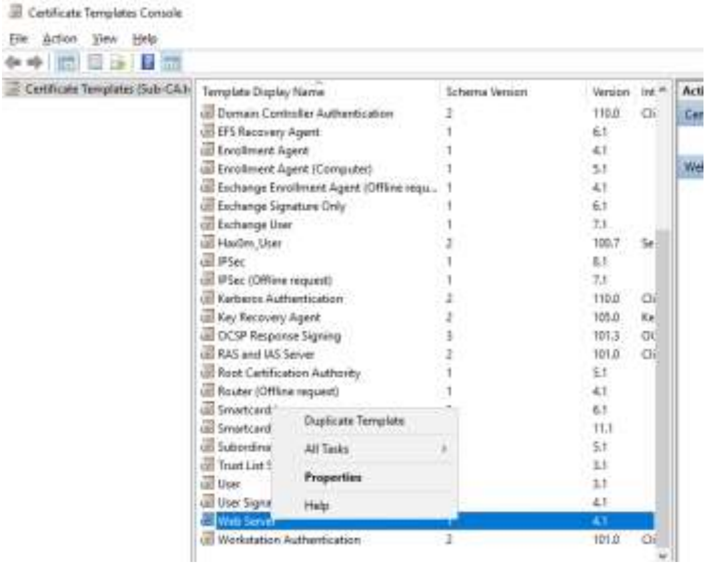
Creating Certificate Templates

We will firstly open Certification Authority where a template will be generated to create user templates such that certificates with the same settings, however, different setups can be generated. A template will be created to assign certification with the common settings desired to be chosen by the user or administrator. From **Server Manager → Tool → Certification Authority**, Certificate Templates will be **managed** to create a custom template.



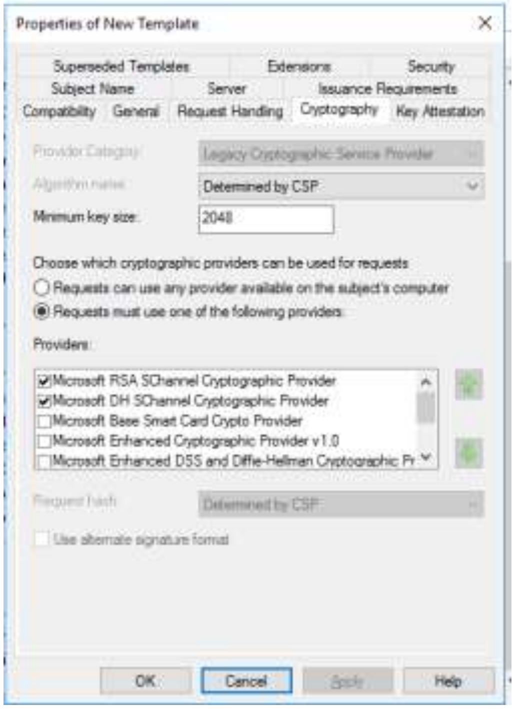
Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Controller	Client Authentication, Server Authentic...
rver	Server Authentication
ter	Client Authentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
nate Certification Authority	<All>
trator	Microsoft Trust List Signing, Encrypting...

From there, the Web Server Template will be duplicated as it already contains most of the features that needed to be added in a scratch template.



Template Display Name	Schema Version	Version	Int
Domain Controller Authentication	2	110.0	Cl
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	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
Hax0m_User	2	100.7	Se
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Cl
Key Recovery Agent	2	105.0	Ke
OCSP Response Signing	3	101.3	OC
RAS and IAS Server	2	101.0	Cl
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard		6.1	
Smartcard		11.1	
Subordina		5.1	
Trust List S		3.1	
User		3.1	
User Signa		4.1	
Web Server	1	4.1	
Workstation Authentication	2	101.0	Cl

From there, the Certification Authority compatibility will be **Windows 2008 R** and the compatible recipient will be **windows 7**. In **General**, the name of the template would be **Hax0mUser.** In **request handling**, exporting private key is set to True while in the **Security** tab, **Authenticated users** will be given enrol option. Lastly, **cryptography** will have the following settings:



Properties of New Template

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

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

● Requests must use one of the following providers:

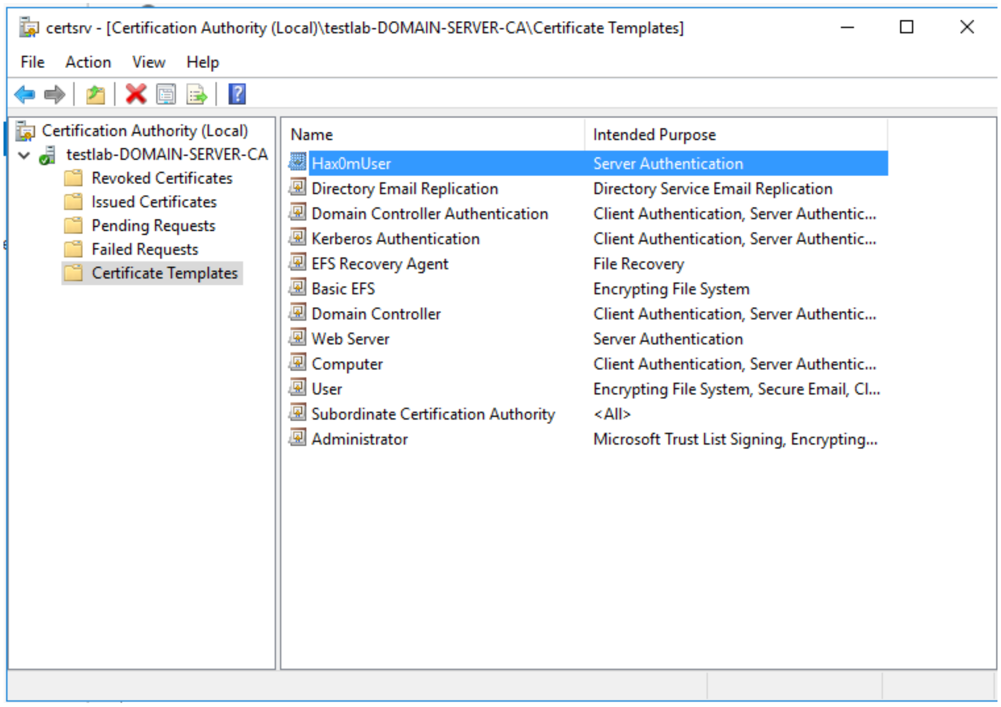
Providers:

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

Request hash: Determined by CSP

☐ Use alternate signature format

Once done, the newly created **Certificate Template** will be issued to the Server called **Hax0mUser**.

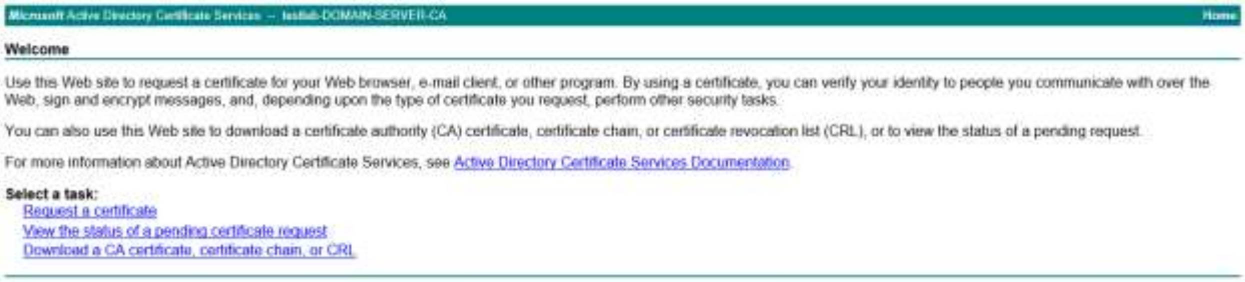


certsrv - [Certification Authority (Local)\testlab-DOMAIN-SERVER-CA\Certificate Templates]

Name	Intended Purpose
Hax0mUser	Server Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Issuing From Website

These certificates can also be assigned from the website which will be demonstrated in the following method.



Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-CA Home

Welcome

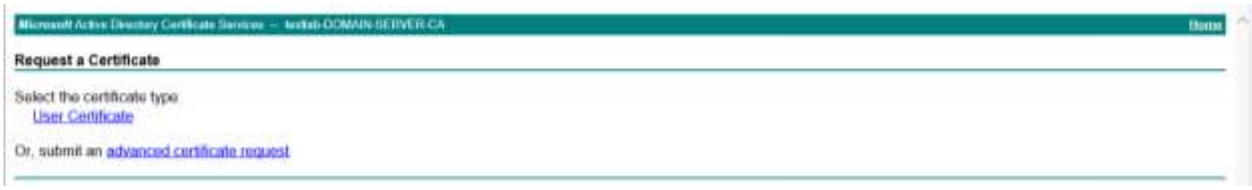
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security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

From here, a certificate will be requested and upon clicking of using advance certificates:



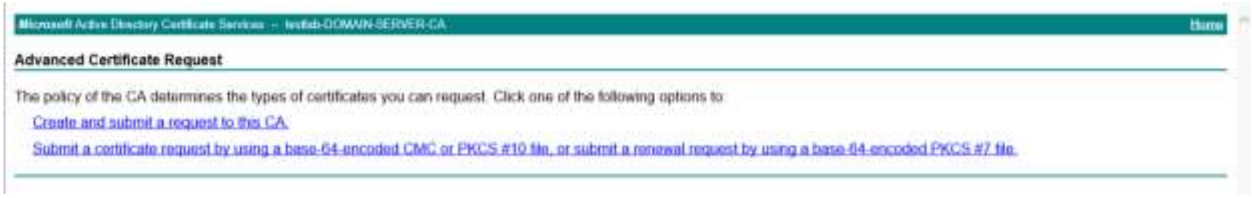
Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-CA Home

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Now, CA will be created and submitted to the server.



Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-CA Home

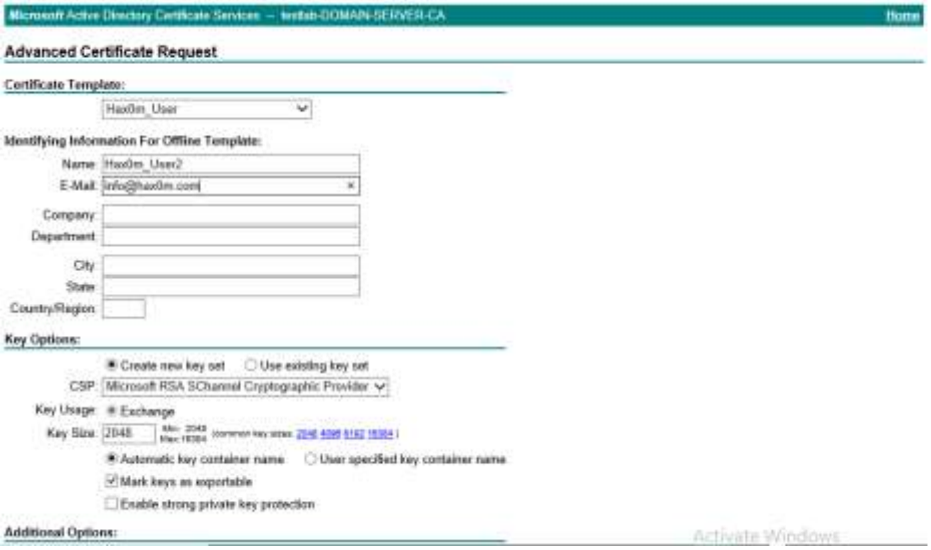
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Here a certificate template will be added for our **User2** (client computer):



Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-CA Home

Advanced Certificate Request

Certificate Template:

Hax0m_User

Identifying Information For Offline Template:

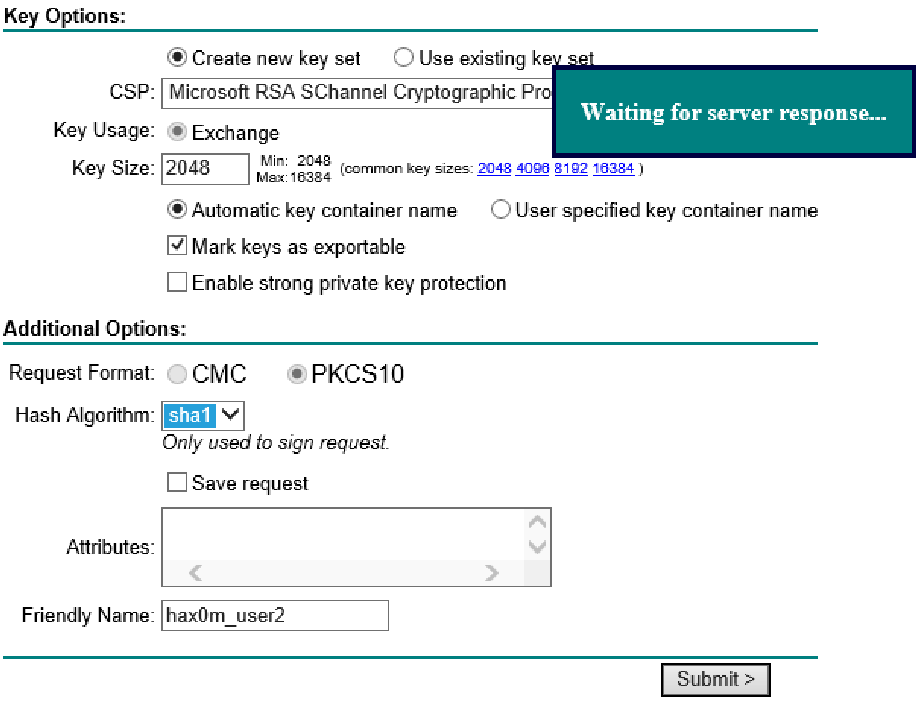
Name: Hax0m_User2
E-Mail: info@hax0m.com
Company:
Department:
City:
State:
Country/Region:

Key Options:

● Create new key set ○ Use existing key set
CSP: Microsoft RSA SChannel Cryptographic Provider
Key Usage: ● Exchange
Key Size: 2048 Min: 2048 Max: 16384 (common key sizes: 2048 4096 8192 16384)
● Automatic key container name ○ User specified key container name
☑ Mark keys as exportable
☐ Enable strong private key protection

Additional Options:

Once we press submit upon using the setting, we will obtain a response from the server that the process is being processed.



Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft RSA SChannel Cryptographic Pro

Waiting for server response...

Key Usage: ● Exchange

Key Size: 2048 Min: 2048 Max: 16384 (common key sizes: 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

□ Enable strong private key protection

Additional Options:

Request Format: ○ CMC ● PKCS10

Hash Algorithm: sha1

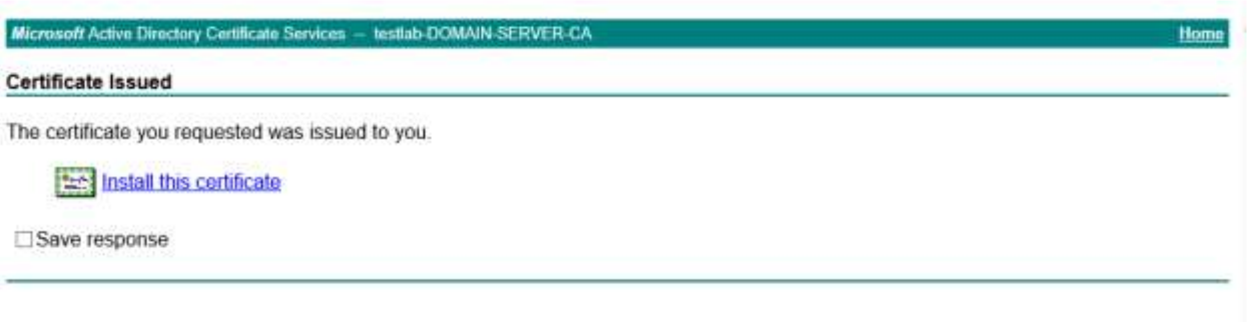
Only used to sign request.

□ Save request

Attributes:

Friendly Name: hax0m_user2

Lastly, the certificate will be installed which will be used to install the **Hax0mUser** template.



Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-CA
Home

Certificate Issued

The certificate you requested was issued to you.

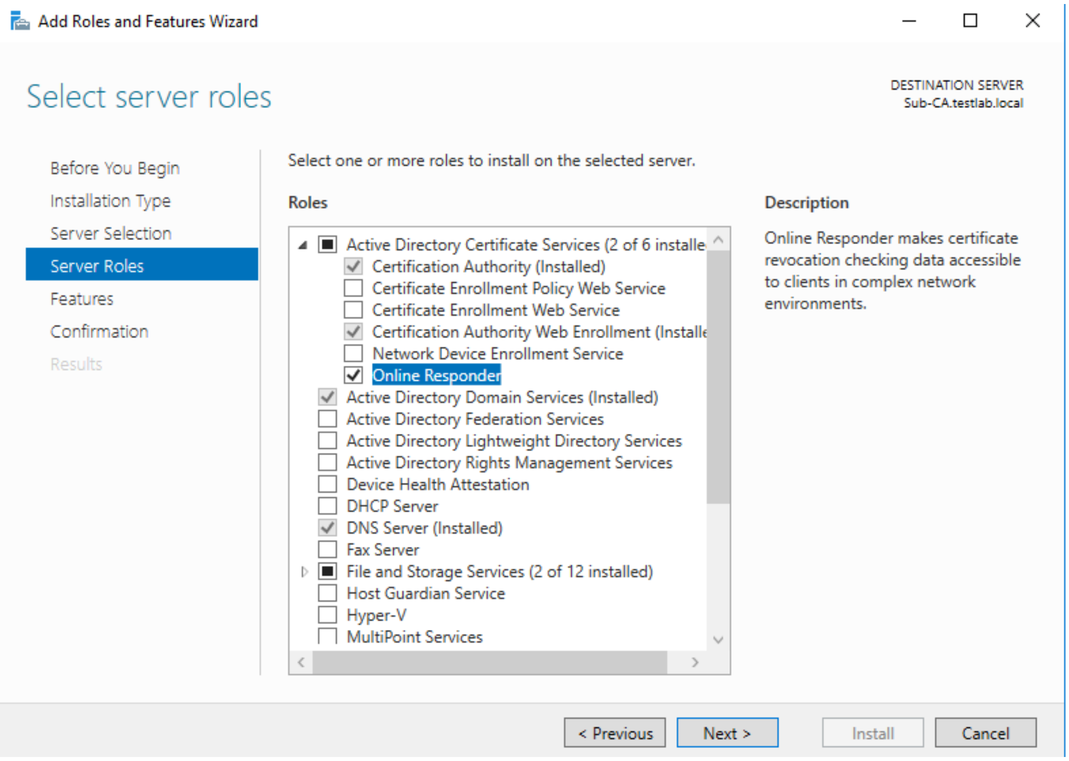
Install this certificate

□ Save response

Online Responder

OCSP Setup

In this stage, the OCSP will be set up. OCSP is used to respond to each client's request for getting the information on the status of the certificate provided to the user, and the amount of requests obtained from the client is constant regardless of how many certificates are revoked. To set up the OCSP, new features and roles wizards will be used.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
Sub-CA.testlab.local

Select one or more roles to install on the selected server.

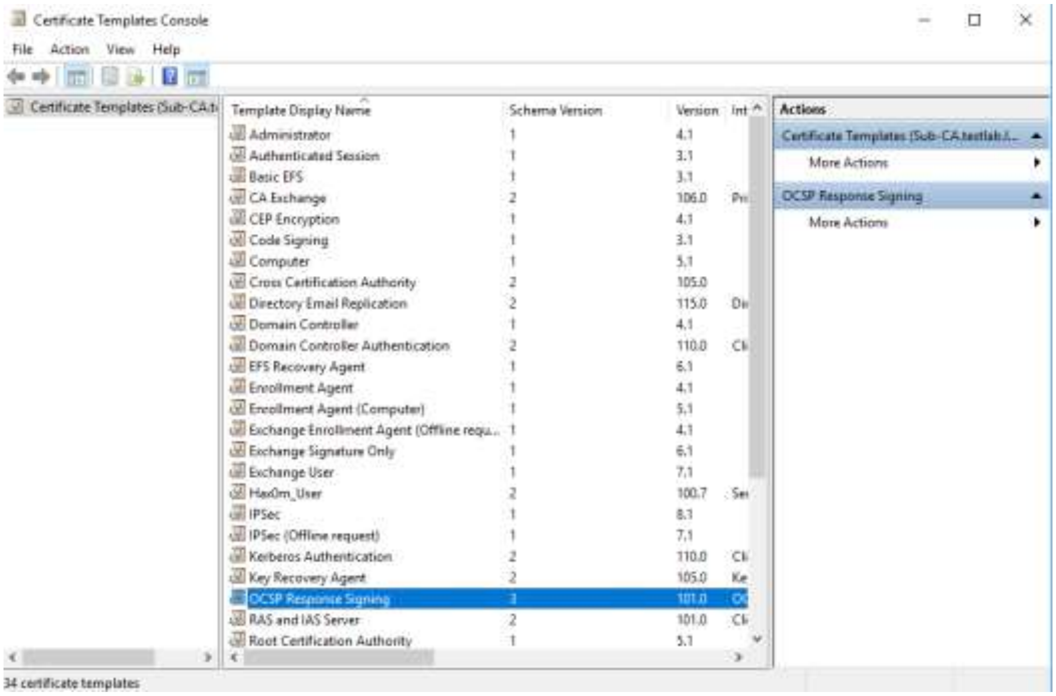
Roles

- ■ Active Directory Certificate Services (2 of 6 installe
  - ☑ Certification Authority (Installed)
  - □ Certificate Enrollment Policy Web Service
  - □ Certificate Enrollment Web Service
  - ☑ Certification Authority Web Enrollment (Installe
  - □ Network Device Enrollment Service
  - ☑ Online Responder
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services

Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

Once it is set up, the certificate template of OCSP will be configured from the **Certificate Authority** present in **Tools** of **Server Console**.



Certificate Templates Console

Template Display Name	Schema Version	Version	Int
Administrator	1	4.1	
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	Pr
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	Di
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Cl
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	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
Hax0m_User	2	100.7	Se
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Cl
Key Recovery Agent	2	105.0	Ke
OCSP Response Signing	3	101.0	OC
RAS and IAS Server	2	101.0	Cl
Root Certification Authority	1	5.1	

Actions

Certificate Templates (Sub-CA.testlab.l...

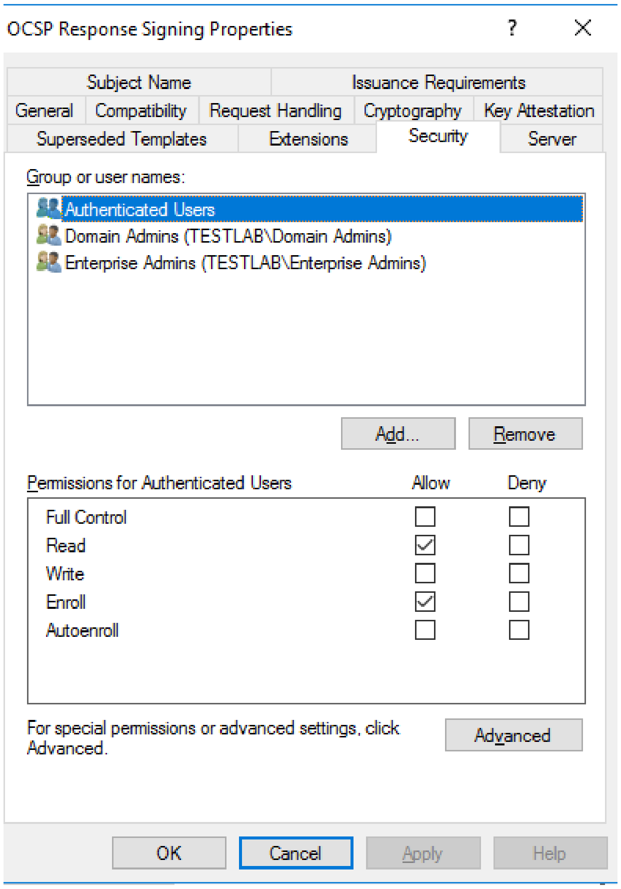
More Actions

OCSP Response Signing

More Actions

34 certificate templates

From its properties of it, in **Cryptography**, the maximum key size will be **4098** while in the **security** tab, authenticated users will be provided with the role of **Enroll.**


OCSP Response Signing Properties

Group or user names:

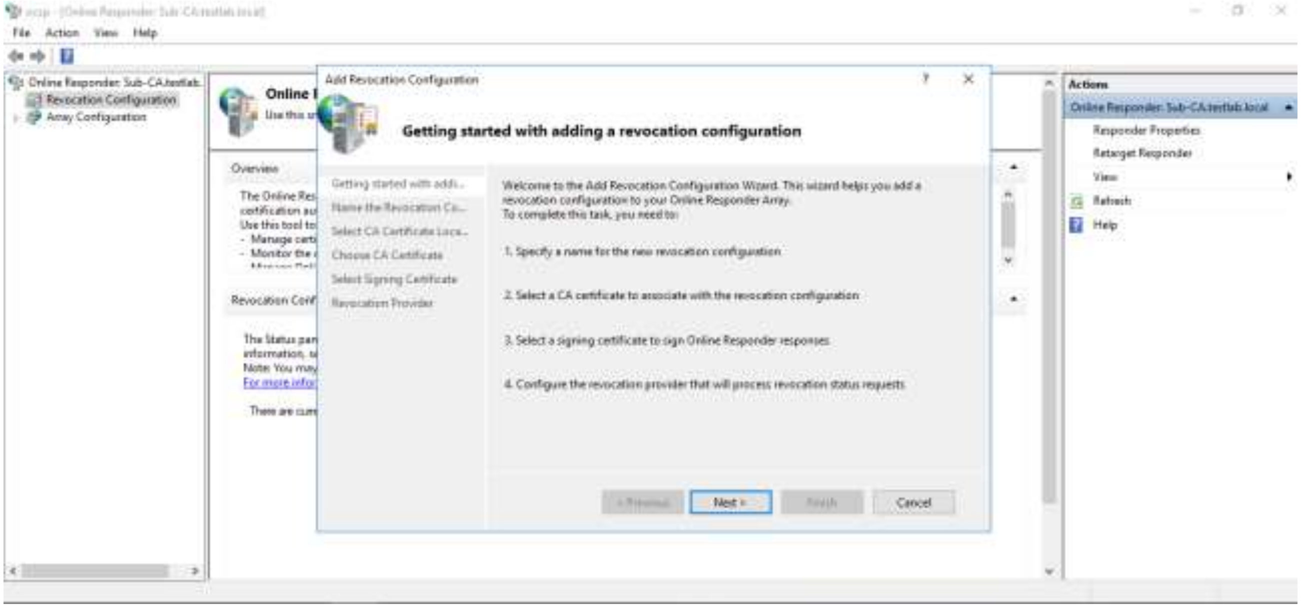
- Authenticated Users
- Domain Admins (TESTLAB\Domain Admins)
- Enterprise Admins (TESTLAB\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

OCSP Configuration

In this stage, the revocation will be configured from **Tools → Online Respondent Management**.


File Action View Help
Online Responder: Sub-CA.testlab...
Revocation Configuration
Array Configuration
Add Revocation Configuration
Getting started with adding a revocation configuration
Getting started with addi...
Name the Revocation Co...
Select CA Certificate Loca...
Choose CA Certificate
Select Signing Certificate
Revocation Provider
< Previous
Next >
Finish
Cancel
Actions
Online Responder: Sub-CA.testlab.local
Responder Properties
Retarget Responder
View
Refresh
Help

Welcome to the Add Revocation Configuration Wizard. This wizard helps you add a revocation configuration to your Online Responder Array.
To complete this task, you need to:

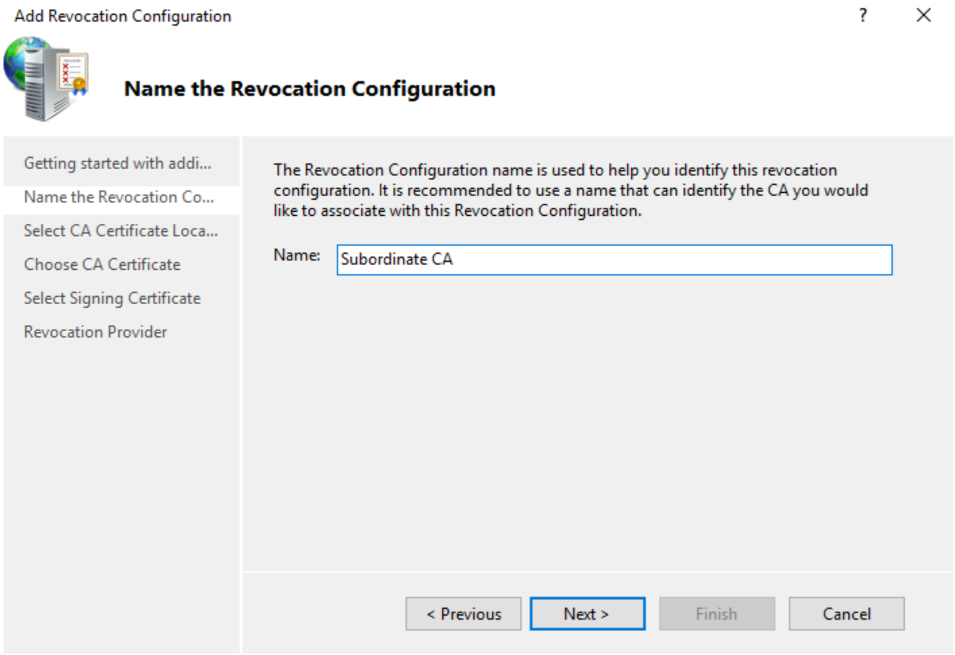
1. Specify a name for the new revocation configuration

2. Select a CA certificate to associate with the revocation configuration

3. Select a signing certificate to sign Online Responder responses

4. Configure the revocation provider that will process revocation status requests

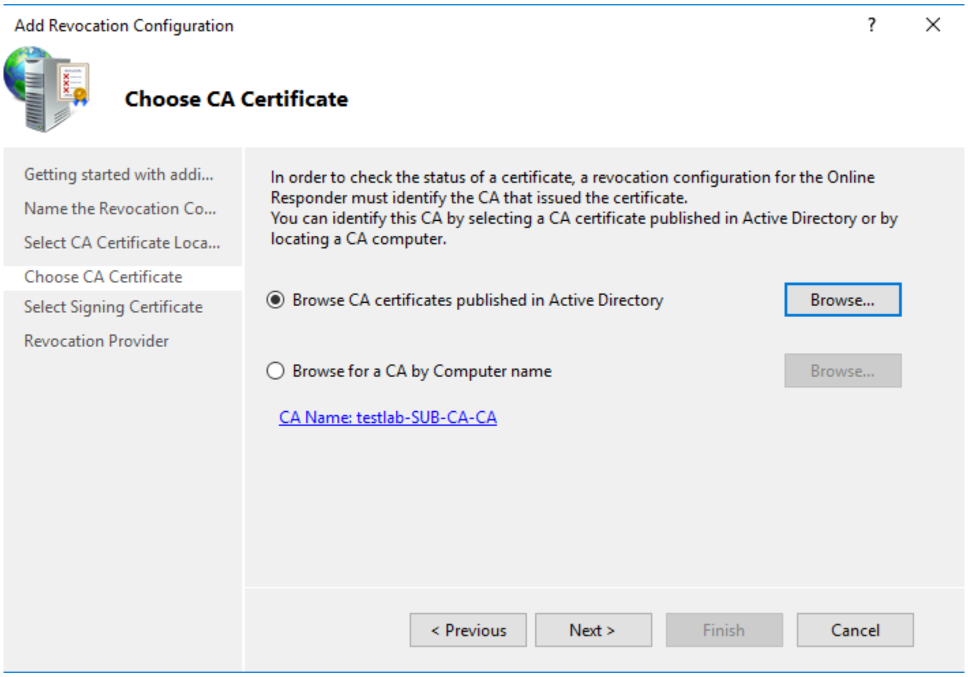
The name for the revocation would be **Subordinate CA**:


Add Revocation Configuration
?
Name the Revocation Configuration
Getting started with addi...
Name the Revocation Co...
Select CA Certificate Loca...
Choose CA Certificate
Select Signing Certificate
Revocation Provider
< Previous
Next >
Finish
Cancel

The Revocation Configuration name is used to help you identify this revocation configuration. It is recommended to use a name that can identify the CA you would like to associate with this Revocation Configuration.

Name: Subordinate CA

While CA certification will be chosen that was created in our past steps.


Add Revocation Configuration
?
Getting started with addi...
Name the Revocation Co...
Select CA Certificate Loca...
Choose CA Certificate
Select Signing Certificate
Revocation Provider
Browse...
Browse...
< Previous
Next >
Finish
Cancel

Choose CA Certificate

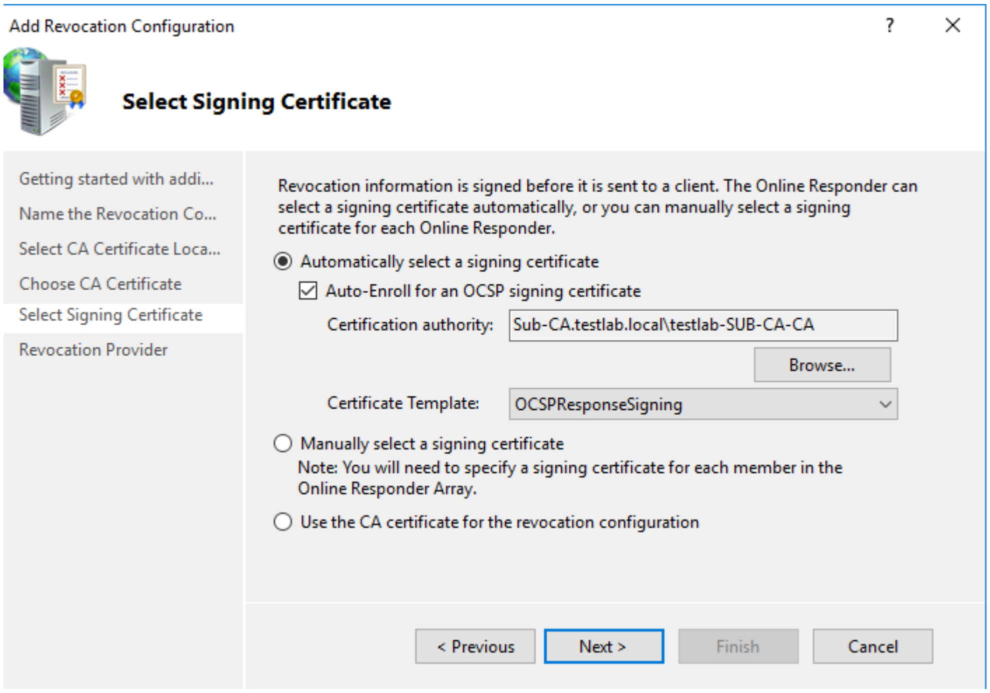
In order to check the status of a certificate, a revocation configuration for the Online Responder must identify the CA that issued the certificate.
You can identify this CA by selecting a CA certificate published in Active Directory or by locating a CA computer.

● Browse CA certificates published in Active Directory

○ Browse for a CA by Computer name

CA Name: testlab-SUB-CA-CA

Lastly, the following configuration will take place:


Add Revocation Configuration
?
Getting started with addi...
Name the Revocation Co...
Select CA Certificate Loca...
Choose CA Certificate
Select Signing Certificate
Revocation Provider
Browse...
< Previous
Next >
Finish
Cancel

Select Signing Certificate

Revocation information is signed before it is sent to a client. The Online Responder can select a signing certificate automatically, or you can manually select a signing certificate for each Online Responder.

● Automatically select a signing certificate

☑ Auto-Enroll for an OCSP signing certificate

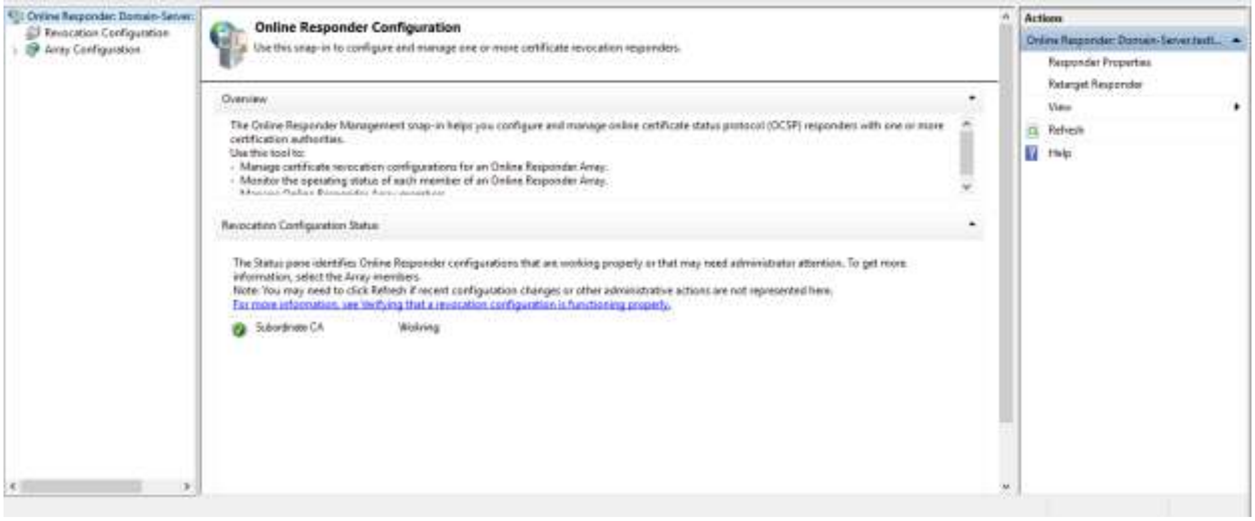
Certification authority: Sub-CA.testlab.local\testlab-SUB-CA-CA

Certificate Template: OCSPResponseSigning

○ Manually select a signing certificate
Note: You will need to specify a signing certificate for each member in the Online Responder Array.

○ Use the CA certificate for the revocation configuration

This in the end will show that the server is up and running.



Online Responder Configuration

Use this snap-in to configure and manage one or more certificate revocation responders.

Overview

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.

Revocation Configuration Status

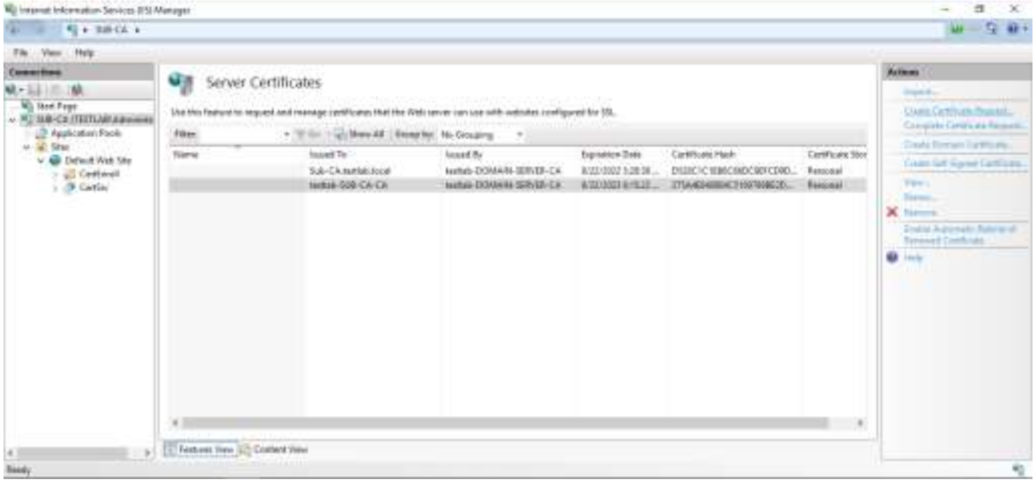
The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

Subordinate CA Working

Encryption SSL & TLS

Issuing Certificate

Certificates can be issued for the websites so that the certificates being obtained are obtained from a secure server, if not, they can alter, revoked, or even replace with original ones, with a lot more methods that can be used by the attacker. However, to protect it from being misused, SSL will be set up. Opening **IIS** from **Server Console's tools**, a new request will be made from the **Server Certificate** option.

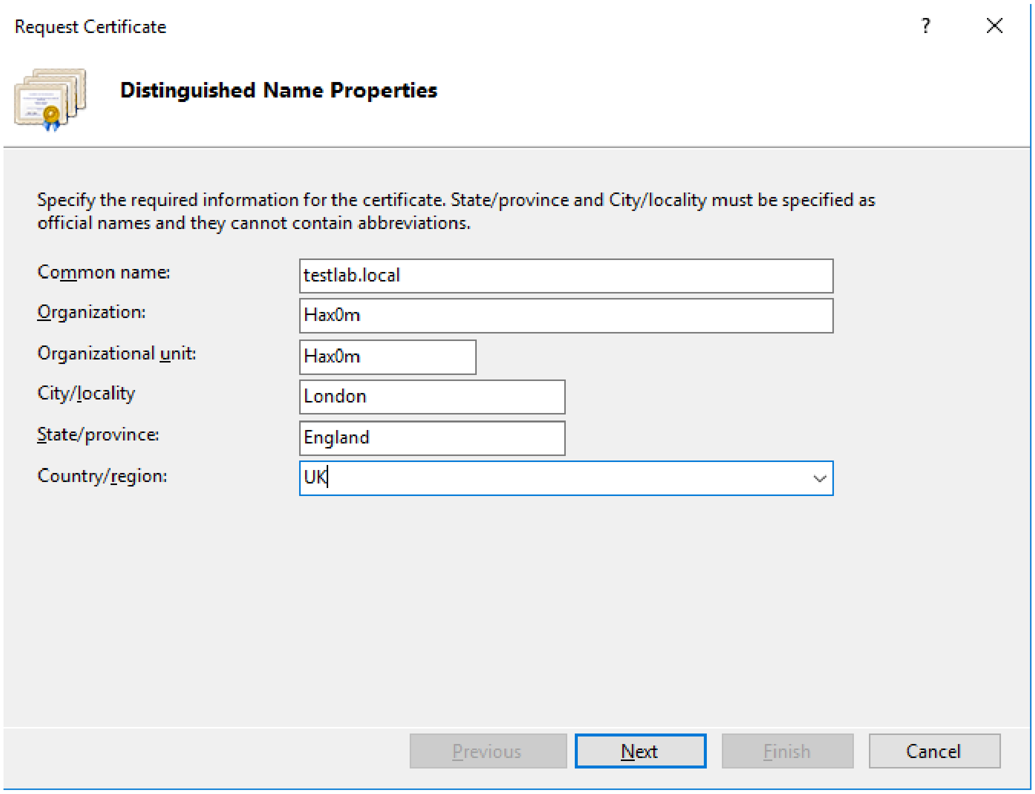

Internet Information Services (IIS) Manager
SUB-CA
File
View
Help
Connections
Start Page
SUB-CA (TESTLAB\Administrator)
Application Pools
Sites
Default Web Site
CertEnroll
CertSrv
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Renew...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Filter:
Show All
Group by:
No Grouping
Features View
Content View
Ready

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Stor
	Sub-CA.testlab.local	testlab-DOMAIN-SERVER-CA	8/22/2022 5:28:38 ...	D533C1C1EB6C6BDC9DFCD8D...	Personal
	testlab-SUB-CA-CA	testlab-DOMAIN-SERVER-CA	8/22/2023 6:15:22 ...	375A4D04B084C1107808D2D...	Personal

The following information will be added to the certificate.



Distinguished Name Properties

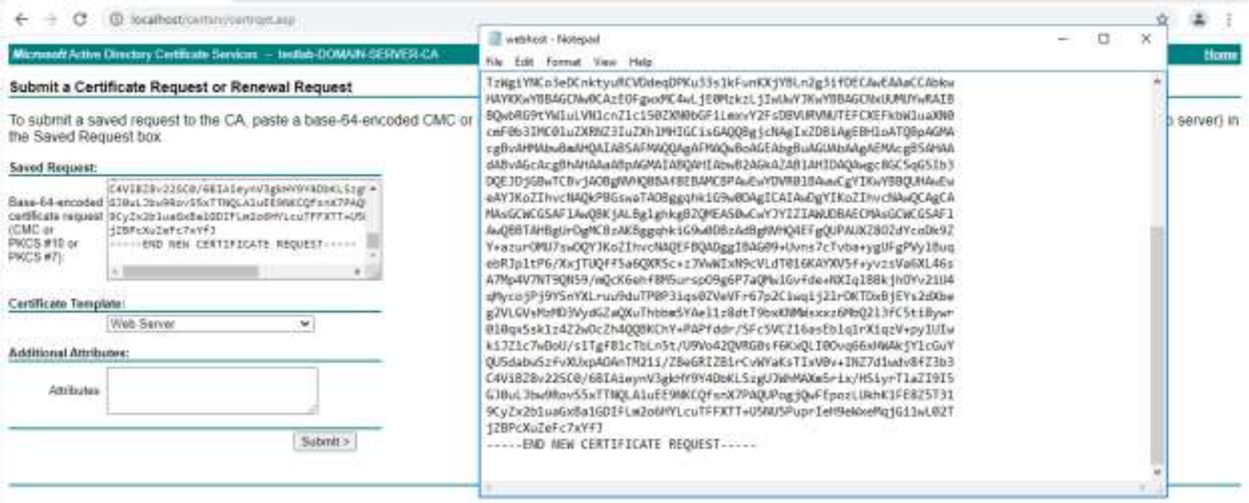
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	testlab.local
Organization:	Hax0m
Organizational unit:	Hax0m
City/locality	London
State/province:	England
Country/region:	UK

And use the bit length of **4098.** The certificate will be saved with the name webhost which will contain the certificate key. The certificate will now be generated by going to the website:

http://testlab.local/certsrv/certqxt.asp

The key in the file that was just saved will be input into the link address and submit will be pressed once the key has been added to generate a secure channel certificate for the server.



localhost/certsrv/certrqxt.asp
Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-CA
Home
webhost - Notepad
File Edit Format View Help

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or ... server) in the Saved Request box

Saved Request:

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

```
C4Vi828v22SC0/68IAieynV3gkHY9Y4DbKL5zg
GJ8uLJbw9Rov55xTTNQLA1uEE9NKCQfsnX7PAQ
9CyZx2b1uaGx8a1GDIFLm2o6HYLcuTFFXTT+U5
jZBPcXuZeFc7xYFJ
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

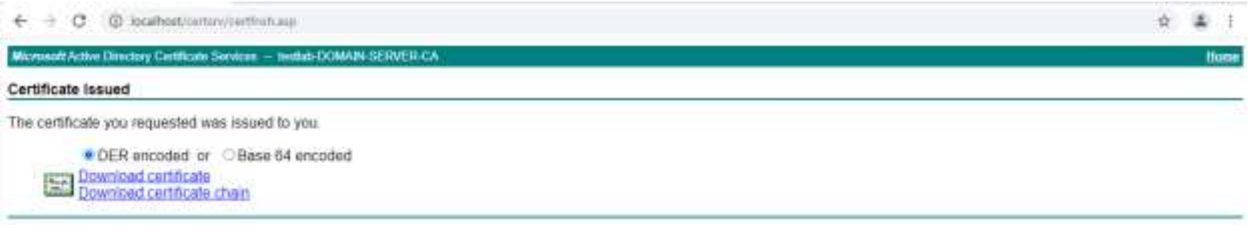
Web Server

Additional Attributes:

Attributes:

```
TzWgiYNKo3eDKnktyuRCVOdeqDPKu33s1kFunKKjY8Ln2g3ifOECAwEAAaCCAbkw
HAYKKwYBBAGCNw0CAzEOFgwxMC4wLjE0MzkzLjIwDwYJKwYBBAGCNxUUMUYwRAIB
BQwbRG9tYWluLVNlcnZlci50ZXN0bGF1LmxvY2FsDBVURVNUTEFCXEFkbWluaXN0
cmF0b3IMC01uZXRNZ3IuZXhlMHIGCisGAQQBgjcNAgIxZDBiAgEBHloATQBpAGMA
cgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAA
dABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZAB1AHIDAQAwgcBGCSqGSIb3
DQEJDjGBwTCBvjAOBgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYBBQUHAwEw
eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
MAsGCWCGSAFlAwQBKjALBglghkgBZQMEASBwCwYJYIZIAWUDBAECMAsGCWCGSAFl
AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUPAUXZ8O2dYcnDk9Z
Y+azurOMU7swDQYJKoZIhvcNAQEFBQADggIBAGA9+Uvns7cTvba+ygUFgPWy18uq
ebRJp1tP6/XxjTUQFf5a6QXRSc+z7WwWIxN9cVLdT016KAYXV5F+yvzsVa6XL46s
A7Mp4V7NT9QN59/mQcK6eh+F8M5ursp09g6P7aQMw1Gv+de+RXIq188kjhOYv21U4
sMycojPj9YSnYXLruu9duTP8P3iqs0ZVeVF+67p2Ciwq1j21rOKTDxBjEYs2dXbe
g2VLGVsMzMD3WydGZaQXuThbbm5YAe11z8dtT9bxKNMaixxz6MbQ213FC5ti8ywr
010qx5sk1z4Z2w0cZh4QQBKChY+PAPfddr/SFc5VCZ16asEb1q1rX1qzV+py1UIw
k1JZ1c7wDoU/s1TgFB1cTbLn5t/U9Vo42QVRGBsF6KxQLI0Ovq66xNWAkjY1cGuY
QU5dabwSzfvXUxpA0AnTM21i/Z8aGRIZB1rCvWYaKsTIxV8v+INZ7d1wdv8fZ3b3
C4Vi828v22SC0/68IAieynV3gkHY9Y4DbKL5zgUJWhMAXm5rix/HSiyrTlaZI9I5
GJ8uLJbw9Rov55xTTNQLA1uEE9NKCQfsnX7PAQUPogjQwFfpozLURhK1FE825T31
9CyZx2b1uaGx8a1GDIFLm2o6HYLcuTFFXTT+U5NU5PuprIeH9eWxeMqjG11wL02T
jZBPcXuZeFc7xYFJ
-----END NEW CERTIFICATE REQUEST-----
```

After submission, the response will be submitted and the certificate can be downloaded to be used in the IIS.



localhost/certsrv/certfnsh.asp

Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-CA

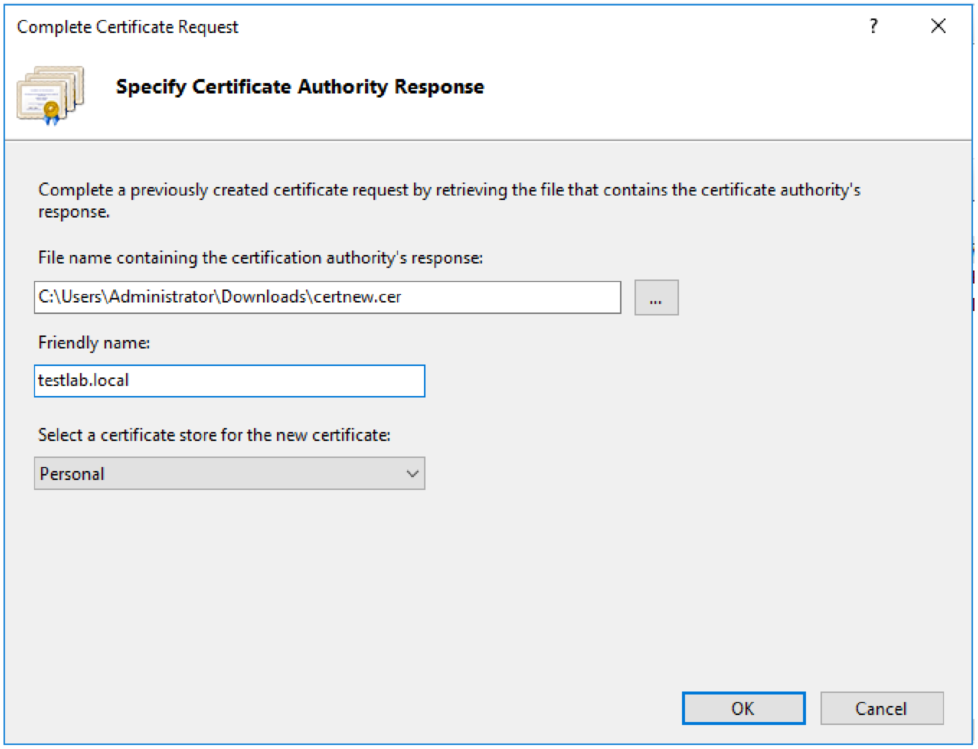
Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

As the certificate is downloaded, it can be installed in the similar way its key was made, that is by going to **SUB-CA → Security Certificates** and from the right pane, choosing the option **complete certificate request.**



Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\Users\Administrator\Downloads\certnew.cer

Friendly name:

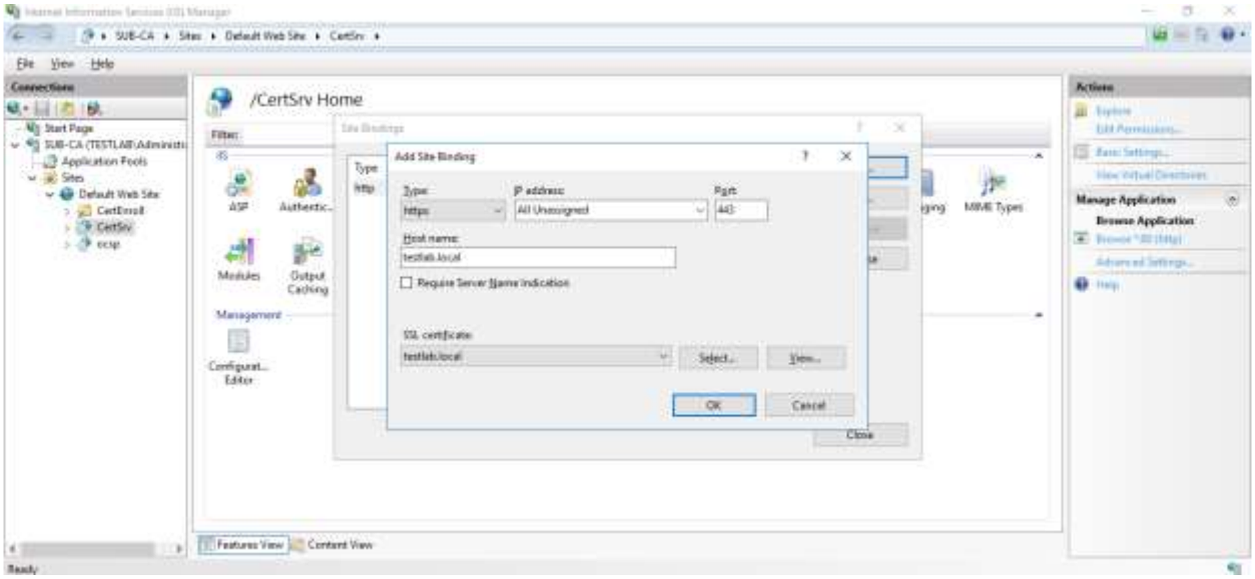
testlab.local

Select a certificate store for the new certificate:

Personal

SSL Encryption

To obtain the certificate, bindings will be made on **certsrv** by right-clicking and providing the following settings:



Add Site Binding

Type: https

IP address: All Unassigned

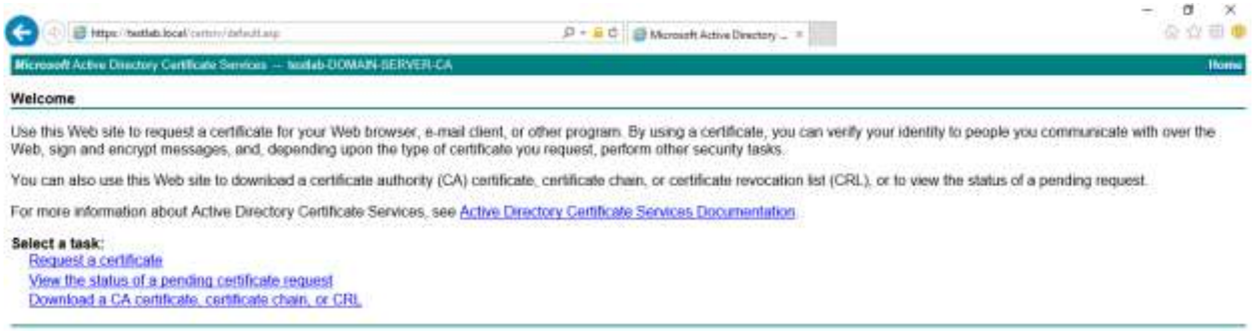
Port: 443

Host name: testlab.local

☐ Require Server Name Indication

SSL certificate: testlab.local

Now if the website is visited with an **HTTPS** response, the lock sign in the URL will be in view, showing that the website is SSL encrypted.


https://testlab.local/certsrv/default.asp
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- testlab-DOMAIN-SERVER-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

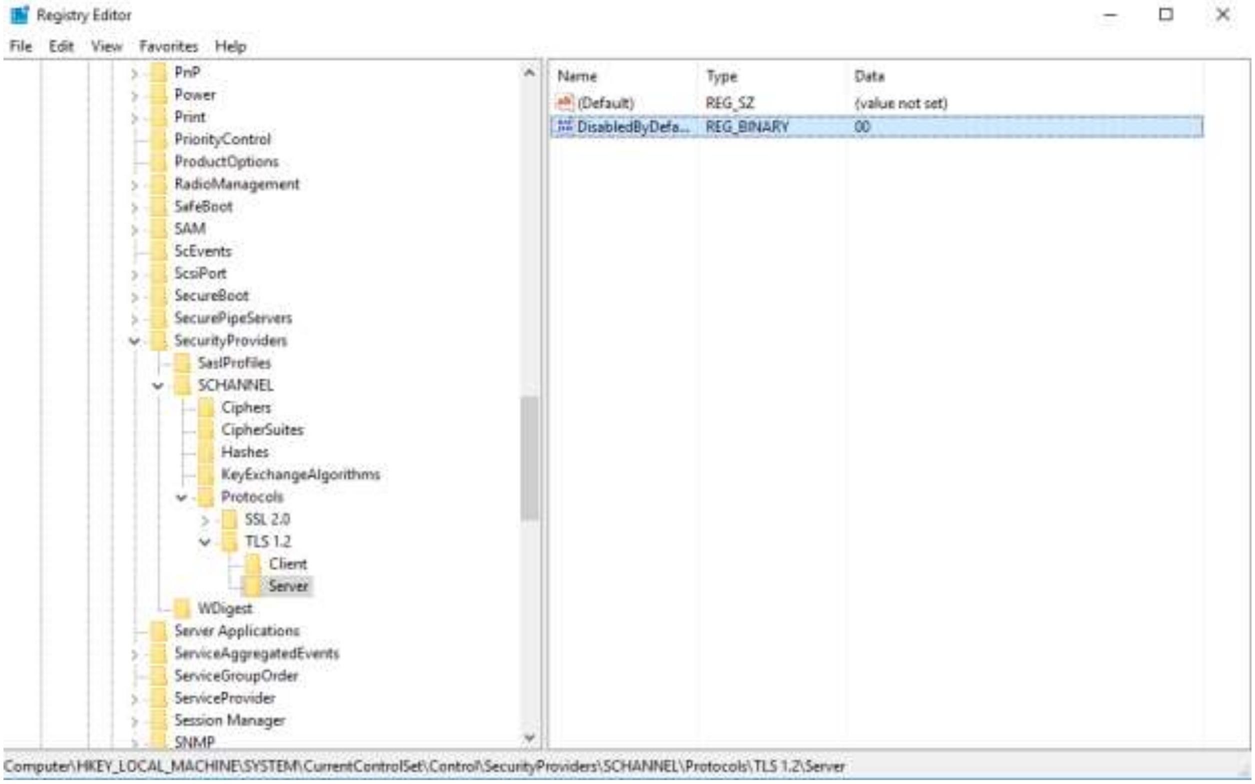
TLS Encryption

TLS can be enabled in a bit different way as it requires the use of a registry editor and it will be used for enabling the TLS encryption. By going to the following location in Regedit:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

a **Key** (folder in Regedit) will be created called TLS 1.2 by right-clicking on the Protocol folder. Within **TLS 1.2,** there will be two keys (Folders) will be made called **Client** and **Server.** For the server, DWORD (32-bit) Value will be made and named as **DisabledByDefault** and lastly, modify it. Its value will be set to 0.

For Clients, DWORD will be made and is named as **Enabled** where when modifying it, the value will be set to 1. Once the server is rebooted, it will now have TLS encryption enabled.



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefa...	REG_BINARY	00

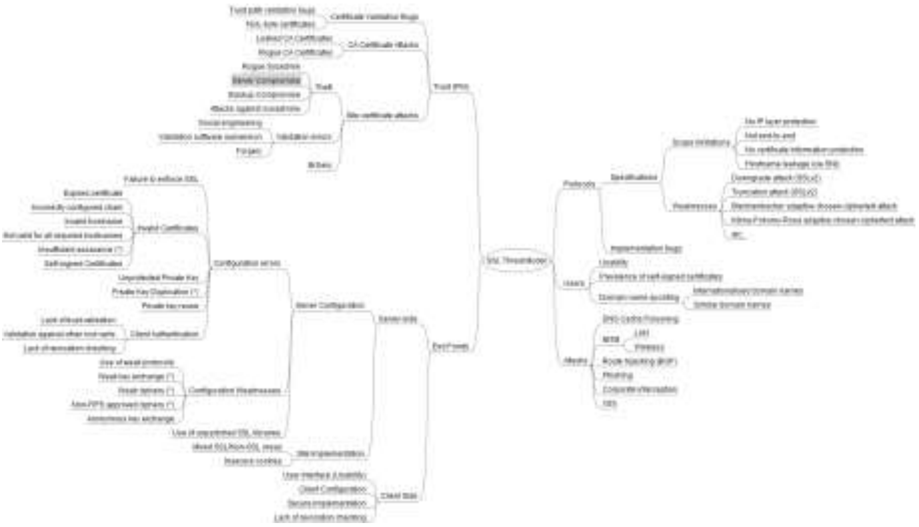
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

While observing for network abnormality, a network detection tool like Wireshark can also be used.

SSL PKI Threats & Ethical Considerations

SSL PKI Threat Model

We will be using this chart that shows the SSL Threat Model which explains the threats present within the SSL PKI Model.

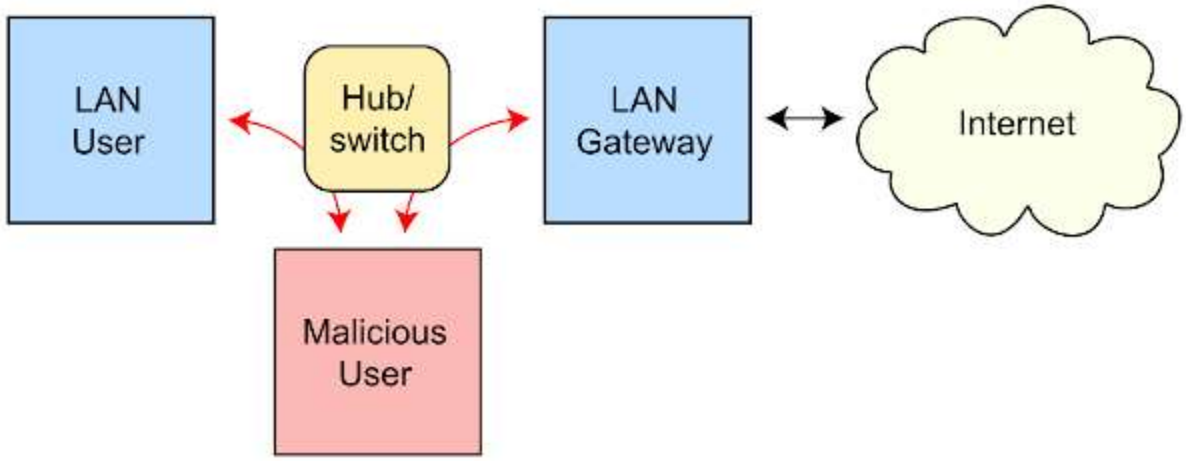


These threats are defined in detail as:

Threats in SSL PKI Architecture

Identity Spoofing Threats

Spoofing of identity takes place when a fraudster takes on another individual/identity entity and utilizes it to conduct fraud. Spoofer robs the credentials of individuals or companies by attacking passwords and capturing credentials. You utilize these credentials to assist the phishing, pharmaceuticals, theft of identities, and compromise on corporate email by relying on the confidence of the original identity. Identity falsification differs from content falsification, in that the spoofer seeks not to convey the content, but to "alter" the identity of the sender. This often results in a breach incorporating email and identity theft, which leads to the loss and/or harm of millions of companies [2].



All rights are linked to their respective owners [3]

Advanced Persistent Malware

Spoofing of identity takes place if a fraudster adopts the identity of someone else and utilizes that identity to conduct fraud. Spoofers Robb credentials of individuals or companies of password attacks and credentials. You are making use of such credentials to allow phishing, pharming, theft of identity, and the compromise of business e-mail (BEC). Spoofing of identity varies from spoofing of content, in that the spotter tries not to send material to "alter" the identity of the sender. These spoofs often lead to a compromising of company email and identity theft and cause millions in losses and/or damages to corporations.

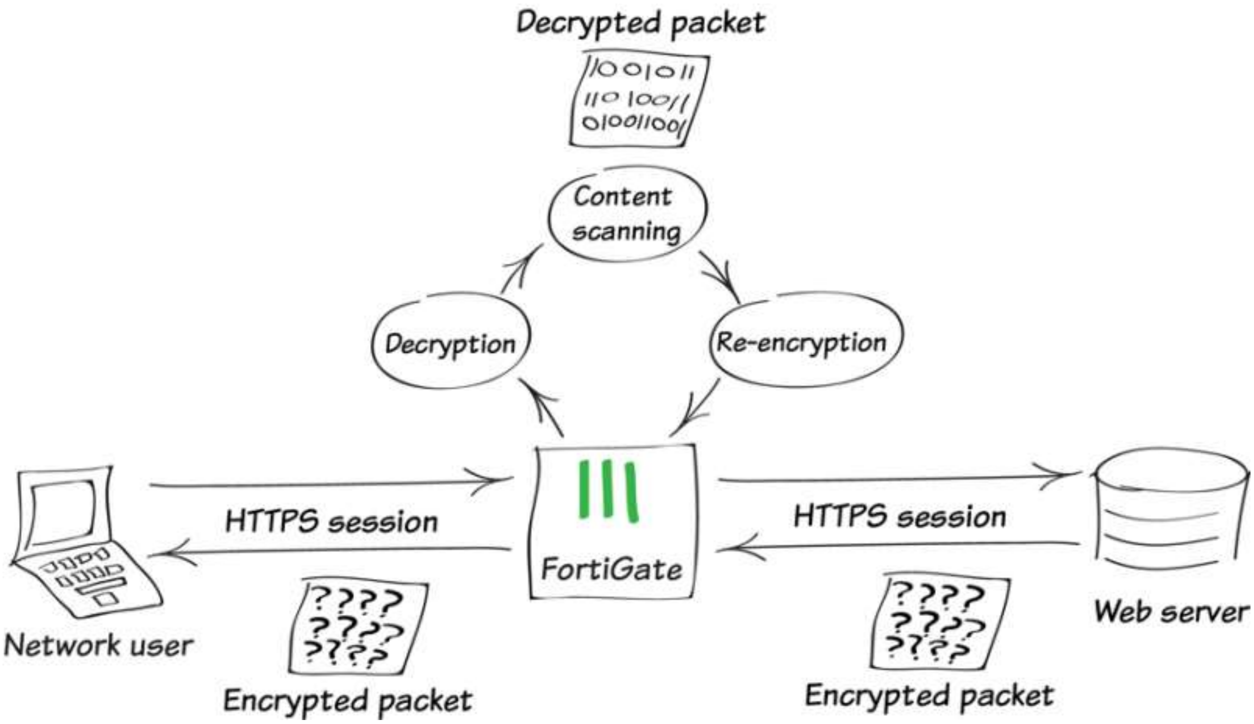
Another The use of malware to steal SSL/TLS keys and services in communications fraud and data exfiltration are increasingly being created. For example, APT operators using the Heartbleed virus stole cryptographic keys and certificates resulting in a compromise of 4.5 million patient records of the Community Health System. The Heartbleed Exploit was utilized to broaden the assault to the highly controlled patient recording against a system behind the CHS firewall [4].

Threats Against Encrypted Traffic

Confidence assaults using encrypted SSL/TLS traffic are becoming widespread and increasing in frequency, sophistication, and brazenness. SSL / TLS vulnerability is low-risk, high-rewards, ensuring that these developments continue and place companies in danger of breaches failed audits, and unexpected system downtimes. Some of the most frequent tactics, the impact on companies, and ideas for how to avoid them are described in the following instances.

Crypted traffic is increasing rapidly and becoming commonplace. Gartner reports that 15-25% of the whole online traffic is covered by SSL, representing a considerable percentage. This figure is noteworthy. SSL use depends on the industry but typically enables secret and sensitive information to be transmitted securely.

Then what is the issue? SSL may potentially cause a company security concern while providing secrecy and security to an individual session. Cybercriminals can utilize SSL to disguise their activities from security systems in a company, including firewalls, IPS, Unified Threat Management (UTM), secure online gateways, data loss prevention (DLP), malware control solutions, and more. Cybercriminals know well about the blind spots of SSL/TLS encryption and are exploiting SSL/TLS to disguise harmful contents, avoid detection and circumvent crucial safety safeguards [5].



All rights are linked to their respective owners [6]

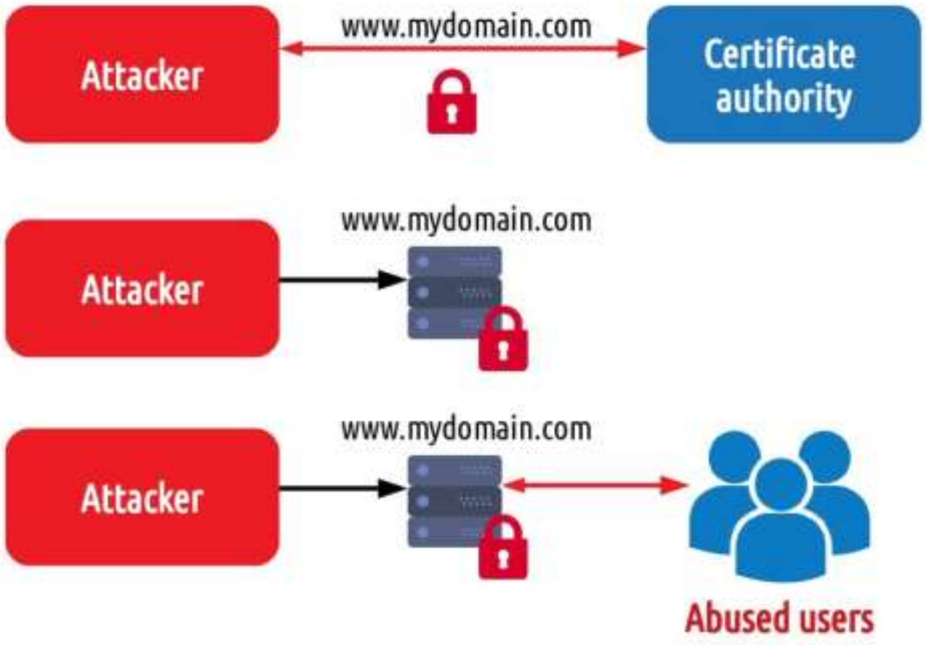
Security professionals know that visibility into and control over SSL traffic is a necessity. And just as importantly, failing to find, use, and secure ALL keys and certificates for decryption undermines existing critical security controls. These tasks are critical:

- Does the inbound traffic decrypt access to keys and certificates? Secure the keys and certificates required for the examination. If traffic is not decrypted and ALL key and certificate decryption is maximized, network assaults can avoid your current investment in security
- Automatic, safe access to all company keys and certificates enhances the quantity of decrypted transmission, allows SSL traffic analysis, and removes blind spots which are otherwise concealed in encrypted transportation. Every additional key and decryption certification implies fewer spots in SSL encrypted sessions for unfair actors to hide threats.
- Blue Coat and Venafi collaborated to assist companies to discover blind spots for encrypted SSL/TLS attacks. The SSL Sight Blue Coat Appliance with the integration of the Venafi TrustForce optimizes traffic to remove blind spots and can be decrypted and examined. Sure, and efficient, Venafi TrustForce provides keys and certificates to Blue Coat SSL visibility devices to reduce the administrative effort [5].

Certificate Authority Threats

In recent years, the PKI ecosystem in which machine identity is developed, maintained, and utilized has demonstrated its vulnerability, with certificates being misused by people, businesses, and governments being attacked.

The use of rogue digital certificates can lead to an attacker intercepting or spying on encrypted communication between the user's device and a safe HTTPS website, as explained in the first part of this blog series. However, hacked machine IDs cannot simply be utilized for monitoring. In the second piece I spoke about how these misleading or impaired digital certificates may also help distribute malware; abuse of the identity of a machine can enable attackers to avoid code signing, inspection, and security measures and access the target machines unnoticed.



All rights are linked to their respective owners [7]

Cybercriminals will often look for a clear reason for targeting the certificates authority (CAs) by themselves; you can, as an assailant, join (and disrupt) this trust circle with users who unknowingly share their personal and confidential information through this supposedly "safe" connection, if you can get their hands on officially signed certificate from CA [8].

Self-Signed and Wildcard Certificates

Server administrators often produce on-demand "wildcard" self-signed certificates using OpenSSL free. Although fast and simple, this approach severely undermines confidence, as no trustworthy CA third-party certificates have ever been verified.

Using a wildcard certificate on a web server in public raises the danger of cybercriminals hosting harmful websites in phishing campaigns. To address this problem, companies, in particular the public sector, should avoid the use of wildcards in production systems. Using subdomain certificates, instead, which are often cycled [4].

SSL client Threats

Man-in-the-Middle (MITM) Attacks

Successful MITM attacks win the confidence of communication parties through a reputable website and safe interactions. SSL/TLS key and certificate access make it easier for Mitm to attack because wireless access points are commonly used for entering unprotected or poorly protected access points.

A malicious actor can destroy SSL/TLS' confidence and start the MITM attack. There are numerous approaches. For example, a server key on a website may be taken so that the attacker may appear as a server. The issuing Certificate Authority (CA) is in certain circumstances hacked and the root key is taken to enable the criminals to create their root key certificates. In addition, MITM may be due to the inability of a client to validate the certificate against trusted CAs or to the compromising of a client and the injection of a fake CA on the client's trusted root authority. The malware performs this behaviour in numerous assaults using MITM to reroute visitors to phoney websites where sensitive information is available. Malware takes this measure in many MITM attacks to reroute visitors to phoney websites, which may easily rob critical information [4].

SSL Server Threats

SSL stripping

SSL stripping is a way where an HTTPS websites downfall to HTTP, making an attacker have an environment where he can enforce an SSL certificate. This method is known by the name SSL downgrading and can be used to expose data and for eavesdropping and manipulation of data. During the load of the site, HTTP is transmitted to HTTPS which for most sites is roughly about 1 second or less at most, however, it is entirely dependent upon server speed. Although in this small-time frame HTTP transmission to HTTPS can be used by the attacker to redirect to the HTTP version of the site, making the data go through a secure tunnel in plain text. Attacker, after decrypting the encryption layer can use the data to his/her desire [9].

Phishing Scams

Malicious actors in phishing mislead individuals to visit a website and submit confidential information in a form. You might be a large corporation, such as a bank or PayPal. When clients are led to a website not protected by SSL, they might discover it during a fraud. There is no locking icon or "HTTPS" in the URL bar of the website. If an SSL secures a website, users may click on the lock icon to view the safety certificate of the firm and check that it is legitimate. Some Web browsers also notify customers if they leave secure websites. SSL cannot prevent phishing entirely; however only authorised websites are made more cautious to browsers and customers [10].

Protected Private Key Threats

One of two kinds of keys in the public key architecture is private keys (or PKI). Private keys should be kept by their owners confidential, while public keys shall be made available for users to start encrypted communication.

For two reasons, private keys are important: 1) they help to decrypt and 2) all of the PKI trust stores in the market, from browsers to OS systems, are blindly reliant. Consequently, if hostile actors find a private key, important data will be exposed via the impersonation of the servers of one company. Indeed, ZScaler stated in its 2018 SSL Threat Report that encrypted payloads using false certificates with legitimate digital signatures increased by 30 percent. 1 Sadly, many companies are still not taking enough safety precautions to protect their private keys. They still use inefficient – and frequently non-compliant – manual methods of key management that allow their important information to be robbed [11].

Ethical Considerations (Protection Methods)

PKIs should generally ensure safety, availability and efficiency in authenticating domains by customers. This research will explain security measures for the above-described threat model:

Server Side

- **Authorized registration of the first certificate.** Only if the certificate meets the conditions laid out in the policy of the infrastructure should the infrastructure approve or register a domain certificate. For example, a certificate can be used as long as it is signed by a non-revoked CA in the root CA list of the client browser. As a second example, domain-centric infrastructure accepts an initial certificate issued by (a set of) authorized entities that are expressly declared confident by the domain owner. Note that there is no certificate registration concept for some PKIs, i.e. X.509.

- **Removal of Malicious traffic**: During the decryption of the data, any malicious traffic should be removed before any kind of malicious activity can be formed. During cyber threats, the IPs of attackers are often reused and a filter object can help in tracking such addresses and attacks.

- **Updates to the legitimate certificate.** The infrastructure should invalidate and replace the domain certificate only if the new certificate fulfils the requirements of the preceding certificate.

- **Attack visibility.** If an opponent conducts an assault on the infrastructure via search bodies successfully, the attack should be openly disclosed, so that it may be identified.

- **Instruments that are simple to operate:** The easy way to develop and manage policy for decryption is also a crucial aspect. In industries that must fulfil HIPAA, the PCI DSS, SOX and other requirements. This is crucial. The best systems include a drag and drop interface for filter creation and the ability to selectively forward or conceal pattern recognition information (such as social security numbers).

- **Tracking Certificates in use:** IT managers should verify the inventory completely and follow up with all of the certificates in use, including the authority that issued certificates, the systems that use certificates and their issuance and expiry dates.

- **Removing Earlier SSL versions:** Several vulnerabilities have been found in SSL protocols, in particular SSL 2.0. On the other side, once successfully breached, the strength of SSL

3.0 was also questioned. The safest protocol nowadays is the TLS yet it is not a susceptible protocol. However, more assurances are offered than their predecessors and the majority of browsers accept them.

- **Prevent CRIME Attack:** The CRIME attack is renowned for its ability in the compression process to decode a security link. To prevent such an is easy as it sounds, deactivating TLS compression.

- **Activate HSTS and check cookie security:** Special characteristics must safeguard all cookies involved in user sessions. This prevents interception of them. To extend security and avoid unencrypted communication to other websites, you must enable HSTS (Strict Transportation Security) on HTTP.

- **Limit private key storage:** On machines, storage of private keys should be limited and restrict access to them. To restrict user access, the utilization of directory systems can do the trick. While this approach is successful because of insufficient access control.

- **Encrypt private keys and save them in a folder secured by password** — this will leave the hacker to brute the password first later on he/she is required to decode the private keys. The breach will be discovered and the key contents modified and revoked at that time. Although successful, it remains very important in terms of the requirement to grow. This approach is also effective.

Client-Side

A client should be willing to take the following measurements to safe keep their data in case of a session hijack or exploit.

- **Staying Sharp:** Always keep looking at the signs of spoofing attacks and look out for the site address during purchase.

- **Hiding IP address:** VPNs can be used to prevent IP spoofing in terms of Identity Spoofing threats so VPNs should be considered.

- **Being wary of Attachments:** Users should give a keen eye over the extension of the file since a wrong extension can lead to allow the spread of malware or other threats.

- **Reporting Threats:** Any kind of spoofing attempts should be reported by email or helpline of the company.

- **Do not trust self-signed certificates:** An ideal usage of the SHA-2 hash technique creates a trustworthy certificate. Extensive validation certificates (EV) also provide websites with a higher degree of confidence. Most browsers indicate websites with EV in green.

Conclusion

In this exploration of data, we successfully implemented CA (Certificate Authority) for the company Hexad0m to make them allow the servers to provide security certificates to the users. Security methods and configurations are also defined to be used as notes to follow and get information on how it can be CA can be added.

From the research above, users and network administrators can gain insight into how a small lack of not focusing on an issue can turn out to be a greater issue in the end. The study also goes on its way explaining how users and network administrators can use easy to implement methods to create an easy solution for fighting the attackers over the network and which methods can be used to protect data from being spoofed, leaked, or even eavesdropped on.

References

[1] Digicirt, "Behind the Scenes of SSL Cryptography," Digicirt, 2013. [Online]. Available: https://www.digicert.com/faq/ssl-cryptography.htm.

[2] Fraud.net, "Identity Spoofing," Fraud.net, 2019. [Online]. Available: https://fraud.net/d/identity-spoofing/.

[3] D. Balaba, "11 Different Types of Spoofing Attacks to Be Aware Of," WebSitePlus, 2020 . [Online]. Available: https://www.websitepulse.com/blog/11-types-of-spoofing-attacks.

[4] Venafi, "Common SSL Attacks: SSL & TLS Key Vulnerability," Venafi, 2017. [Online]. Available: https://www.venafi.com/education-center/ssl/common-ssl-attacks.

[5] Venafi, "Is Your SSL Traffic Hiding Attacks?," Venafi, 2019. [Online]. Available: https://www.venafi.com/blog/your-ssl-traffic-hiding-attacks-0.

[6] Fortinet, "Why you should use SSL inspection," Fortinet Document Library, 2016. [Online]. Available: https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/605938/why-you-should-use-ssl-inspection.

[7] C. Bracos and T. Damonnevile, "CertStreamMonitor: use Certificate Transparency to improve your Threats Detection," SpeakerDeck, 2018. [Online]. Available: https://speakerdeck.com/cbrocas/2018bis-hack-it-n-certstreammonitor-use-certificate-transparency-to-improve-your-threats-detection.

[8] Venafi, "SSL/TLS Attacks, Part 3: Who’s at Risk from Compromised Digital Certificates?," Venafi, 2019. [Online]. Available: https://www.venafi.com/blog/ssl-attacks-part-3-whos-risk-compromised-digital-certificates.

[9] Venafi, "What Are SSL Stripping Attacks?," Venafi , 2018. [Online]. Available: https://www.venafi.com/blog/what-are-ssl-stripping-attacks.

[10] FTC, "How To Recognize and Avoid Phishing Scams," Federal Trade Commision, 2021. [Online]. Available: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

[11] R. Stubbs, "Cryptographic Key Management - the Risks and Mitigation," CryptoMathic, 2018. [Online]. Available: https://www.cryptomathic.com/news-events/blog/cryptographic-key-management-the-risks-and-mitigations.