Microsoft

Active Directory Certificate Services

2022 and 2025

Integration Guide

u.trust Anchor Se-Series

6.0.0, 6.1.1, and 6.2.0

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2025-11-20
Status	PUBLISHED
Document No.	IG-2025-0029

Table of Contents

1 Introduction 6
1.1 About This Guide 6
1.2 Target Audience 6
1.3 Document Conventions 6
1.4 Abbreviations 7
2 Overview 10
2.1 Microsoft Active Directory Certificate Services 10
2.2 Online Certificate Service Protocol 10
2.3 Utimaco CryptoServer HSM 10
3 Integration Requirements and Prerequisites 11
3.1 Tested Versions 11
3.2 Hardware and Software Requirements 11
3.3 Prerequisites 12
4 Software Download and Installation 13
4.1 Download Utimaco Software 13
5 Configuring the CSP-CNG Provider 14
5.1 Introduction and Prerequisites 14
5.2 Creating HSM Users 14
5.2.1 Creating a Key Manager User 14
5.2.2 Creating a Crypto User 15
5.3 Setting up the CSP/CNG Provider 17
5.3.1 Testing Connection 20
6 Installing Microsoft AD CS with Windows Enterprise 22
6.1 Installing and Configuring the AD CS 22
6.2 Testing the AD CS 34
7 Install and Configure AD CS with Windows Server Core 38
8 Configuring the Auto-Enrollment Group Policy for a Domain 40
9 Configuring the Certificate Enrollment to use CA templates on the AD CS Server 44
10 Private Key Archiving and Recovery 52
10.1 Archive the CA Key 52
10.1.1 Archiving Process 52

10.1.2 Add a Key Recovery Agent (KRA) template to CA ... 52
10.1.3 Issue the Key Recovery Agent Certificate ... 55
10.1.4 Issue the KRA Certificate ... 57
10.1.5 Retrieve the issued certificate from CA ... 58
10.1.6 Configure the CA to support Key Archival ... 60
10.1.7 Create a Template with Key Archival Enabled ... 61
10.1.8 Add a new Template to CA for Issuing ... 64
10.1.9 Issue a user template with key archival enabled ... 65
10.2 Perform Key Recovery ... 68
11 Migrating the Microsoft Software Key of AD CS to Utimaco HSM ... 71
11.1 Installing AD CS with Locally Stored Primary Key ... 71
11.2 Create a Backup of CA Database ... 83
11.3 Importing Private Key to HSM ... 83
11.4 Synchronizing HSMs ... 84
11.5 Reintroduce the Certificate ... 86
11.6 Configuring AD CS to Use Utimaco CryptoServer Key Storage Provider ... 88
12 Installing and Configuring the AD CS Failover Cluster ... 90
12.1 Installing AD CS Server role on first cluster node ... 90
12.2 Detach the shared storage form the first cluster node ... 94
12.3 Import MBK and Restore the databases on second cluster node ... 94
12.4 Installing AD CS Server role on second cluster node ... 96
12.5 Installing Failover Cluster feature on both the cluster nodes ... 99
12.6 Create a Failover Cluster ... 102
12.7 Configure Role for ADCS Failover ... 104
12.8 Creating the CRL Objects in Active Directory ... 106
12.9 Updating the CA configuration in Active Directory ... 107
13 Online Certificate Status Protocol Service ... 109
13.1 Prepare certificate template for OCSP Signing ... 109
13.2 CA Configuration ... 113
13.3 Request a certificate from OCSP Response Signing template ... 114
13.4 Install and configure Online Responder ... 119
13.5 Make a Revocation Configuration ... 123
13.6 Test the Online Responder ... 126
14 Further Information ... 127

15 References 128

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All of Utimaco SecurityServer product documentation is available from Utimaco's website at https://utimaco.com/.

1.1 About This Guide

This guide describes how to enable HSM integration with Microsoft Active Directory Certificate Services (AD CS) including installation and set-up of Microsoft CA and integration with Online Certificate Service Protocol (OCSP). For more detailed information regarding Microsoft Active Directory Certificate Services and Online Certificate Service Protocol, please refer to the documentation provided by Microsoft.

1.2 Target Audience

This guide is intended for Microsoft AD CS and OCSP administrators and HSM administrators.

1.3 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the **OK** button.
`Monospaced`	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file `example.conf` in the `/exmp/demo/ directory`.

Convention	Use	Example
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *u.trust Anchor - csadm Manual* or [CSADM].

Table 1: Document Conventions

Special icons are used to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

1.4 Abbreviations

Abbreviation	Meaning
AIA	Authority Information Access
AD CS	Active Directory Certificate Services
CA	Certificate Authority
CAT	CryptoServer Administration Tool
CER	Certified Emissions Reductions

Abbreviation	Meaning
CLI	Command Line Interface
CNG	Cryptography API Next Generation
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HSM	Hardware Security Module
KRA	Key Recovery Agent
MBK	Master Backup Key
MMC	Microsoft Management Console
OCSP	Online Certificate Service Protocol
PS	PowerShell
RSA	Rivest-Shamir-Adleman

Abbreviation	Meaning
URL	Uniform Resource Locator

Table 2: Abbreviations

2 Overview

2.1 Microsoft Active Directory Certificate Services

A Microsoft Active Directory Certification Authority is responsible for attesting to the identity of users, computers, and organizations. The CA authenticates an entity and vouches for that identity by issuing a digitally signed certificate. The CA can also manage, revoke, and renew certificates. The CA can be public or private. A public CA provides certification services, typically for a fee, to the public over the Internet. A private CA provides this service to the members of a delimited population such as the employees of a business or members of some other private group.

If the security of the generated keys and certificates needs to be enhanced, the Microsoft Active Directory Certification Authority needs to be configured to use a Hardware Security Module (HSM). When the HSM module is enabled with Microsoft Active Directory Certification Authority, this strengthens the protection of keys and certificates.

2.2 Online Certificate Service Protocol

Online Certificate Status Protocol is an Internet Protocol and is used by certificate authorities to check the revocation status of specific digital certificates. The Online Responder Service is the component by Microsoft Windows service that is responsible for managing the configuration of OCSP responder by retrieving revocation information from revocation providers, signing responses, and auditing changes to the configuration of the OCSP responder.

The OCSP and CA uses Utimaco HSM for performing different operations like key generation, certificate signing, CRL signing and protecting their private keys.

2.3 Utimaco CryptoServer HSM

CryptoServer is a hardware security module developed by Utimaco IS GmbH. CryptoServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Integration Requirements and Prerequisites

Ensure the system environment you will be using meets the following hardware and software requirements.

3.1 Tested Versions

These are the integrations that have been successfully tested with the Utimaco HSM and the Microsoft Active Directory Certificate Services (AD CS).

Operating Systems	Utimaco Security Server Version	Utimaco HSM
Windows Server 2019 Windows Server 2016 Windows 2012 R2	Security Server 4.45.5.0	CryptoServer CSe-Series/Se-Series

Table 3: List of Tested Versions

3.2 Hardware and Software Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.45.5.0 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.45.5.0 or higher

Table 4: List of Hardware Requirements

Software	Software Requirements
Java	Version 8, Update 271 or higher
HSM Interfaces	CSP/CNG

Table 5: List of Software Requirements

Set up an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com/

3.3 Prerequisites

Before you begin, please ensure that you have:

Before you begin, please ensure that you have installed/setup:

- Operating system listed in Tested Versions
- SecurityServer listed in Tested Versions
- CryptoServer Default Admin should be replaced with a new admin user
- MBK must be created and stored onto each HSM. Refer the CryptoServer documentations to setup the MBK
- CryptoServer is setup and configured. Refer the CryptoServer documentations to setup the HSM
- If you are using Smartcard Authentication, make sure to install PIN PAD Driver through SecurityServer software file, configure PIN PAD and start PIN Pad Daemon. Refer to the CryptoServer documentations for more information about PIN PAD driver installation and configuration.
- Microsoft SDK Installed and configured listed in Tested Versions

4 Software Download and Installation

This section describes the process of installing Utimaco HSM software with Microsoft AD CS and OCSP.

4.1 Download Utimaco Software

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation.

If you have purchased an HSM from Utimaco, locate the included product bundle, which contains the Linux software packages.

Install the latest version of the CryptoServer software as described in the CryptoServer Manual for the HSM. We recommend that you uninstall any CryptoServer software before installing the new software.

5 Configuring the CSP-CNG Provider

5.1 Introduction and Prerequisites

A CSP (Cryptographic Service Provider) is a general-purpose cryptography standard, developed by Microsoft. On one side it defines a cryptographic interface to be used by applications (CryptoAPI). On the other side it defines an interface to be used by manufacturers to integrate their cryptographic hardware.

A CNG (Cryptography API Next Generation) is the second-generation cryptographic interface, developed by Microsoft. It offers updated cryptographic algorithms and is intended for a long-term replacement of CSP.

When installing the CryptoServer Setup make sure to select the CPS/CNG - Cryptographic Service Provider (Microsoft) interface. A Cryptographic User should be created as well as an MBK should be generated.

Generating the MBK is necessary for the HSM to become operational. Without the MBK one cannot run any cryptographic operations.

5.2 Creating HSM Users

Start the CryptoServer Administration Tool and login a user with the permission level of at least 02000000.

5.2.1 Creating a Key Manager User

If the Key manager and Crypto user roles are separated, a Key Manager user might need to be created.

More users with the permission level 00000010 might be needed (Group 1) to enforce "m of n" security policy for the key management and smart card authentication might need to be used.

For this guide only one Key Manager User will be created.

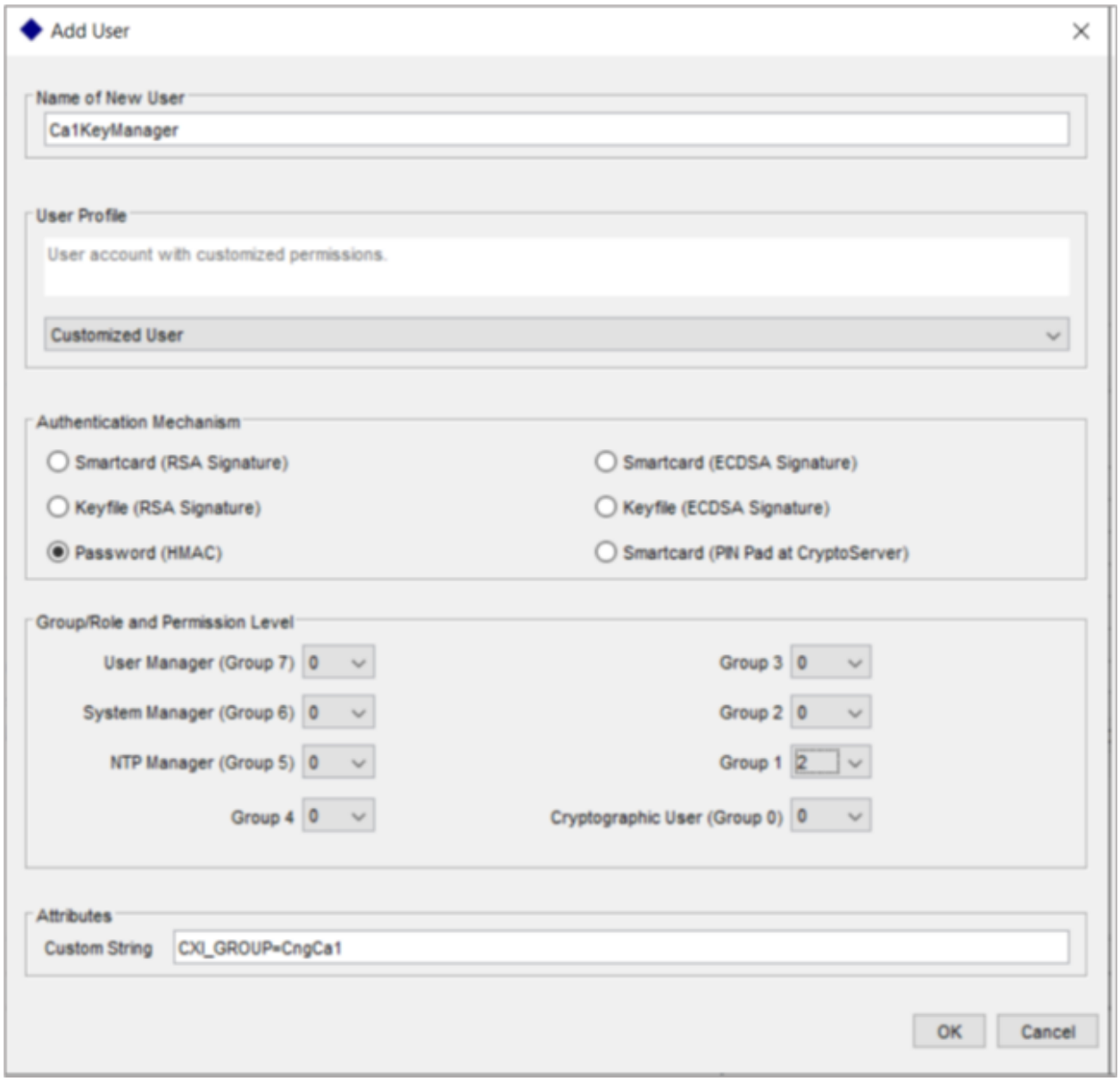

Figure 1: Creating Key Manager User

5.2.2 Creating a Crypto User

When a Root CA with Subordinates is created, smart card authentication and the "m of n" rule with permission level of 00000001 needs to be used. Because issuing certificates for subordinate CAs is not an automated task, smart card authentication allows higher level of security to be achieved.

For subordinate CAs, where certificates are issued automatically, the credentials will have to be stored in the .cng configuration file and Crypto Users with permission level of 00000002 will

have to be created. Use encrypted passwords. For this guide, a user with permission level of 00000002, CXI Group "CngCa1" and HMAC password will be created.

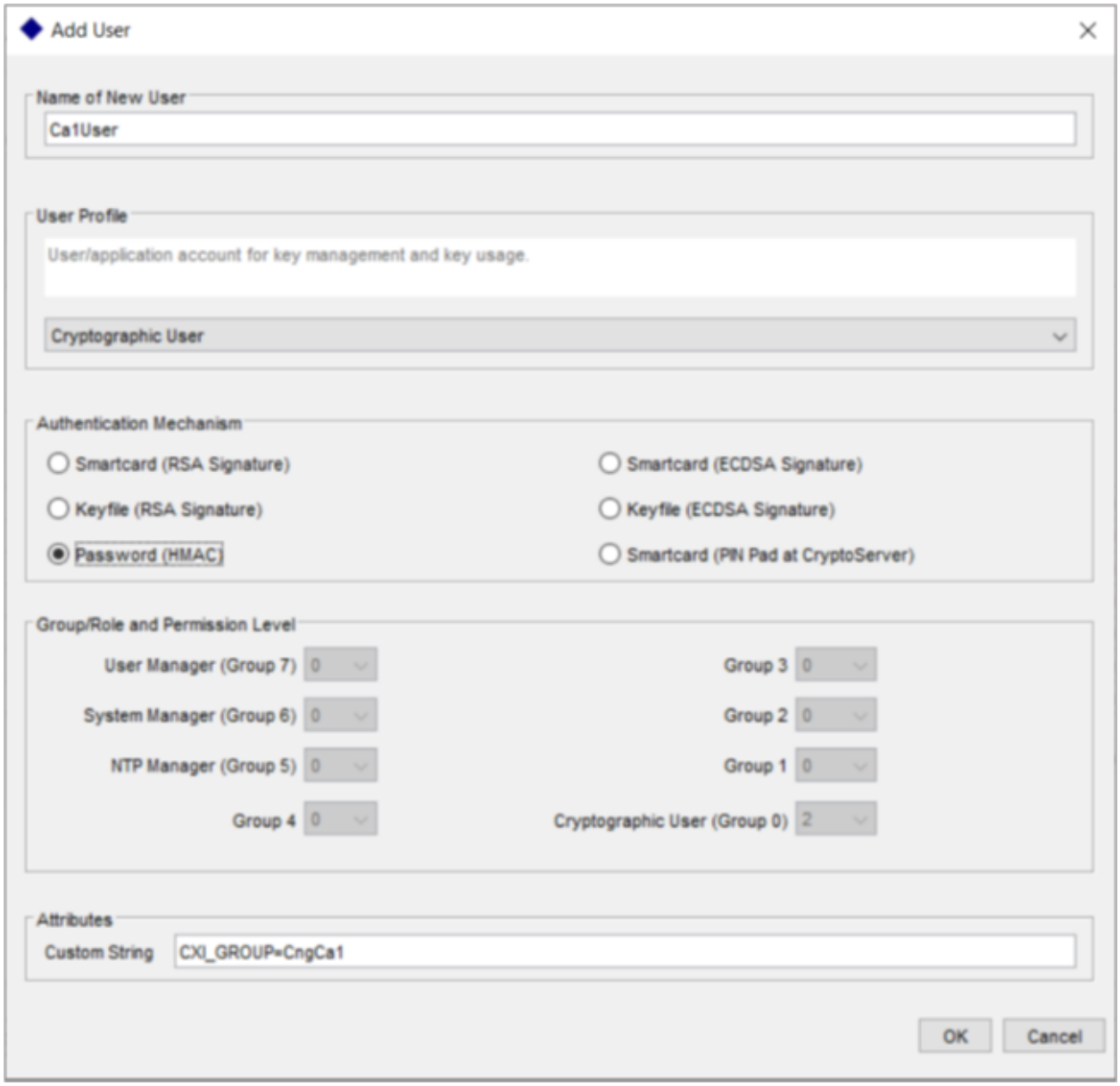

Figure 2: Creating a Crypto User

Based on your requirement, the user can use Password (HMAC), Smart Card or KeyFile protection type. If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

5.3 Setting up the CSP/CNG Provider

The `CS_CNG_CFG` environment variable contains the path and name of the configuration file. By default, it is located at `C:\ProgramData\Utimaco\CNG\cs_cng.cfg`.

For advanced configuration, refer CryptoServer_Manual_CSP_CNG.pdf found on the product CD in the Documentation directory.

1. Open the cs_cng.cfg file with an appropriate text editor.

›_ Console

```
notepad %CS_CNG_CFG%
```

2. For this installation set the path to the log file and set the log level to "TRACE".

example.file

```
# Path to the logfile (name of logfile is attached by the API)
Logpath = C:\Logs\CNG\
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 4
```

To make your testing easier, it would be good to enable the CNG log file. That can be enabled by editing the Logging Loglevel. Set the LogPath and Logging Loglevel to 1. For testing you may want to increase it to 4.

The added LogPath points to a writable directory, not to a file.

If you encounter problems, check the log file named cs_cng.log in the LogPath defined directory. When you are done testing, you should change Logging to 1 or 2. This will limit the logging to only critical and important messages.

3. Set the Login. In this case, the name of the Cryptographic User is "Ca1User" with an HMAC password "Utimaco19".

example.file

```
Login = Ca1User,HMACPwd=Utimaco19
```

If using Smartcard or KeyFile protection make the appropriate change in the Login Section as shown below:

```
Login = username,RSASign=filename#password
```

```
Login = "SmartCardUser,RSASign=:cs2:auto:USB0@<HSM-IP>"
```

For additional information refer CryptoServer_csadm_Manual_Systemadministrators.pdf document, found on the product CD in the Documentation directory.

4. Set the IP address of the HSM.

example.file

```
[CryptoServer]
# Device specifier (here: CryptoServer is CSLAN with IP address 10.44.223.141)
Device = 10.44.223.141
```

5. The Configuration File used in this document.

example.file

```
# Path to the logfile (name of logfile is attached by the API)
Logpath = C:\Logs\CNG\

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 4

# Maximum size of the logfile in bytes
Logsize = 8mb

# Keys are stored in an external or internal database
KeysExternal = false

# Path to the external keystore. Directory must be given, not file!
KeyStore = C:\ProgramData\Utimaco\CNG\keys

# Export policy for newly created keys: 0=allow all, 1=deny plain export
(standard), 2=deny all
ExportPolicy = 1

# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true

# Timeout of the open connection command in ms
ConnectionTimeout = 3000

# Timeout of command execution in ms
CommandTimeout = 60000

# CXI group for all keys. The user has to have access to this group.
Group = CngCa1

# Auto-login for CNG provider. This should be used for automated server
(re)start.
Login = Ca1User,HMACPwd=Utimaco19

# default device and fallback devices
Device = 10.44.223.141
```

For more information regarding the commands and command parameters please check the Utimaco documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

`Device = 288@<HSM IP address> Hardware (LAN) HSM`

OR

`Device = /dev/cs2.0 Hardware (PCIe) HSM`

5.3.1 Testing Connection

To enumerate providers, use the following command:

›_ Console

```
> cngtool EnumProvider
Microsoft Key Protection Provider
Microsoft Passport Key Storage Provider
Microsoft Platform Crypto Provider
Microsoft Primitive Provider
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Microsoft SSL Protocol Provider
Windows Client Key Protection Provider
Utimaco CryptoServer Key Storage Provider
```

To get the provider information, use the following command:

›_ Console

```
>cngtool ProviderInfo

Provider : Utimaco CryptoServer Key Storage Provider Device : 10.44.223.141

Group : CNG

Mode : Internal Key Storage

------------------------------------------------------------

Name : Utimaco CryptoServer Key Storage Provider

Name : Utimaco CryptoServer Key Storage Provider Version : 0x02010000

Impl. -Type : 0x00000011 MaxNameLength : 0x00000104 Device : 10.44.223.141

Group : CNG

Mode : Internal Key Storage
```

6 Installing Microsoft AD CS with Windows Enterprise

6.1 Installing and Configuring the AD CS

To create an AD-integrated CA, that is, an Enterprise CA, an account with Enterprise Administrator level privileges is required for the role configuration.

1. Join a machine to the Domain and Log in as a user with Administrative privileges
2. Select Start then select on Server Manager to open Server Manager
3. Select Manage, then select Add Roles & Features. The Before you begin window opens.

Click Next

4. On the Select installation type window, make sure the default Role or Feature Based

Installation is selected. Click Next

5. On Server selection, select a server from the server pool. Click Next
6. On the Select server roles window, select the Active Directory Certificate Services role

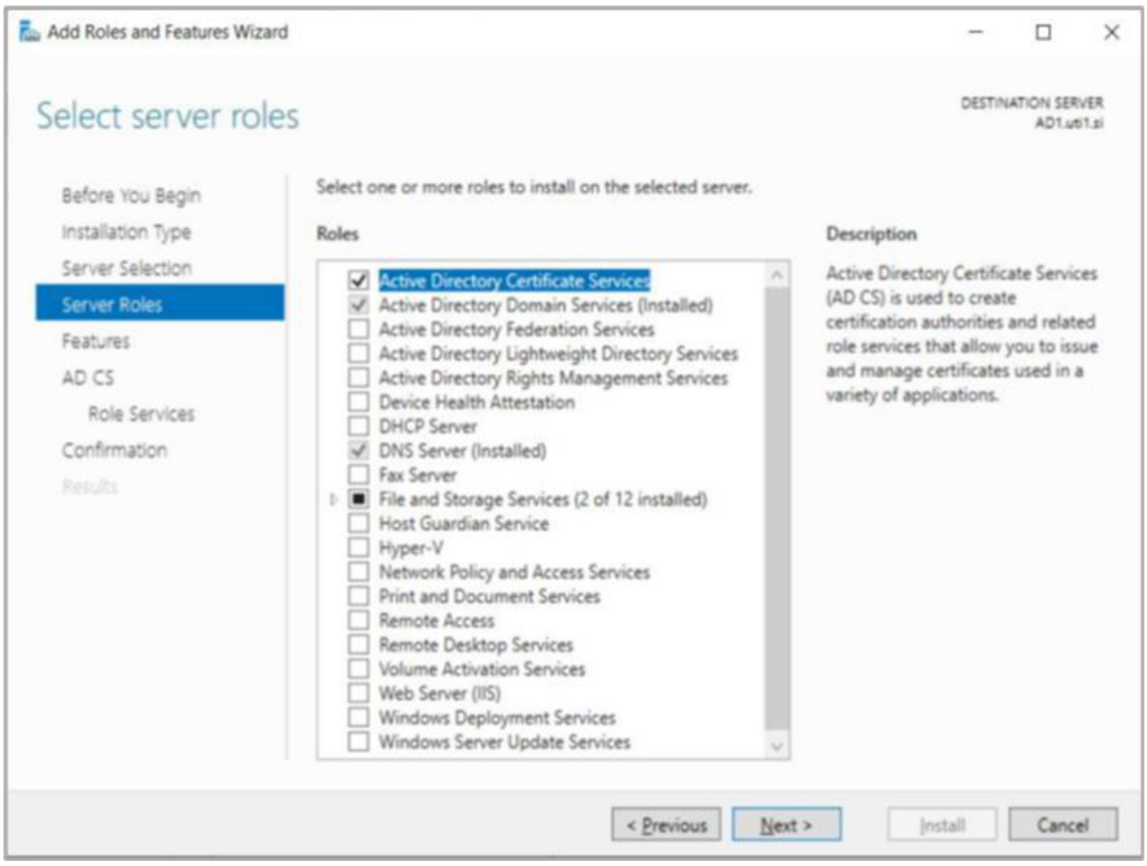

Figure 3: Select server roles window

7. When prompted to install Remote Server Administration Tools, select Add Features. Click Next

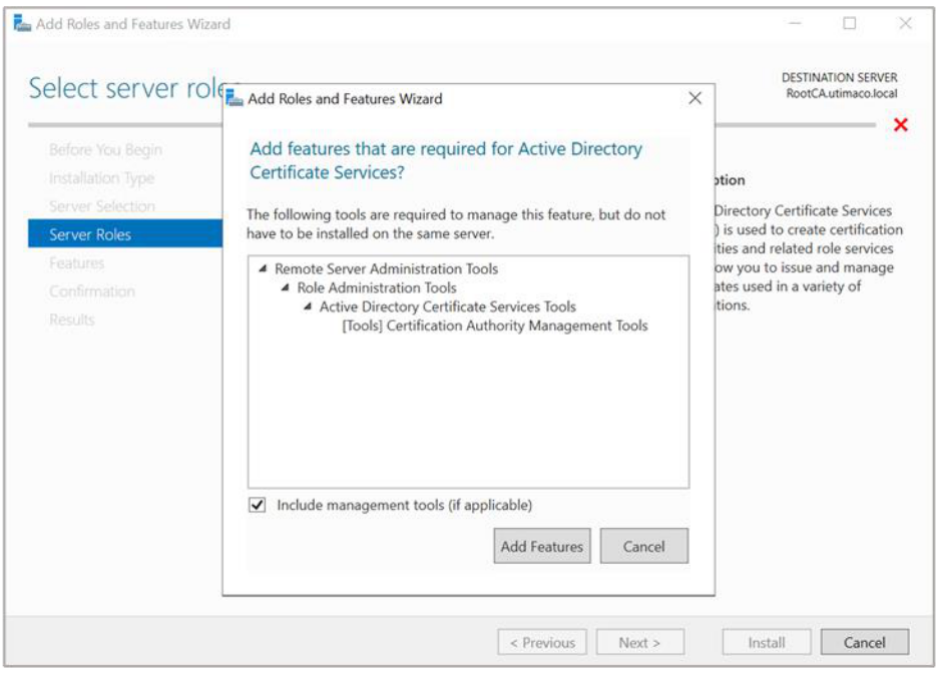

Figure 4: Add Roles and Features window

8. On the Select features window, click Next

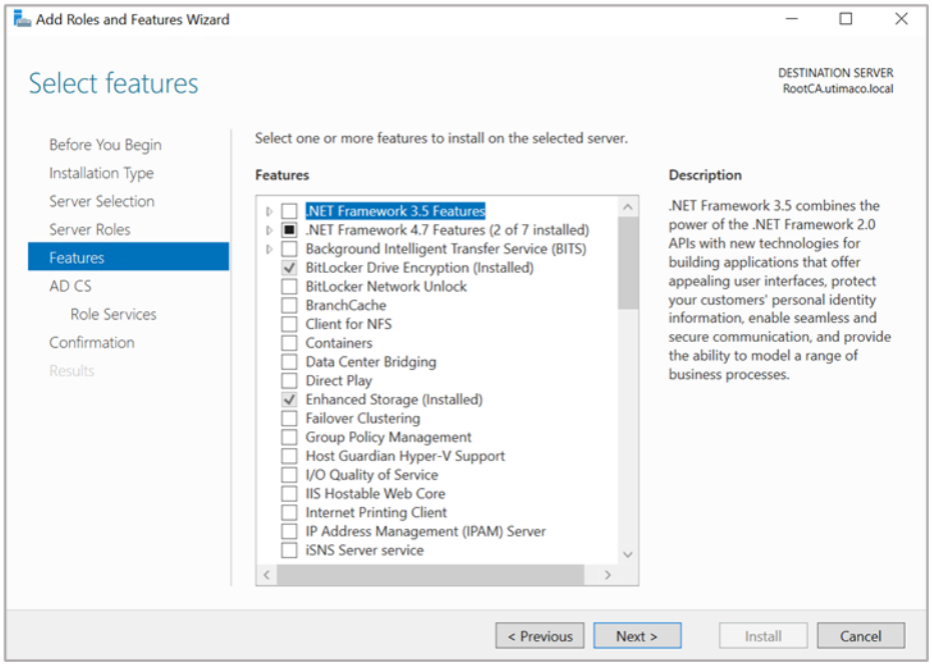

Figure 5: Select features window

9. On the Active Directory Certificate Services window, click Next

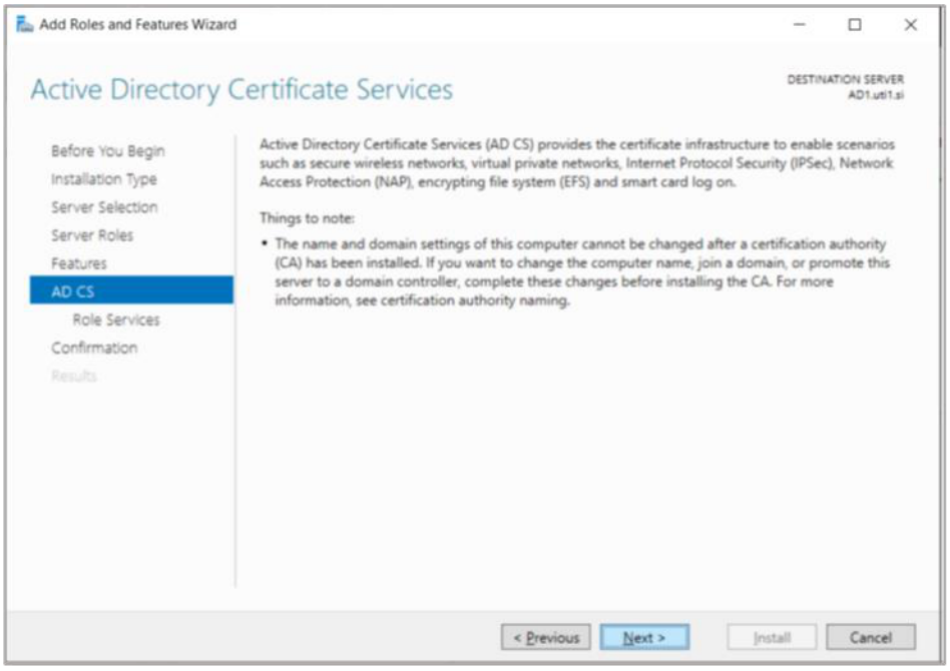

Figure 6: Active Directory Certificate Services window

10. On the Select role services window, the Certification Authority role is selected by default. Click Next

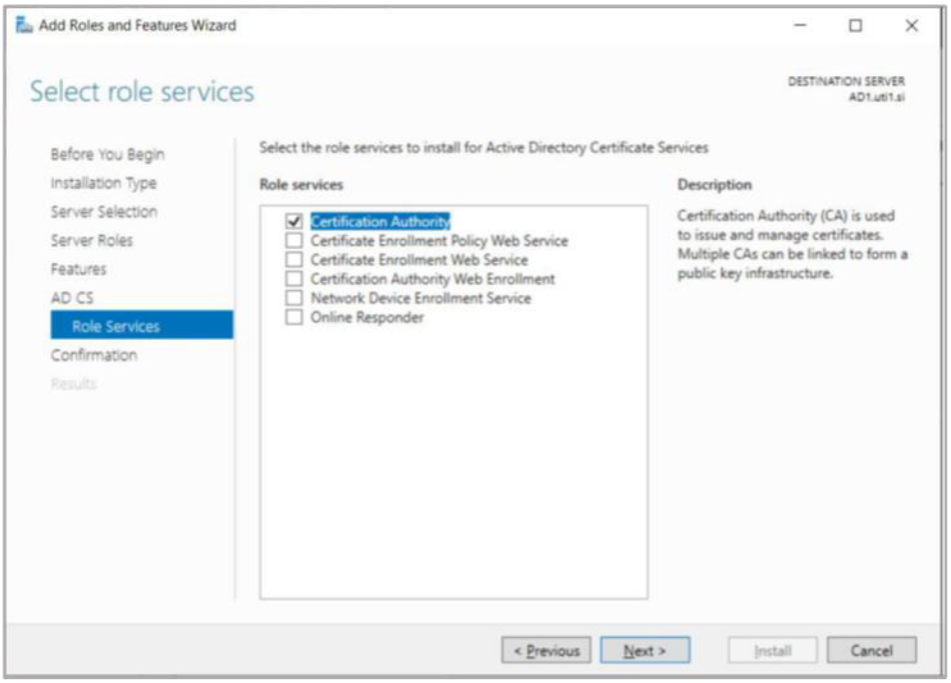

Figure 7: Select role services window

11. On the Confirm installation selections window, check, and verify the information then click Install

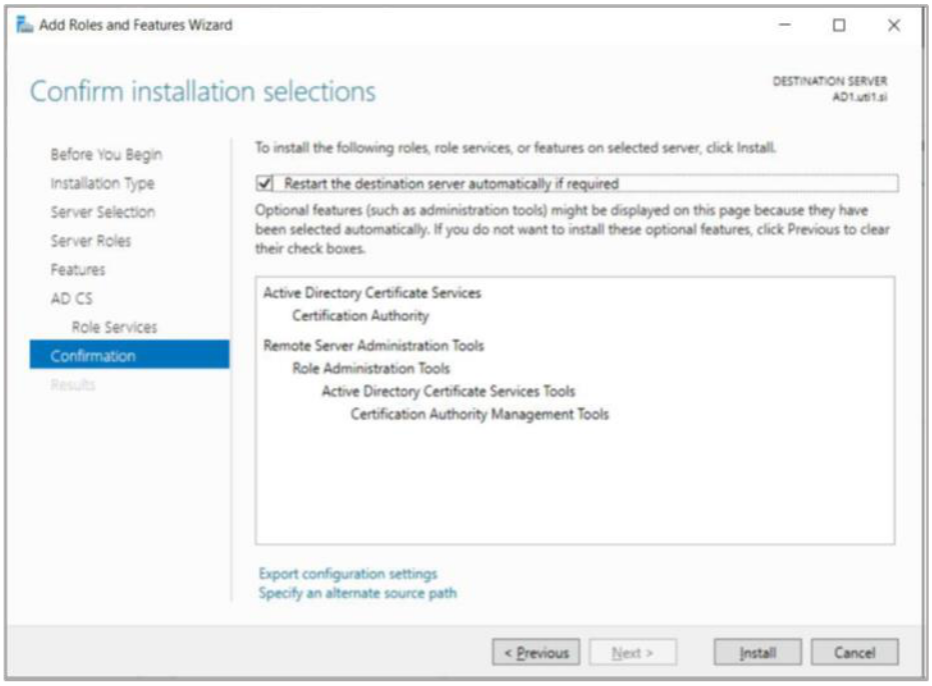

Figure 8: Confirm installation selections window

12. When the installation is complete, click on the Configure Active Directory Certificate Services on the destination server link

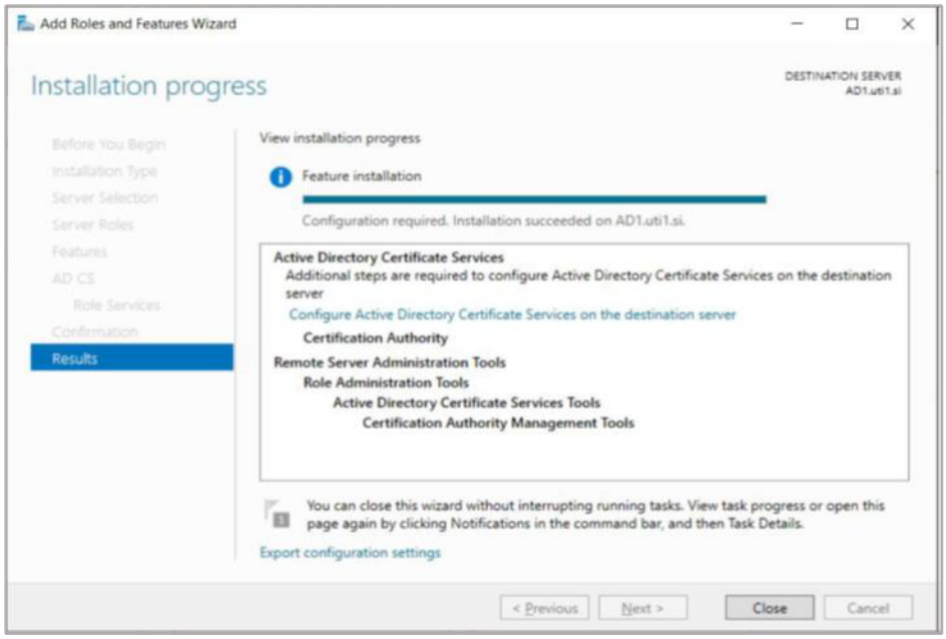

Figure 9: Installation Progress window

13. On the Credentials window, make sure that Administrator's credentials are displayed in the Credentials box. If not, select Change and specify the appropriate credentials. Click

Next

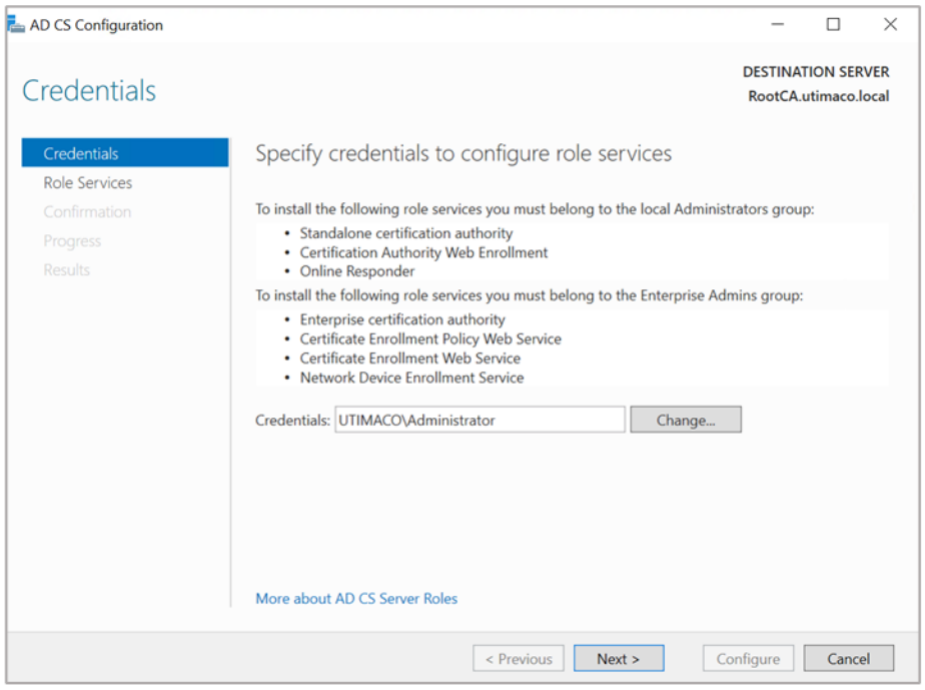

Figure 10: Credentials window

14. On the Role Services window, select Certification Authority. This is the only available selection when the certification authority role is installed on the server, Click Next

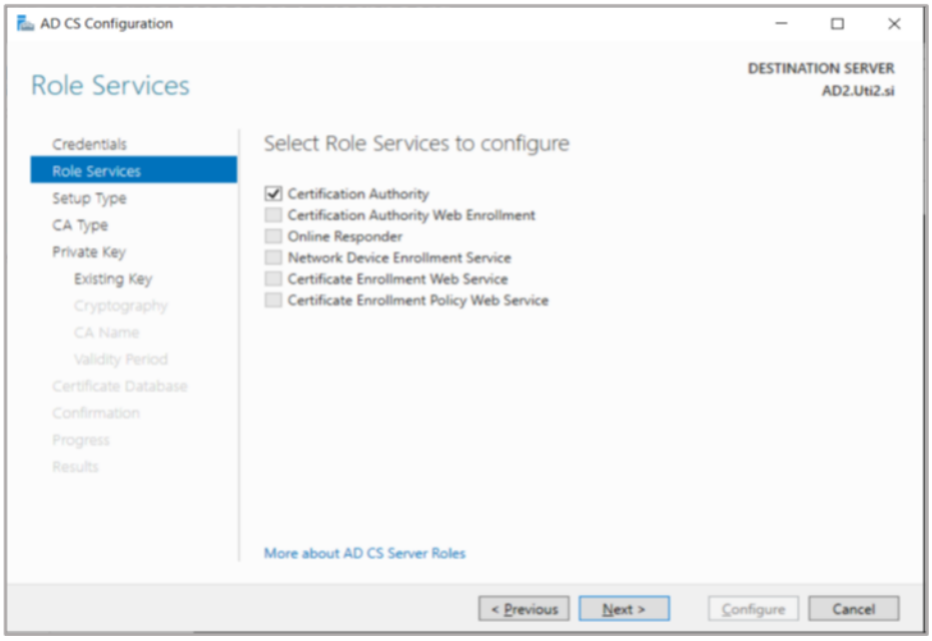

Figure 11: Role Services window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert

Smartcard and enter the pin. Then press OK button on the PIN Pad.

15. On the Setup Type window, select the appropriate CA setup type for your requirements.

Click Next

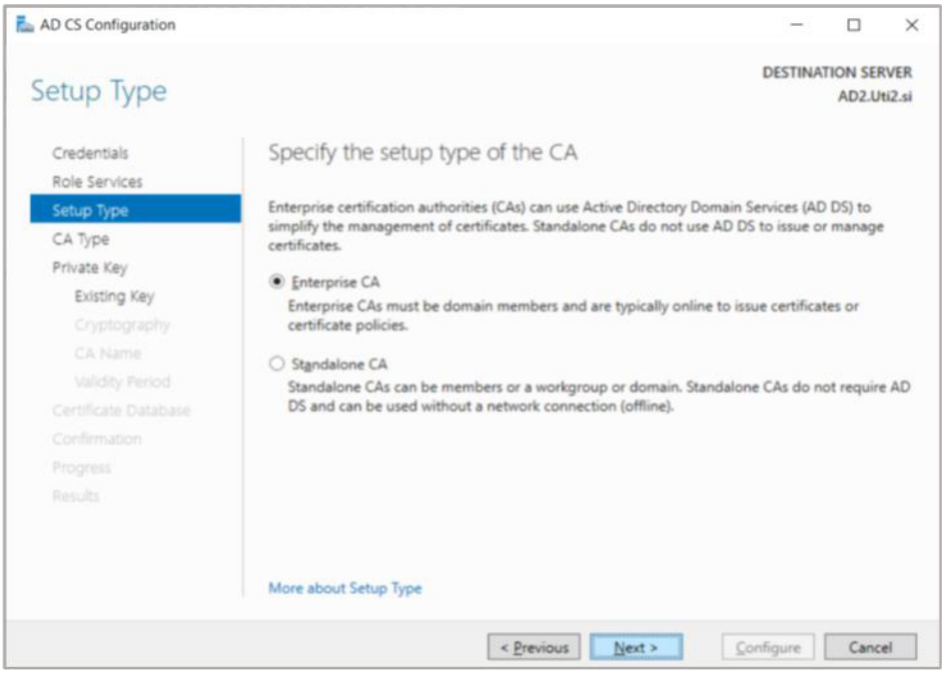

Figure 12: Setup Type window

16. On the CA Type window, Root CA is selected by default. Click Next

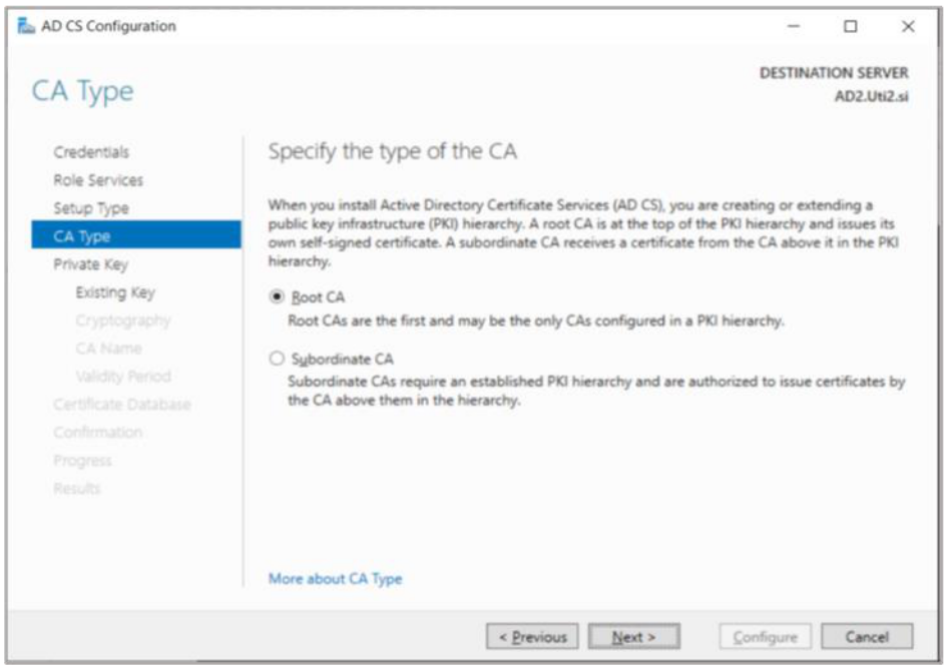

Figure 13: CA Type window

17. On the Private Key window, leave the default selection to Create a new private key selected. Click Next

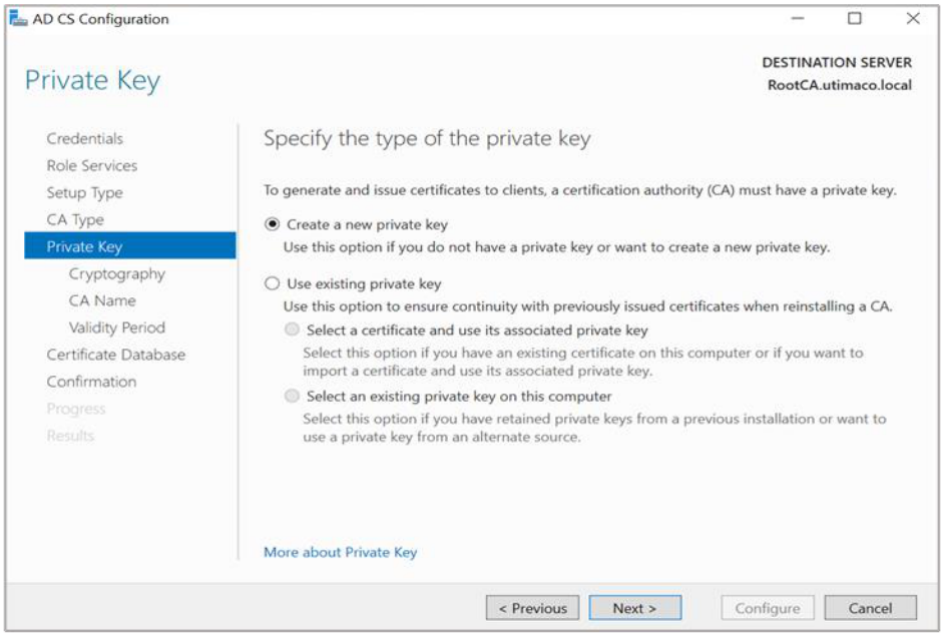

Figure 14: Private Key window

18. On the Cryptography for CA window, select the appropriate Utimaco CryptoServer cryptographic provider along with the key type, key length, and suitable hash algorithm:

- RSA #Utimaco CryptoServer Key Storage Provider
- ECDSA_P256 #Utimaco CryptoServer Key Storage Provider
- ECDSA_P384 #Utimaco CryptoServer Key Storage Provider
- ECDSA_P521 #Utimaco CryptoServer Key Storage Provider

If KeyFile or SmartCard protection is used, select the Allow administrator interaction when the private key is accessed by the CA option.

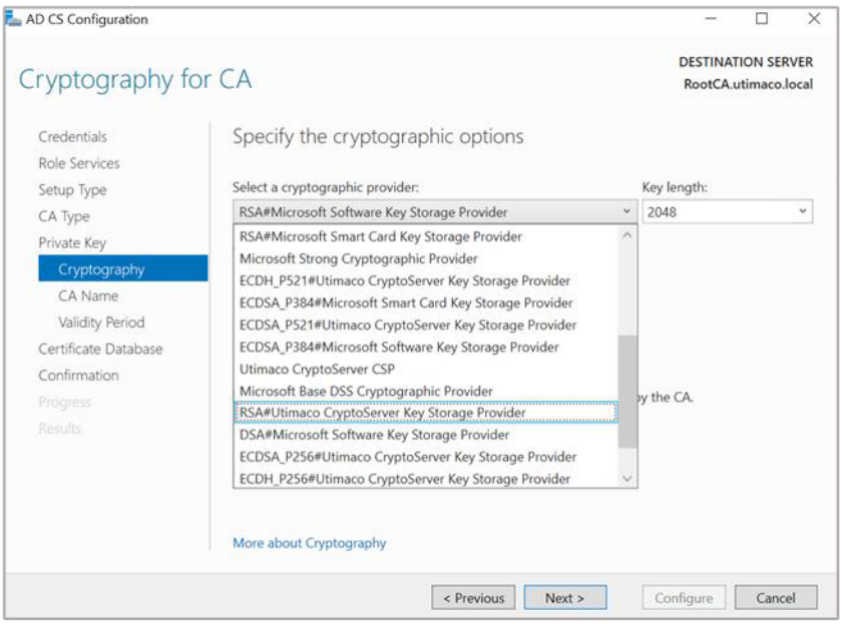

Figure 15: Cryptography for CA window

19. Click Next

20. On the CA Name window, give the appropriate CA name. Click Next

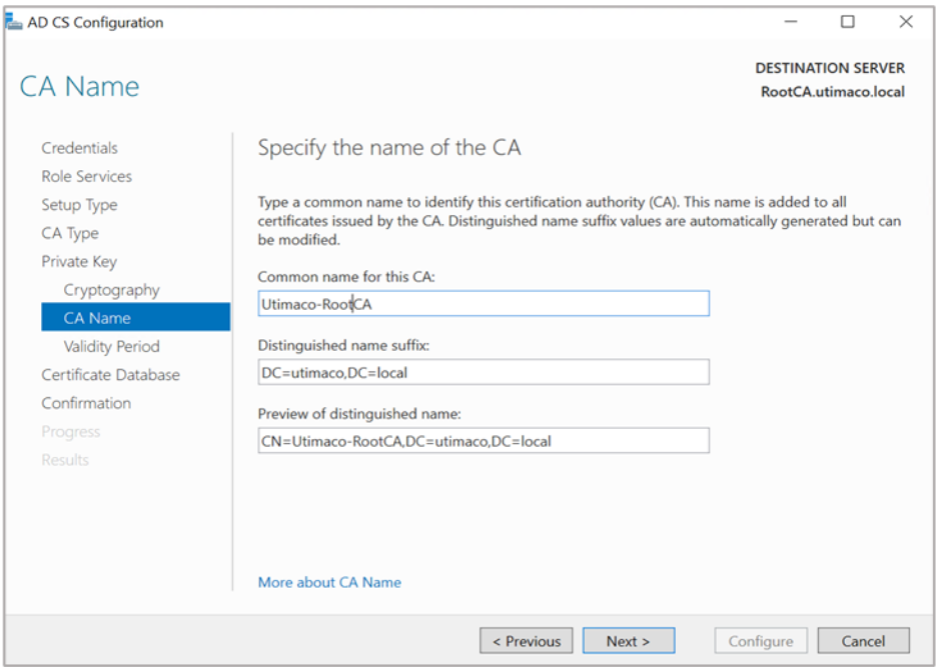

Figure 16: CA Name window

21. On the Validity Period window, enter the number of years for the certificate to be valid.

Click Next

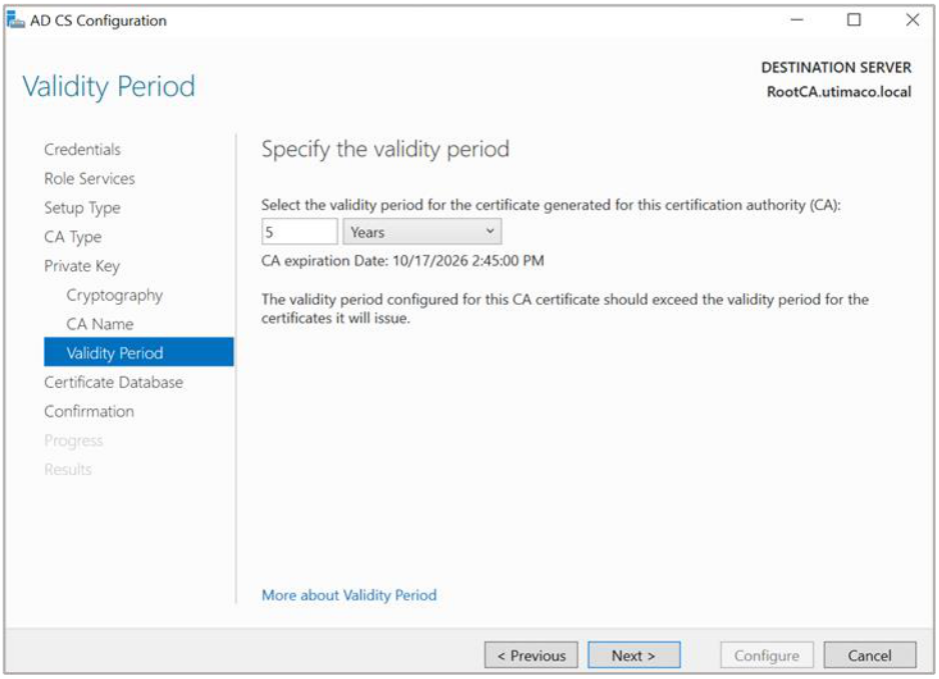

Figure 17: Validity Period window

22. On the CA Database window, leave the default locations for the database and database

log files. Click Next

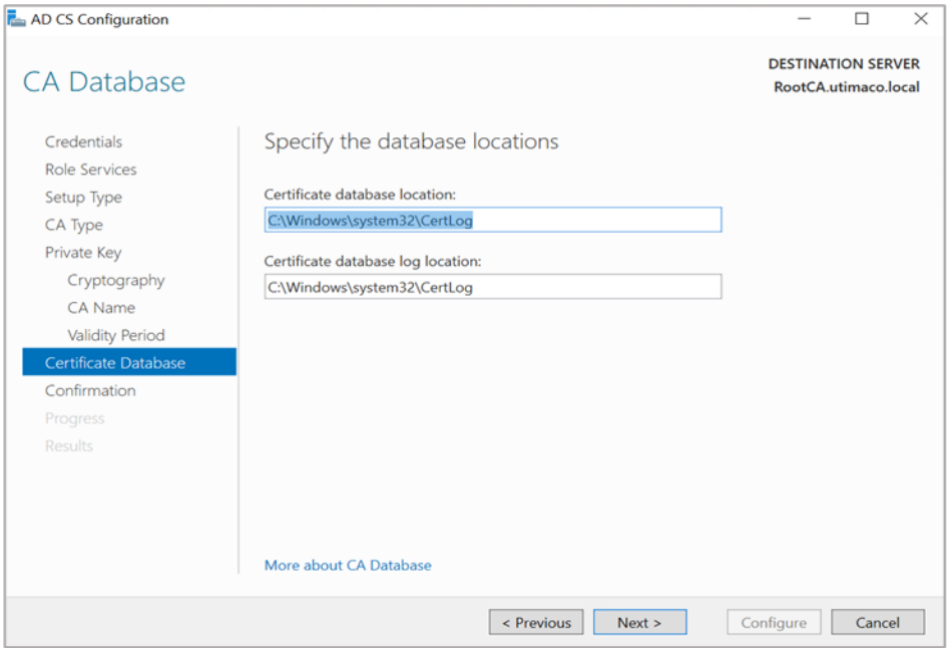

Figure 18: CA Database window

23. On the Confirmation window, click Configure

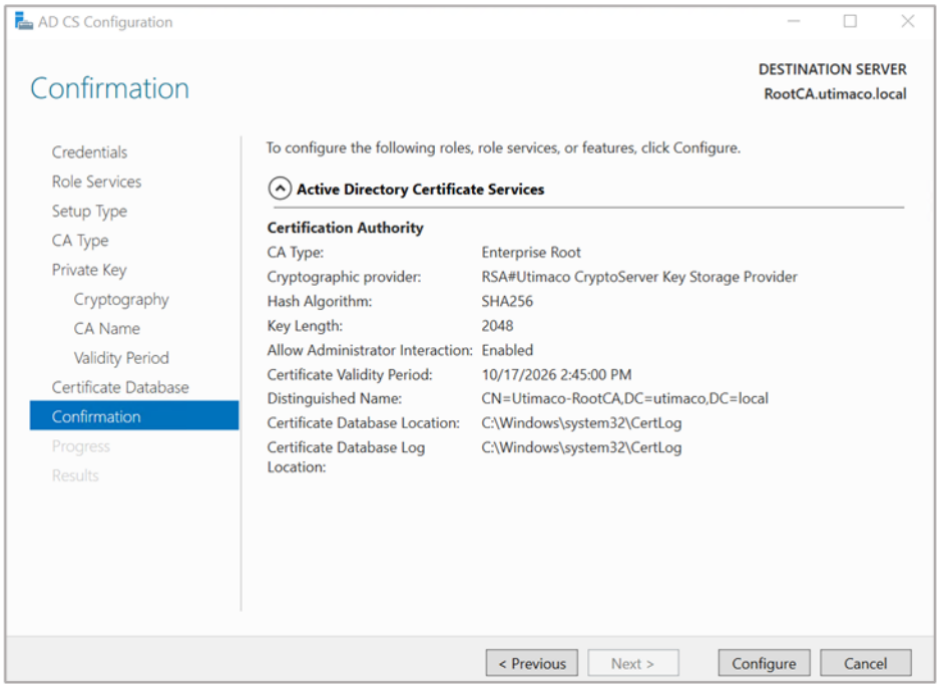

Figure 19: Confirmation window

24. Click Close to exit the AD CS Configuration wizard after viewing the installation results. A

private key for the CA will be generated and stored on the HSM

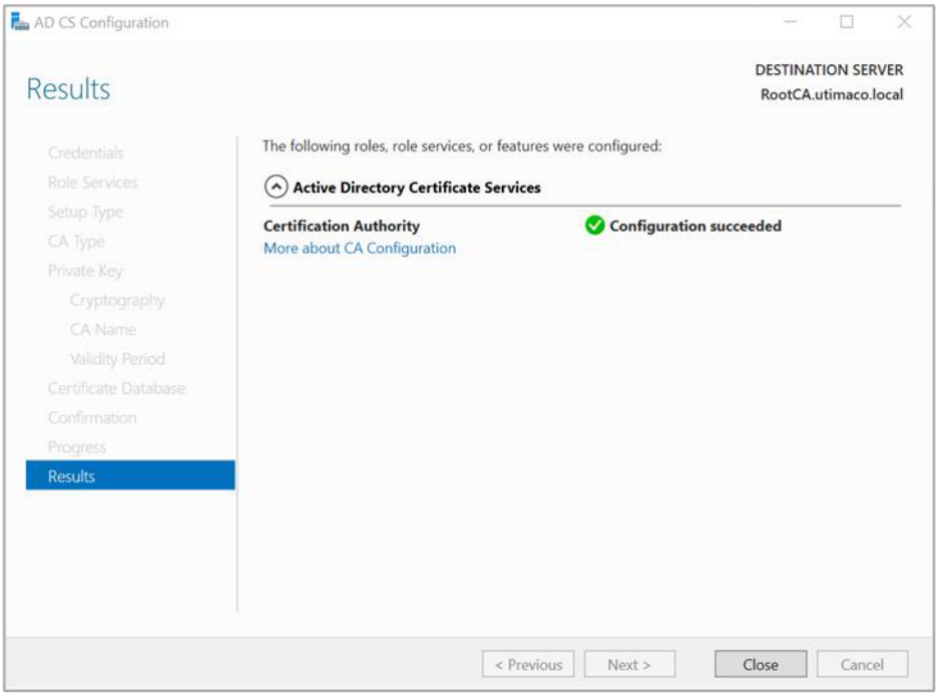

Figure 20: Results window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert

Smartcard and enter the pin. Then press OK button on the PIN Pad.

25. Open a command prompt and run the following command to verify that service is running:

```
> sc query certsvc
```

26. Open a command prompt and run the following command to verify the CA key

```
> certutil -verifykeys
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert

Smartcard and enter the pin. Then press OK button on the PIN Pad.

The result of the command shows the CA keys have successfully been verified.

6.2 Testing the AD CS

To test the installation is successful, try to issue a certificate.

1. Open the command prompt and run certmgr.msc command

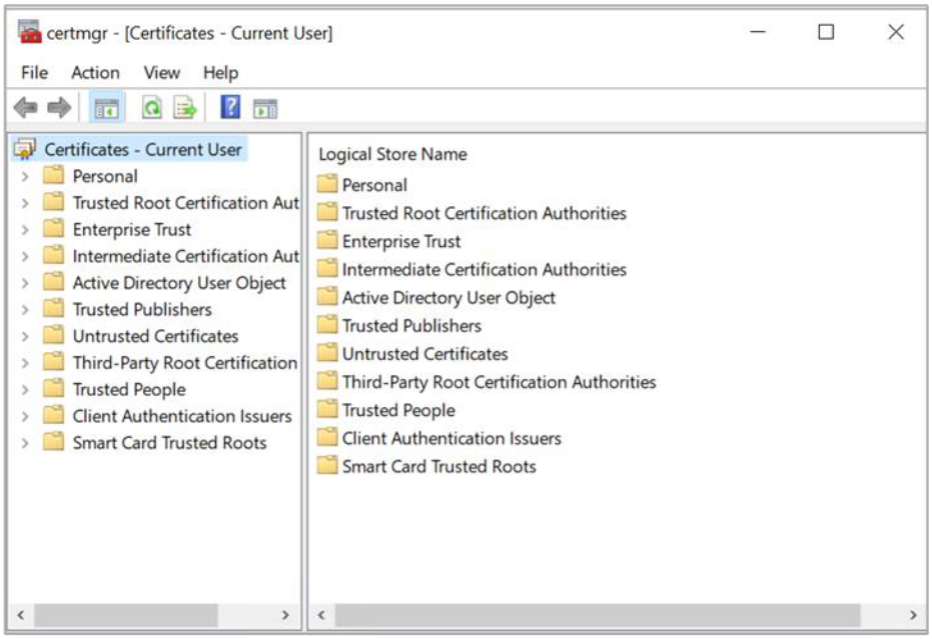

Figure 21: Certificate Manager Console window

2. Go to the Certificates then select Current User then select on Personal and select on

Certificates directory

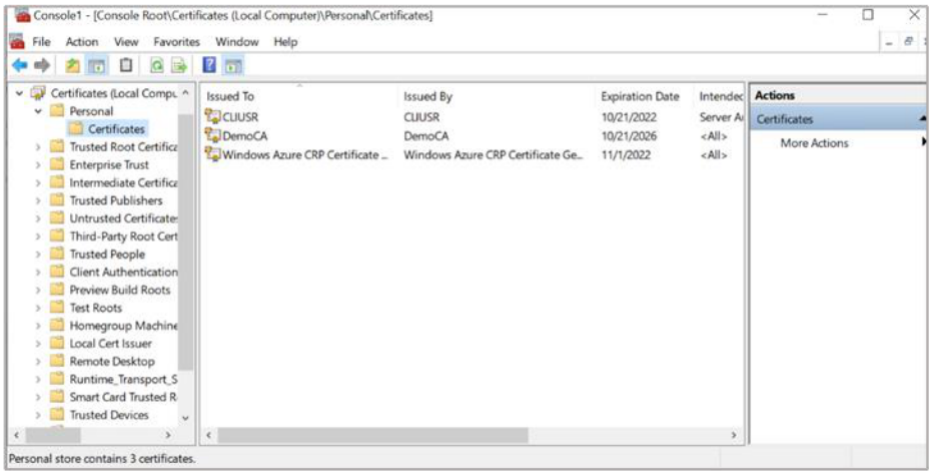

Figure 22: Certificate Directory window

3. Right-click on the directory Certificates then select All tasks select Request New Certificate

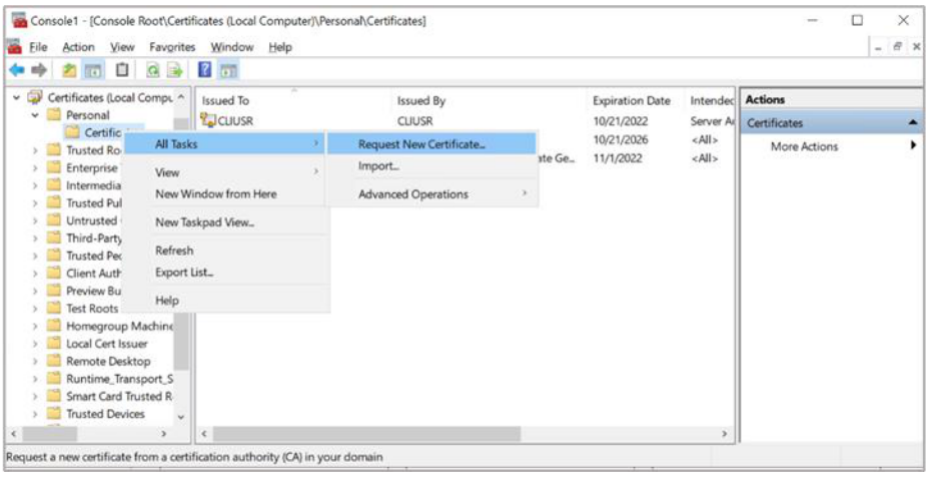

Figure 23: Certificate Directory window

4. In Before You Begin window, click Next

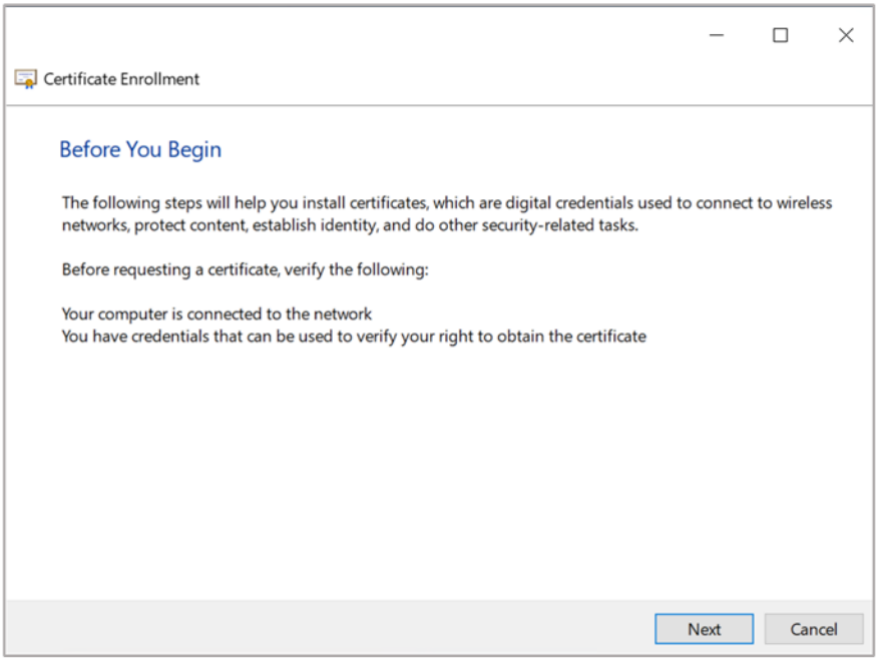

Figure 24: Before You Begin window

5. In Select Certificate Enrollment Policy window, click Next

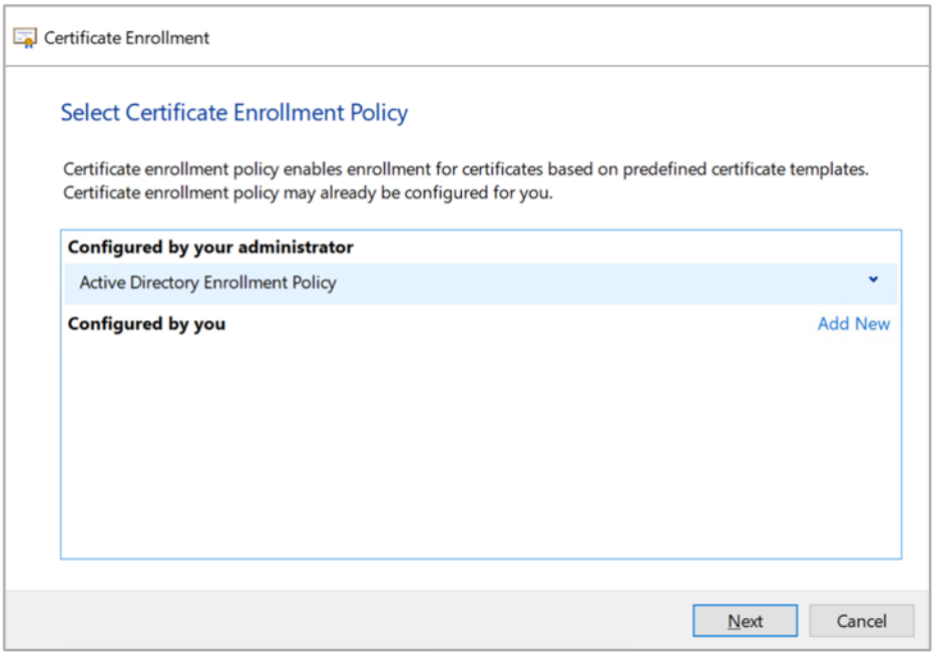

Figure 25: Certificate Enrollment window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

6. Enable the checkbox for User template, Click Enroll

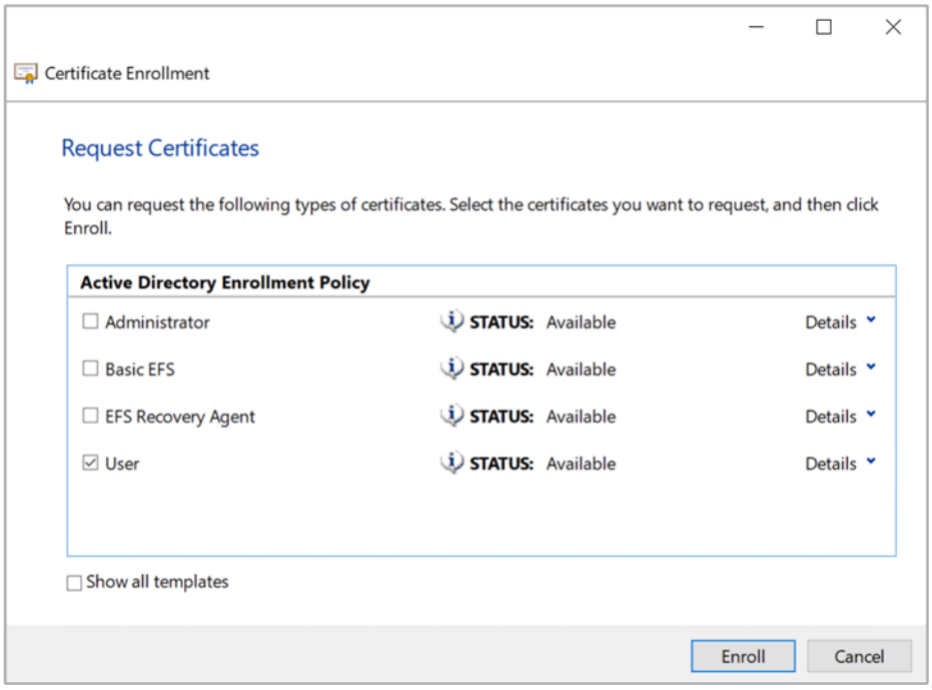

Figure 26: Request Certificates window

Verify the certificate is enrolled successfully. The enrollment wizard shows if the certificate enrollment was successful.

7 Install and Configure AD CS with Windows Server Core

1. Join the domain by running the command

›_ Console

```
> netdom join $(hostname) /domain:<full_DNS_domain_name>
/userd:<user_name> /passwordd:<password>
```

2. Restart the machine after joining the domain by running the command

›_ Console

```
> shutdown /r /t 0
```

3. Enable WOW64 if you are working with 32-bit applications

4. Run PowerShell as admin user

5. Install CA binaries via PowerShell, by running the command

›_ Console

```
> PS> Add-WindowsFeature ADCS-Cert-Authority --IncludeManagementTools
```

6. Configure CA via PowerShell, by running the command

›_ Console

```
PS> Install-AdcsCertificationAuthority -AllowAdministratorInteraction -
caType EnterpriseRootCA -CryptoProviderName ECDSA_P256#HSM_KSP_NAME -
KeyLength 256 -HashAlgorithmName SHA256
```

Example

›_ Console

```
PS> Install-AdcsCertificationAuthority -AllowAdministratorInteraction -
caType EnterpriseRootCA -CryptoProviderName "ECDSA_P384#Utimaco
CryptoServer Key Storage Provider" -KeyLength 384 -HashAlgorithm SHA384 -
CACommonName Root-CA
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

7. When the confirmation message appears, type A and press Enter

8. To verify that the CA service has started, open a command prompt, and run the command

›_ Console

```
> sc query certsvc
```

8 Configuring the Auto-Enrollment Group Policy for a Domain

To complete the integration, you must configure the auto-enrollment as a group policy.

1. On the domain controller, select Start then click on Administrative Tools then click on Group Policy Management
2. Select Forest, then select your Domain and expand it

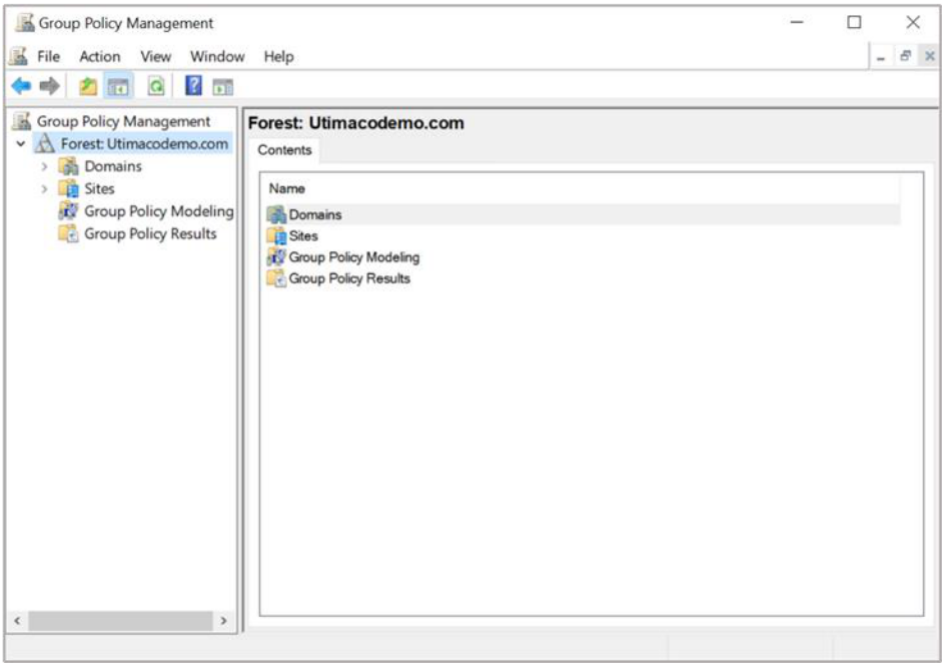

Figure 27: Group Policy Management window

3. Double-click Group Policy Objects in the forest

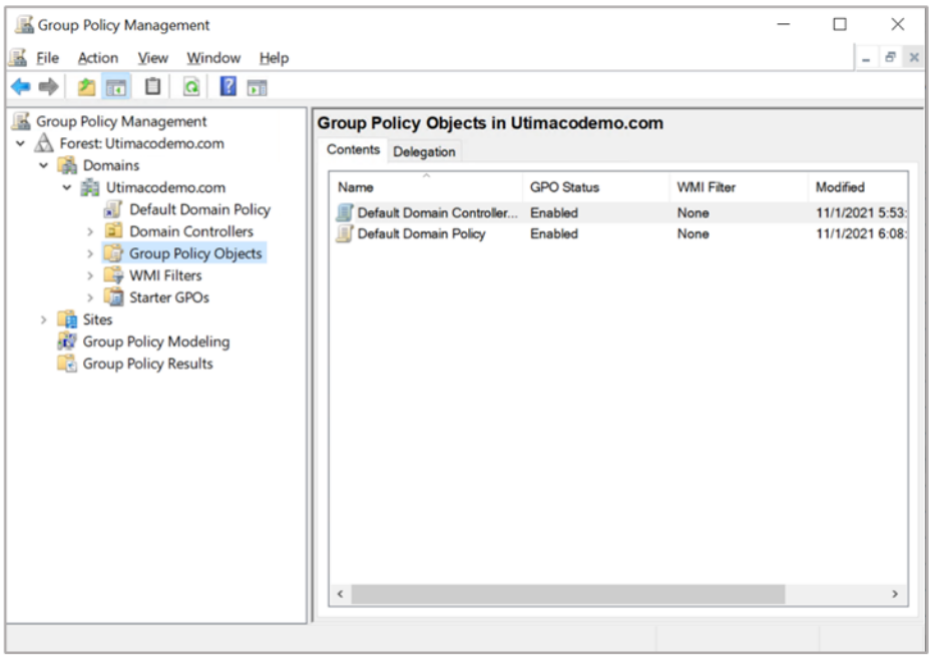

Figure 28: Group Policy Management window

4. Right-click the Default Domain Policy, then select Edit

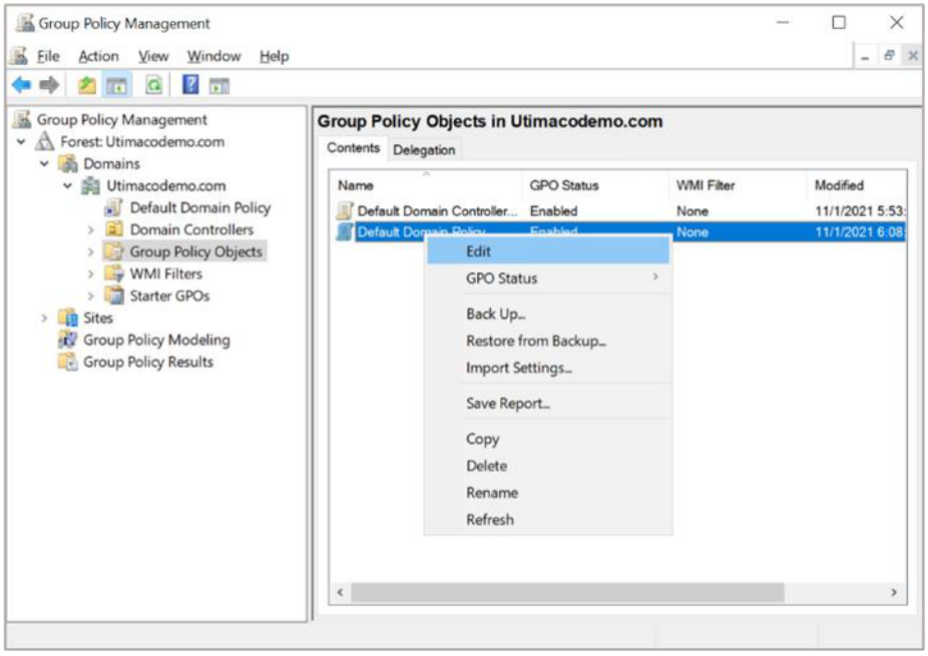

Figure 29: Group Policy Management window

5. In the Group Policy Management Editor, select Computer Configuration click on Policies

then click on Windows Settings click on Security Settings and then click on Public Key

Policies

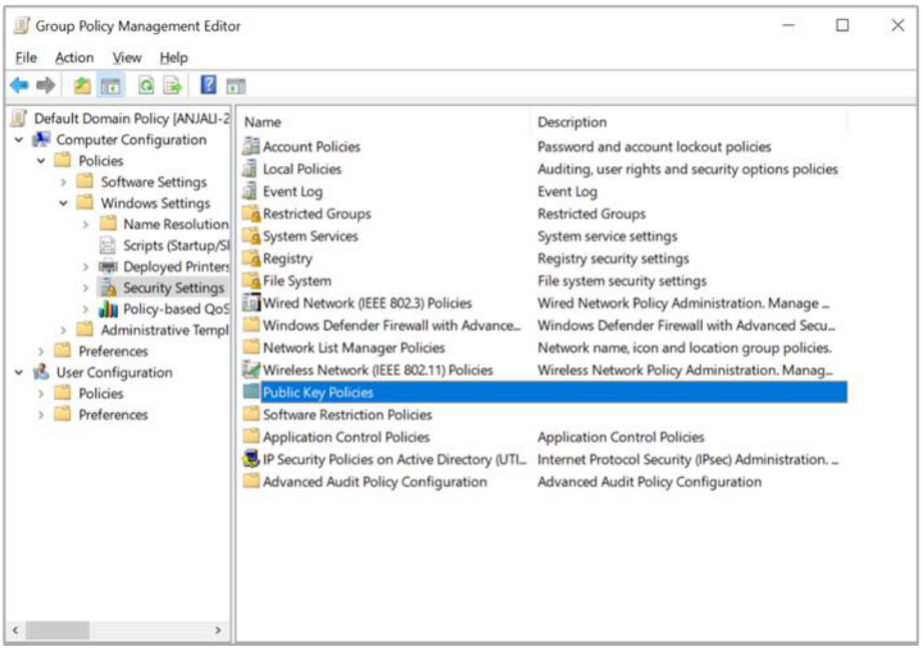

Figure 30: Group Policy Management Editor window

6. Double-click Certificate Services Client click on Auto-Enrollment

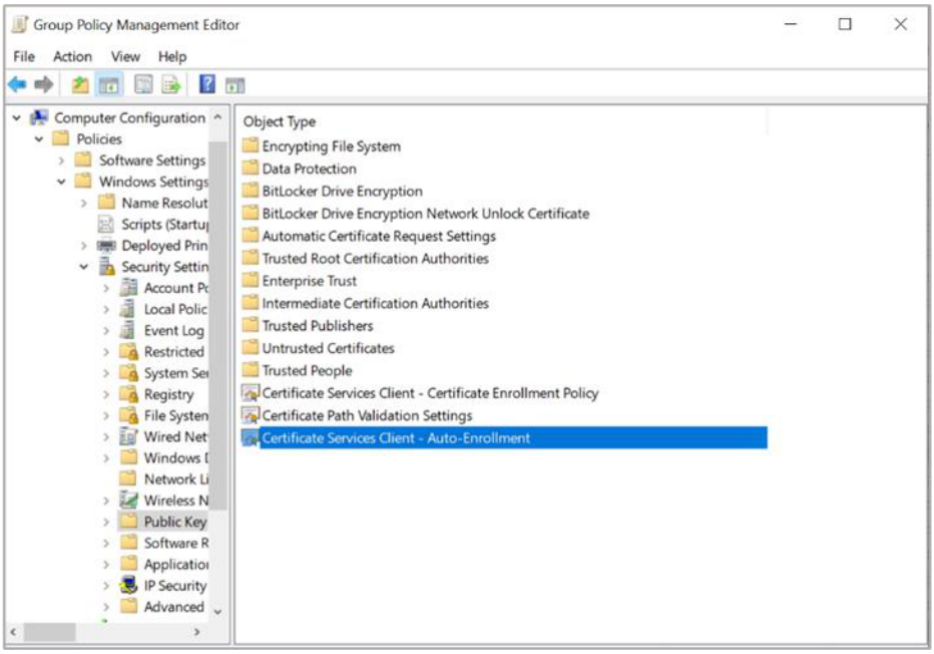

Figure 31: Group Policy Management Editor window

7. In Configuration Model, select Enabled to enable auto-enrollment. Select the following options:

- Renew expired certificates, update pending certificates, remove and revoke certificates
- Update certificates that use certificate template

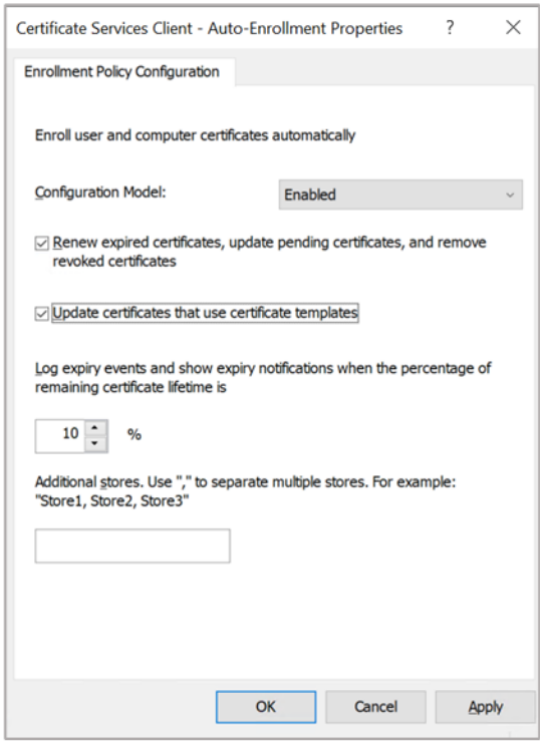

Figure 32: Enrollment Policy Configuration window

8. Select Apply and OK to accept your changes and close the Editor

9 Configuring the Certificate Enrollment to use CA templates on the AD CS Server

This section describes how to create certificate templates when the private key is managed using an HSM. All subscribers who enroll for a certificate based on such a template must have a client connection to the HSM.

If a CA installed on Windows Server Core is managed remotely, the snap-ins in this section must run on a separate machine with GUI capabilities.

To integrate the CA certificate enrollment functionality with a CA private key generated by the Utimaco HSM:

1. Create a CA template that uses the Utimaco HSM

a) Open Command prompt and run the certtmpl.msc command

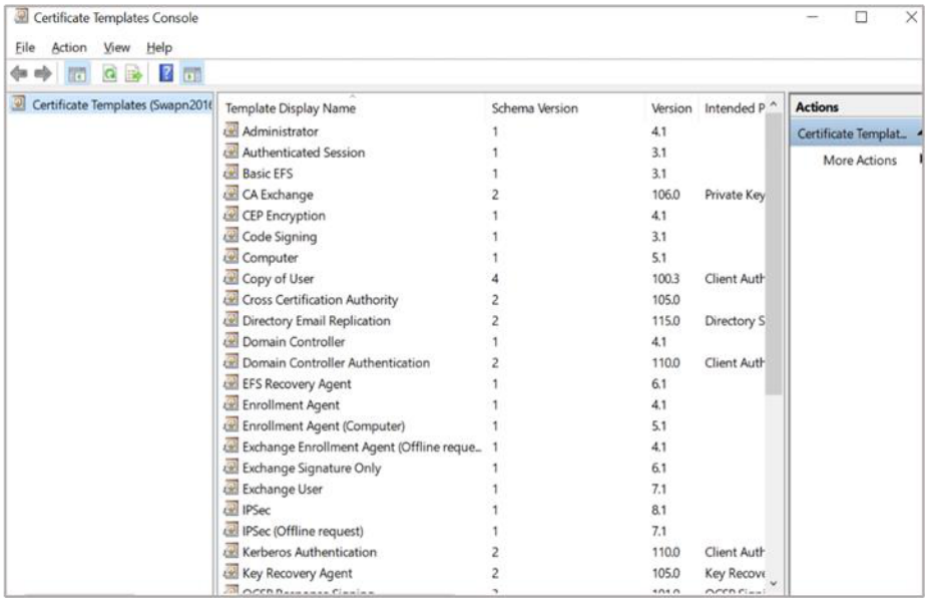

Figure 33: Certificate Template Console window

b) Right-click the Administrator template, then select Duplicate Template. The Properties window opens, showing Compatibility tab

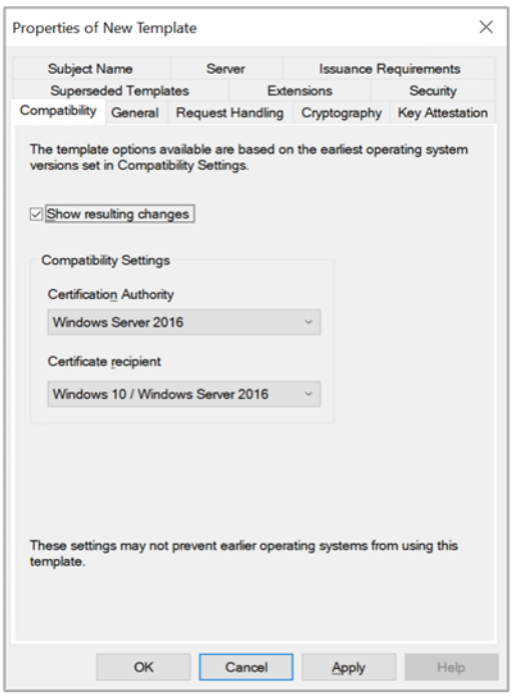

Figure 34: Compatibility Tab window

c) Select appropriate windows version under Certificate Authority and Certificate Recipient drop-down box

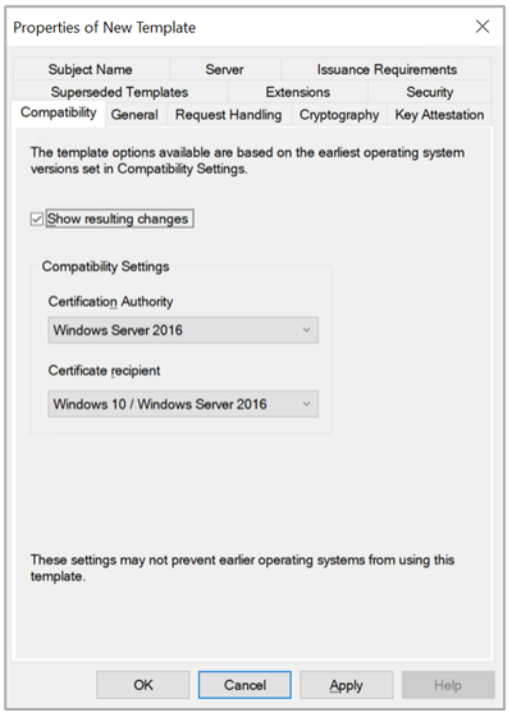

Figure 35: Compatibility Tab window

d) Select the General tab. In Template display name, type a name for the template

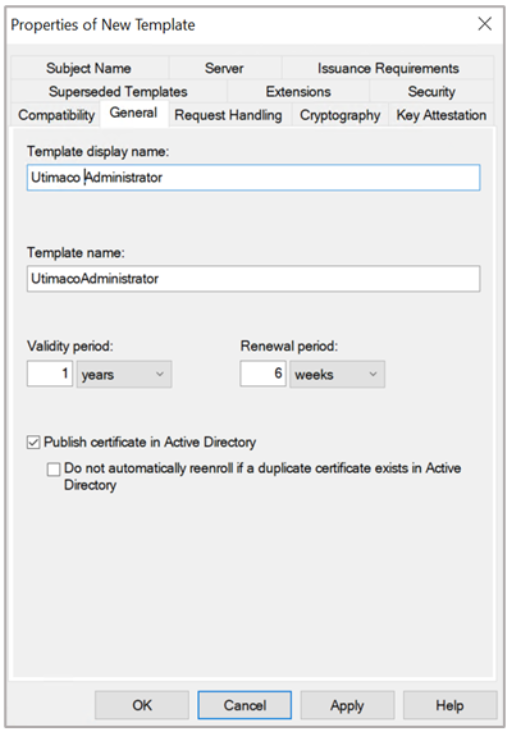

Figure 36: General Tab window

e) Select the Request Handling tab, and in Purpose select Signature and deselect Allow private key to be exported

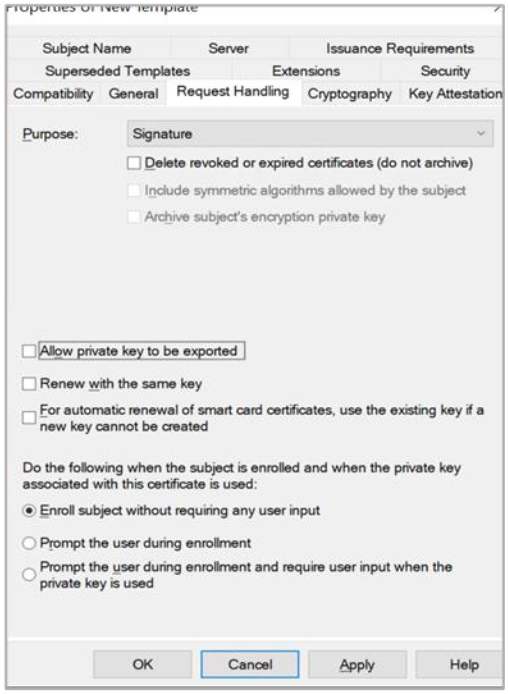

Figure 37: Request Handling Tab window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

f) Select the Cryptography tab and in the Provider, category select Key storage provider

g) In Algorithm Name, select the algorithm from the list

h) Click on the radio button for Requests must use one of the following providers and in Providers, select Utimaco CryptoServer Key Storage Provider only

If CA is on Windows Server Core and you are managing it remotely using certtmpl.msc on a

different PC, you need to install the Utimaco CryptoServer Key Storage Provider on the PC

that is running certtmpl.msc. Otherwise, the Utimaco CryptoServer provider will not appear.

i) In Request Hash, select a hash type

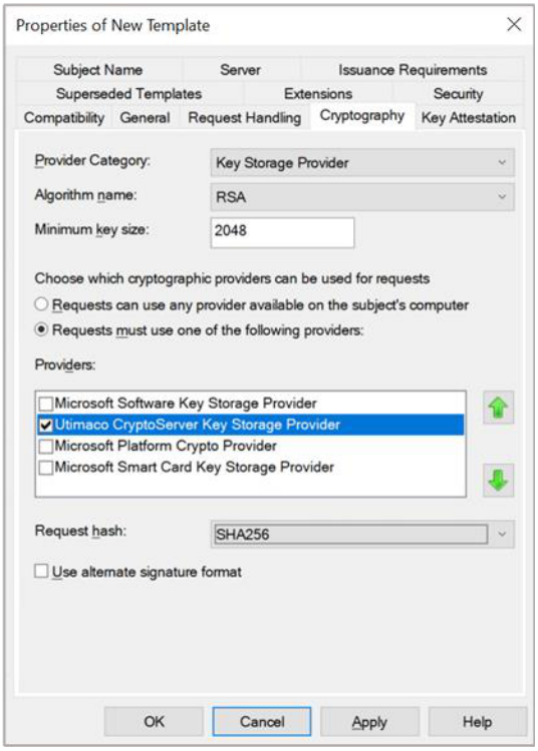

Figure 38: Cryptography Tab window

j) Select Subject Name tab and deselect Include e-mail name in subject name and deselect E-mail name

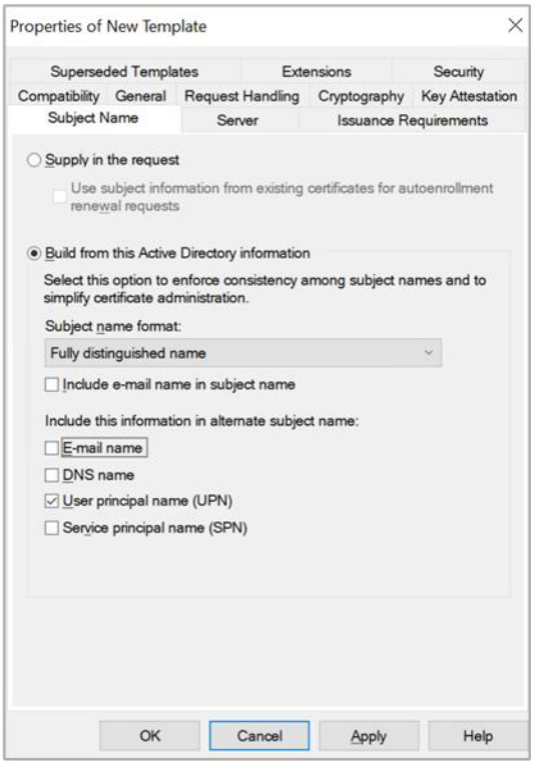

Figure 39: Subject Name Tab window

k) Select Apply and OK to save the template settings and close the Certificate Template console

2. Open Command prompt and run the certsrv.msc command

Windows Server Core: If a CA is configured on Windows Server Core and is managed via the Microsoft Management Console (MMC) from a different machine, you might get an error which states: Cannot manage Active Directory Certificate Services. To fix this, select OK, then in the certsrv.msc~ console that appears, select Action click on Retarget Certification Authority. In the window that appears, select Another Computer, then select Browse to find the CA you want to manage.

Windows Server Core: Sometimes an error appears indicating that the RPC server is unavailable. To fix this, sign into the Windows Server Core machine and minimize the command prompt. A window prompts you to load a key. Complete the steps in the window and attempt to select the CA again from certsrv.msc.

3. In the left-hand pane, select the Certificate Authority name

4. Right-click the Certificate Template node, then select New then select Certificate Template to Issue

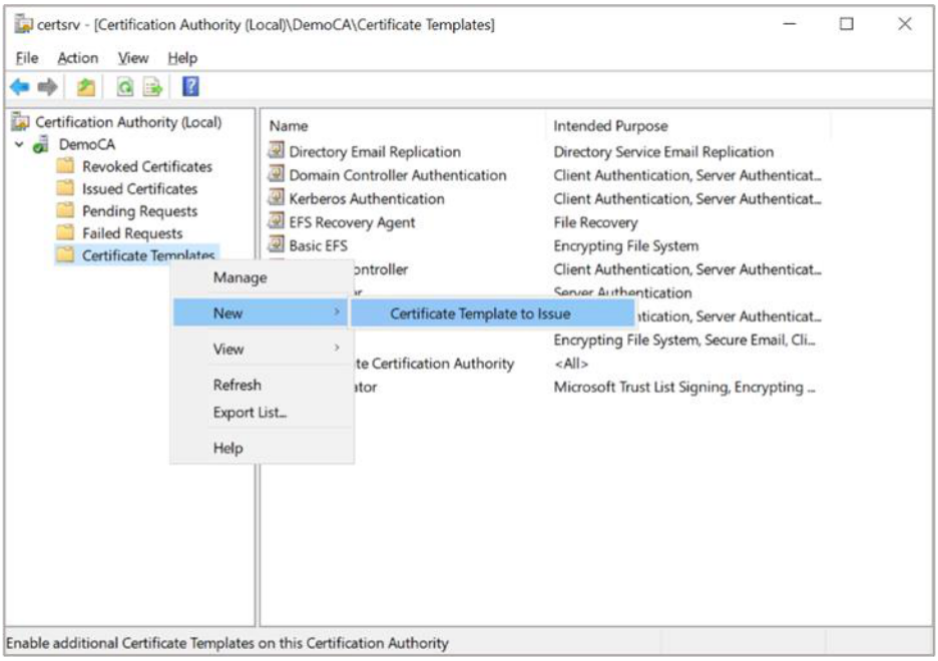

Figure 40: Certificate Templates Tab window

5. Select the template you just created, then click OK

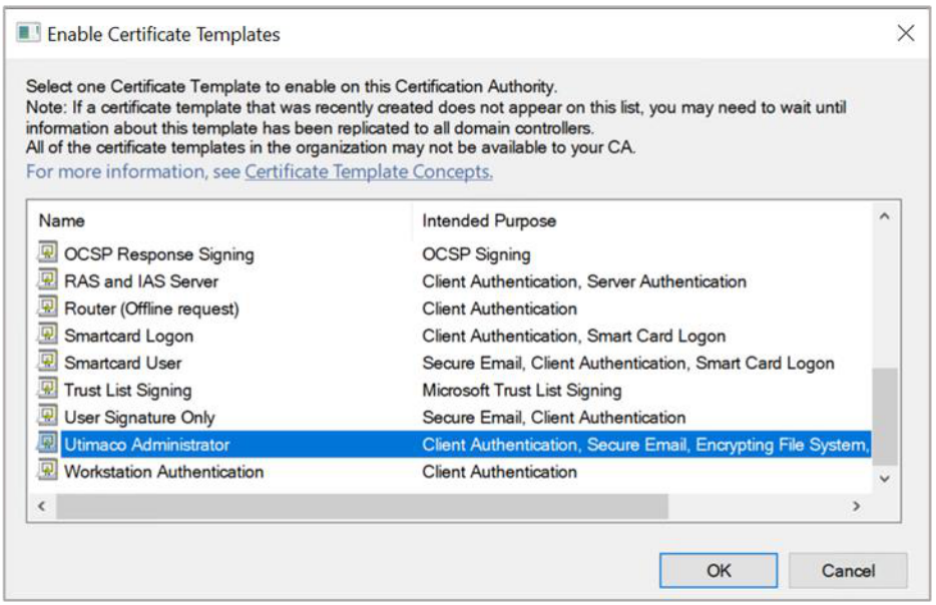

Figure 41: Enable Certificate Templates window

6. Request a certificate based on the template:

a) Open the command prompt and run the certmgr.msc command

b) In the left-hand pane, right-click the Personal node, then select All Tasks select Request New Certificate

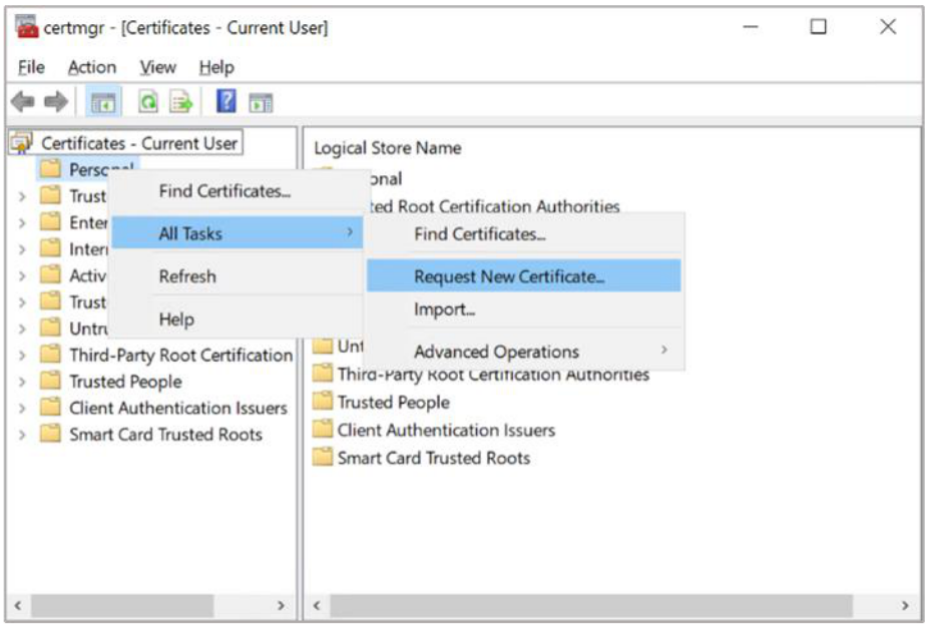

Figure 42: Certificate Manager window

c) Select Next in the first two windows

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

d) Select template that you created, then Click Enroll

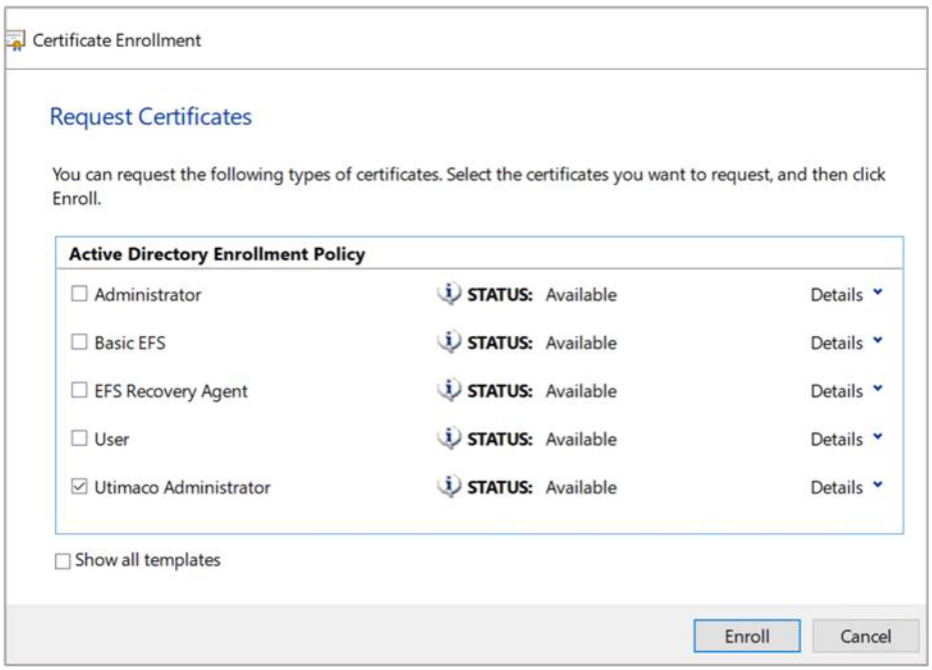

Figure 43: Certificate Enrollment window

e) The Certificate Installation Results window should show STATUS: Succeeded. Select Finish

7. Verify that the certificate is enrolled successfully. If the certificate fails to enroll because the CA is not started or the RPC ports are blocked, the following error is displayed:

> *Error: the RPC server is unavailable. 0x800706ba (win32: 1722 RPC_S_SERVER_UNAVAILABLE*

The enrollment wizard shows if the certificate enrollment was successful or failed.

Use Details to check the main information.

10 Private Key Archiving and Recovery

10.1 Archive the CA Key

To validate that the configurations that are possible with the Utimaco HSM and that do not interfere with the CA key archival functionality.

To complete archiving the Certificate Authority-Key you must follow the tasks below:

10.1.1 Archiving Process

1. Log in as a user with Administrative Privileges

2. The steps to install the Microsoft Active Directory Certificate Services are same as the **Installing Microsoft Active Directory Certificate Services with Windows Enterprise** section. After Microsoft ADCS is successfully installed, continue with the below steps

3. Verify the Certificate Authority is installed successfully

10.1.2 Add a Key Recovery Agent (KRA) template to CA

1. Open command prompt and run the certtmpl.msc command. Right-click on the Key

Recovery Agent template, then select Duplicate Template

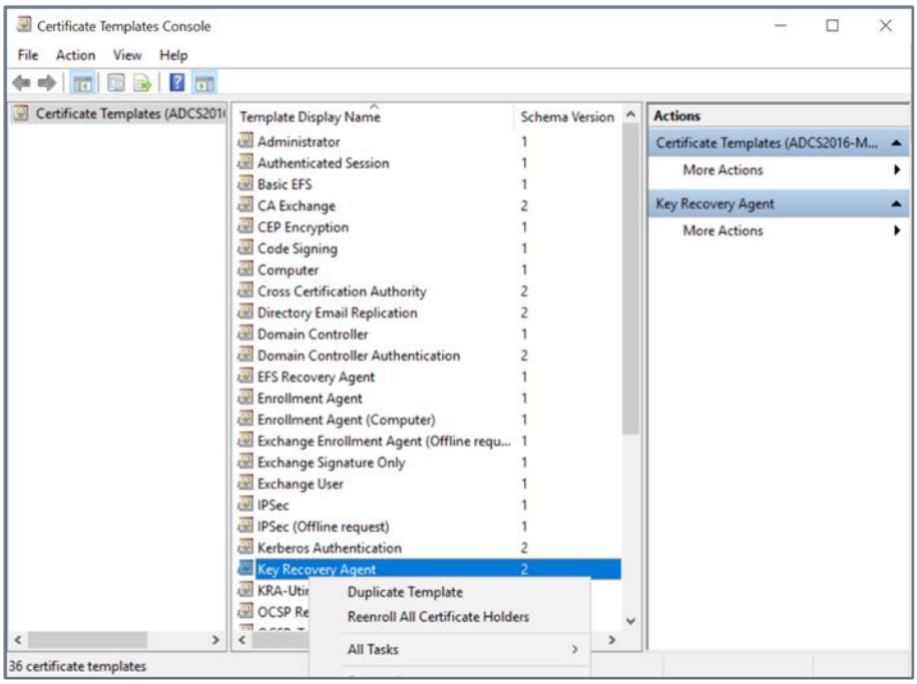

Figure 44: Certificate Template window

2. The Properties window opens, showing Compatibility tab. Select appropriate windows version under Certificate Authority and Certificate Recipient drop-down box

Figure 45: Compatibility Tab window

3. Select the General tab. In Template display name, type a name for the template
4. Select the Request Handling tab, and in Purpose select Encryption and Allow private key to be exported is selected

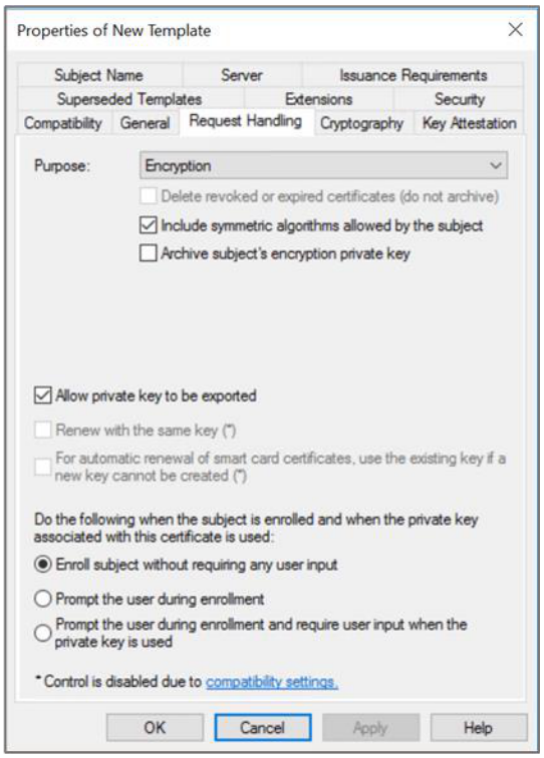

Figure 46: Request Handling window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

5. Select the Issuance Requirement tab, deselect CA Certificate manager approval
6. Select the Cryptography tab, and in the Provider category select Key storage provider
7. In Algorithm Name, select the algorithm from the list
8. Select Requests must use one of the following providers, and in Providers select Utimaco CryptoServer Key Storage Provider only

If CA is on Windows Server Core and you are managing it remotely using certtmpl.msc on a different PC, you need to install the Utimaco CryptoServer Key Storage Provider on the PC that is running certtmpl.msc. Otherwise, the Utimaco CryptoServer provider will not appear.

9. In Request Hash, select a hash type
10. From the Security tab, verify if Domain Admins and Enterprise Admins are having Enroll Permissions
11. Select Apply and click OK to save the template settings and close the Certificate Template console\
12. Open the command prompt and run the certsrv.msc command\
13. Right-click the Certificate Templates node. Select New then select Certificate Template to Issue
14. Select the template created in the above steps and click OK

10.1.3 Issue the Key Recovery Agent Certificate

1. Open the command prompt and run the certmgr.msc command

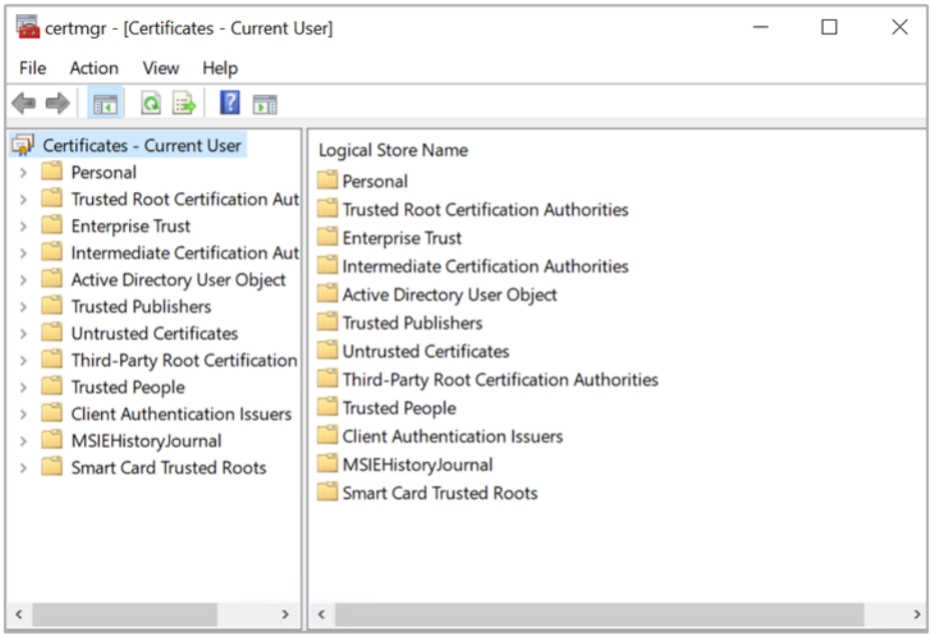

Figure 47: Certificate Manager window

2. Right-click Personal node. Select All Tasks then select Request new certificate…

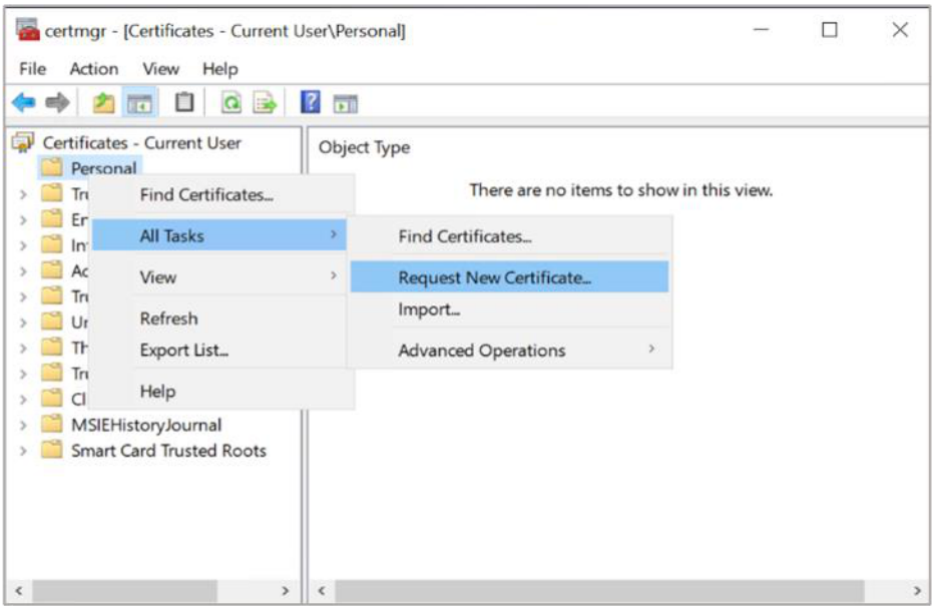

Figure 48: Certificate Manager window

3. Click Next

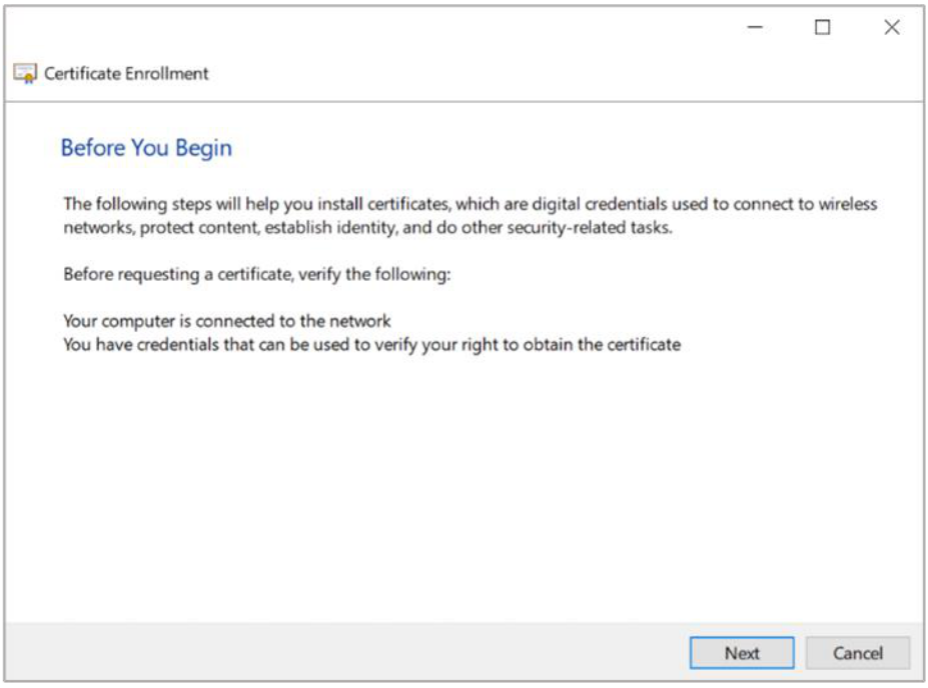

Figure 49: Before You Begin window

4. Select Certificate Enrollment Policy and click Next

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

5. Select the above created Key Recovery Agent check box and click Enroll

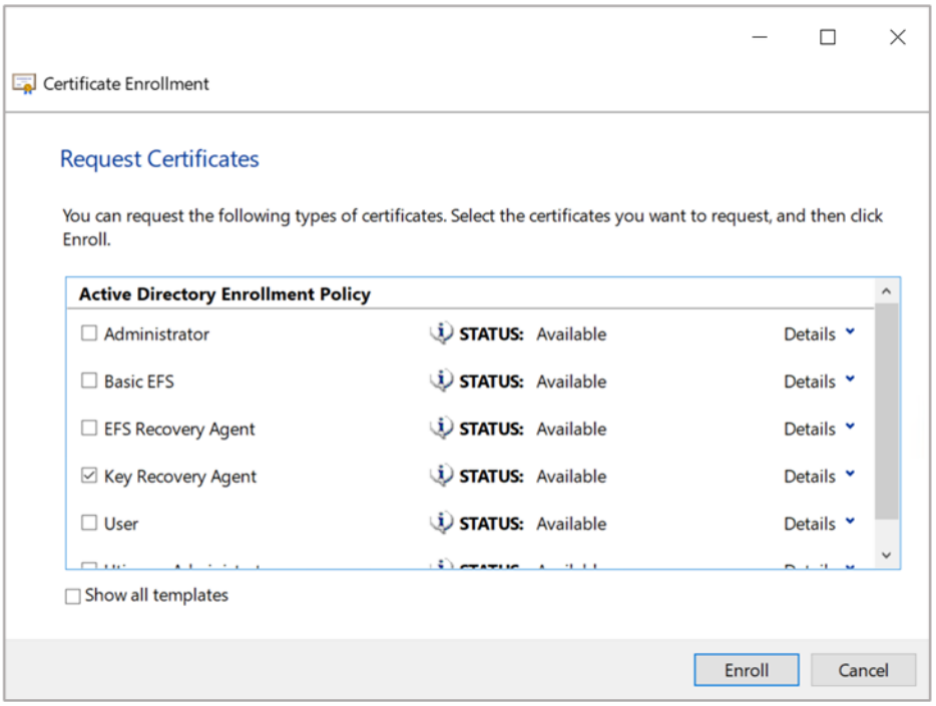

Figure 50: Certificate Enrollment window

6. Verify the Enrollment is pending and click Finish

10.1.4 Issue the KRA Certificate

1. Open the command prompt and run the `certsrv.msc` command
2. Select the Pending Requests node. Right-click on the latest request for the KRA template. Select All Tasks and click Issue

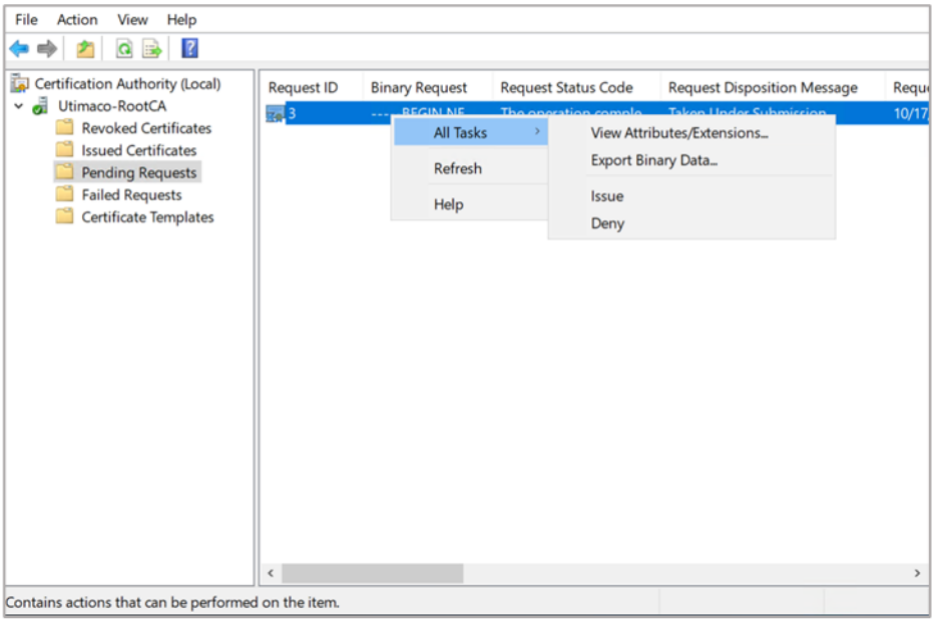

Figure 51: Certificate Authority window

3. Select the Issued Certificates

4. Verify that the new certificate is issued

10.1.5 Retrieve the issued certificate from CA

1. Open the command prompt and run certmgr.msc command
2. Right click on the Certificates then select Current User
3. Select All Tasks and select Automatically Enroll and Retrieve Certificates… and click Next

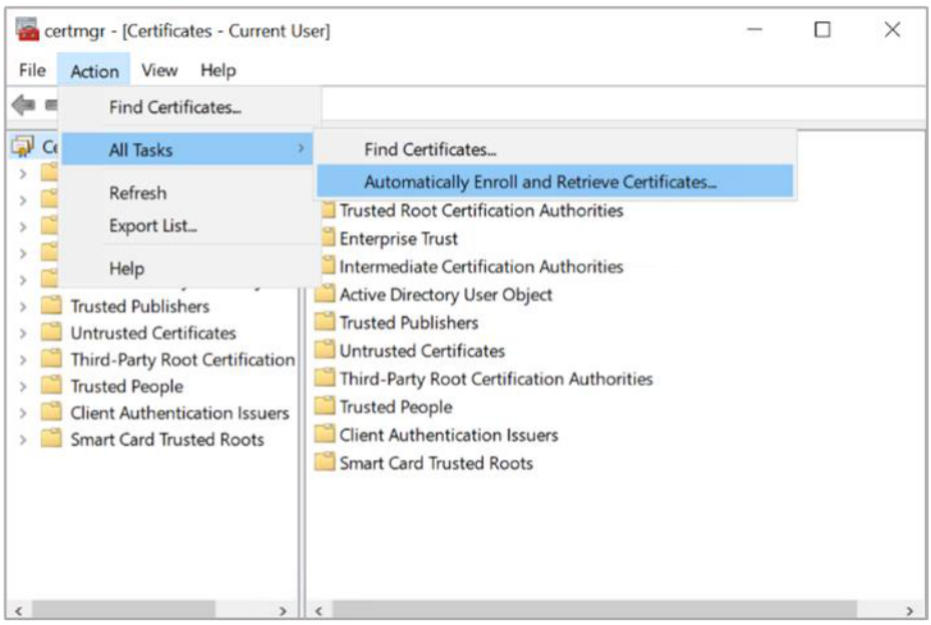

Figure 52: Certificate Manager window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

4. Select the KRA certificate you just issued and enroll it

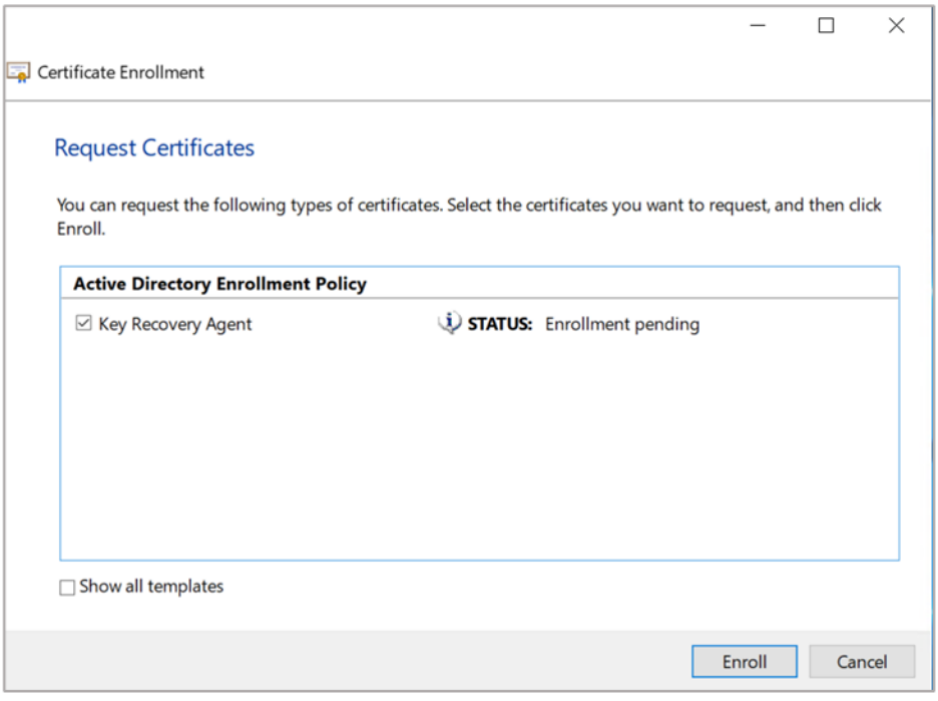

Figure 53: Request Certificates window

5. Click Finish

10.1.6 Configure the CA to support Key Archival

1. Open the command prompt and run the certsrv.msc command
2. Right click CA Name and select Properties
3. Select the Recovery Agent tab

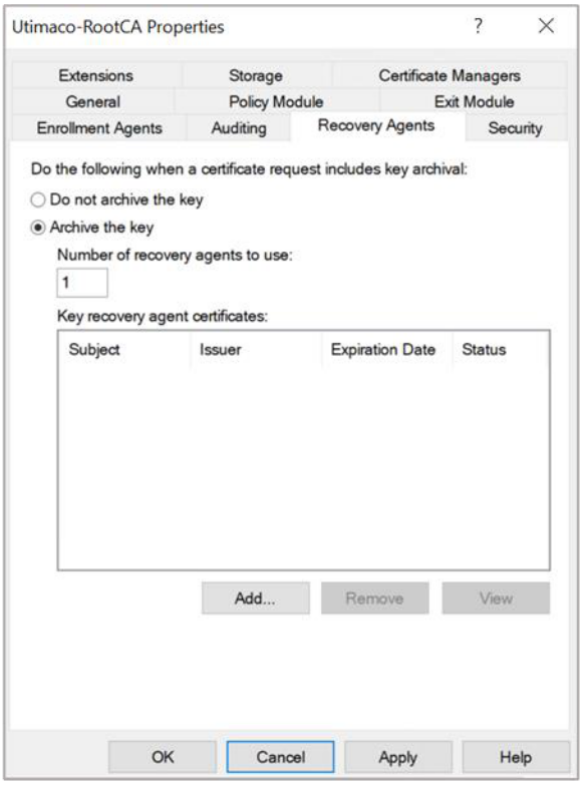

Figure 54: Recovery Agents Tab window

4. Select the radio button for Archive the key
5. Click Add

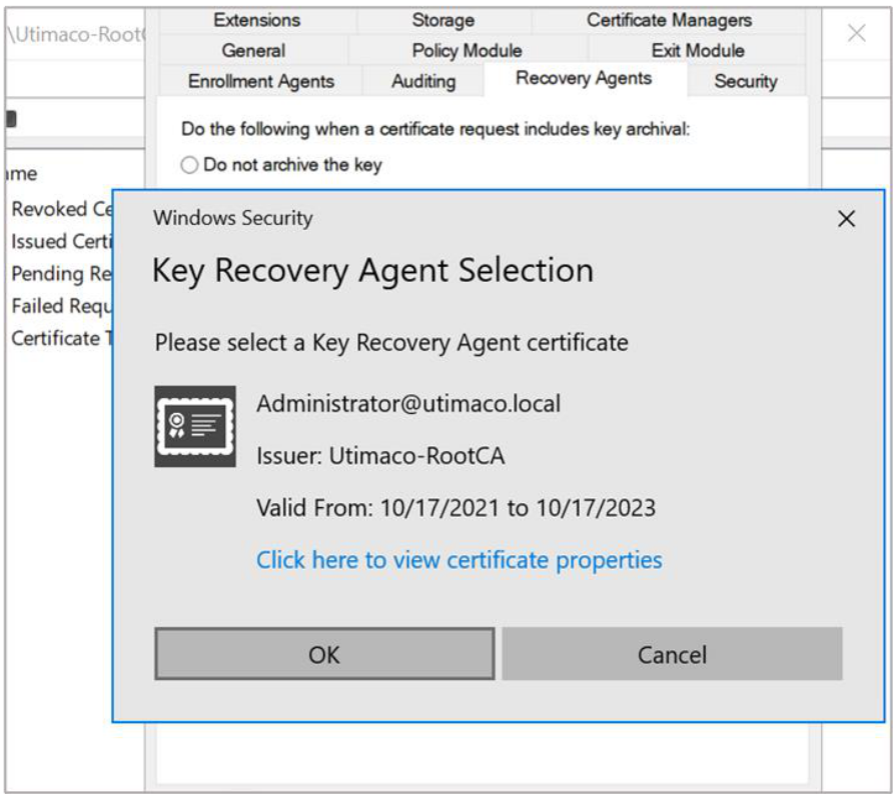

Figure 55: Key Recovery Agent Selection window

6. Select the KRA certificate you just issued and Click OK

7. Click OK

8. Click Yes to restart the AD CS

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

10.1.7 Create a Template with Key Archival Enabled

1. Open the command prompt and run the certtmpl.msc command
2. Right-click the User template and select Duplicate Template

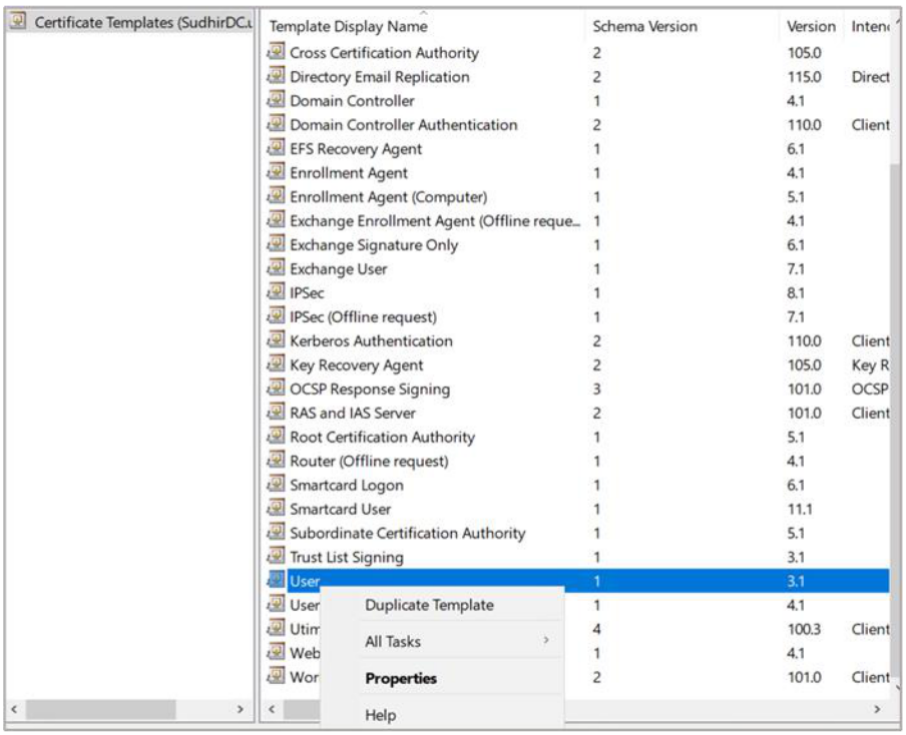

Figure 56: Certificate Template window

3. Select appropriate windows version under Certificate Authority and Certificate Recipient drop-down box under Compatibility Settings
4. Click OK

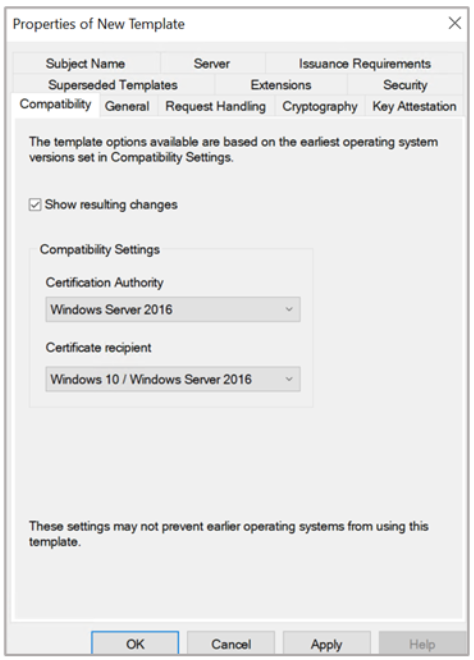

Figure 57: Compatibility window

5. On the Resulting Changes menu click OK
6. Go to the General tab and enter a name for the template (UserKeyArchival)
7. Go to the Request Handling tab and select the check box for Archive Subject's encryption private key

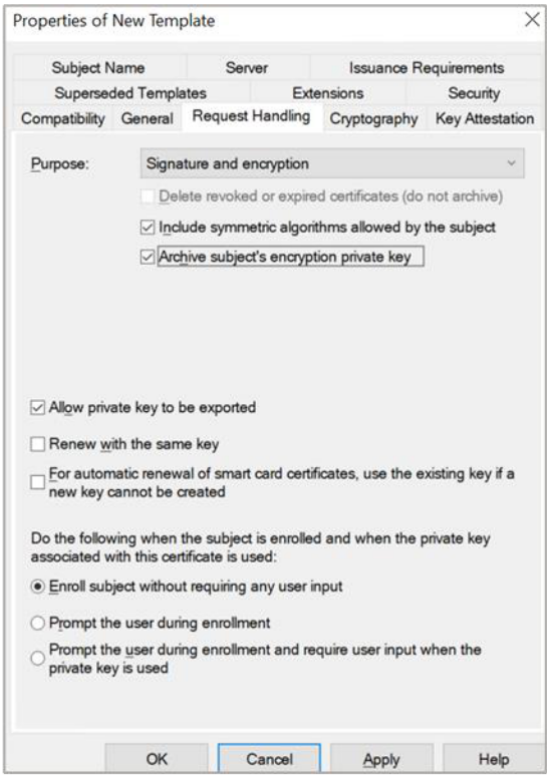

Figure 58: Request Handling window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

8. Select the Subject Name tab. Uncheck the check box for Include e-mail name in subject name and uncheck the check box for E-mail name

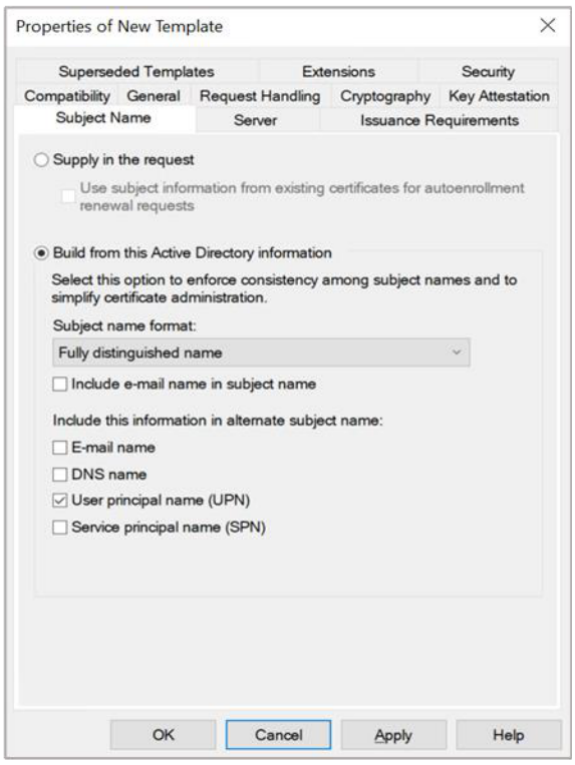

Figure 59: Subject Name Tab window

9. Click Apply and then Click OK

10.1.8 Add a new Template to CA for Issuing

1. Open the command prompt and run the certsrv.msc command
2. Right-click on the Certificate Templates node. Select New and then select Certificate Template to Issue

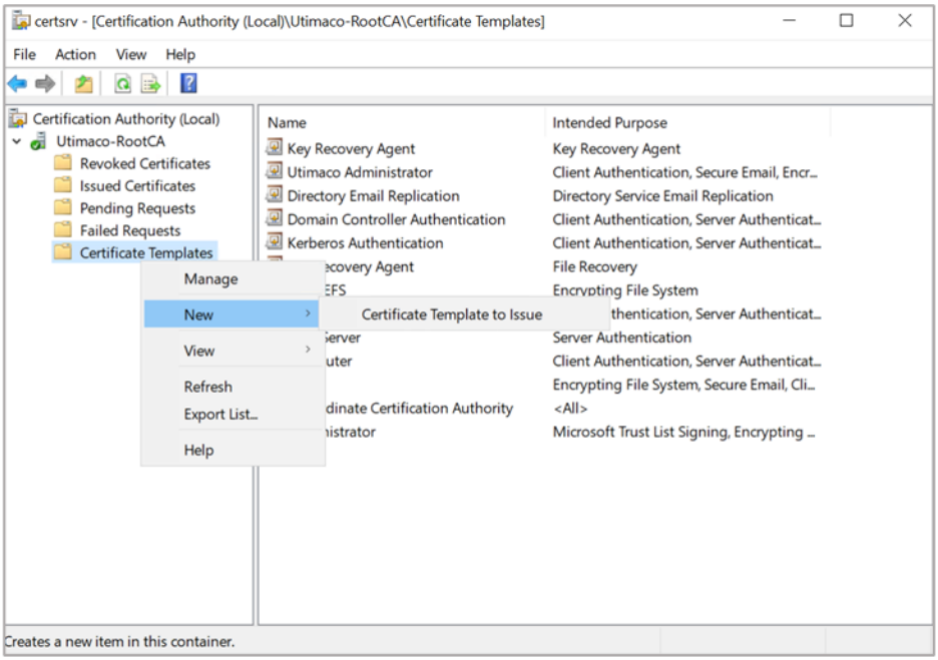

Figure 60: Certificate Authority window

3. Select new template for key archival, click OK

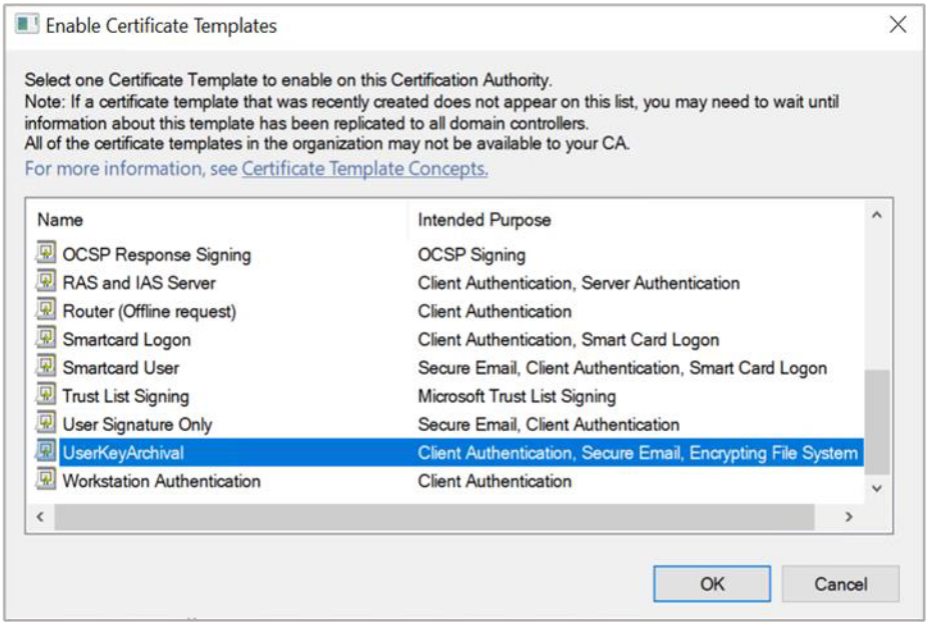

Figure 61: Enable Certificate Templates window

10.1.9 Issue a user template with key archival enabled

1. Open the command prompt and run the certmgr.msc command

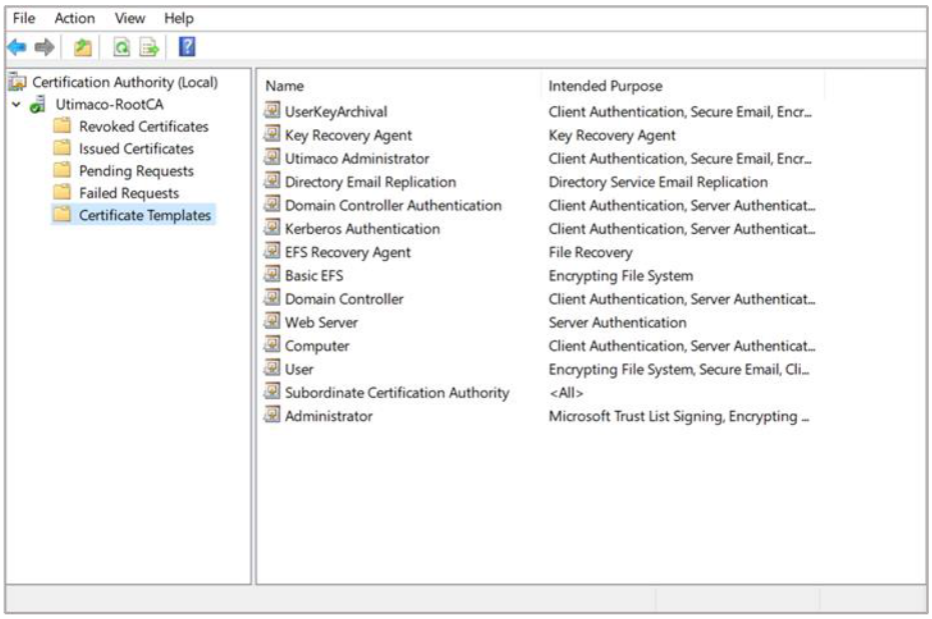

Figure 62: Certificate Templates window

2. Right-click Personal node. Select All Tasks and select Request New Certificate, Click Next for next two windows

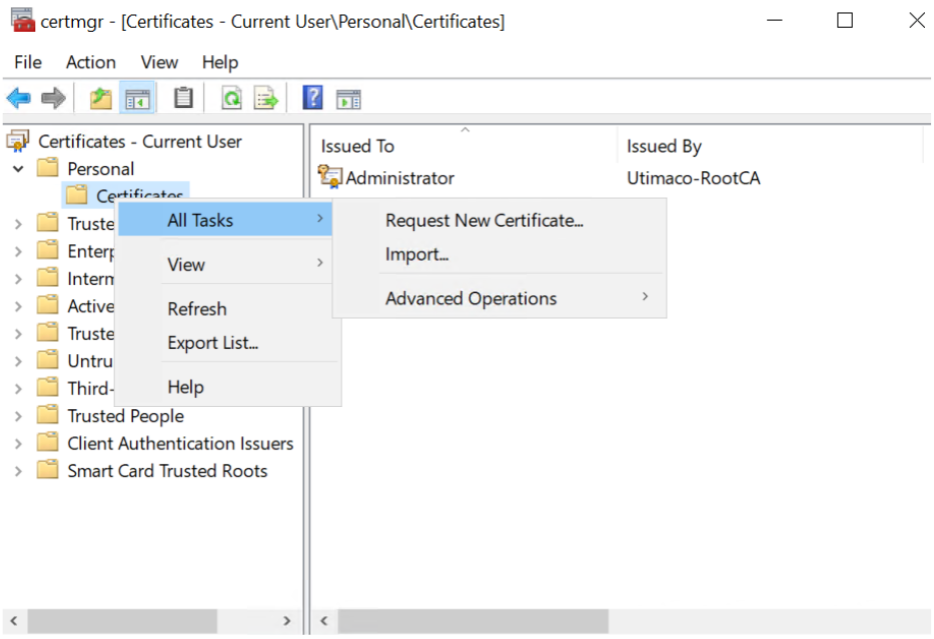

Figure 63: Certificate Manager window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

3. Select the check box for New template for key archival and click Enroll

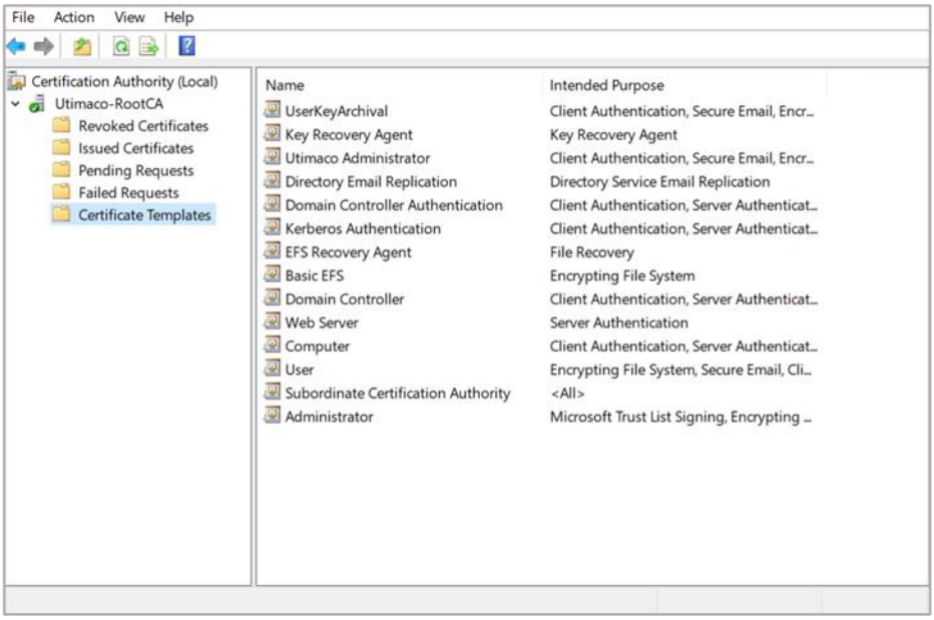

Figure 64: Certificate Templates window

4. The Enrollment Wizard displays. Verify the enrollment is successful and click Finish

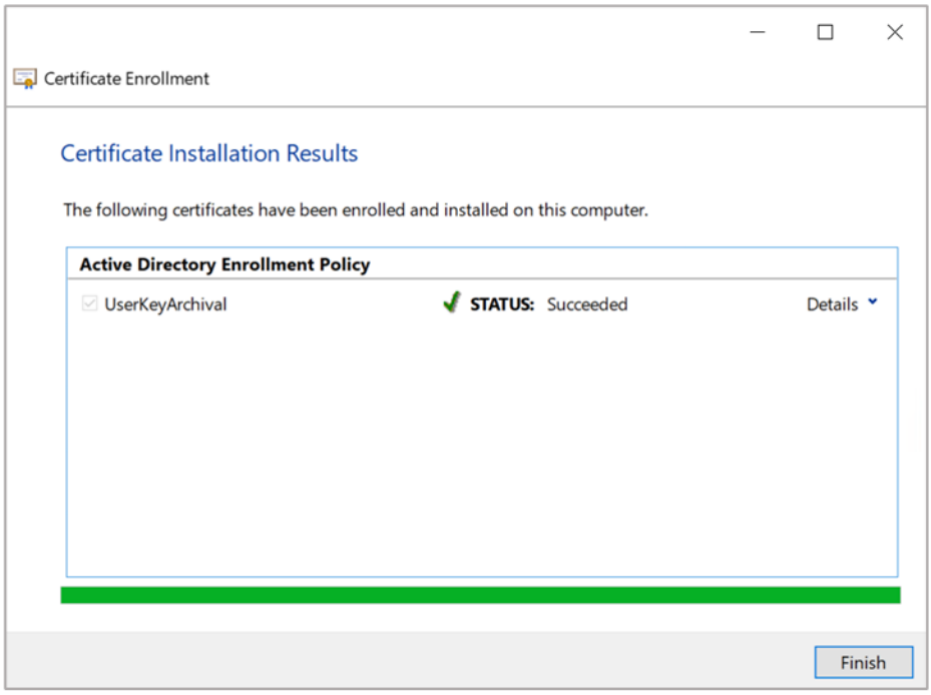

Figure 65: Certificate Enrollment window

10.2 Perform Key Recovery

You can recover archived keys. To perform a key recovery:

1. Open the command prompt and run the certsrv.msc command
2. In the console tree, double-click Certificate Authority, and then click Issued Certificates
3. Select View and select Add/Remove Columns
4. In Add/Remove Columns, in Available Column select Archived Key, and then click Add.Archived Key should now appear in Displayed Columns

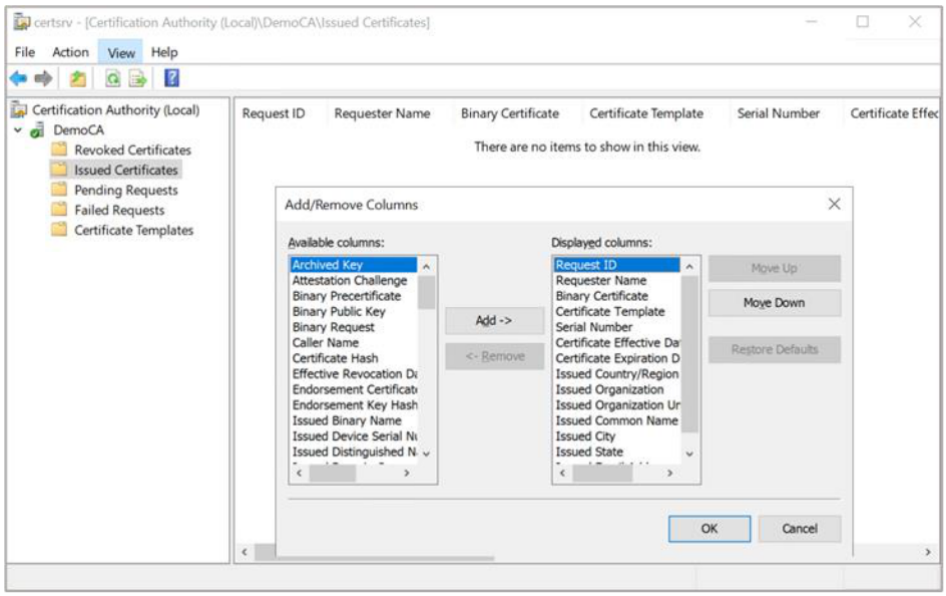

Figure 66: Archived Key window

5. Click OK and then in the details pane, scroll to the right and confirm that the last issued certificate to UserKeyArchival has a Yes value in the Archived Key column

A certificate template must have been modified so that the Archive bit and Mark Private Key as Exportable attributes were enabled. The private key is only recoverable if there is data in the Archived Key column.

6. Double-click the Archive User certificate
7. Select the Details tab and write down the serial number of the certificate
8. Click OK
9. Close the Certification Authority

10. Recover the private key into output file, open the command prompt and run the command below

›_ Console

```
> Certutil -getkey <serialnumber> output
```

11. Recover the certificate, open the command prompt and run the command below

›_ Console

```
> Certutil -recoverkey output user.pfx
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

12. When prompted, enter the following information:

Enter new password: password

Confirm new password: password

13. Type exit, and then press ENTER
14. Close all windows and log off as the current user
15. Import the recovered private key/certificate

a) Open the command prompt run the certmgr.msc command

b) Right-click Certificates (Current User), and then select Find Certificates

c) In Find Certificates, under Contain type CA Name and then click Find Now

d) In Find Certificates, on the Edit menu, click Select All

e) In Find Certificates, on the File menu, click Delete

f) In Certificates, click YES

g) Close Find Certificates

16. Import the certificate at c:\user.pfx and let the certificates be placed by the system

a) In the console tree, right-click Personal and then select All Tasks and then click Import

b) In the Certificate Import Wizard, click Next

c) In the Files to Import, in the File name box, type c:\user.pfx and then click Next

d) In Password, type password and then click Next

e) In Certificate Store, select Automatically select the certificate store based on the type of certificate and then click Next

f) In the Completing the Certificate Import Wizard, click Finish

17. Verify the serial number of the imported certificate

a) In the console tree, double-click Personal and then click Certificates

b) Double-click the certificate

c) In Certificate, go to the Details tab. Verify that the serial number matches the original

11 Migrating the Microsoft Software Key of AD CS to Utimaco HSM

11.1 Installing AD CS with Locally Stored Primary Key

1. Join a machine to the Domain and Log in as a user with Administrative privileges
2. Select Start and select Server Manager to open Server Manager. Select Manage, then select Add Roles & Features

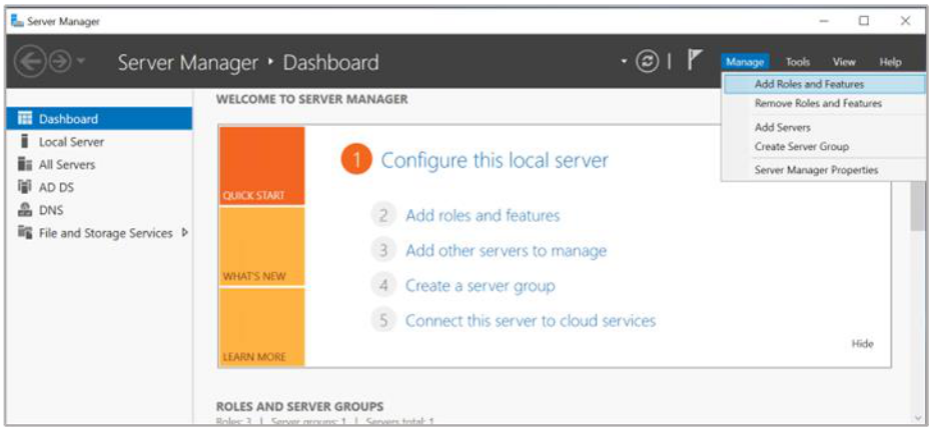

Figure 67: Server Manager window

3. The Before you begin window opens. Select Next

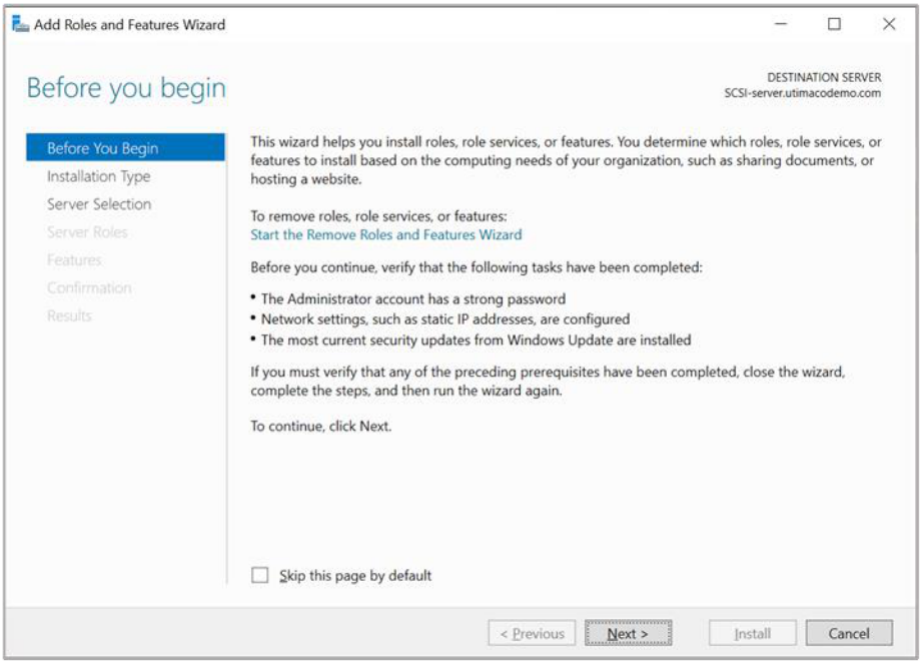

Figure 68: Before You Begin window

4. On the Select installation type window, make sure the default Role or Feature Based Installation is selected. Click Next

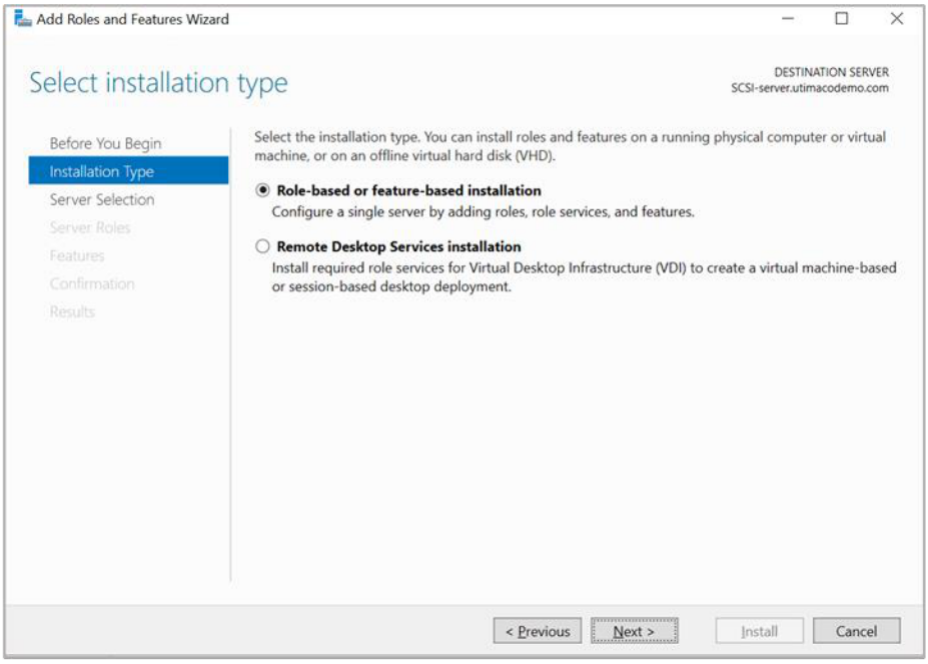

Figure 69: Select Installation Type window

5. On Server selection, select a server from the server pool. Click Next

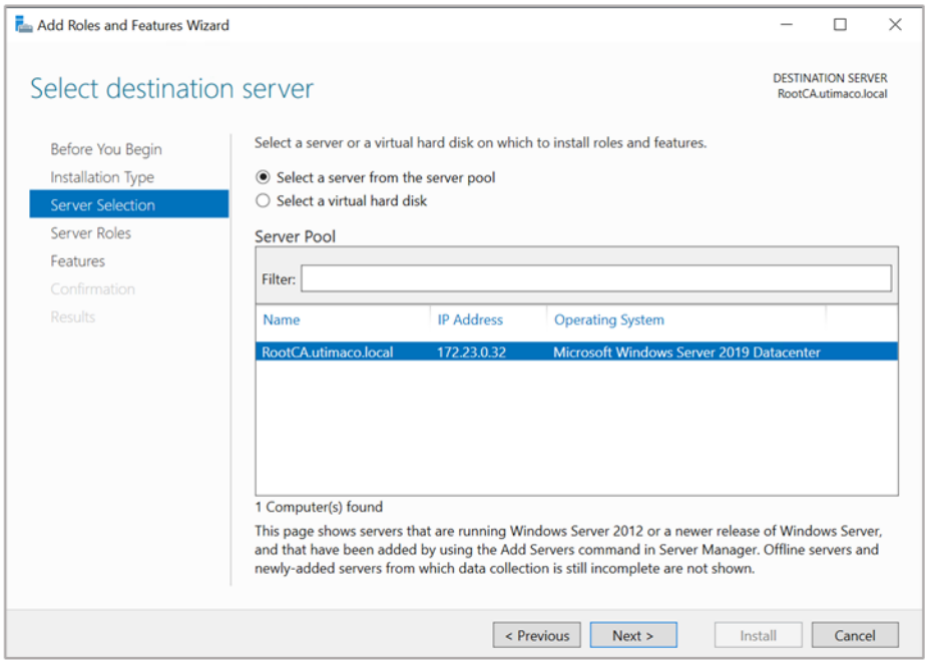

Figure 70: Select Destination Server window

6. On the Select server roles window, select the Active Directory Certificate Services role

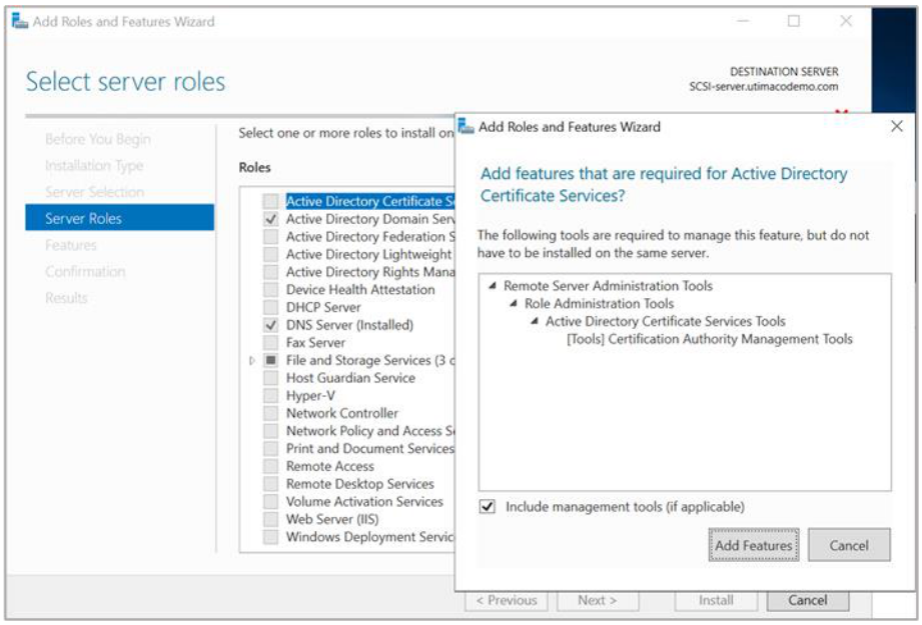

Figure 71: Select Destination Server window

7. When prompted to install Remote Server Administration Tools, select Add Features. Click Next
8. On the Select features window, click Next
9. On the Active Directory Certificate Services window, click Next

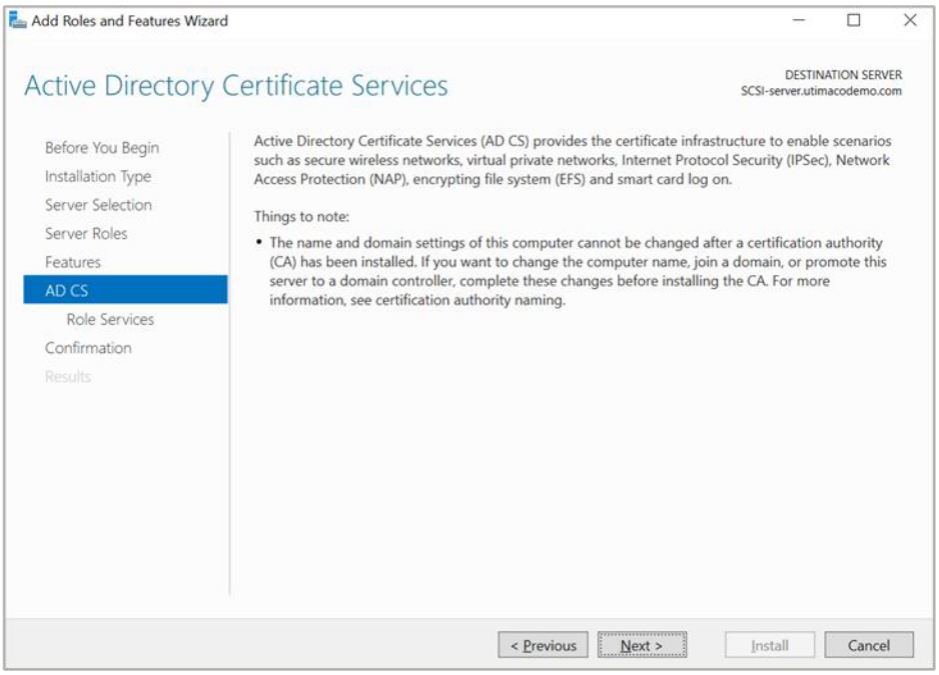

Figure 72: Active Directory Certificate Services window

10. On the Select role services window, the Certification Authority role is selected by default. Click Next

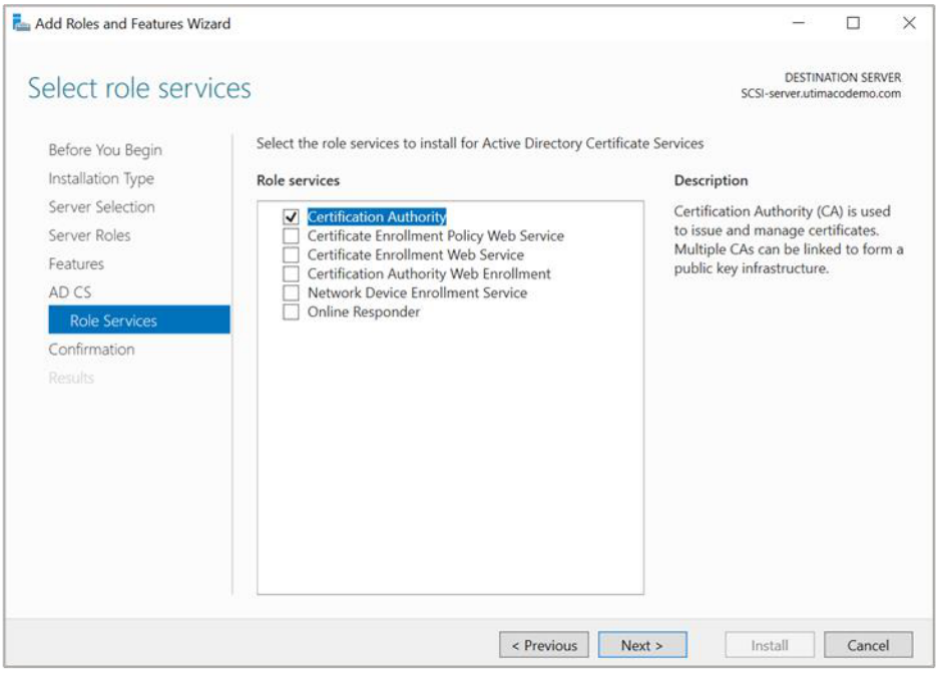

Figure 73: Select Role Services window

11. On the Confirm installation selections window, verify the information then click Install

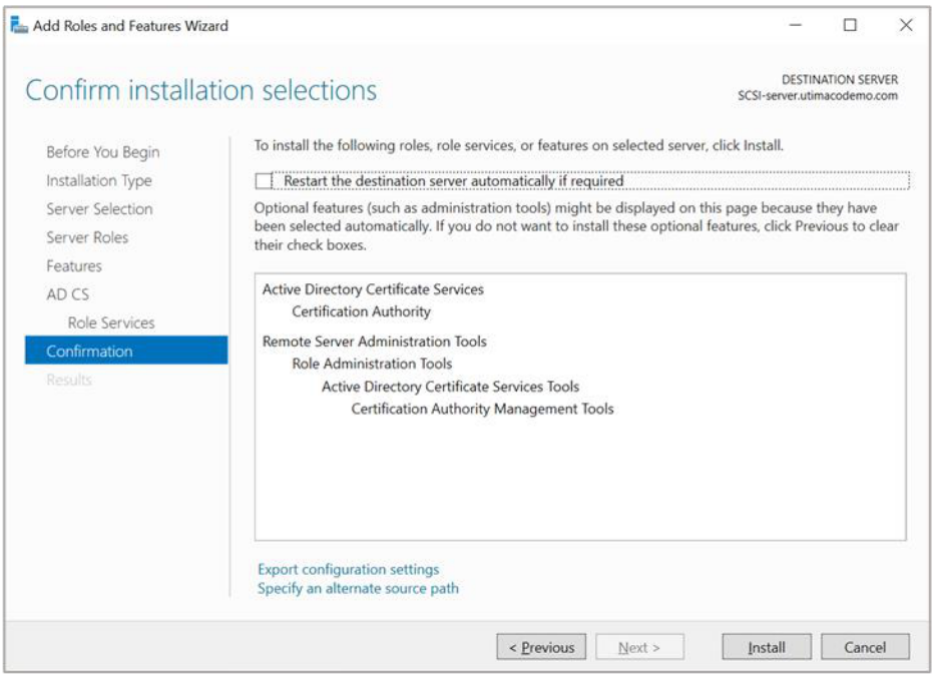

Figure 74: Confirm Installation Selections window

12. When the installation is complete, select the Configure Active Directory Certificate Services on the destination server link

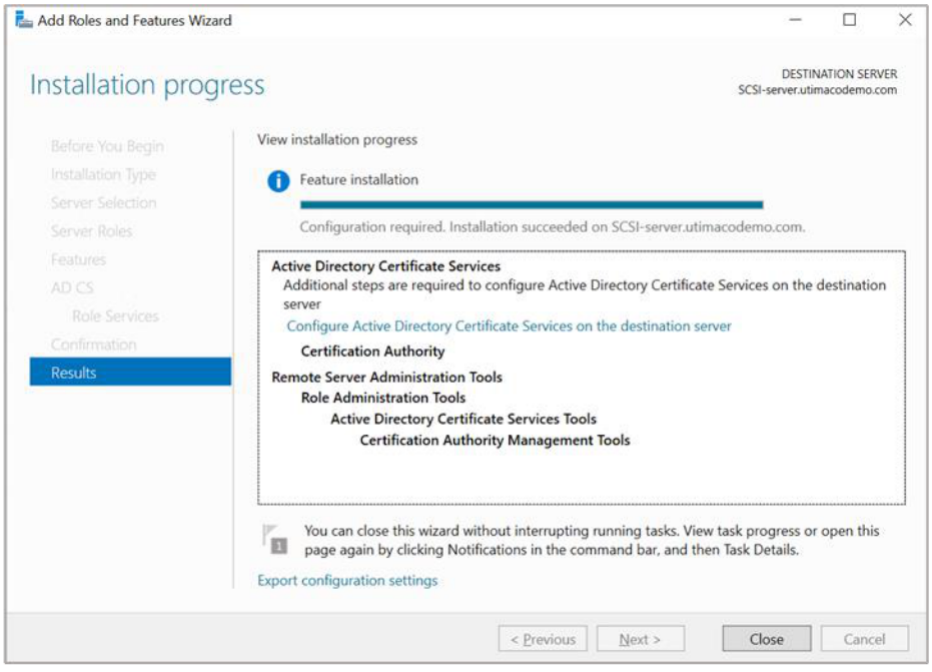

Figure 75: Installation Progress window

13. On the Credentials window, make sure that Administrator's credentials are displayed in the Credentials box. If not, select Change and specify the appropriate credentials. Click Next

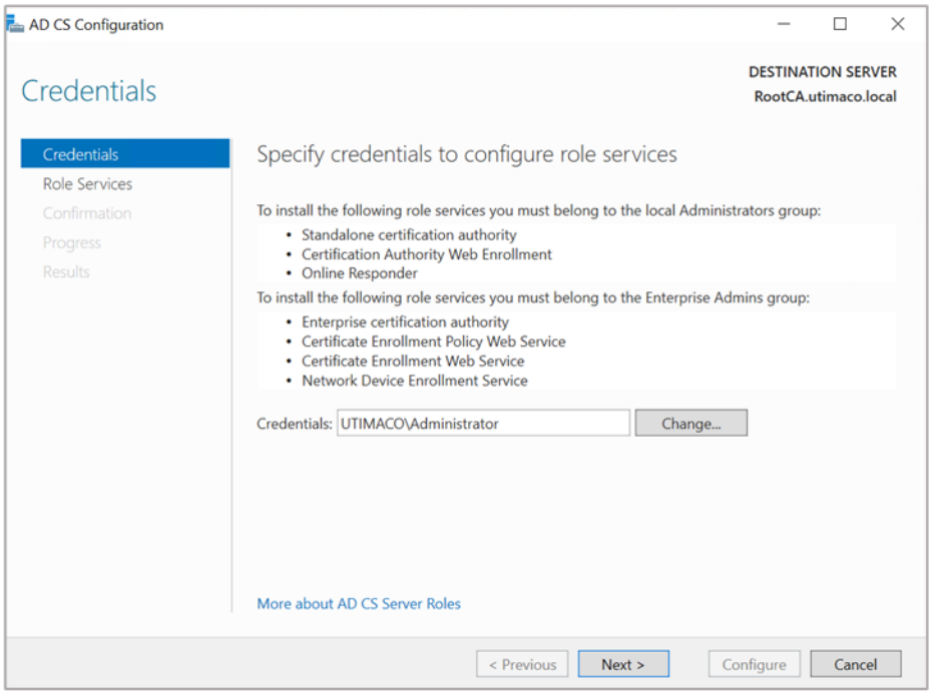

Figure 76: Credentials window

14. On the Role Services window, select Certification Authority. This is the only available

selection when the certification authority role is installed on the server, click Next

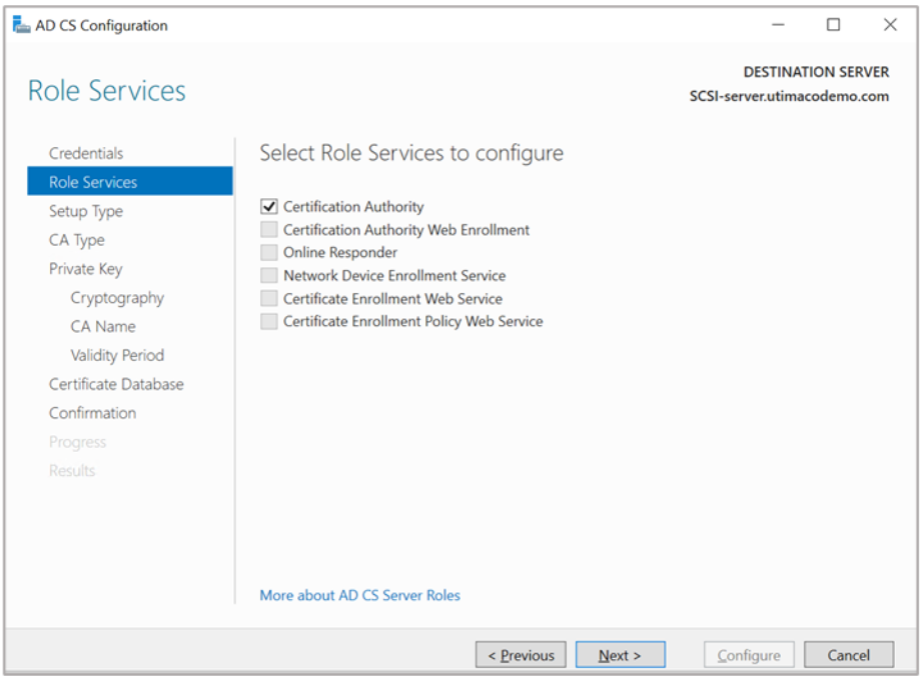

Figure 77: Credentials window

15. On the Setup Type window, select the appropriate CA setup type for your requirements. Click Next

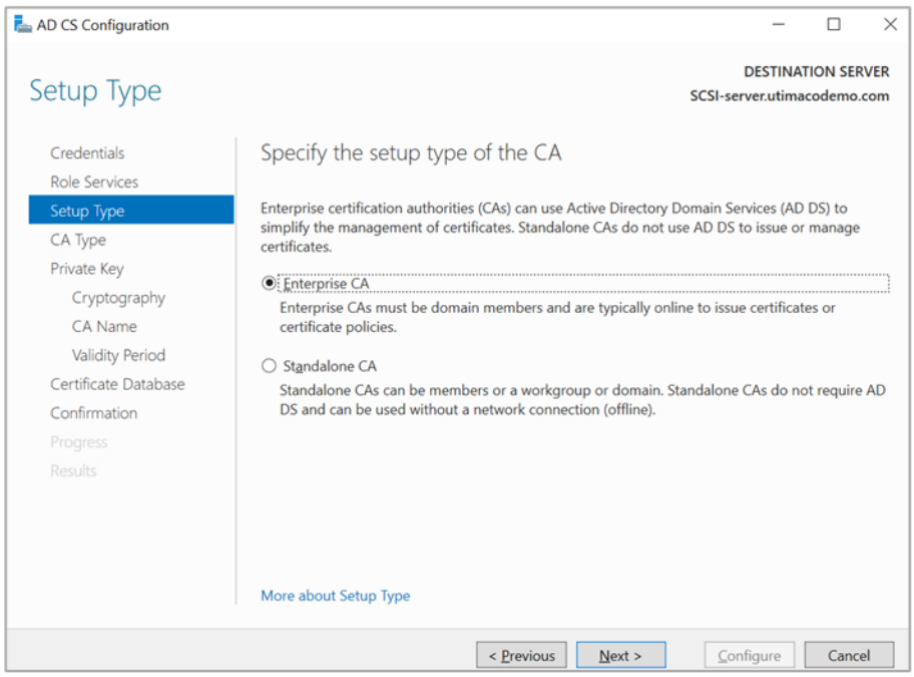

Figure 78: Setup Type window

16. On the CA Type window, Root CA is selected by default. Click Next

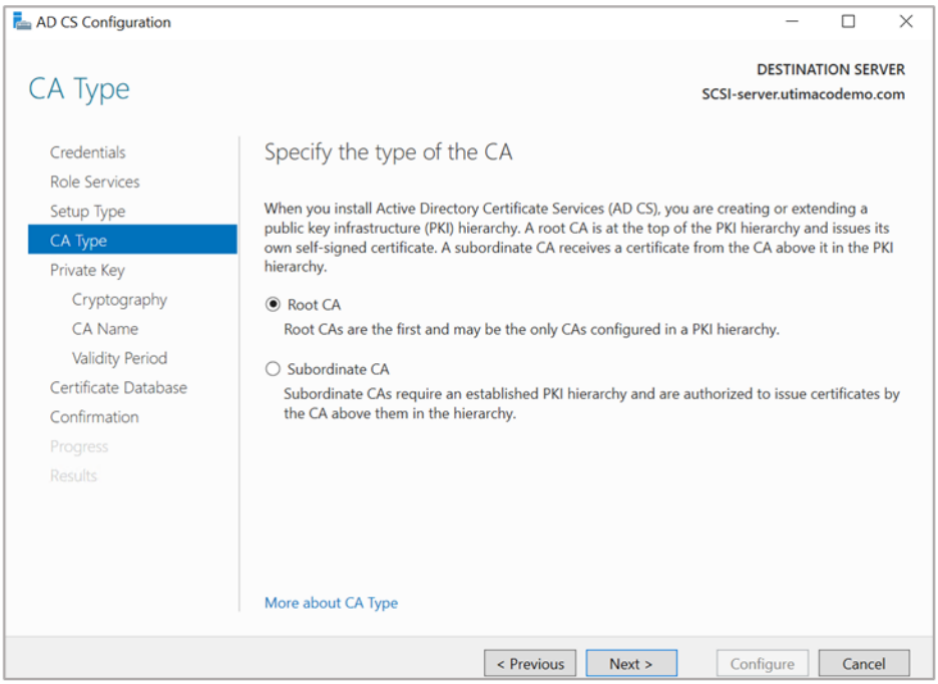

Figure 79: CA Type window

17. On the Private Key window, leave the default selection to Create a new private key selected. Click Next

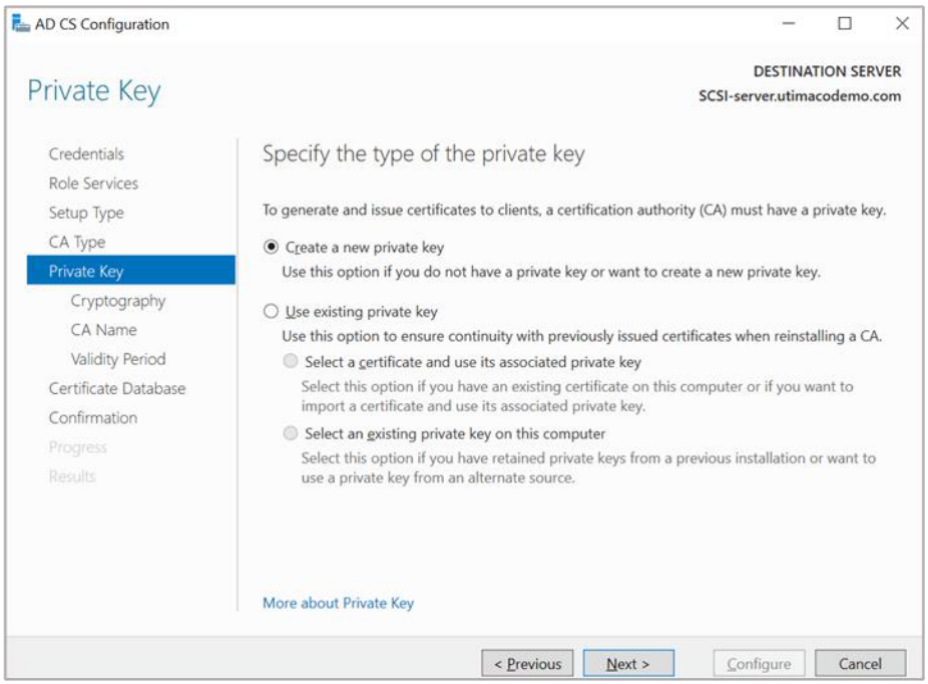

Figure 80: Private Key window

18. On the Cryptography for CA window, select the appropriate Microsoft cryptographic provider along with the key type, key length, and suitable hash algorithm and click Next

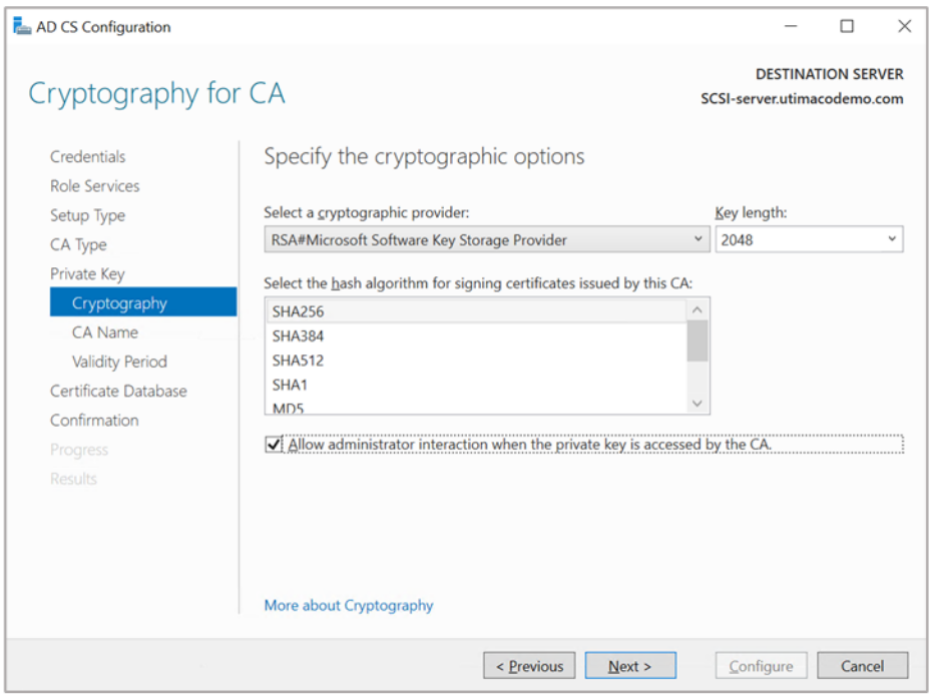

Figure 81: Cryptography for CA window

19. On the CA Name window, give the appropriate CA name. Click Next

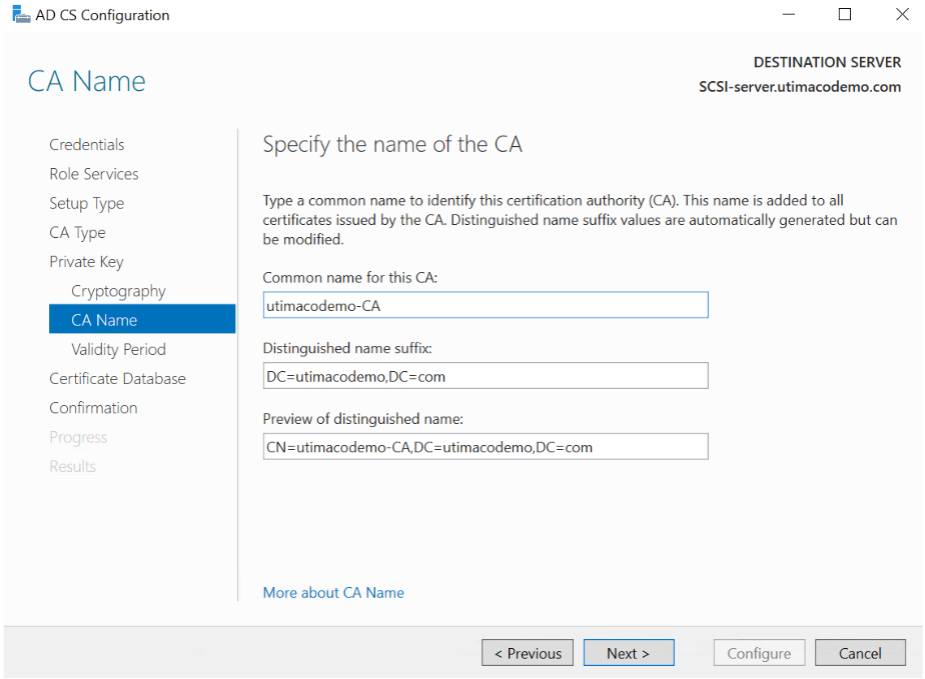

Figure 82: CA Name window

20. On the Validity Period window, enter the number of years for the certificate to be valid. Click Next

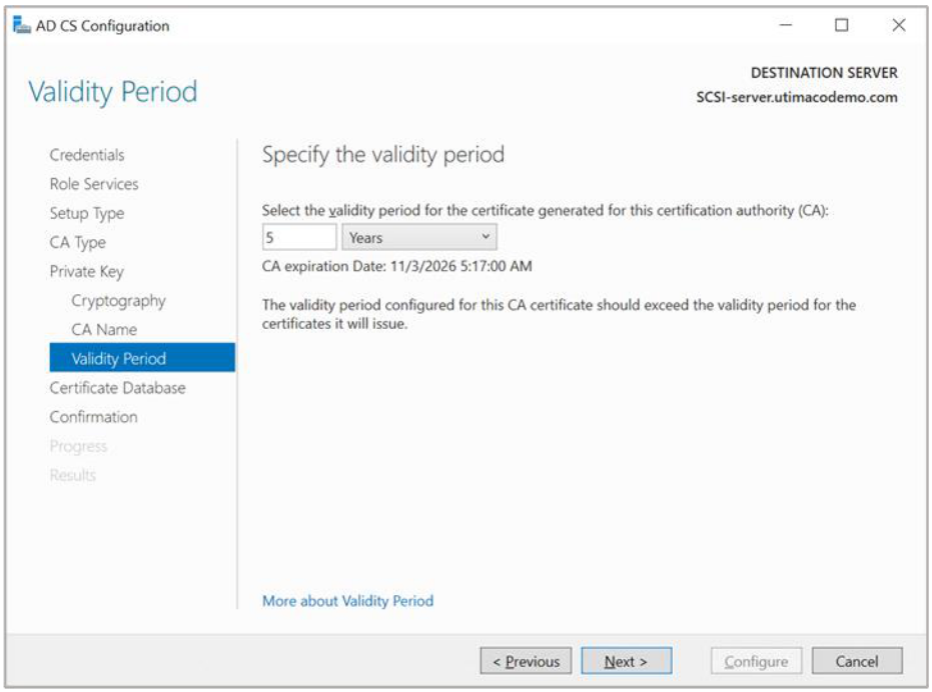

Figure 83: Validity Period window

21. On the CA Database window, leave the default locations for the database and database log files. Click Next

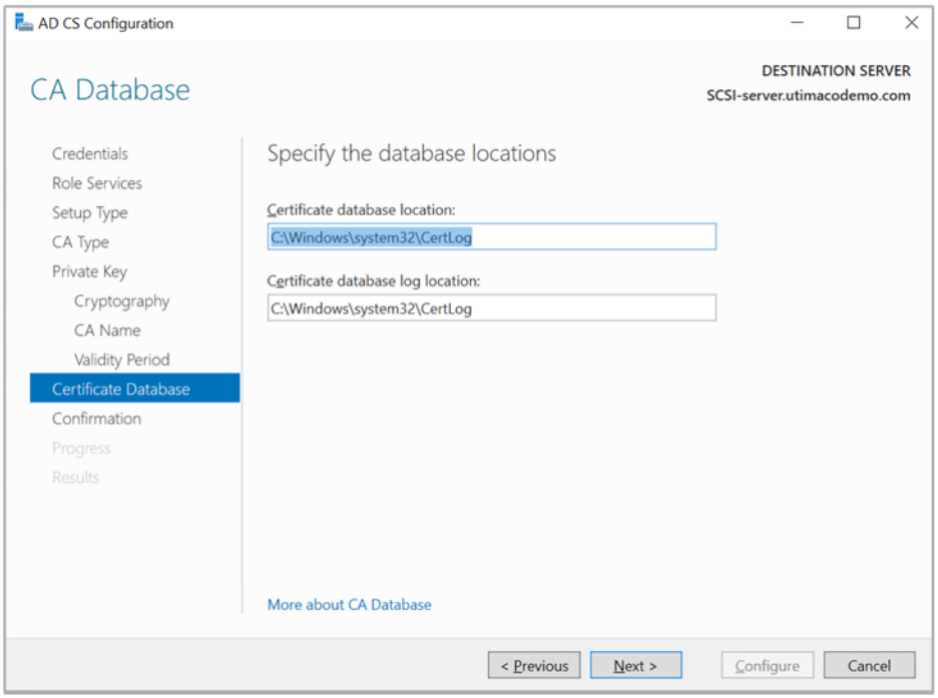

Figure 84: CA Database window

22. On the Confirmation window, click Configure

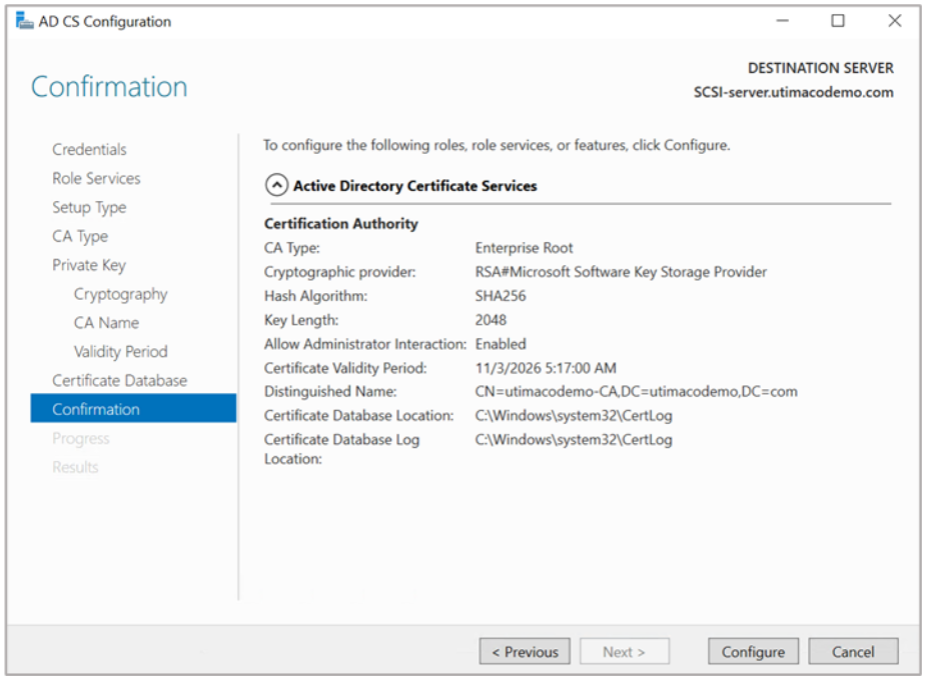

Figure 85: Confirmation window

23. Click Close to exit the AD CS Configuration wizard after viewing the installation results. A private key for the CA will be generated and stored on the HSM

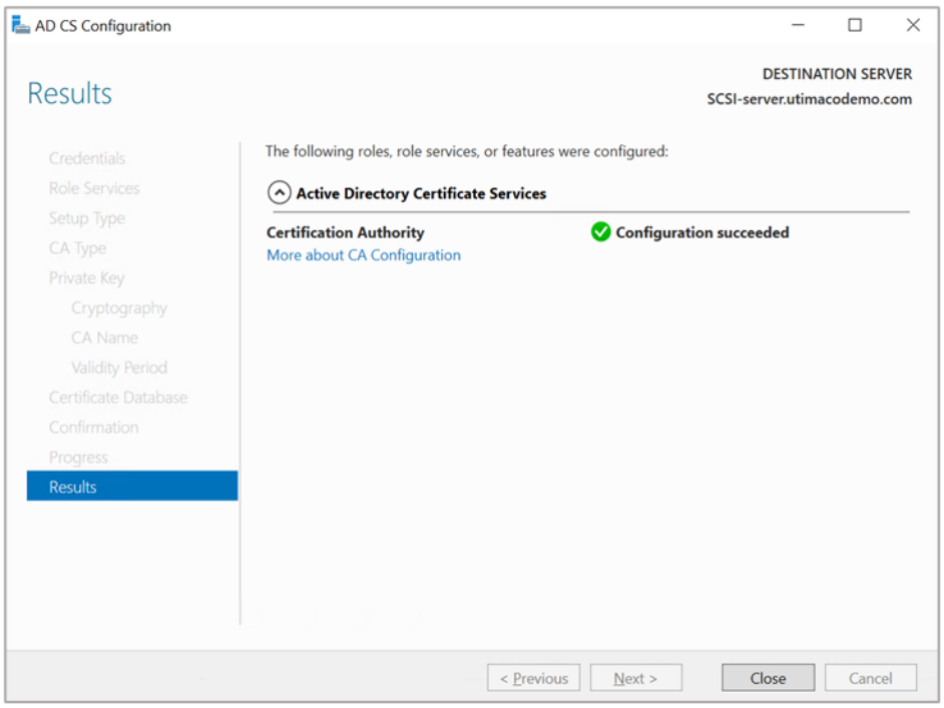

Figure 86: Results window

24. Open a command prompt and run the following command to verify that service is running:

›_ Console

```
> sc query certsvc
```

25. Open a command prompt and run the following command to verify the CA key:

›_ Console

```
> certutil -verifykeys
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

11.2 Create a Backup of CA Database

›_ Console

```
#Create a database and private key backup

> certutil.exe -backup <drive>:\CaBackup

#Create a certificate backup

> certutil -ca.cert "<drive>:\CaBackup\<CA_Name>.cer"

#Create a registry export

>reg export HKLM\SYSTEM\CurrentControlSet\services\CertSvc

<drive>:\CaBackup\CAregistry.reg

#stop the AD CS service

> net stop certsvc
```

11.3 Importing Private Key to HSM

The private key, created with the backup command (check the Section Create a Backup of CA Database), needs to be imported to the HSM

1. Open a command prompt as an Administrator and use the below command to import the .p12 file to the HSM

›_ Console

```
> cngtool Name=<key_name> [Spec=<key_specifier>] [Type=<type>]
[Password=<pass>] ImportKey=<filename>
```

Example

›_ Console

```
> cngtool Name=PrivateKey Spec=0 Type=PKCS8 Password=123456
ImportKey=C:\CaBackup\Root-CA.p12
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

2. Check with the cngtool whether the private key was imported successfully

›_ Console

```
> cngtool ListKeys
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

11.4 Synchronizing HSMs

If the environment has a High Availability setup, the HSMs must be synchronized.

1. Open the Crypto Administration Tool
2. Make sure the HSM is connected and in an operational mode
3. Select on Login/Logoff to open the Login/Logoff User window
4. Login the appropriate users to achieve the permission level of at least 22000000
5. Select Backup/Restore to open the CryptoServer Database Backup/Restore Wizard window

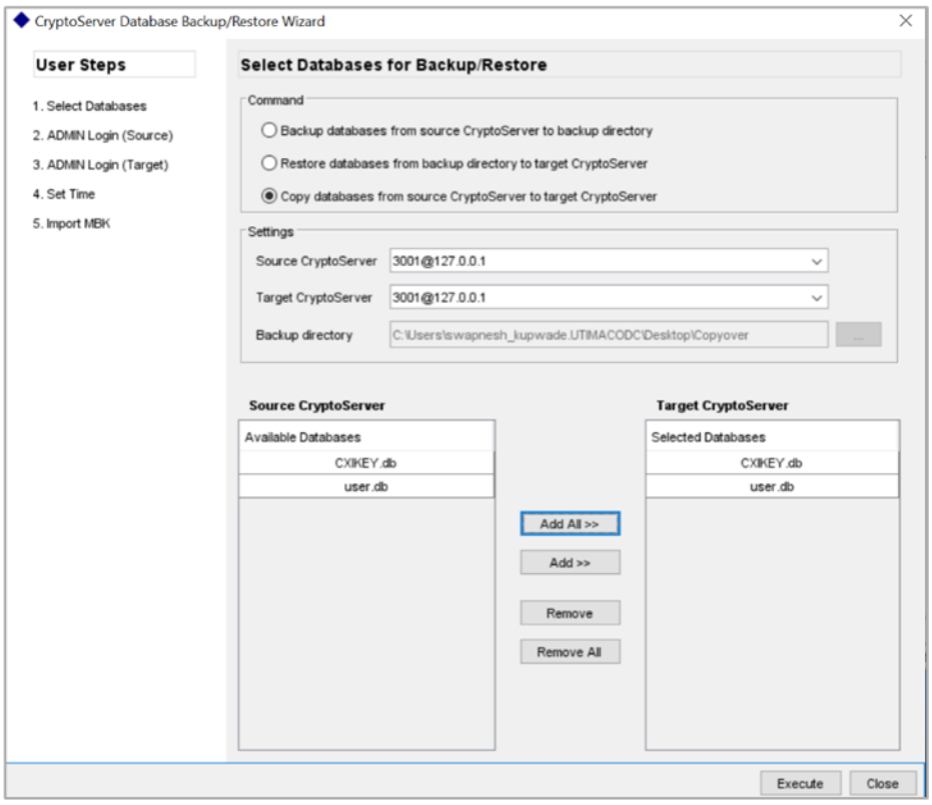

Figure 87: CryptoServer Database Backup/Restore Wizard window

6. In the Command section select Copy databases from Source CryptoServer to Target CryptoServer

7. In the Settings section Select the appropriate Source CryptoServer, if available select the appropriate Target CryptoServer, In the Backup directory section type the appropriate backup directory path (set to `C:\Program Files\Utimaco\CryptoServer\Administration` as default) or click … to browse to the appropriate directory

8. Select the databases to copy

9. Click Execute

10. A confirmation window appears

11.5 Reintroduce the Certificate

The certificate must be deleted and imported to connect it with the key that is stored in the HSM. PowerShell was used for this task.

1. Get the certificate thumbprint

›_ PowerShell

```
PS> Get-ChildItem -Path cert:\LocalMachine\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint Subject

---------- -------

BE82E0FEC4B7F9DA33FF5CC2A0CC4D987F04A11B CN=DemoRootCa, DC=Uti2, DC=si

Then we extract the container name

PS> certutil -store my BE82E0FEC4B7F9DA33FF5CC2A0CC4D987F04A11B | findstr

"Subject: sha1 Unique Provider"

Subject: CN=DemoRootCa, DC=Uti2, DC=si

Cert Hash(sha1): be82e0fec4b7f9da33ff5cc2a0cc4d987f04a11b

Unique container name: 2fc25277ec718baa2886124e04bc16e7_36ed1a95-76e3-

4398-a4c7-c31d5fce304f

Provider = Microsoft Software Key Storage Provider
```

2. Make sure that the file is located on the local disk (one of the two possibilities, depending on the installation)

›_ PowerShell

```
PS> Get-Item C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\<container>
PS> Get-Item C:\ProgramData\Microsoft\Crypto\Keys\<container>
```

3. Delete the certificate

›_ PowerShell

```
PS>Remove-Item -Path cert:\LocalMachine\My\<thumbprint> -DeleteKey
```

4. Check if the certificate was deleted (one of the two possibilities, depending on the installation)

›_ PowerShell

```
PS> Get-Item C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\<container>
PS> Get-Item C:\ProgramData\Microsoft\Crypto\Keys\<container>
```

5. Import the certificate

›_ PowerShell

```
PS> certutil -addstore -f "My" "<CaName>.cer"
Signature matches Public Key
Certificate "DemoRootCa" added to store.
CertUtil: -addstore command completed successfully.
```

6. To create a link between the certificate and the private key, first find the certificate serial number

›_ PowerShell

```
PS> certutil "<CaName>.cer" | findstr Serial
Serial Number: 3a9f8a8c61129593400f6738896afcc0
```

7. And use the certutil command to repair the link

›_ PowerShell

```
PS> certutil –f –repairstore –csp "Utimaco CryptoServer Key Storage
Provider" my <serial>
CertUtil: -repairstore command completed successfully
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

11.6 Configuring AD CS to Use Utimaco CryptoServer Key Storage Provider

1. Create a .reg file and run it as an administrator or edit registry manually to configure the AD CS to use the private key stored in the HSM

`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CertSvc\Configuration\<CaName>\CSP] "Provider"="Utimaco CryptoServer Key Storage Provider"`

2. Start the service and check the status of the AD CS

›_ Console

```
> net start certsvc
```

3. Verify that the CA service has successfully started by running the command

›_ Console

```
>sc query certsvc
```

4. Verify the CA key by running the command:

›_ Console

```
>certutil -verifykeys
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

12 Installing and Configuring the AD CS Failover Cluster

The following sections describe the installation and configuration of a CA on a failover cluster running on Windows Server. Register Utimaco CryptoServer Key Storage Provider.

12.1 Installing AD CS Server role on first cluster node

1. Join a machine to the Domain and Log in as a user with Administrative privileges
2. The steps to install the Microsoft Active Directory Certificate Services are same as the Installing Microsoft Active Directory Certificate Services with Windows Enterprise section. After Microsoft ADCS is successfully installed, continue with the below steps
3. Open the command prompt and run certsrv.msc and then click OK

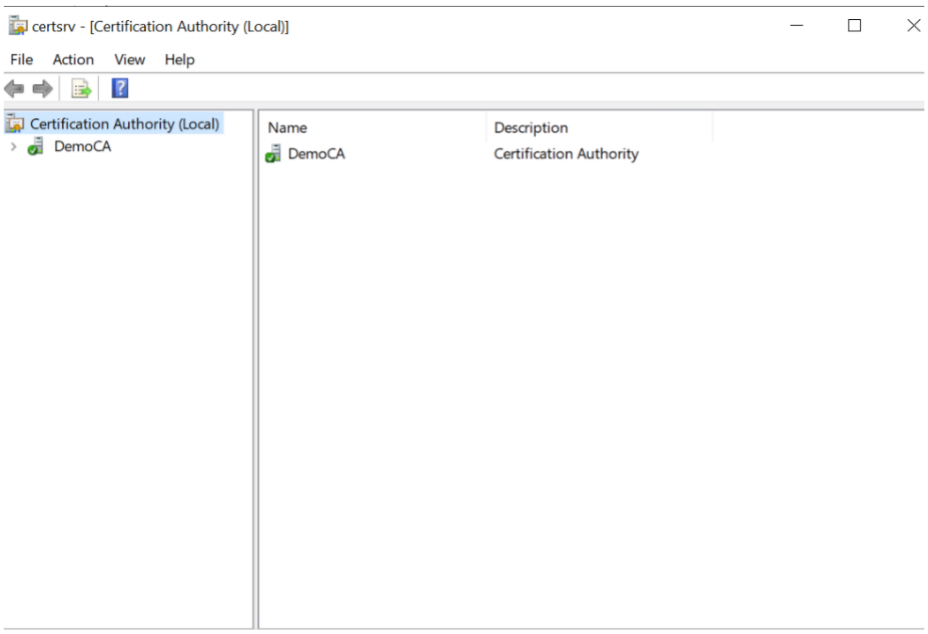

Figure 88: Certificate Authority window

4. Select the Certificate Authority node in the left pane
5. In the Action menu, select All Tasks and then select Backup CA

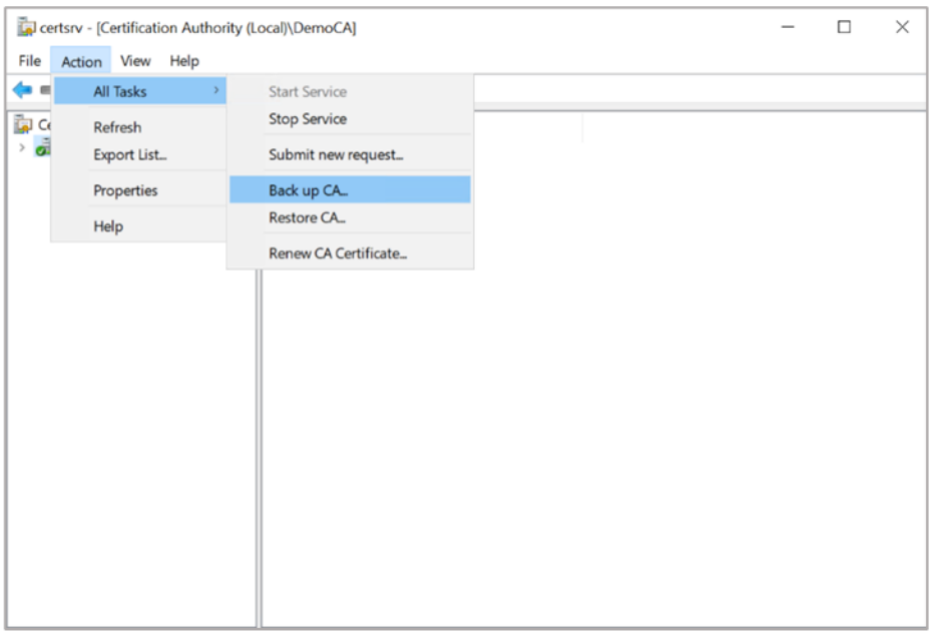

Figure 89: Certificate Authority window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

6. On the Welcome page of the CA backup wizard, click Next
7. Select Private key and CA certificate and provide a directory name where you will temporarily store the CA certificate and optionally the key. Click Next
8. Provide a password to protect the CA key and click Next

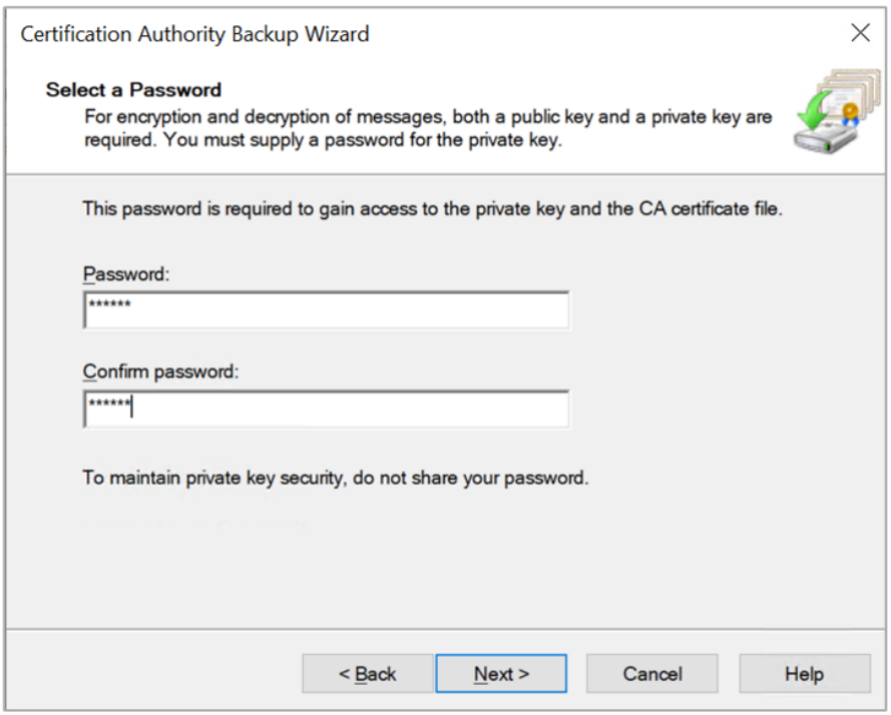

Figure 90: Certification Authority Backup window

9. Click Finish

Figure 91: Certification Authority Backup window

You will receive a warning message that the private key cannot be exported. This is expected behavior because the private key will never leave the Utimaco HSM

10. Click OK to continue
11. Export the CA Certificate

›_ Console

```
>certutil --ca.cert rootca_certificate.cer

CertUtil: -ca.cert command completed successfully.
```

12. Generate MBK and backup of the databases from first node using CryptoServer Administrator Tool (CAT)

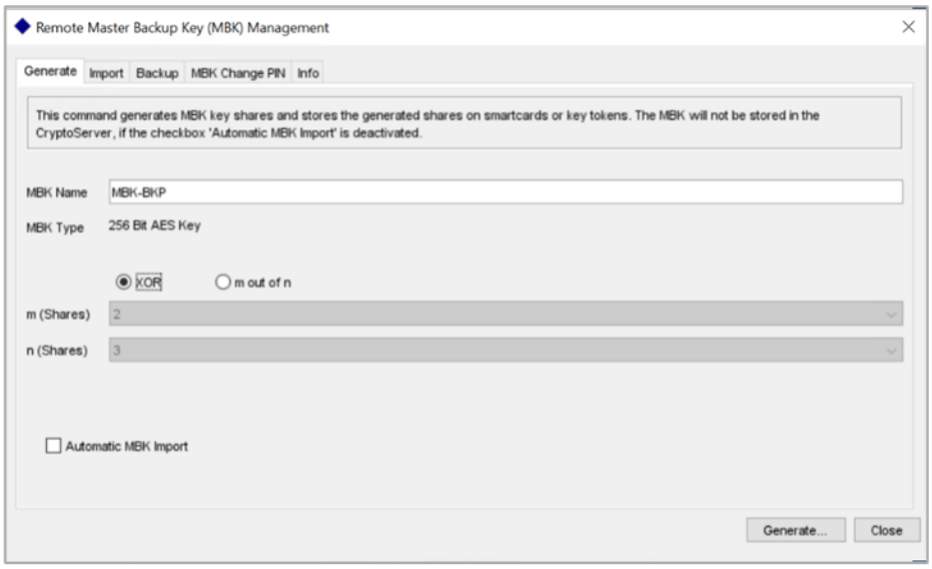

Figure 92: Remote master Backup Key Management window

13. Stop the certsvc service. Run:

›_ Console

```
>net stop certsvc
```

12.2 Detach the shared storage form the first cluster node

1. Select Start then select Server Manager to open Server Manager
2. Select the File and Storage Services. Select Disks, select shared disk resource, right click on it, and select Take Offline

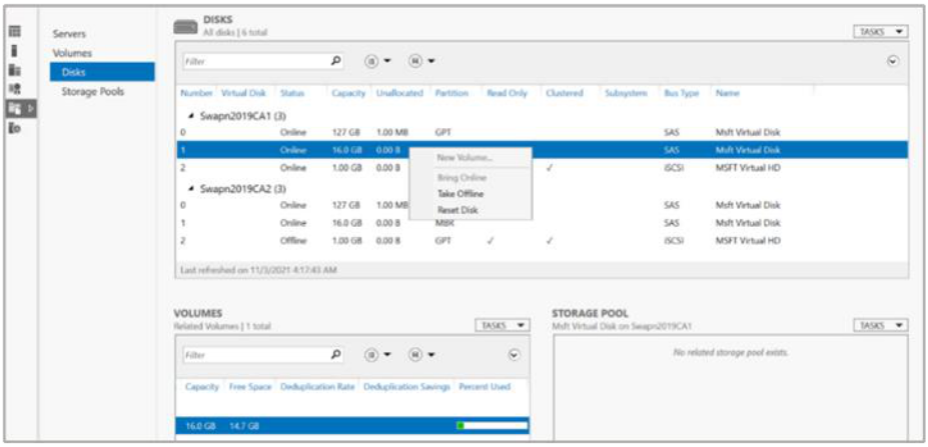

Figure 93: Server Manger window

12.3 Import MBK and Restore the databases on second cluster node

1. Copy the MBK shares and databases files from first cluster node onto second cluster node
2. Using CAT utility, log in to the CryptoServer with administrative privileges
3. Select Manage MBK and select Import tab and import the MBK shares which copied from first cluster node

Figure 94: Remote Master Backup Key Management window

4. Select Backup/Restore button on CAT tool and select radio button for Restore databases from backup directory to target Cryptoserver
5. Add CXIKEY.db and user.db to target Crytoserver and click Execute

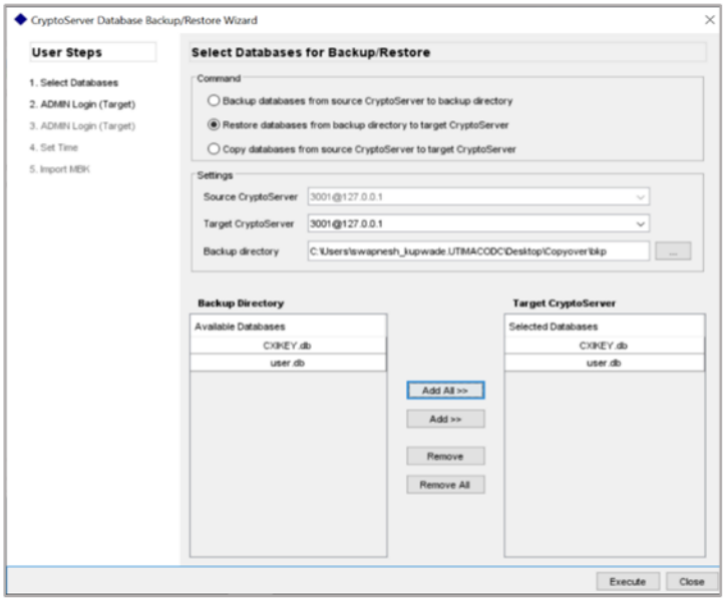

Figure 95: CryptoServer Database Backup/Restore window

6. Restart the CryptoServer service and ensure that users and keys got restore successfully
7. Check with the cngtool whether the private key was imported successfully

›_ Console

```
> cngtool ListKeys
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

12.4 Installing AD CS Server role on second cluster node

To install the CA on the second node, complete the following tasks

1. Log in as a user with Administrative privileges
2. Select Start then select Server Manager to open Server Manager
3. Select the File and Storage Services. Click Disks

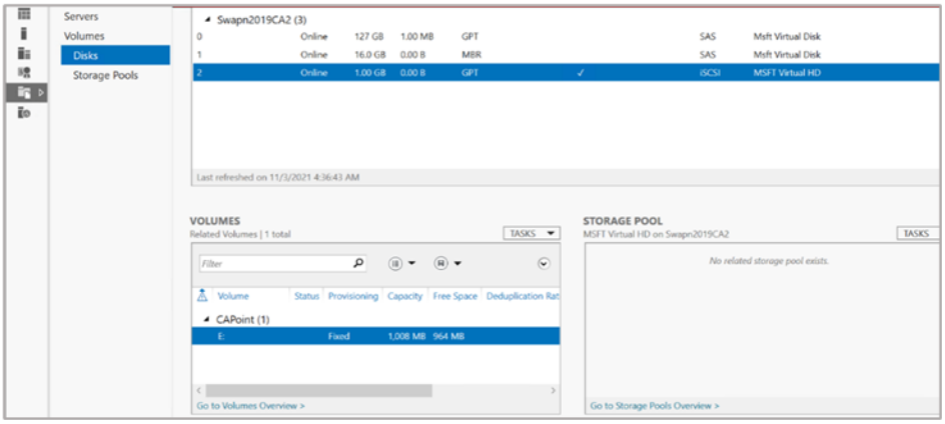

Figure 96: Server Manager window

4. Bring that the shared disk online on second cluster node
5. Copy the exported CA certificate on second cluster node
6. Import the CA certificate that was previously created on the first cluster node

›_ PowerShell

```
PS> certutil -addstore -f "My" "<CaName>.cer"

Signature matches Public Key

Certificate "DemoRootCa" added to store.

CertUtil: -addstore command completed successfully.
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

7. To create a link between the certificate and the private key, first find the certificate serial number

›_ PowerShell

```
PS> certutil "<CaName>.cer" | findstr Serial
Serial Number: 3a9f8a8c61129593400f6738896afcc0
```

8. And use the certutil command to repair the link

›_ PowerShell

```
PS> certutil –f –repairstore –csp "Utimaco CryptoServer Key Storage
Provider" my <serial>
CertUtil: -repairstore command completed successfully
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

9. Open Server Manager under Configure this Local Sever and click Add Roles and Features

10. The Add Roles and Features Wizard displays
11. Click Next. Select radio for the Role-based or feature-based installation and click Next
12. Select radio button for a server from the server pool and select the second cluster node from the server pool and click Next
13. Select the Active Directory Certificate Services check box from the Server Roles
14. Add features that are required for Active Directory Certificate Services? window displays. To add a feature, click the Add Features button
15. Click Next
16. Click Next
17. Select the check box for Certification Authority from the Role services list and click Next
18. Click Install
19. Once installation is complete, select the link Configure Active Directory Certificate Services on the destination server the AD CS Configuration wizard displays
20. In the Credentials page of the AD CS Configuration wizard click Next
21. Select the check box for Certification Authority and click Next
22. Select Enterprise CA as Setup Type and click Next
23. Select Root CA as type of CA and click Next
24. Select the radio button for Use existing private key and choose the option Select a certificate and use its associated private key and click Next
25. Select the CA certificate that was generated on the first cluster node and click Next
26. Change the default paths for the database and log location to the share disk and Click Next
27. A dialog box displays stating that an existing database was found displays, click Yes to overwrite
28. In the Confirmation page click Configure
29. Verify that the CA service has successfully started by running the command

›_ PowerShell

```
>sc query certsvc
```

12.5 Installing Failover Cluster feature on both the cluster nodes

Please execute the following steps on both the cluster nodes

1. Log in to cluster node as a user with Administrative privileges
2. Select Start and then Server Manager to open Server Manager

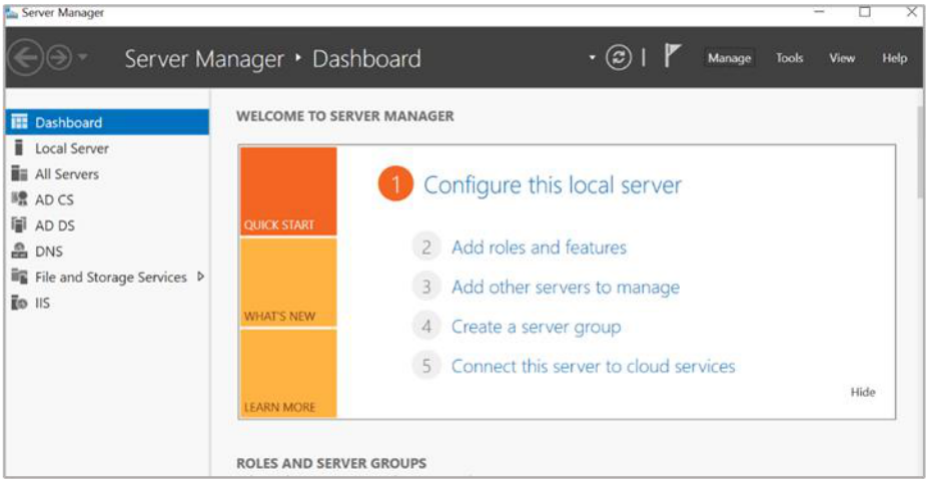

Figure 97: Server Manger window

3. Under Configure this Local Sever and click Add Roles and Features. The Add Roles and Features Wizard displays. Click Next

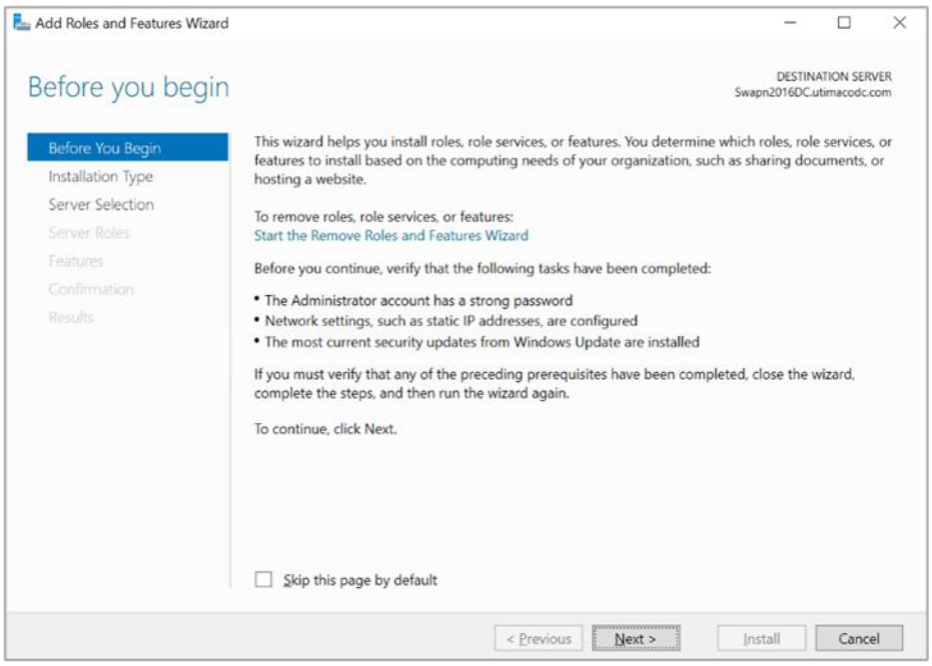

Figure 98: Before You Begin window

4. Select the radio button for Role-based or feature-based installation and click Next

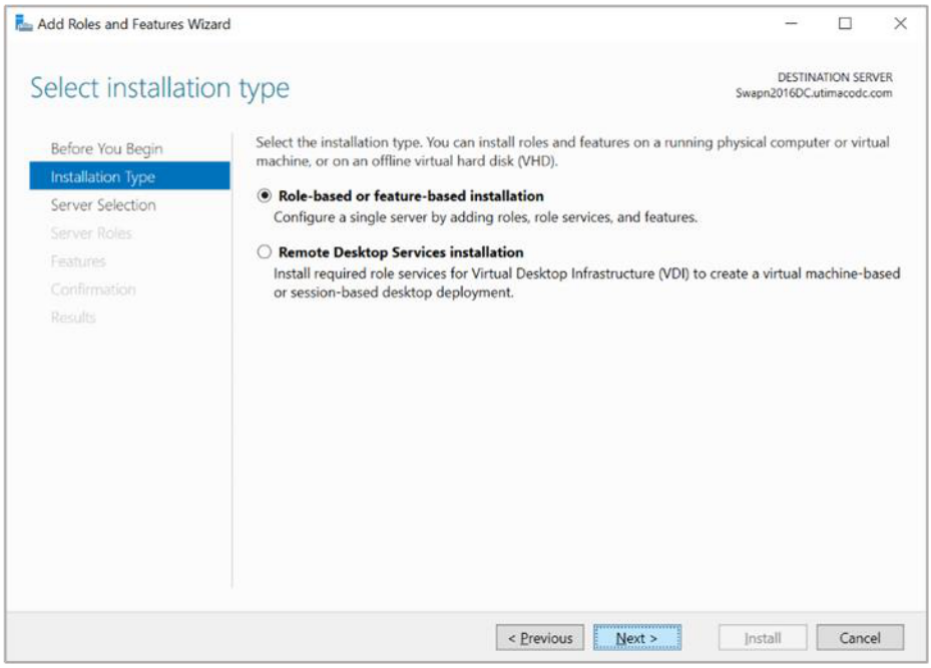

Figure 99: Select installation type window

5. Select the radio button for Select a server from the server pool option and from Server Pool. Select cluster node and click Next

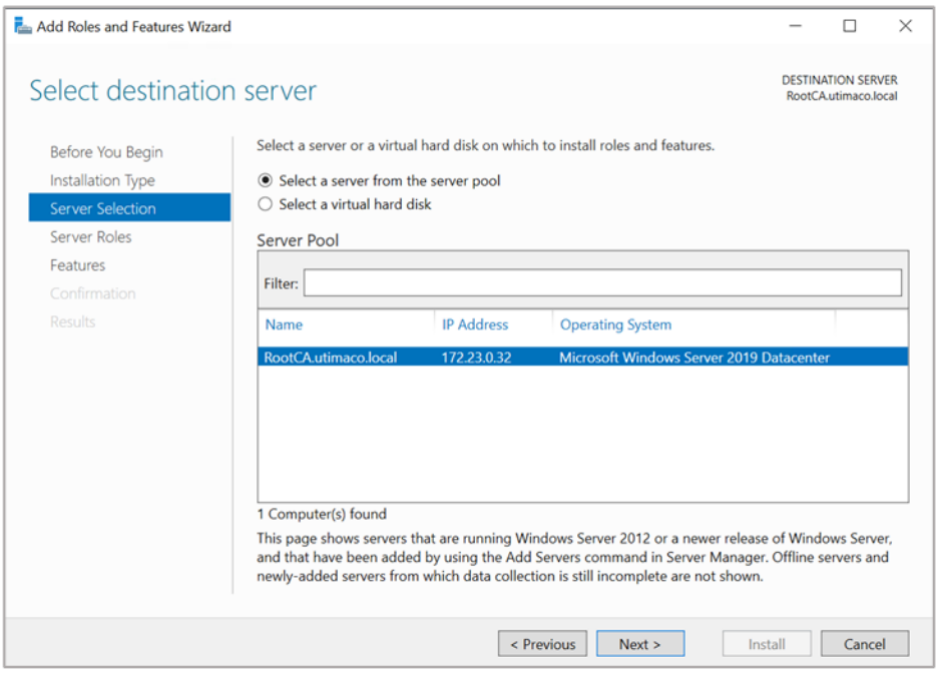

Figure 100: Select Destination Server window

6. Click Next
7. From the list of available features, select the Failover Clustering check box and click Next

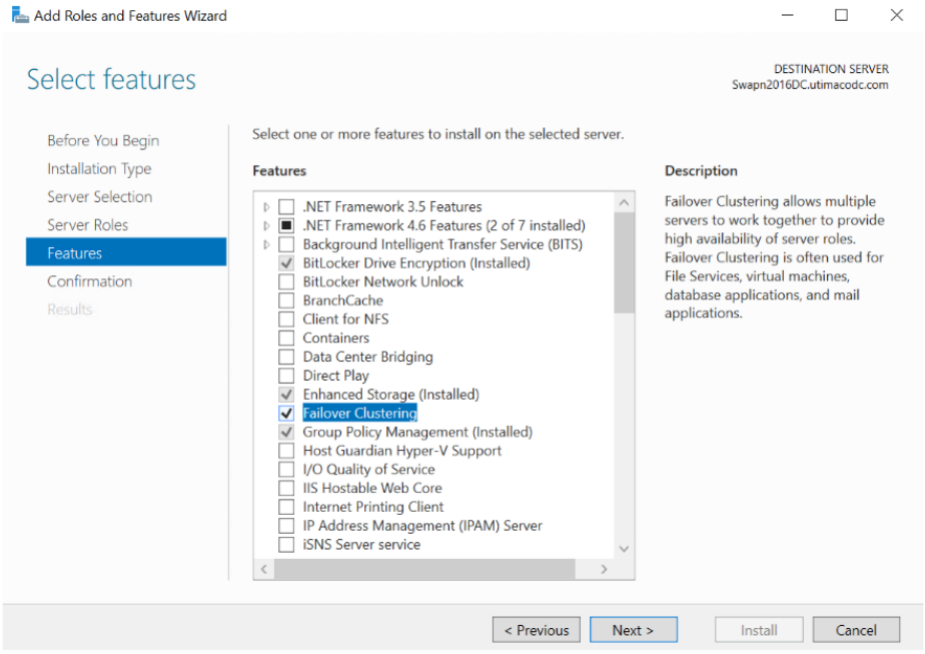

Figure 101: Select Features window

8. A pop-up display stating Add features that are required for Failover Clustering? To add a feature, click the Add Features button

9. Click Next
10. Click Install
11. Once Feature installation is complete, click Close

12.6 Create a Failover Cluster

1. Log in to cluster node as a user with Administrative privileges where disk is attached
2. Open Server Manager, Select Tools and select Failover Cluster Manager

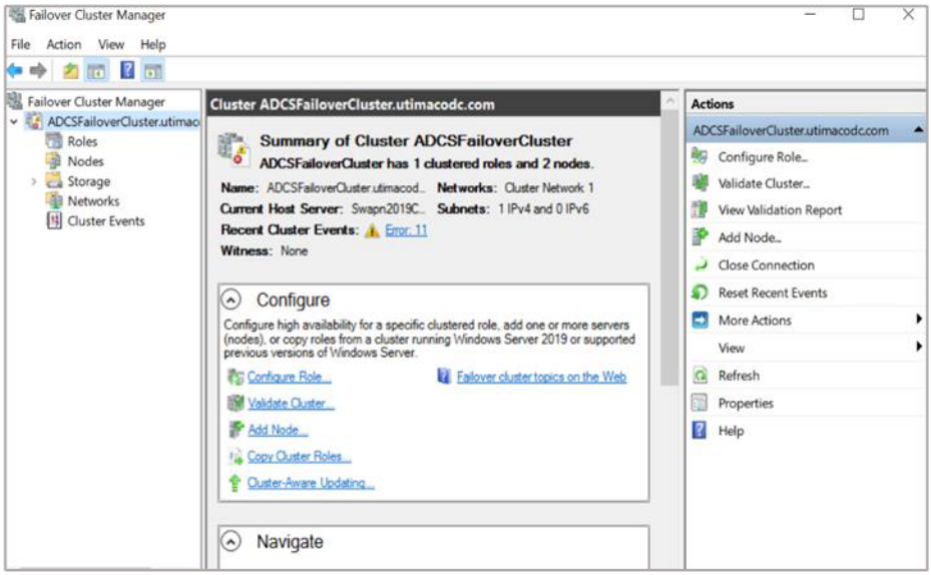

Figure 102: Failover Cluster Manager window

3. From the Actions menu, click Create a Cluster

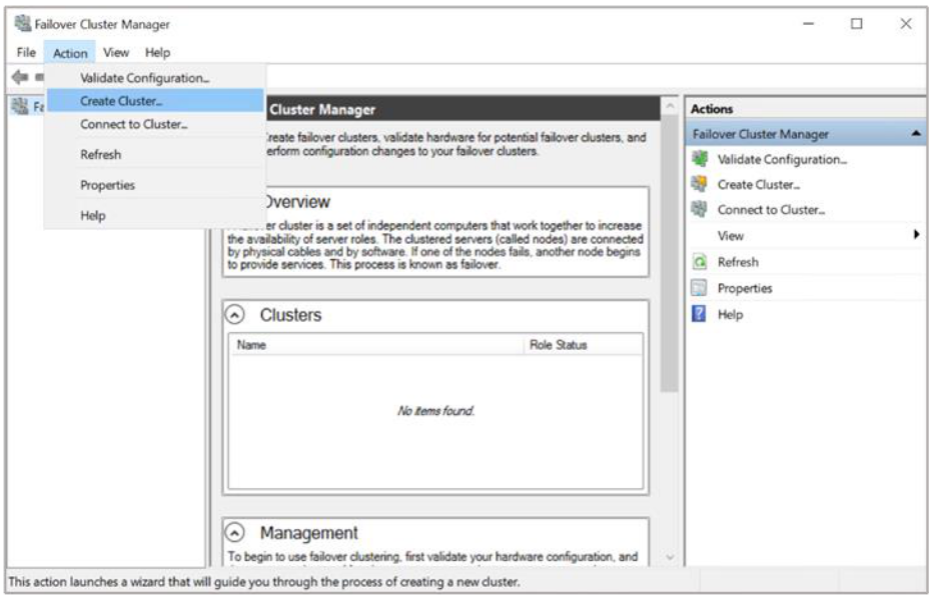

Figure 103: Failover Cluster Manager window

4. On the Before You Begin page, click Next

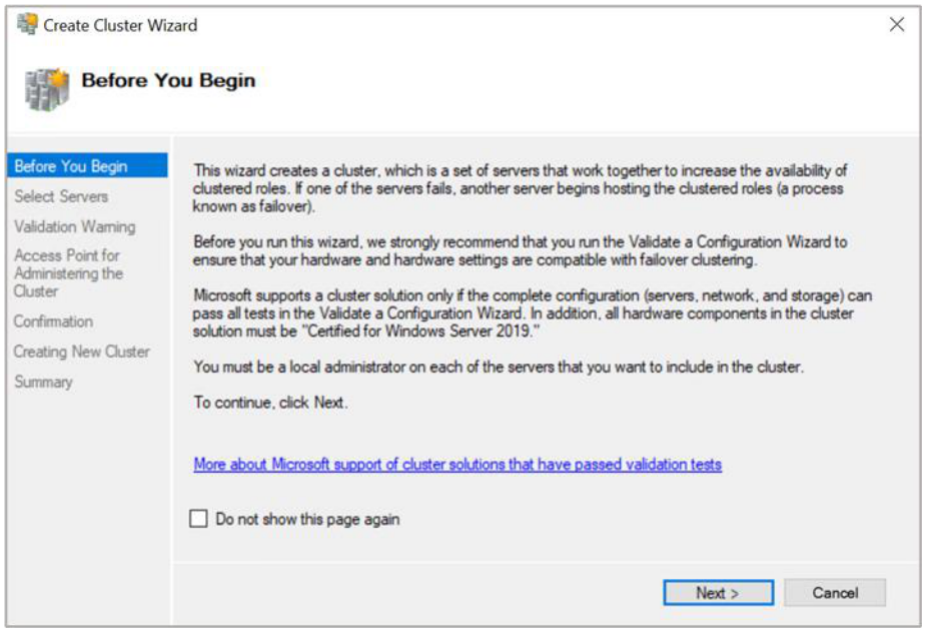

Figure 104: Before You Begin window

5. Enter the first cluster node name in the Enter Server Name field and click Add
6. Enter the second cluster node name in the Enter Server Name field and click Add
7. Click Next
8. Enter the Cluster Name and click Next until you reach the Summary page

9. To perform the validation tests, chose Yes and click Next two times
10. Keep the default option to Run all tests and click Next two times
11. Verify the test report and click Finish
12. Provide the cluster name and click Next until you reach the Summary page

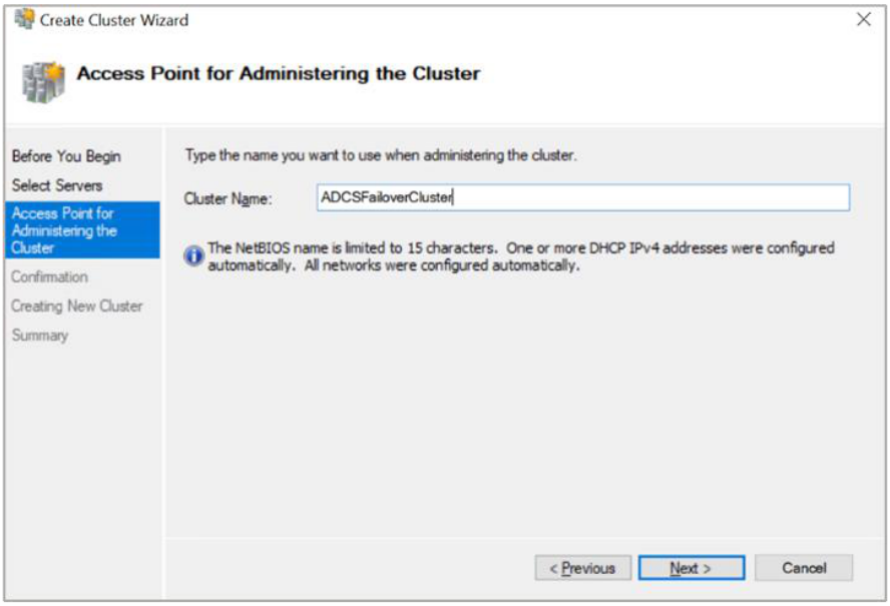

Figure 105: Access Point for Administering the Cluster window

13. Verify the cluster got configured successfully. Check the status of both nodes, disk, and network. It should be in green

12.7 Configure Role for ADCS Failover

1. In the Failover Cluster Management snap-in, right-click Role and select Configure Role
2. On the Before you Begin page, click Next
3. From the role list, select Generic Service and click Next

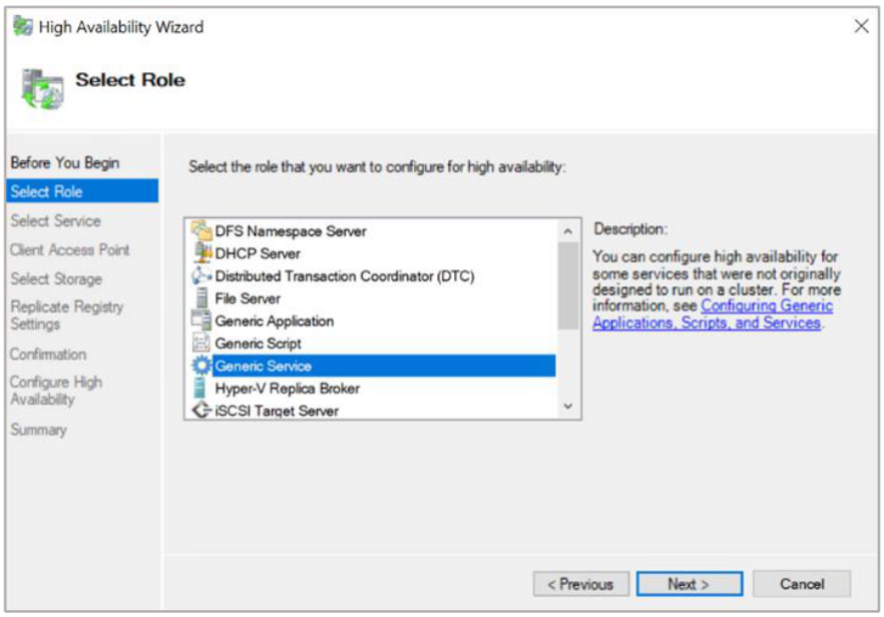

Figure 106: Select Role window

4. From the service list, select Active Directory Certificate Services and click Next
5. On the Client Access Point page, enter the role name in the Name field and click Next

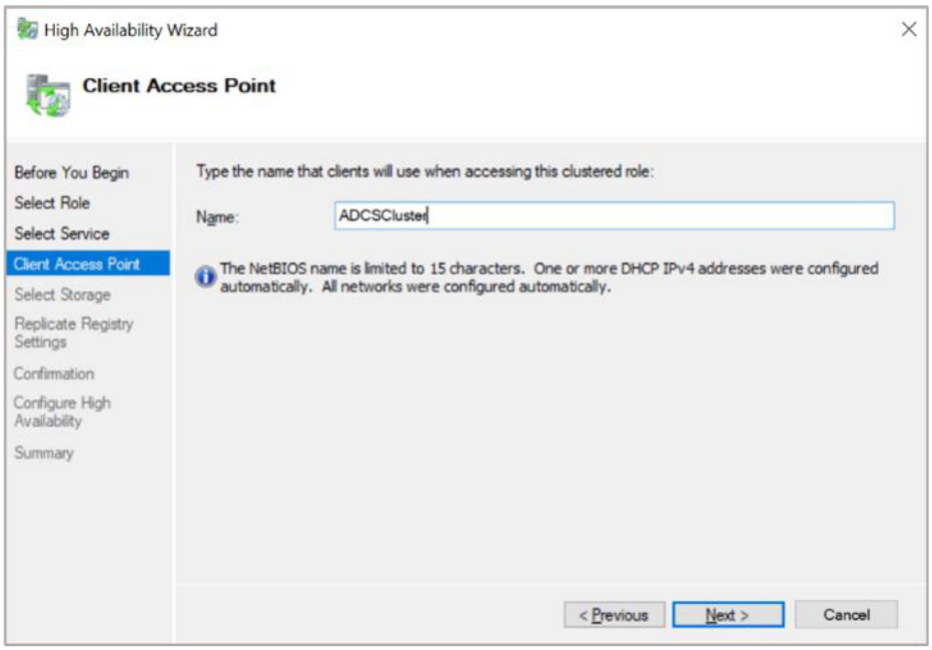

Figure 107: Client Access Point window

6. Select the disk storage that is still mounted to the node and click Next

7. Configure a shared registry hive, select the Add button, enter

`SYSTEM\CurrentControlSet\Services\CertSvc and click OK`

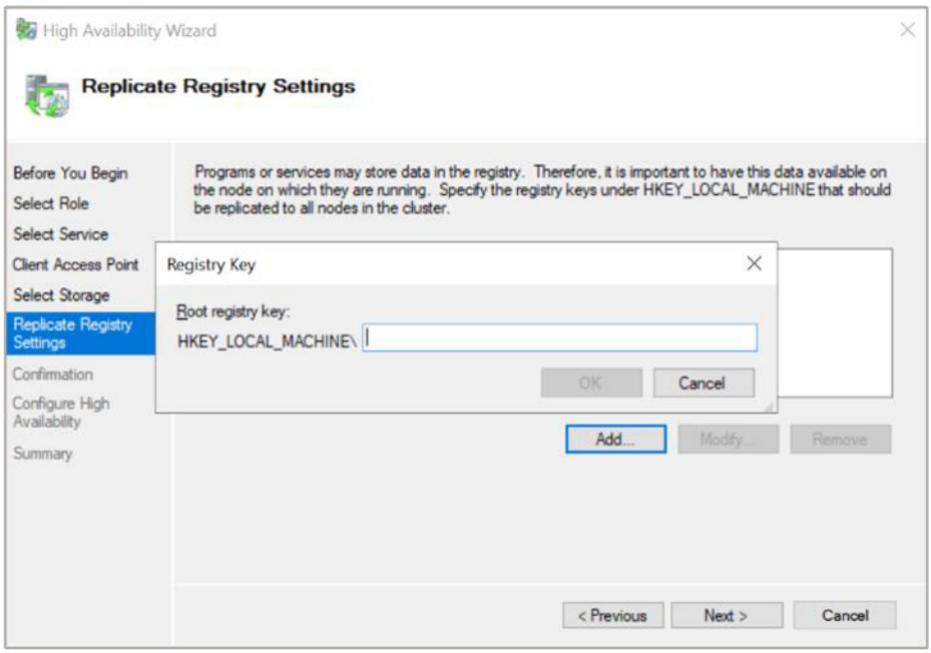

Figure 108: Replicate Registry Settings window

8. Click Next on the Confirmation page

9. Click Finish to complete the failover role configuration
10. Open the Failover Cluster Manager and verify that the newly created Roles Status is in the Running state and Green
11. The AD CS Failover got configured successfully. At this stage, you can move the certification authority between all nodes.

12.8 Creating the CRL Objects in Active Directory

The CRL container must be created in Active Directory manually, and the CRL must be published manually.

1. Log on to the active cluster node with enterprise permissions
2. On the command prompt type

›_ Console

```
> cd %WINDIR%\System32\CertSrv\CertEnroll

> certutil -f -dspublish {CRLfile}

For example:

> certutil -f -dspublish "CA Cluster.crl"
```

12.9 Updating the CA configuration in Active Directory

1. Log on to the Domain Controller with enterprise permissions
2. Click the Start button, open Run and type dssite.msc and then click OK
3. Select the top node in the left pane
4. In the View menu, select Show services node
5. In the left pane, select the Services and Public Key Services, and then select AIA

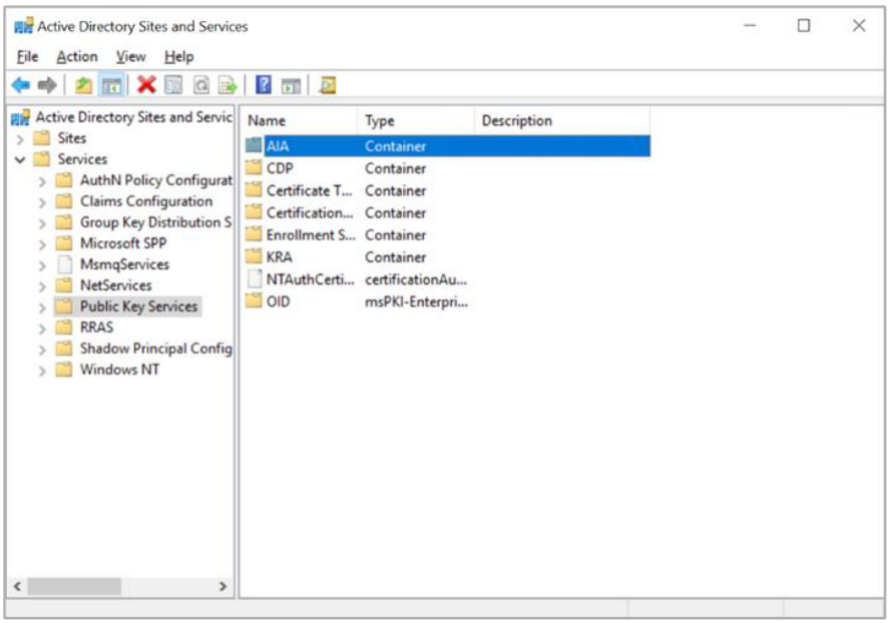

Figure 109: Active Directory Sites and Services window

6. In the middle pane, select the CA name as it shows in the Certification Authority MMC Snap-in

7. In the Action menu, select Properties
8. Click Security
9. Click Add
10. Select Object Types then select Computers, and then click OK
11. Type the computer name(s) of the other cluster node(s) as the object name and click OK
12. Make sure that the computer accounts of all cluster nodes have Full Control permissions
13. Click OK
14. All cluster nodes also have to be permitted on the Enrollment Services container
15. In the left pane, select Enrollment Services.
16. In the middle pane, select the Certificate Authority name
17. In the Action menu, select Properties. Select the Security tab and click Add....
18. Select Object Types, select Computers and click OK
19. Type the computer name(s) of the all-cluster node(s) as the object name
20. Make sure that the computer accounts of all cluster nodes have Full Control permissions
21. Click OK
22. In the left pane, select KRA
23. In the middle pane, select the Certificate Authority name
24. In the Action menu, select Properties then select the Security tab and click Add
25. Select Object Types, select Computers and then click OK
26. Type the computer name of all cluster node as object name and click OK
27. Make sure that the computer accounts of all cluster nodes have Full Control permissions
28. Click OK

13 Online Certificate Status Protocol Service

Before integrating the Utimaco CryptoServer with Microsoft Windows Server Online Certificate Status Protocol Service (OCSP), first complete the Utimaco CSP/CNG Installation.

It is strongly recommended to use the external key storage for OCSP if using HSMs in cluster mode. Therefore, the servers which serve OCSP should be separated from the certificate authorities.

You can install OCSP if you are already running an enterprise certificate authority.

The following steps are necessary to install OCSP in general:

- Prepare certificate template for OCSP signing
- CA Configuration
- Install and configure online responder
- Make a revocation configuration
- Test the online responder

13.1 Prepare certificate template for OCSP Signing

First, it is necessary to prepare a template to enroll OCSP servers for a certificate which uses the Utimaco CryptoServer.

1. Open the command prompt and run the certtmpl.msc command
2. Right-click the OCSP Response Signing template and click Duplicate Template
3. Select appropriate windows version under Certificate Authority and Certificate Recipient drop-down box under Compatibility Settings
4. Click OK

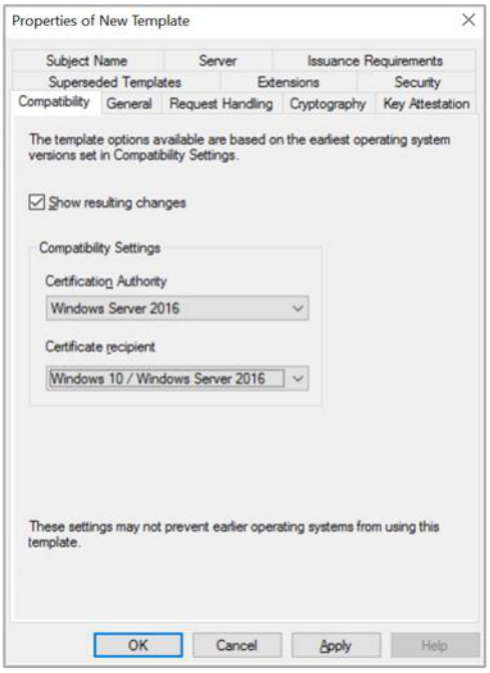

Figure 110: Compatibility Tab window

5. In the Resulting Changes menu click OK
6. Go to the General tab and enter a name for the template
7. Select the Subject Name tab

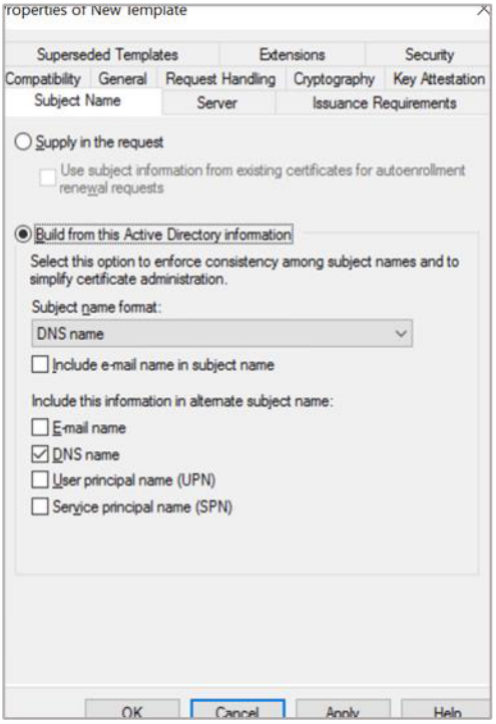

Figure 111: Subject Name Tab window

8. Uncheck the Include e-mail name in subject name check box
9. Uncheck the E-mail name check box
10. In the Request Handling tab, select the Purpose as Signature from the drop-down list.

    Select Authorize additional service accounts to access the private key checkbox

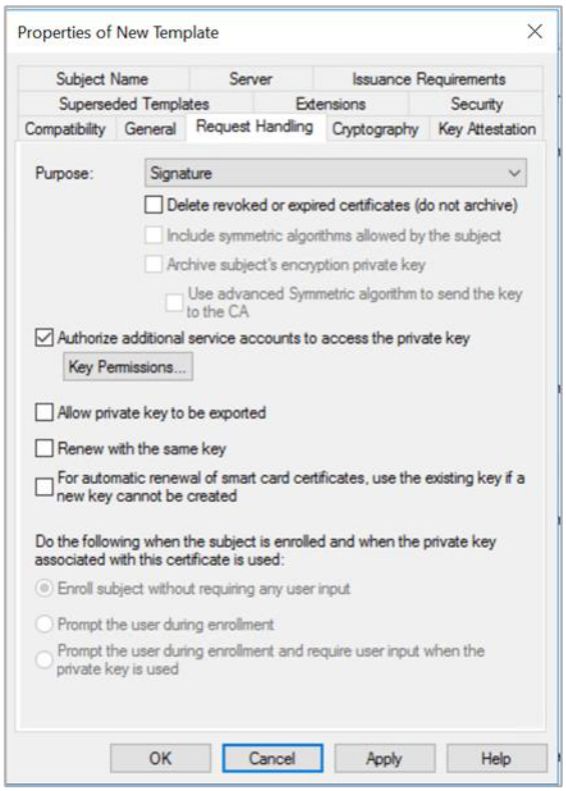

Figure 112: Request Handling window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

11. Go to Cryptography tab, select Key Storage provide in the Provider category then select Algorithm name then Key Size. Check on the radio button for Request must use one of the following providers then select radio button for Utimaco CryptoServer Key storage provider and select the appropriate Hash Value

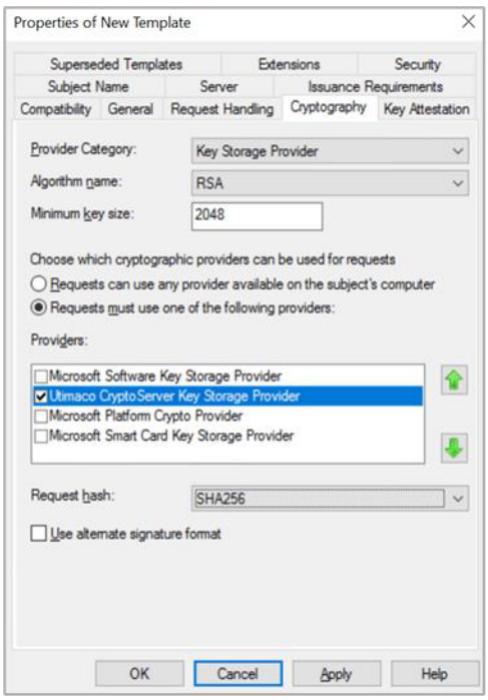

Figure 113: Cryptography Tab window

12. Go to Security Tab. Add the Computer Account and give Read, Write and Enroll permissions. Ensure Domain Admins and Enterprise Admins are having Enroll Permissions
13. Click Apply and then Click OK
14. Open the command prompt and run the certsrv.msc command

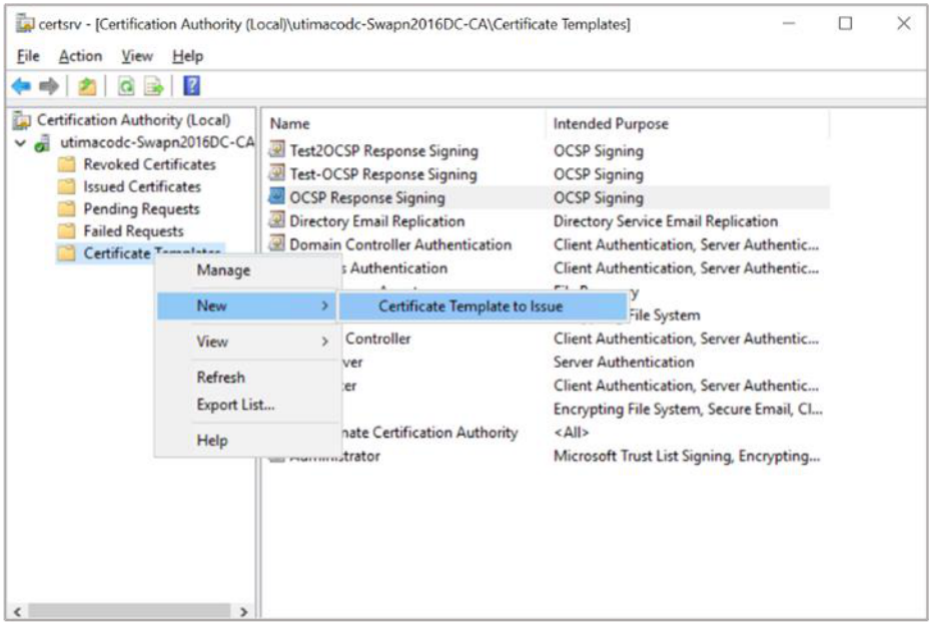

Figure 114: Certificate Authority window

15. Right-click the Certificate Templates node
16. Select New then select Certificate Template to Issue
17. Select new template for OCSP Response Signing, click OK

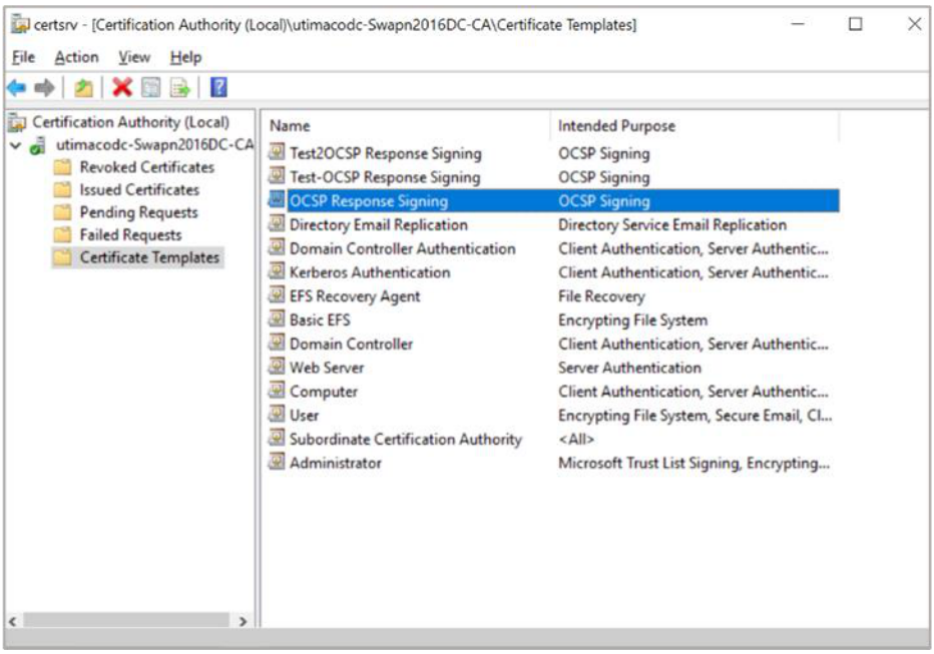

Figure 115: Certificate Authority window

13.2 CA Configuration

Some more steps are necessary to use OCSP with a CA. Perform the next steps on the CA server.

1. Open the command prompt and run the certsrv.msc command
2. Right click Certificate Authority Name and select Properties

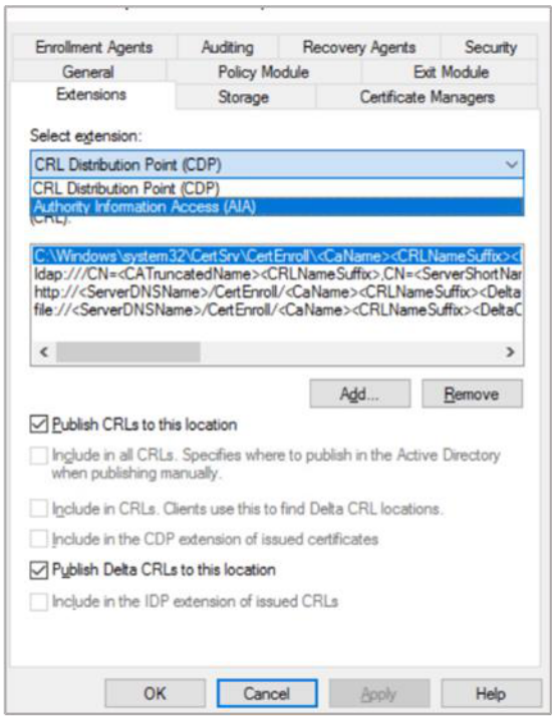

Figure 116: Extensions Tab window

3. Change to the Extensions tab and select Authority Information Access (AIA). Add the URL of the OCSP service. Typically, this is the FQDN of the OCSP server with the path OCSP, e.g., `http://FQDN-OF-SERVER/ocsp` Click OK. After adding select the URL previously entered, select Include in the online certificate status protocol (OCSP) extension. Click Apply and then click on OK

4. You will receive a pop-up window to restart the AD CS, for the changes to take effect. Click Yes and Click OK

13.3 Request a certificate from OCSP Response Signing template

1. Select the Start menu, open Run and type mmc and click OK

2. In the mmc console that appears, select File then select Add/Remove Snap-in…

3. In the Add or Remove Snap-Ins pop-up dialog that appears, find the Certificates snap-in (under the Available snap-ins section)

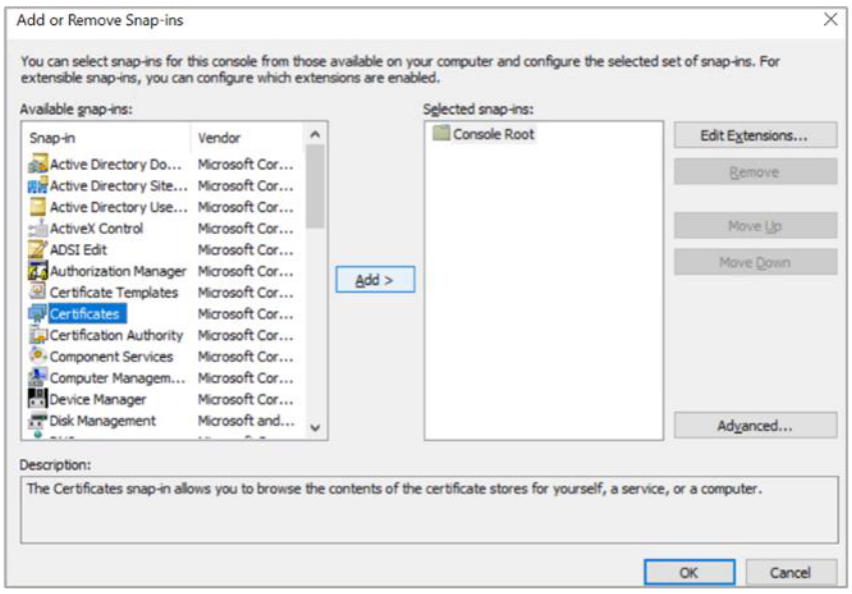

Figure 117: Add/Remove Snap-in window

4. Select the snap-in and click Add
5. In the dialog that appears, select the radio button for Computer Account and then click Next

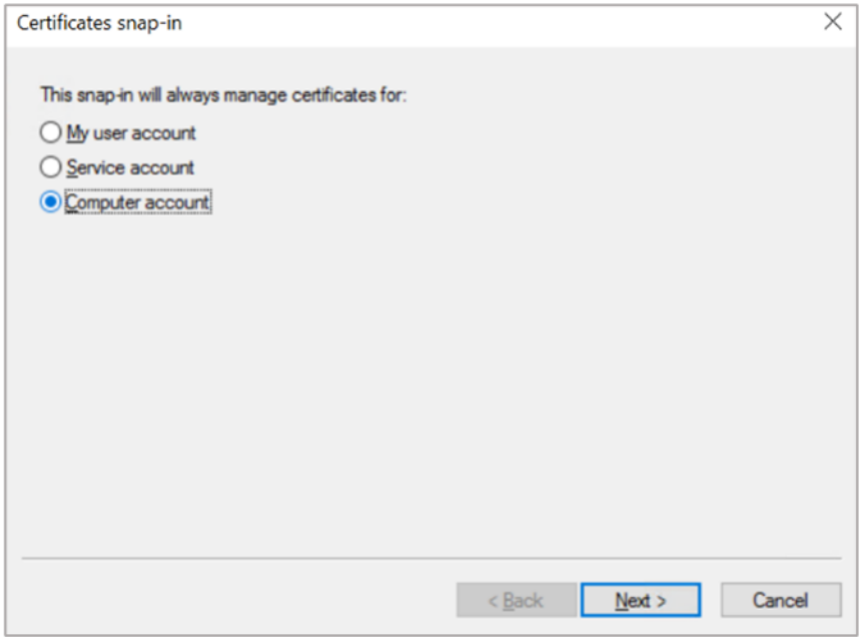

Figure 118: Certificate Snap-in window

6. In the Select Computer dialog, ensure that Local Computer is selected and click Finish

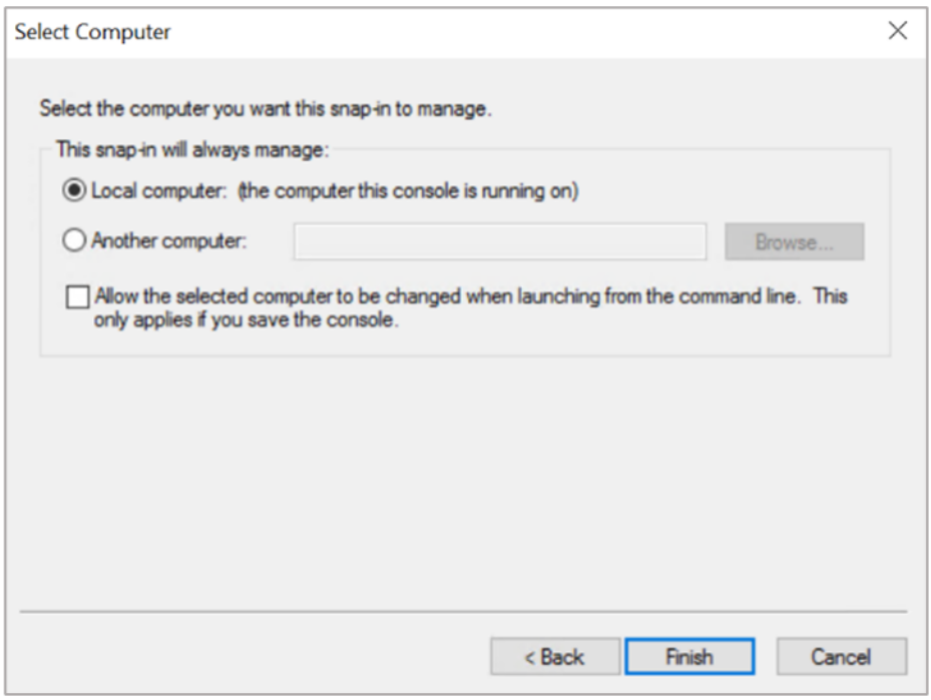

Figure 119: Select Computer window

7. Click OK
8. Under the Console Root, select the Certificates heading
9. Select the Personal folder and expand it
10. Right Click on Certificates and select All Tasks and select Request New Certificate

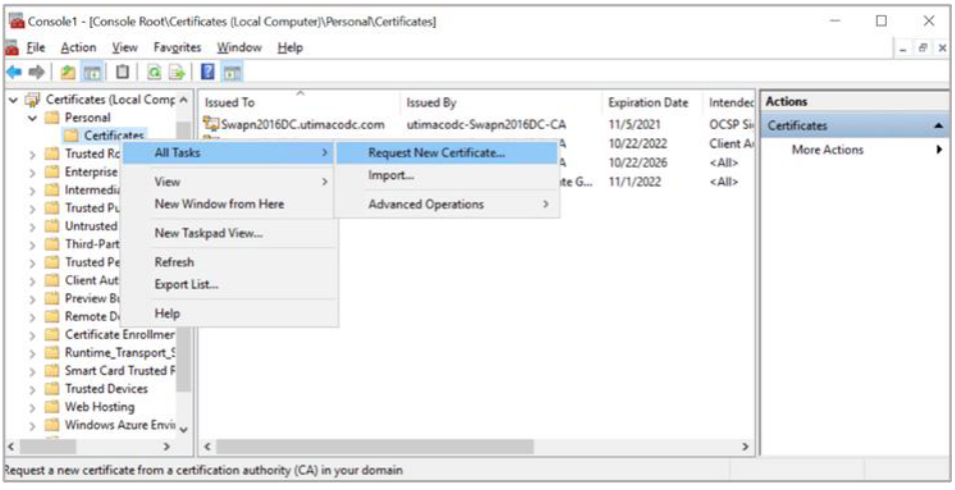

Figure 120: Console window

11. On Before You Begin page, Click Next

12. On Select Certificate Enrollment Policy page, Click Next

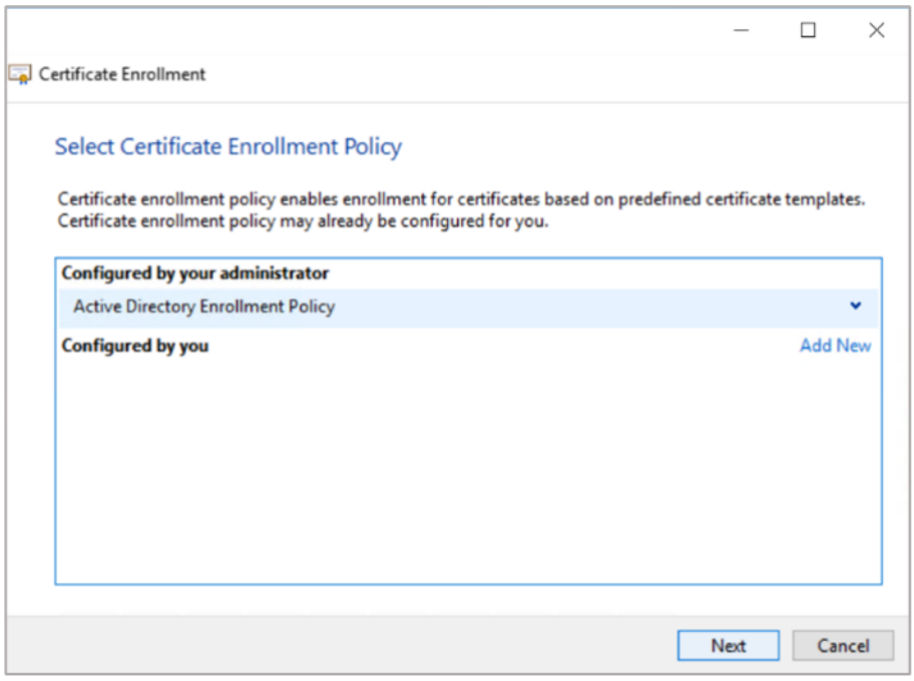

Figure 121: Certificate Enrollment Policy window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insertSmartcard and enter the pin. Then press OK button on the PIN Pad.

13. On Request Certificates page, select OCSP Response Signing template and Click Enroll

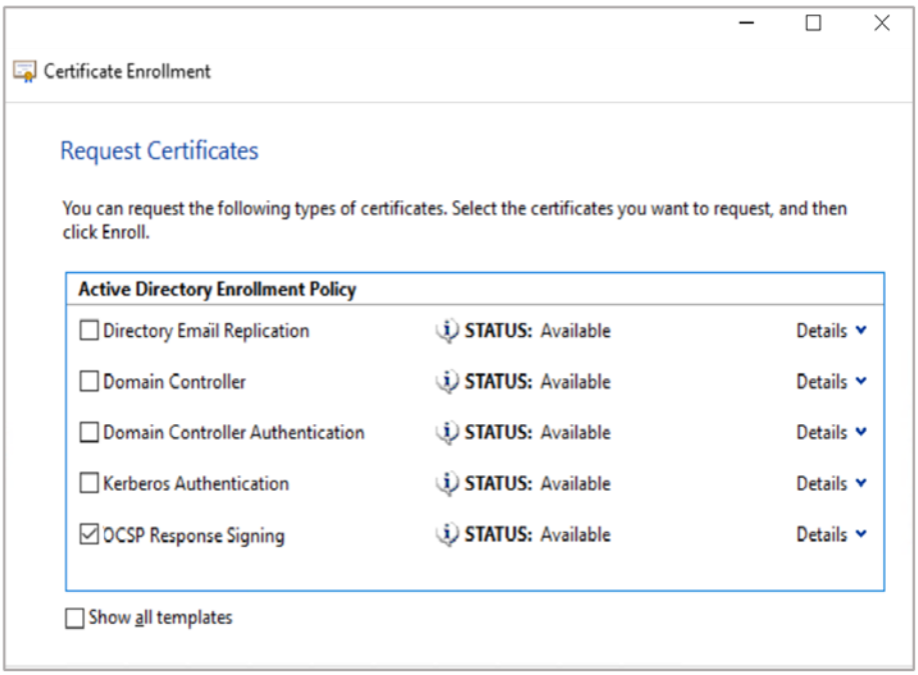

Figure 122: Certificate Enrollment Policy window

14. On Certificate Installation Results page, click Finish

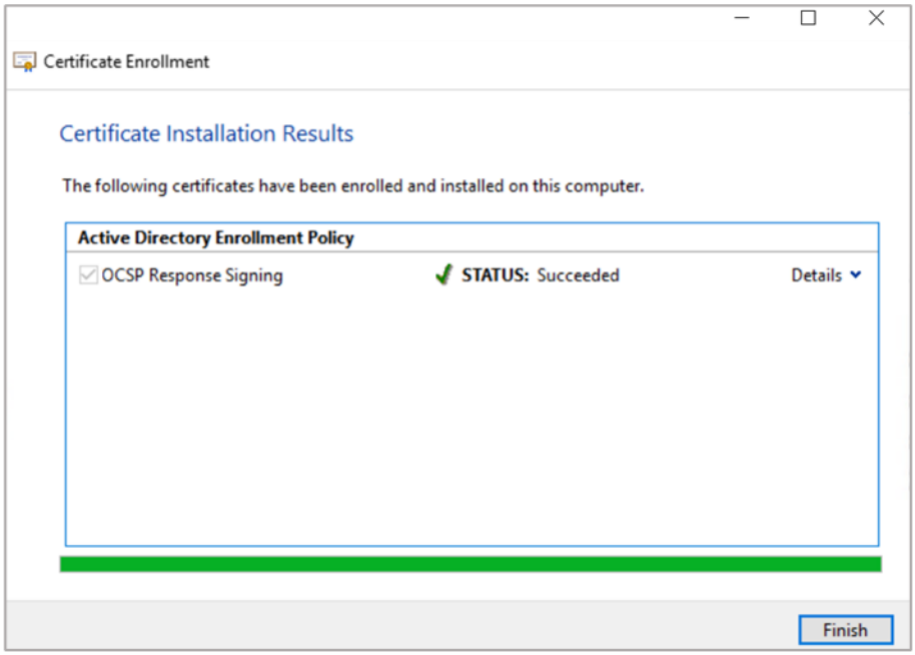

Figure 123: Certificate Installation Results window

13.4 Install and configure Online Responder

Now change to your OCSP server and install the OCSP service.

1. Select Start then select Server Manager to open Server Manager
2. Select Manage then select Add Roles & Features. The Before you begin window opens. Click Next

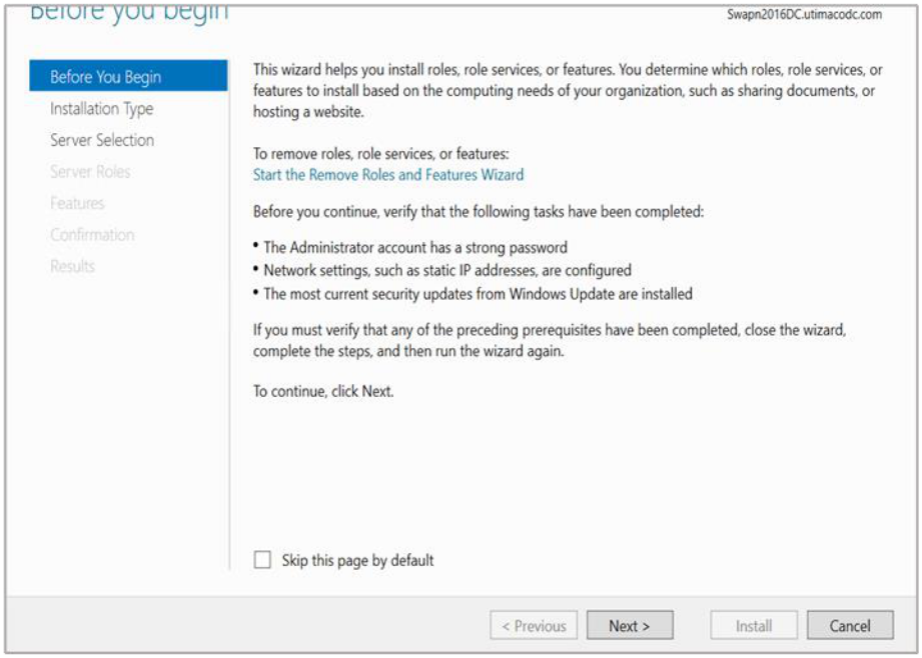

Figure 124: Before You Begin window

3. On the Select installation type window, make sure the default Role or Feature Based Installation is selected. Click Next
4. On Server selection, select a server from the server pool. Click Next
5. On the Select server roles window, select the Active Directory Certificate Services role
6. When prompted to install Remote Server Administration Tools, select Add Features. Click Next
7. On the Select features window, click Next
8. On the Active Directory Certificate Services window, click Next
9. On the Select role services window, select the Online Responder. Click Next

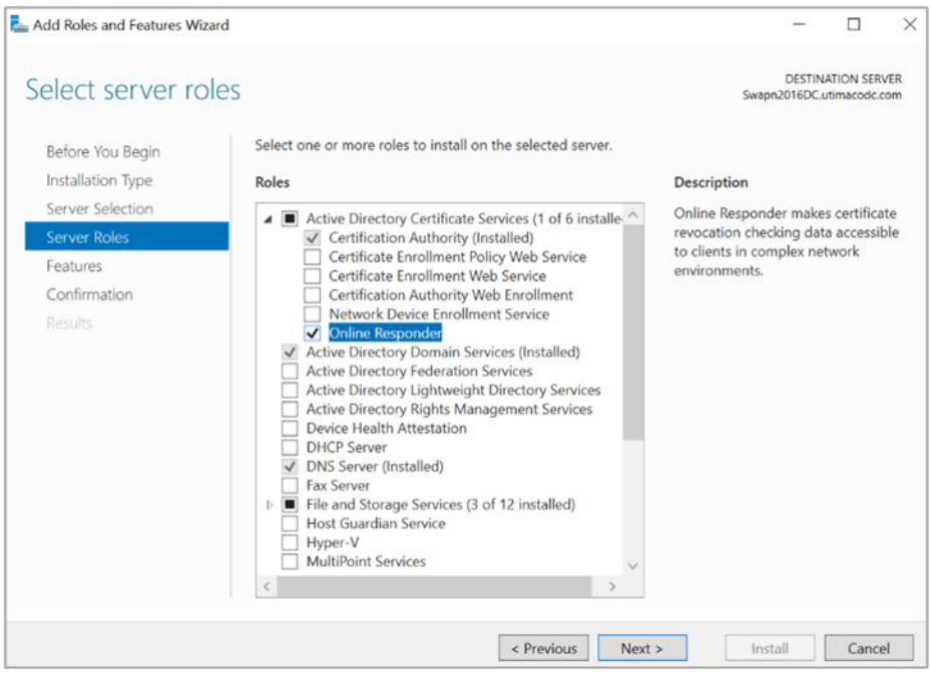

Figure 125: Select Server Roles window

10. When prompted to install Remote Server Administration Tools, select Add Features. Click Next

11. On the Confirm installation selections window, verify the information then click Install

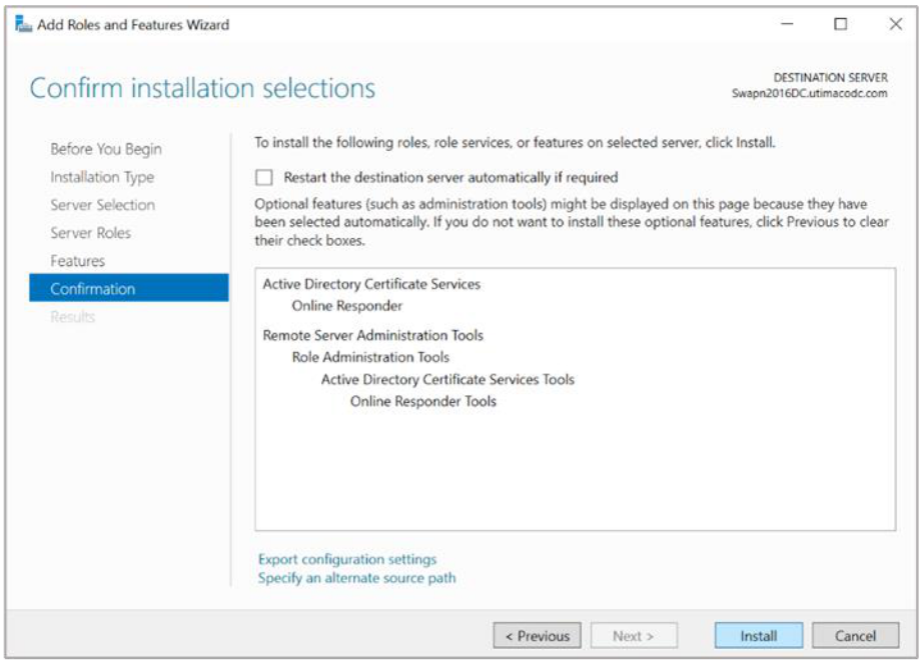

Figure 126: Confirm Installation Selections window

12. Click Configure Active Directory Certificate Server on the destination server. The ADCS Configuration Wizard displays

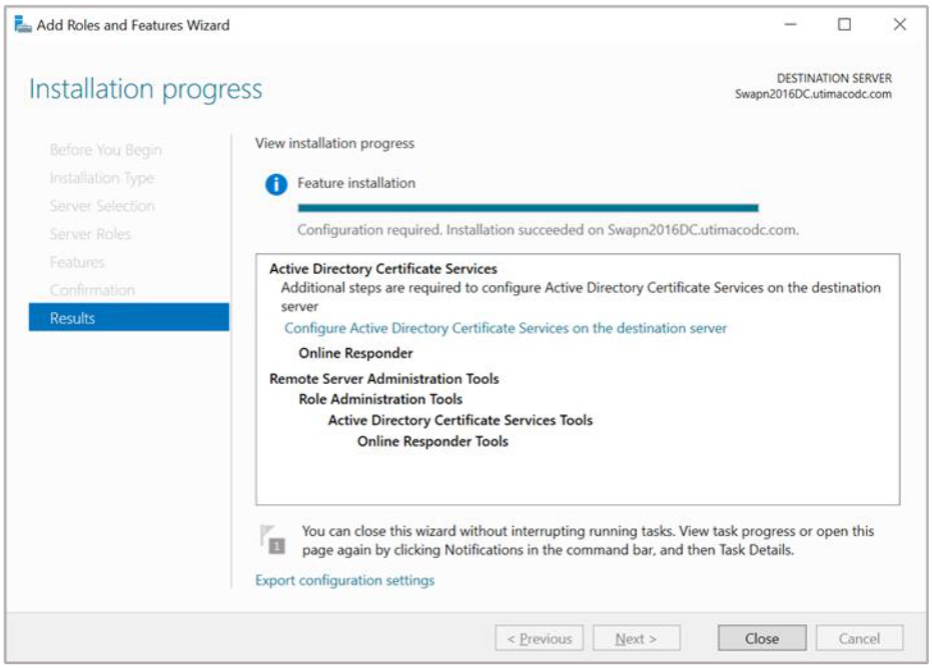

Figure 127: Installation Progress window

13. On the Credentials page click Next

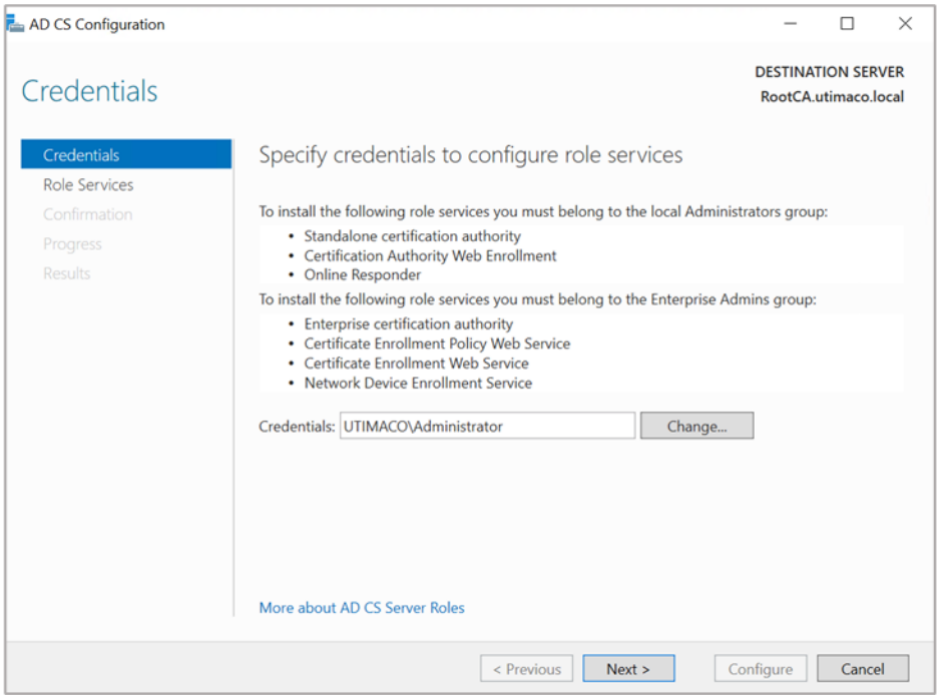

Figure 128: Credentials window

14. On the Role services page select the Online Responder check box. Click Next

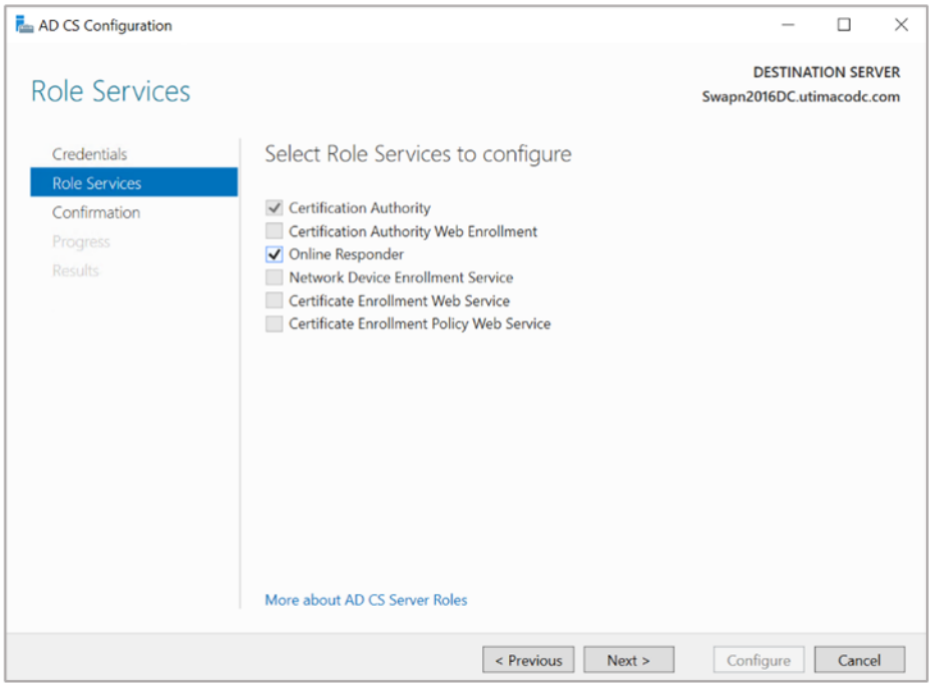

Figure 129: Role Services window

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

15. On the Confirmation page, click Configure and wait for the confirmation message. A message displays after successful configuration

16. On the Results page click Close to exit the ADCS Configuration Wizard

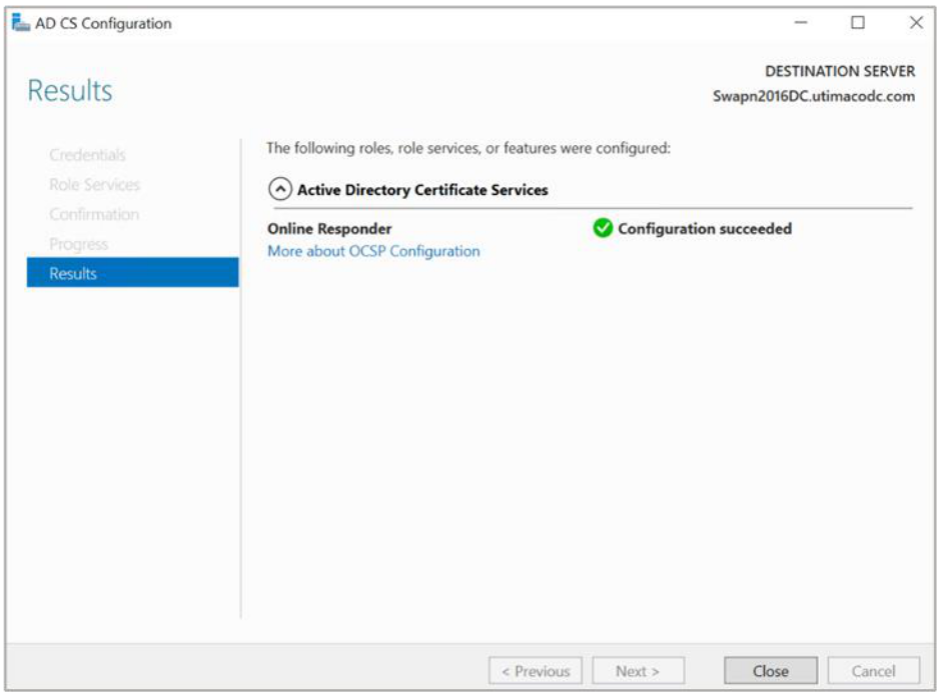

Figure 130: Results window

13.5 Make a Revocation Configuration

To use OCSP you must create a new revocation configuration.

1. Open the Administrative tool, select Online Responder Management
2. Launch the Online Responder Management console
3. Select Revocation Configuration and then click on Action and then Add Revocation Configuration
4. On the Add revocation wizard, click Next then enter a Name for your configuration

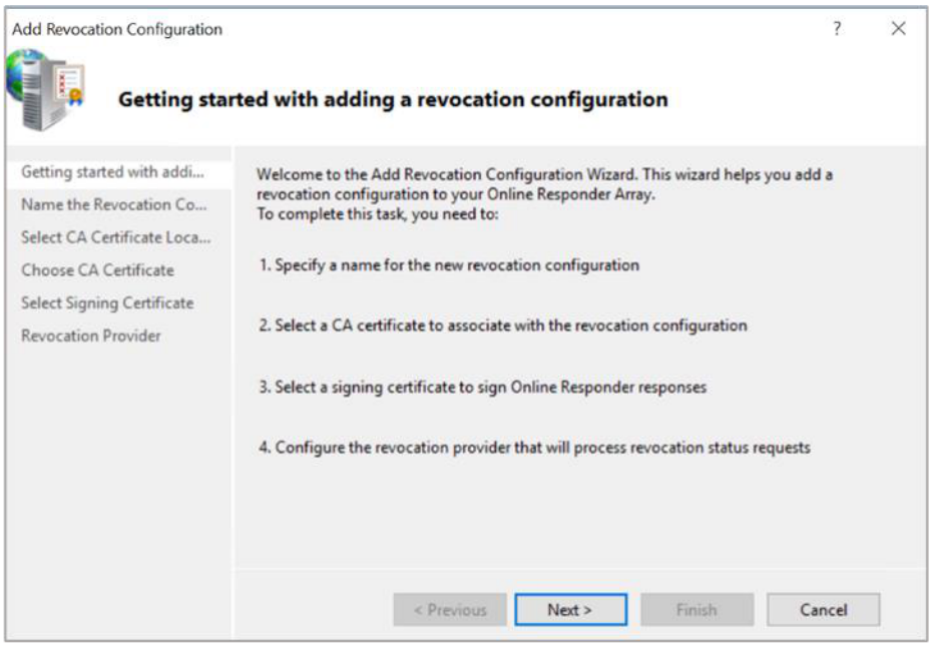

Figure 131: Add Revocation Configuration window

5. Specify the location of your CA certificate relative to your environment

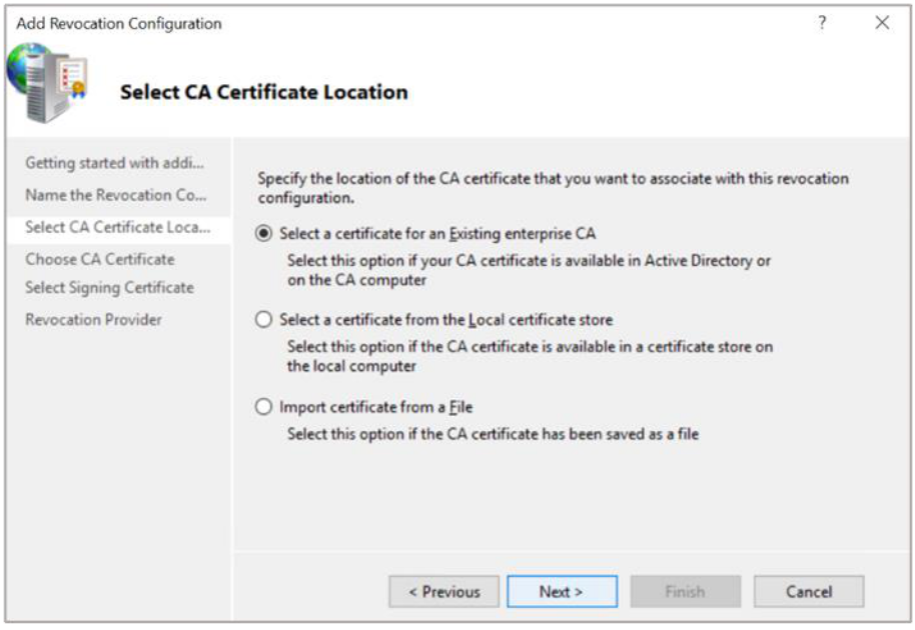

Figure 132: Select CA Certificate Location window

6. Select the OCSP certificate template created earlier and click Browse
7. Click Next on the Select signing certificate wizard, click Next

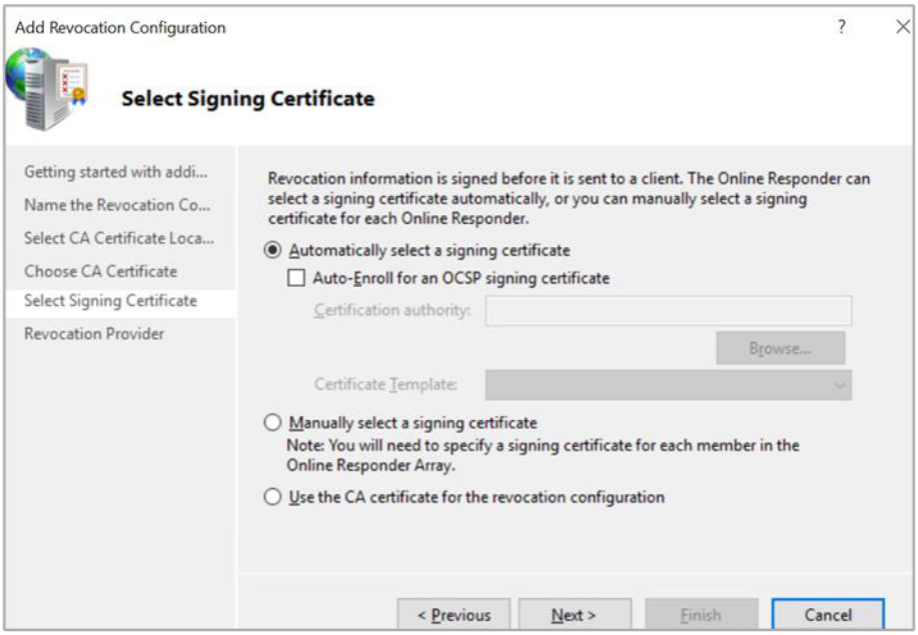

Figure 133: Select Signing Certificate window

8. To finish, configure the revocation provider. It is the location where the CRLs or Delta CRLs are stored. The configuration automatically retrieves this information in the CDP extension of the certificate

9. Once you have setup the Revocation Configuration, The Revocation Configuration Status Box displays the Online Responder status. The status should display Bad Signing on Array Controller.

10. To fix this, click on Revocation Configuration in the left-hand pane. Right-click on the certificate and select Edit Properties.

11. Click on the Signing tab. Deselect the Do not prompt for credentials for cryptographic operations check box. Click OK.

12. Go back to the Online Responder Management tool. Open Actions and click Refresh. Its status would be working now.

13. You can check if the key to this certificate is really created and stored by the Utimaco CNG provider. To do this, open a PowerShell and enter cngtool listkeys. If there is a key, then you can be assured that your Online Responder Service uses the Utimaco CryptoServer HSM correctly

›_ Console

```
>cngtool listkeys

------------------------------------------------------------------------

Provider : Utimaco CryptoServer Key Storage Provider

Device : 192.168.0.1

Group : win16ocsp

Mode : External Key Storage

------------------------------------------------------------------------

Index AlgId Size Group Name Spec

------------------------------------------------------------------------

1 RSA 2048 win16ocsp tr-OCSPResponseSigning!0028Uti... 0
```

If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

13.6 Test the Online Responder

To test the online responder, you can create a new computer certificate. After you have exported this certificate to a CER file run `certutil –URL c:\temp\MyCertificate.cer`. This command opens the window.

Select OCSP and click Retrieve. The status of this certificate should change to Verified. Now you can revoke this certificate on your CA and publish the CRL again. If you now, click again on Retrieve the status should change to Revoked.

14 Further Information

This document forms a part of the information and support which is provided by the Utimaco

IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website:

https://utimaco.com/

15 References

Reference	*Title/Company*	*Document No.*
[CSADMIN]	CryptoServer – csadm Manual / Utimaco IS GmbH	2009-0003
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSLAN]	CryptoServer LAN V5 Manual Systemadministrators.pdf	2018-0010
[CSP-CNG]	CryptoServer Manual CSP CNG.pdf	2008-0002