Microsoft
Internet Information Services (IIS)

Integration Guide

SecurityServer

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	2025-12-09
Status	PUBLISHED
Document No.	IG-2025-0027

Table of Contents

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 Utimaco SecurityServer product documentation is available from Utimaco's web site at https://utimaco.com/

1.1 About This Guide

This guide describes how to enable HSM integration with Microsoft IIS. Utimaco HSM is used to secure the private keys for SSL certificate and offload cryptographic operations on the HSM.

1.1.1 Target Audience for This Guide

This guide is intended for Microsoft Internet Information Services and HSM administrators.

1.1.2 Contents of This Guide

After the introduction this guide is divided up as follows:

Chapter 2 Overview

Chapter 3 Integration Requirements and Prerequisites

Chapter 4 Configuring the Utimaco CSP-CNG Provider

Chapter 5 Integrating Microsoft IIS with Utimaco HSM

Chapter 6 Troubleshooting

Chapter 7 Further Information

1.1.3 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.
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *CryptoServer - csadm Manual* or [CSADMIN].

Table 1: Document conventions

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

Here you find additional notes or supplementary information.

Here you find important safety information that should be followed.

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

1.1.4 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	*Meaning*
API	Application Programming Interface

CA	Certificate Authority
CD	Compact Disc
CNG	Cryptography API Next Generation
CSADM	CryptoServer Command-line Administration Tool
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
CXI	Cryptographic eXtended Interface
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IIS	Internet Information Services
IP	Internet Protocol
JDK	Java Development Kit
LAN	Local Area Network

MBK	Master Backup Key
PCIe	PCI Express Interface

Abbreviation	*Meaning*
PIN	Personal Identification number
PKCS#11	Public-Key Cryptography Standard #11
RSA	Rivest-Shamir-Adleman
SSL	Secure Socket Layer

Table 2: List of Abbreviations

1.2 Overview

1.2.1 Microsoft Internet Information Services (IIS)

Microsoft Internet Information Services (IIS) for Windows Server is a flexible, secure, and manageable Web server for hosting anything on the Web. From media streaming to web applications, IIS's scalable and open architecture is ready to handle the most demanding tasks.

1.2.2 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.

2 Integration Requirements and Prerequisites

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

This guide assumes that the user has already installed and configured required Software.

2.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with Microsoft IIS.

Operating System	*Windows IIS*	*Utimaco Security Server Version*	*Utimaco HSM*
Windows Server 2019	10.0	SecurityServer 4.45.5	CryptoServer CSe-Series/Se- Series

Table 3: List of Tested Versions

2.2 Software Requirements

Software	*Software Requirements*
HSM Interfaces	CryptoServer CSP/CNG Provider
Microsoft IIS	10.0
JDK 8	JDK 8u341

Table 4: List of Software Requirements

2.3 Hardware Requirements

Hardware	*Hardware Requirements*
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.45.5 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.45.5 or higher

2.4 Prerequisites

Table 5: List of Hardware Requirements

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

- CryptoServer is setup and configured. Refer the CryptoServer documentations to setup the HSM
- MBK must be created and stored onto each HSM. Refer the CryptoServer documentations to setup the MBK
- CryptoServer Default Admin should be replaced with a new admin user
- Operating system listed in Tested Versions
- SecurityServer listed in Tested Versions
- Admin user is required for installing software

2.5 Configuring the Utimaco CSP-CNG Provider

2.5.1 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.

2.5.2 Creating HSM Users

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

2.5.2.1 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.

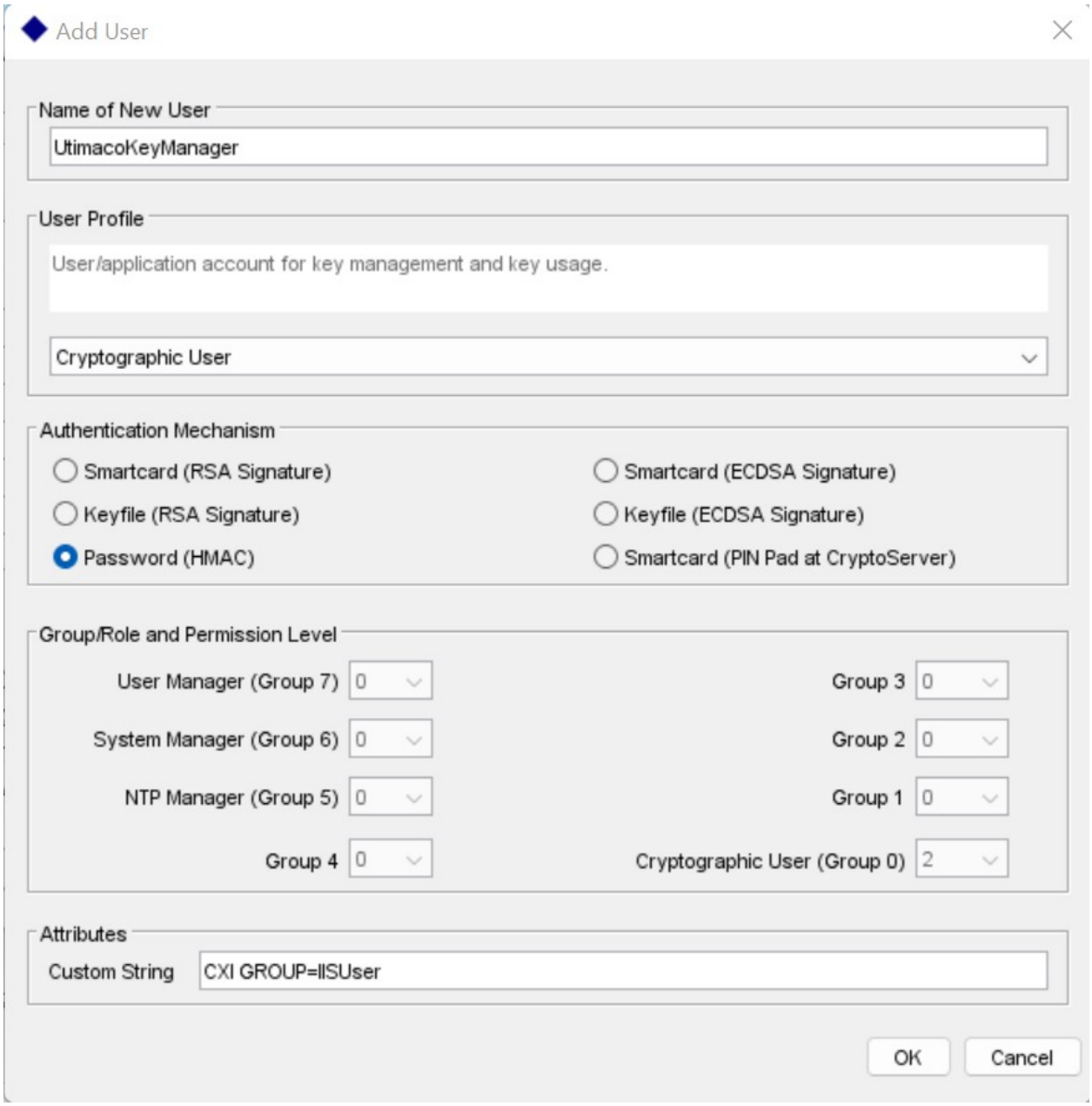


Figure 1: Creating Key Manager User

2.5.2.2 Creating a Crypto User

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 "IISUser" and HMAC password will be created.

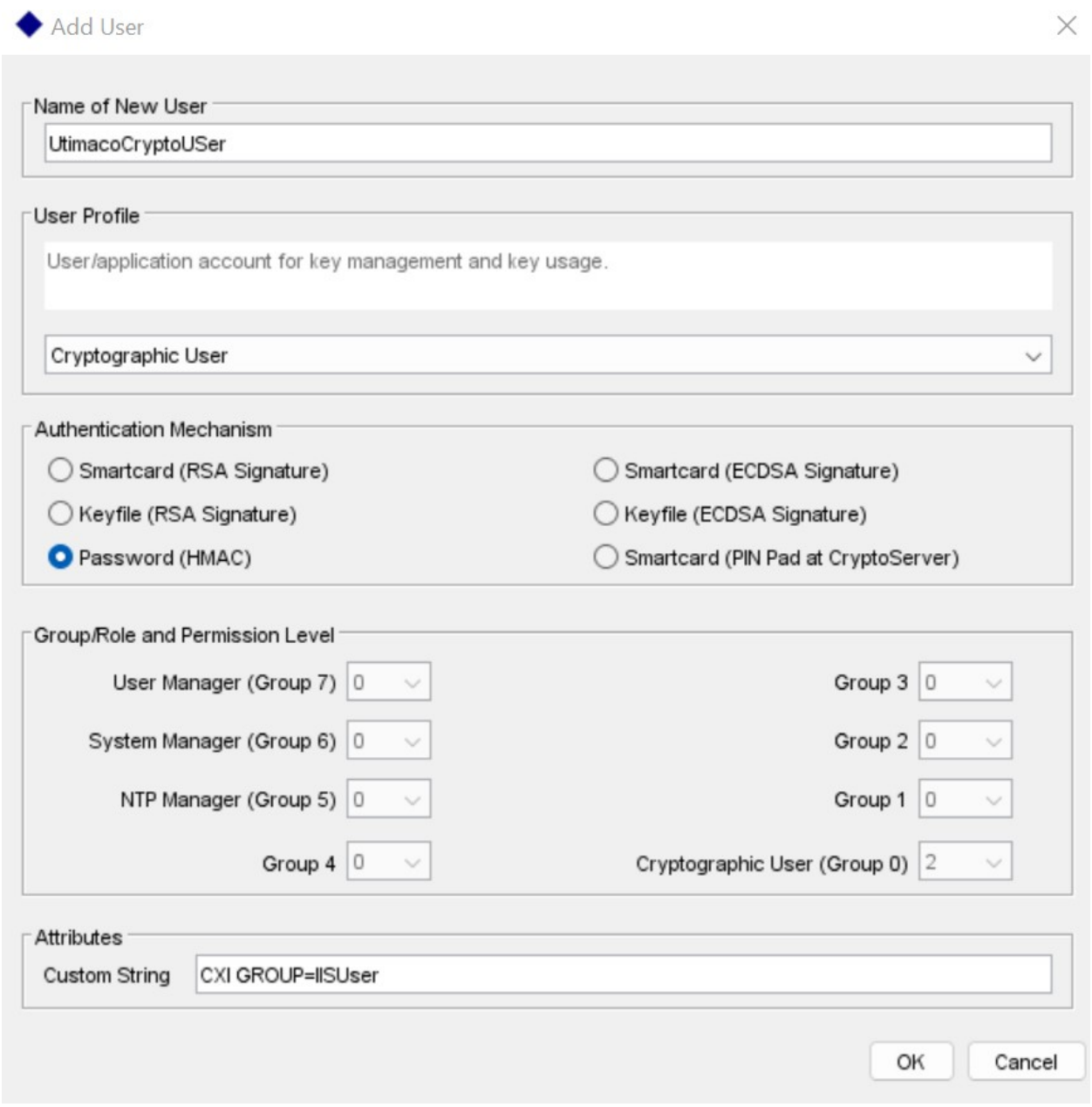


Figure 2: Creating a Crypto User

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.

2.5.3 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 more advanced configuration, refer to [CspCng];

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 "ERROR"

cs_cng.cfg

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

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 "UtimacoCryptoUser" with an HMAC password "Utimaco19"

cs_cng.cfg

```
Login = UtimacoCryptoUser,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 group name and IP address of the HSM

cs_cng.cfg

```
Group = IISUser
# default device and fallback devices Device = <HSM_IP>
```

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
```

2.5.3.1 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 : IISUser

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 : IISUser

Mode : Internal Key Storage
```

2.6 Integrating Microsoft IIS with Utimaco HSM

2.7 Install Microsoft IIS

1. Open Server Manager by clicking on Start button and selecting Server Manager

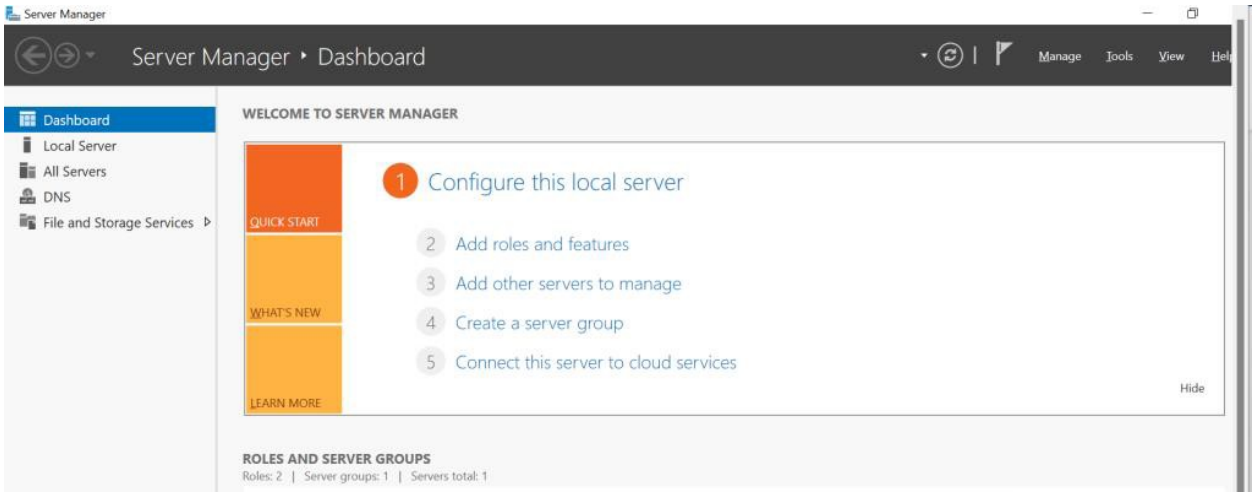


Figure 3: Server Manager Dashboard

2. Click on Manage and then click on Add Roles and Features..
3. On Before you begin screen, click on Next

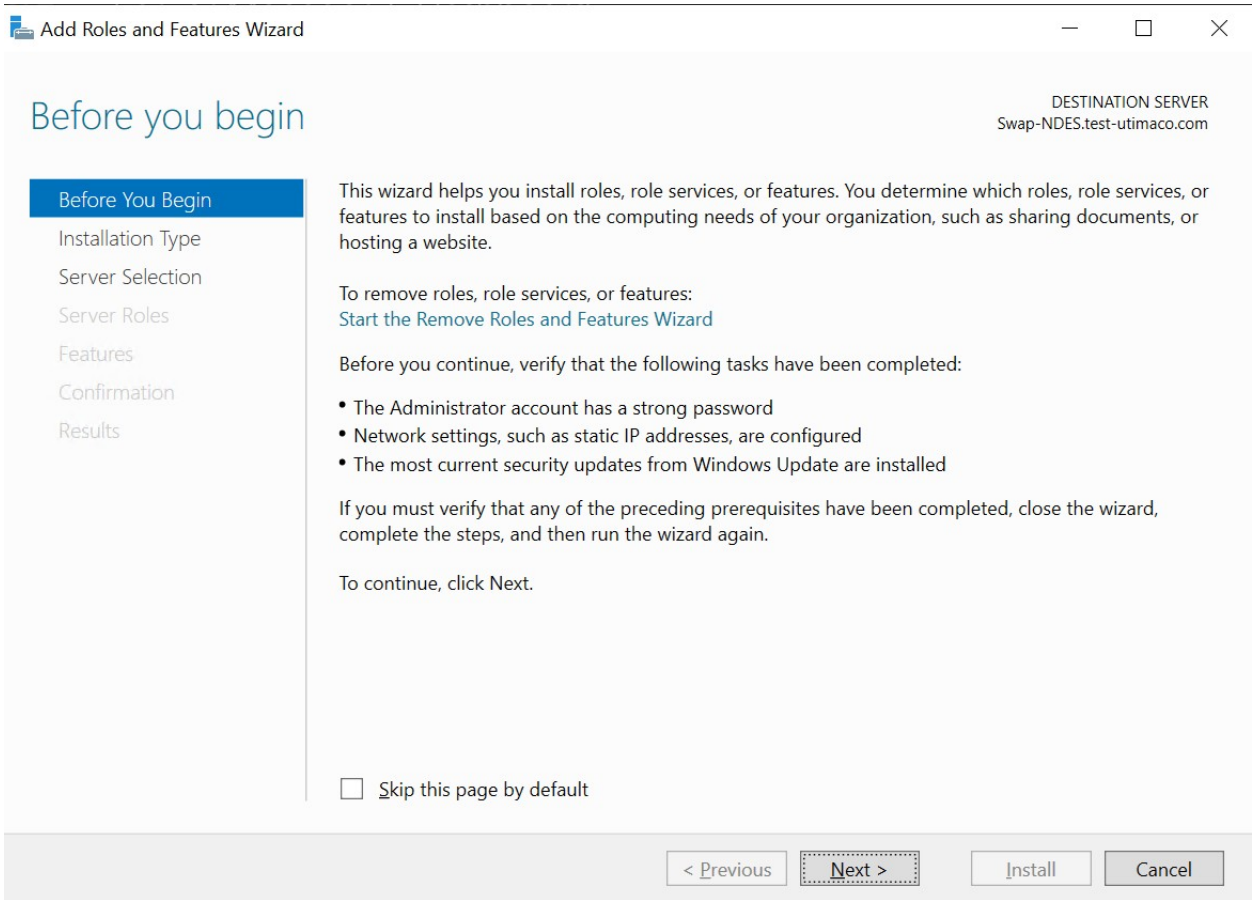


Figure 4: Add Roles and Features Wizard

4. On the Select installation type screen, ensure the default selection of Role or Feature Based Installation is selected and select Next

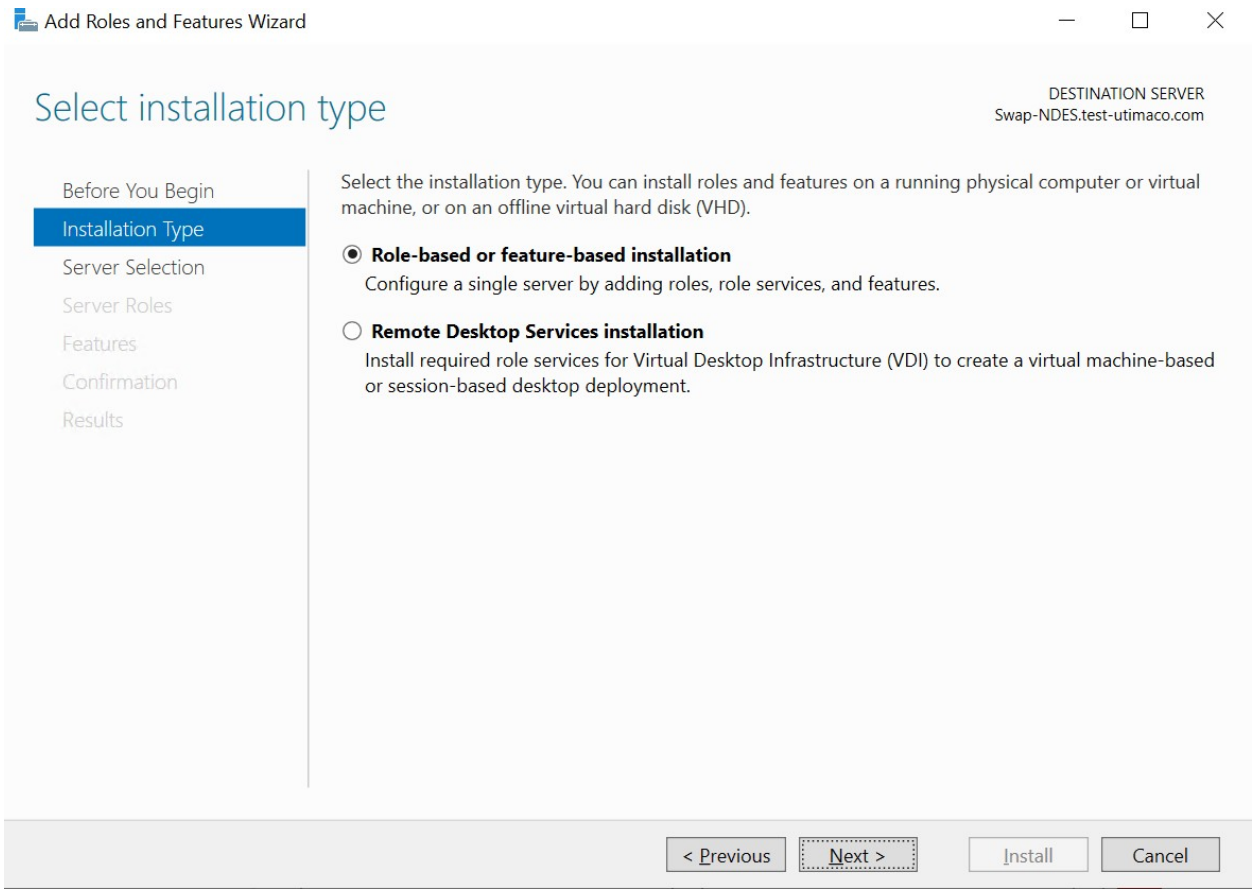


Figure 5: Installation Type Window

5. On the Server Selection screen, select a server from the server pool and select Next

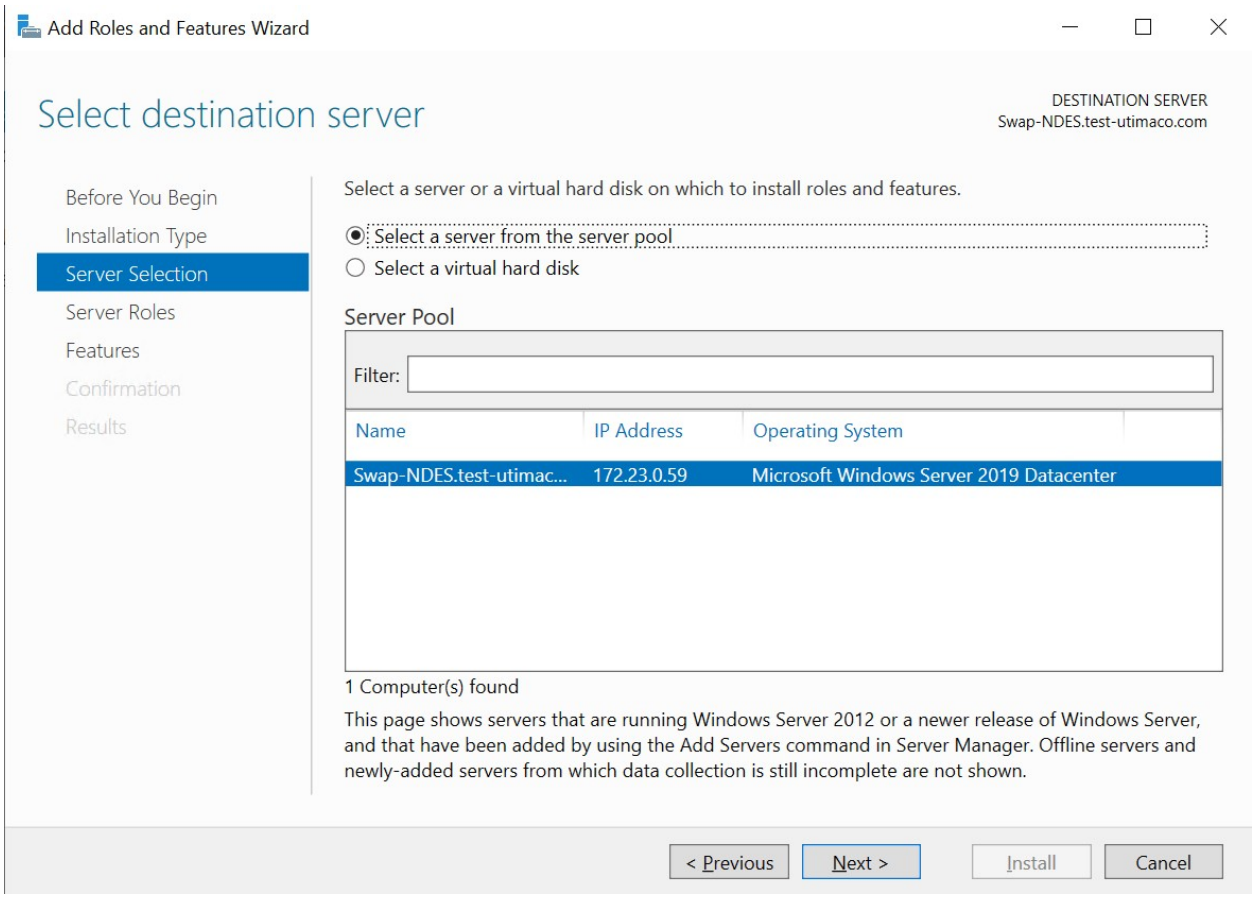


Figure 6: Destination Server Wizard

6. On the Select server roles screen, select the Web Server (IIS) Role, and select Next

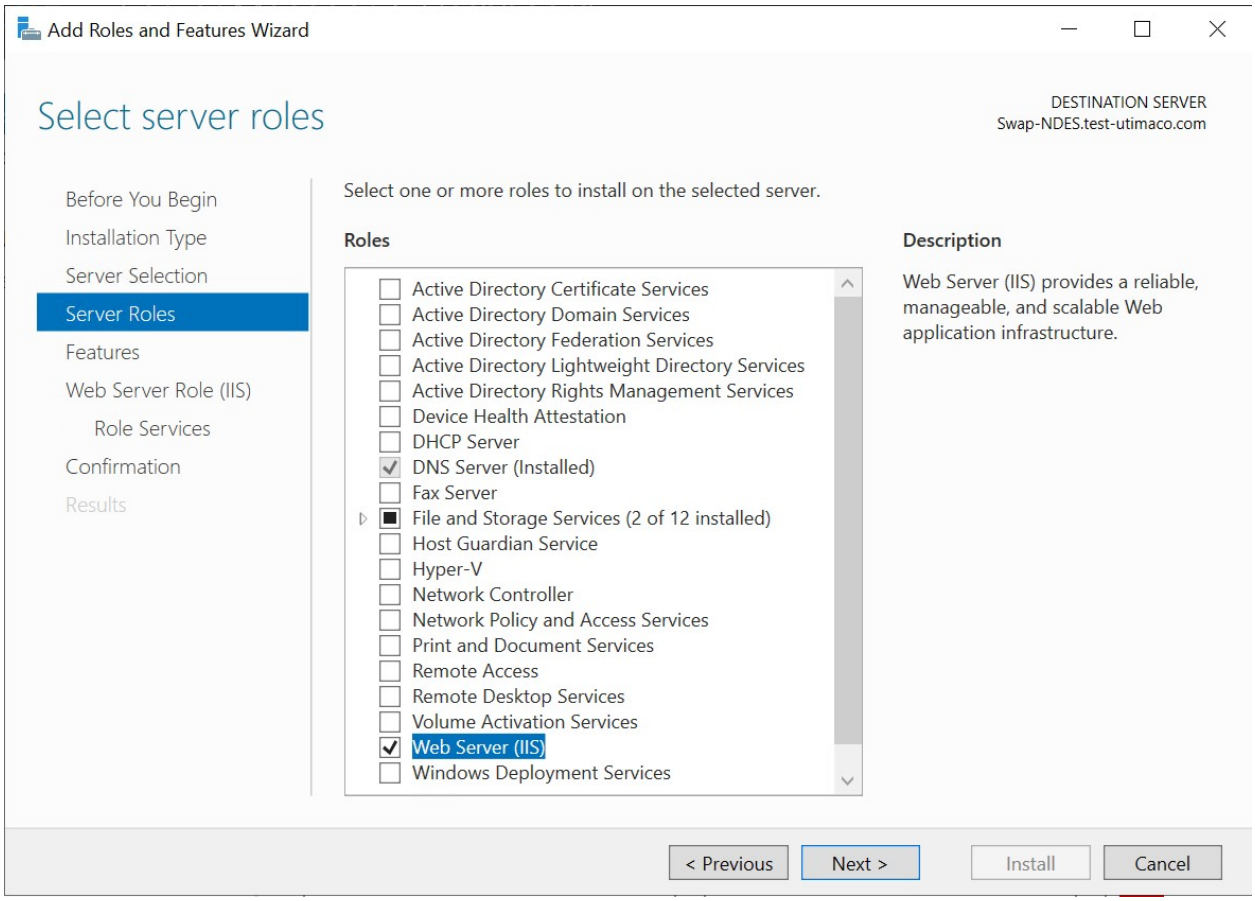


Figure 7: Select Server Roles

7. When prompted to install Remote Server Administration Tools, select Add Features, and select Next
8. On the Select features screen, keep the default selection, and select Next
9. On the Web Server Role (IIS) screen, select Next
10. On the Select Role Service screen, select Next
11. On the confirmation screen, select Install

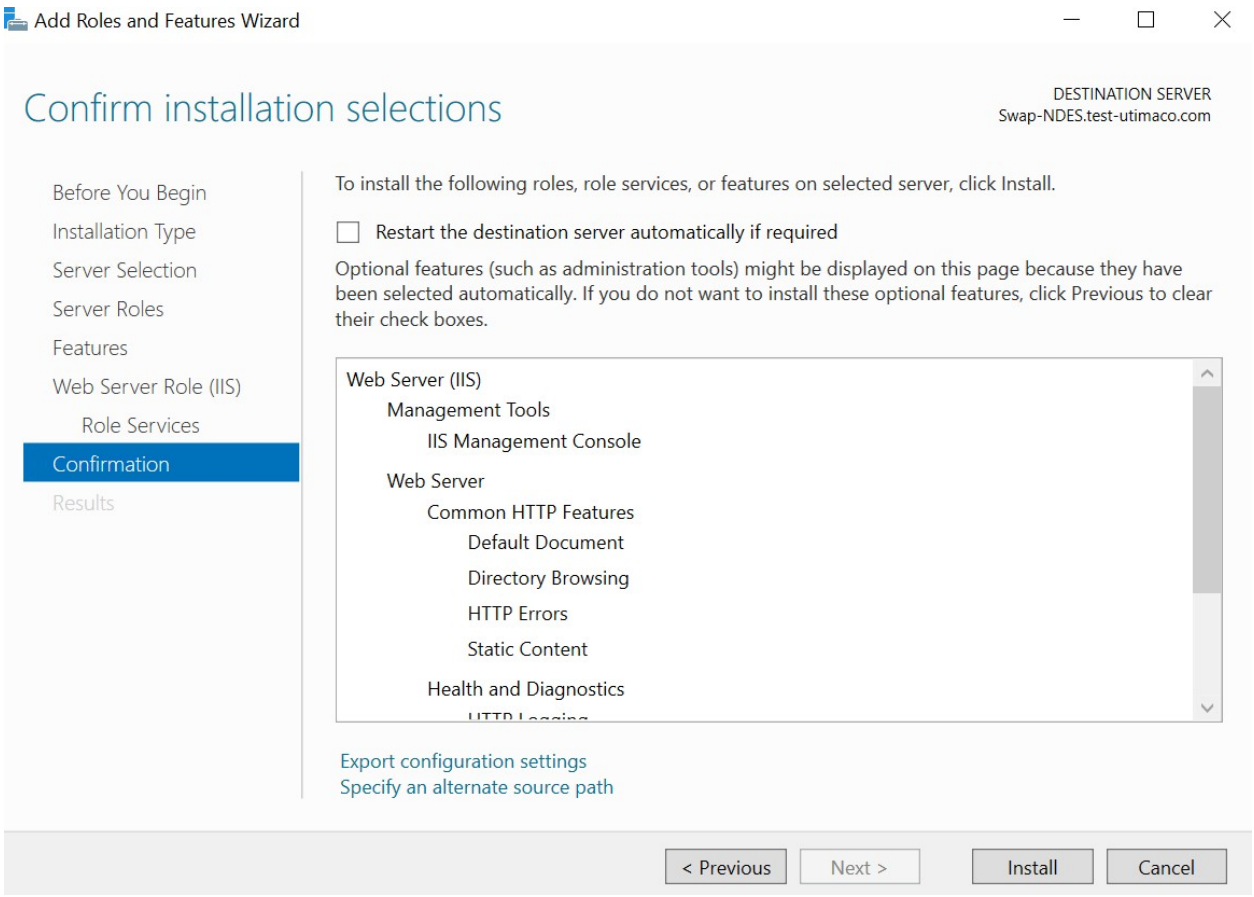


Figure 8: Confirm Installation Selections Wizard

12. Once the installation completes, Select Close

2.8 Generating a Certificate Request for IIS

There are two ways to generate CSR for IIS

- Generate CSR by certreq command line tool
- Generate CSR by GUI Tool

2.8.1 Generate CSR by certreq Command Line Tool

1. To make sure the Utimaco CryptoServer Key Storage Provider are listed, use below command

›_ Console

```
cngtool EnumProvider
```

2. Set up a template file:

    a. Generate a request for an SSL certificate linked to a 2048 RSA key by creating a file called request.inf with the following information

    b. Specify the subject details of the IIS Server

    c. Specify the key algorithm and key length as required, for example RSA 2048

    d. Specify the Provider name as Utimaco CryptoServer Key Storage Provider

    e. When you have set up the template successfully, save it as request.inf on the C:\ drive

›_ Console

```
[Version]
Signature= "$Windows NT$" [NewRequest]
Subject = "CN=utimaco.com,C=IN,ST=MH,L=testing,O=UtimacoCom,OU=IISServer"
 HashAlgorithm = SHA256
KeyAlgorithm = RSA KeyLength = 2048
ProviderName = "Utimaco CryptoServer Key Storage Provider" KeyUsage = 0xf0
MachineKeySet = True [EnhancedKeyUsageExtension] OID = 1.3.6.1.5.5.7.3.1
```

3. Open a command prompt and go to the local drive, in this case C:\

4. To create the certificate request for the Certification Authority, execute the command:

›_ Console

```
C:\ certreq.exe -new request.inf IISCertRequest.csr
CertReq: Request Created.
```

A certificate request called IISCertRequest.csr is generated and placed on the C:\ drive.

2.8.2 Generate CSR by GUI Tool

1. Open Run and use certlm.msc command

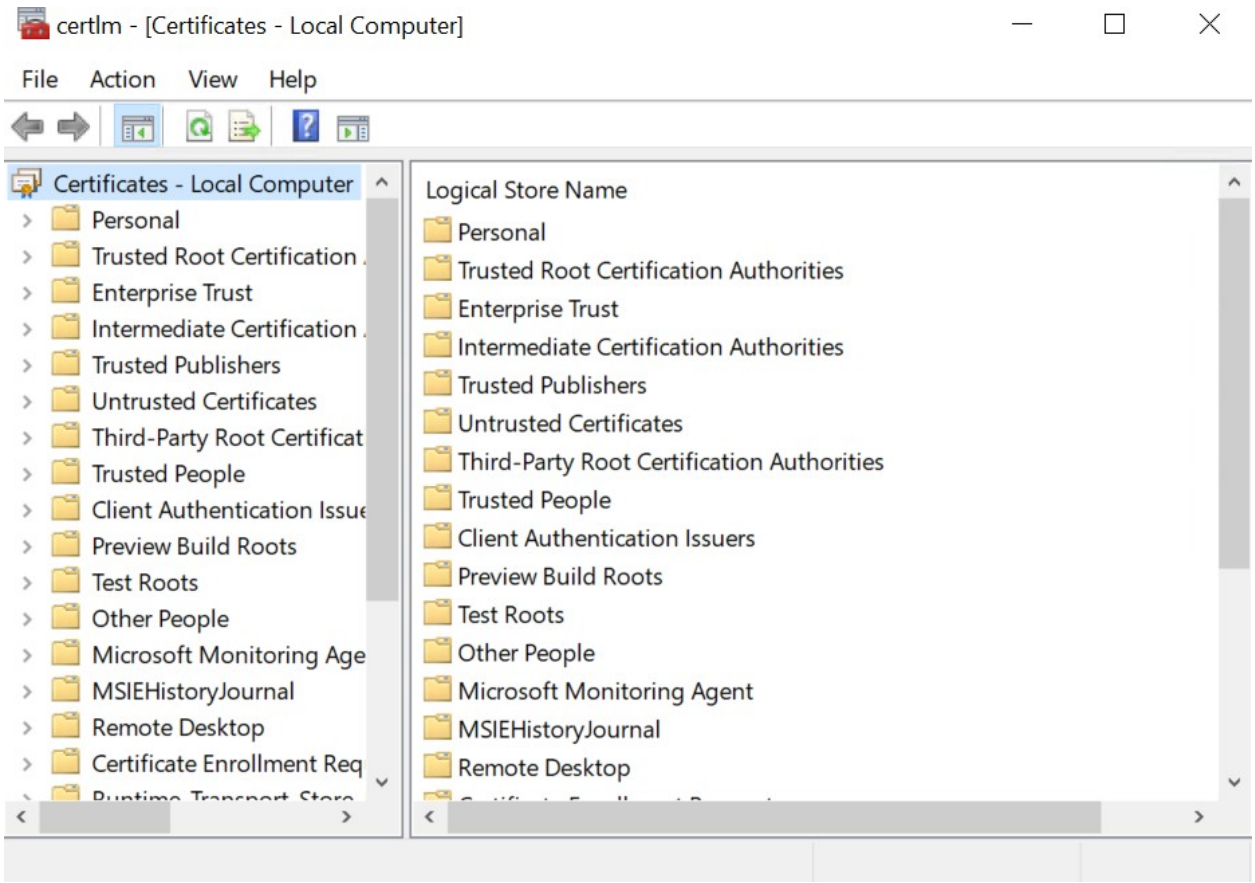


Figure 9: Local Computer – Certificates

2. `Right click on Personal → All Tasks → Advanced Operations → Create custom requests`

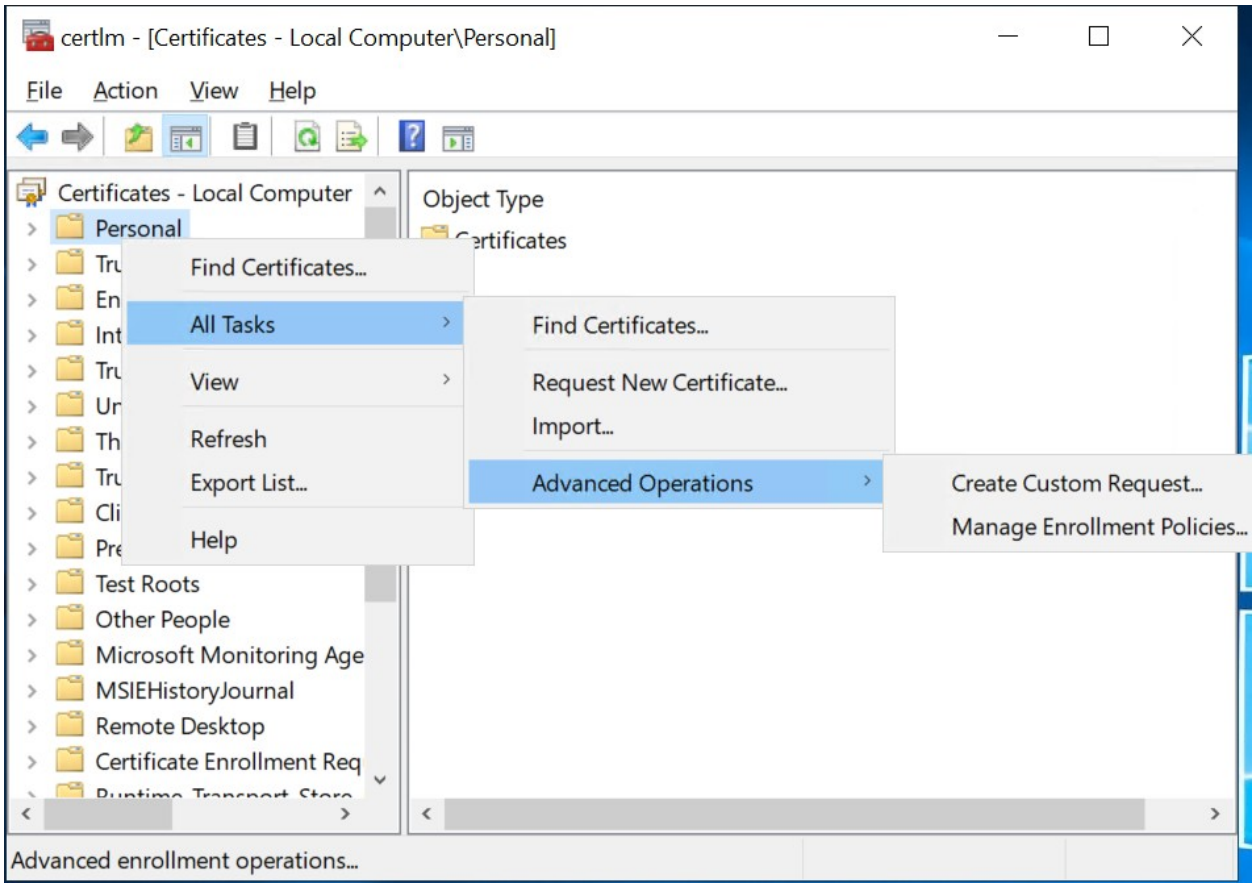


Figure 10: Create Custom Request

3. Click next button on Before you begin wizard screen
4. Select next on Select Certificate Enrollment Policy wizard
5. On Custom Request wizard use Template (No Template) CNG Key and Request format PKCS #10 and click next

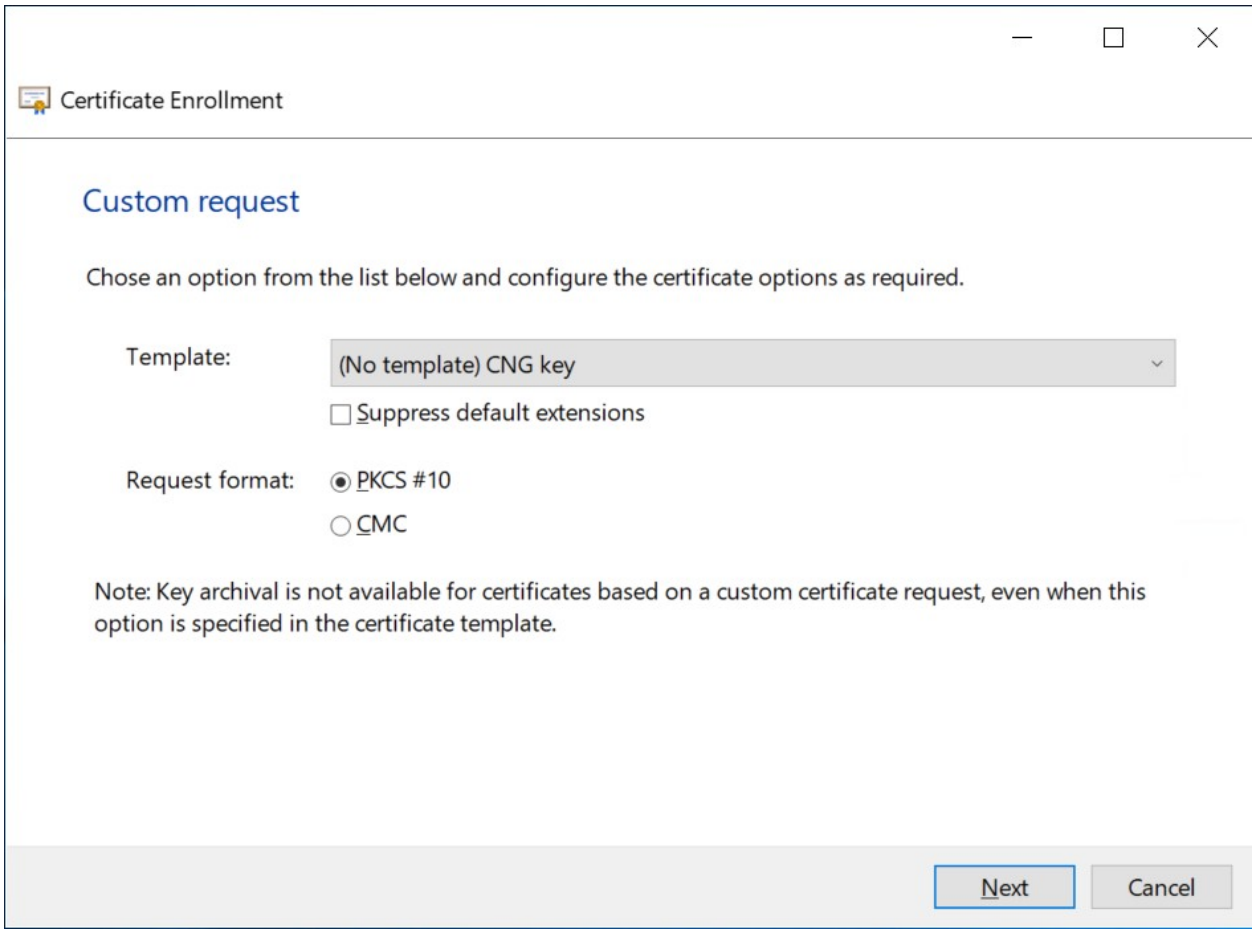


Figure 11: Certificate Enrollment - Custom request

6. Select details and click on Properties button

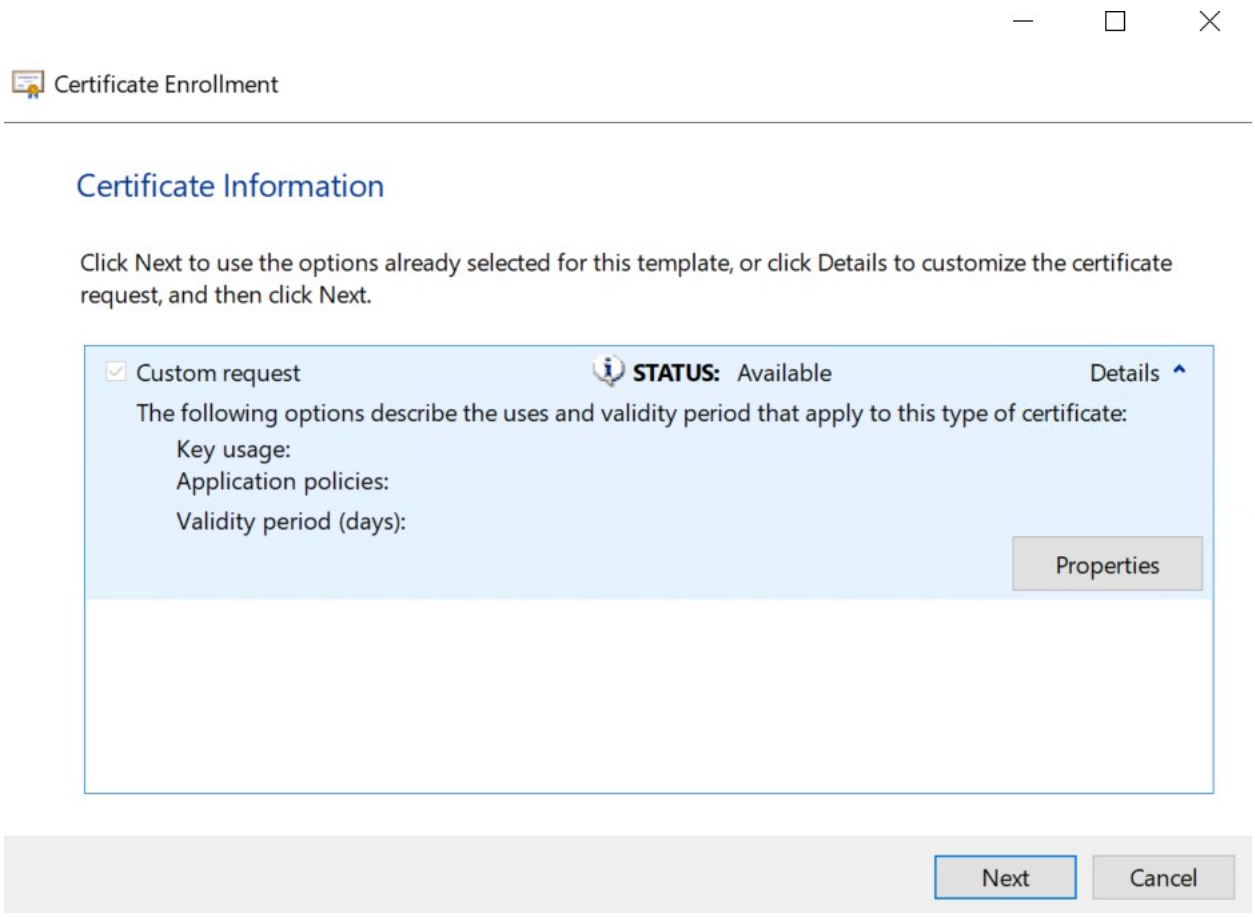


Figure 12: Certificate Information

7. On Certificate Properties Assign Friendly name and Description

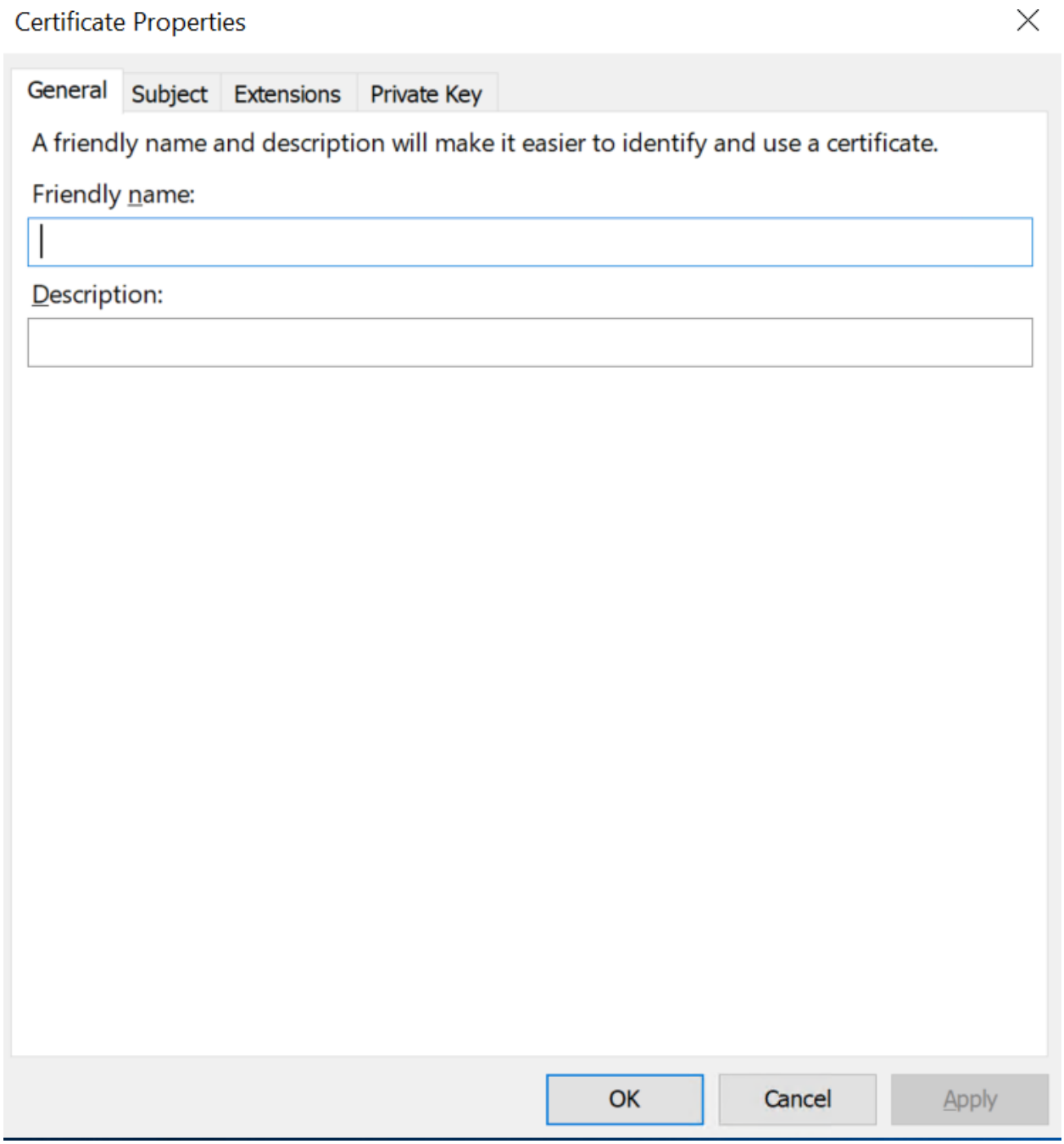


Figure 13: Certificate Information

8. On Subject tab select Subject Name Type and enter information for Full DN, Common Name, Country, Email, Given Name, Locality, Organization, Organization Unit, State etc.,

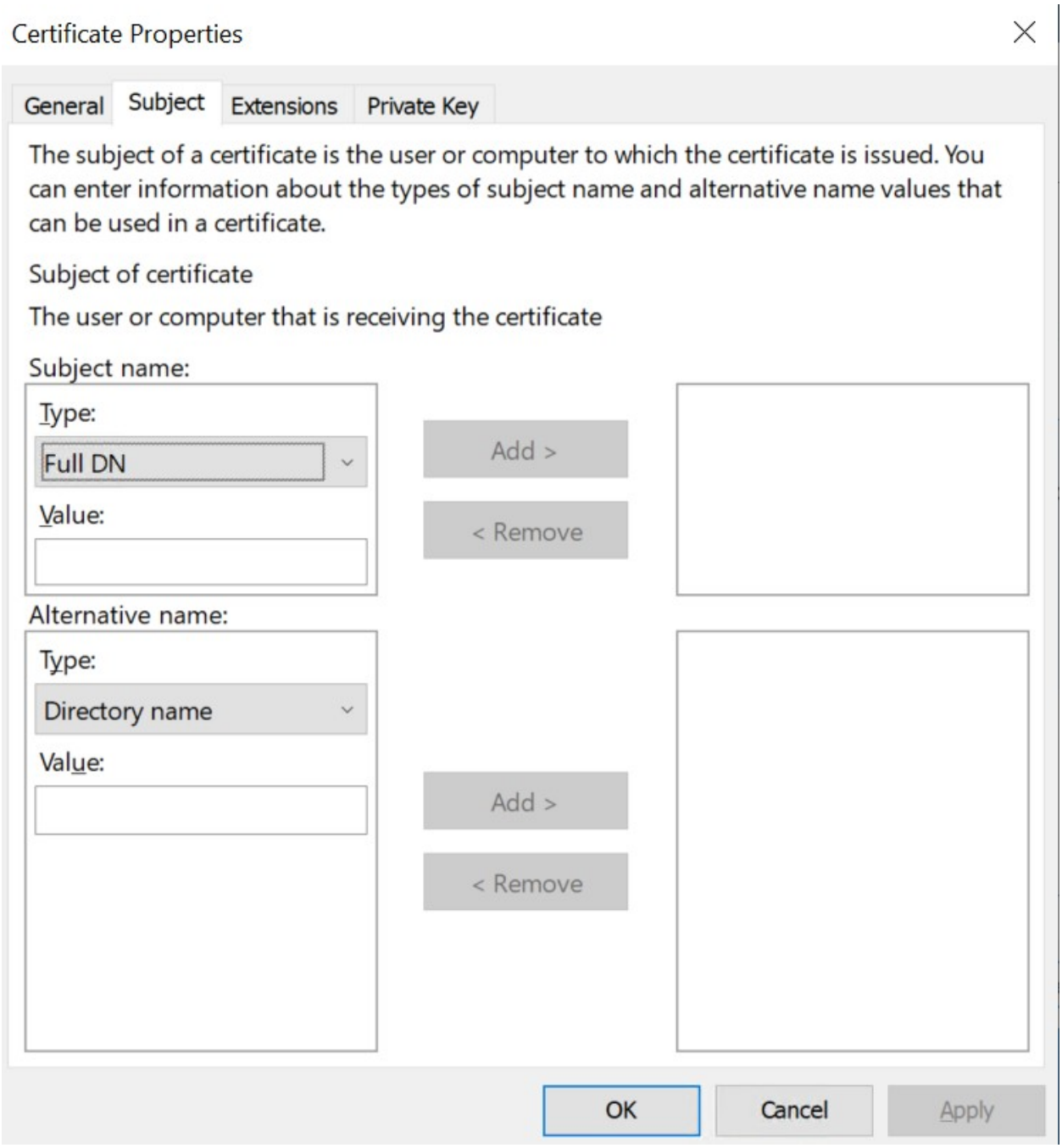


Figure 14: Certificate Properties – Subject

9. On Private Key Tab Click on Cryptographic Service Provider and unselect the RSA, Microsoft Software Key Storage Provider and Select RSA, Utimaco CryptoServer Key Storage Provider

10. On select Hash Algorithm select sha256

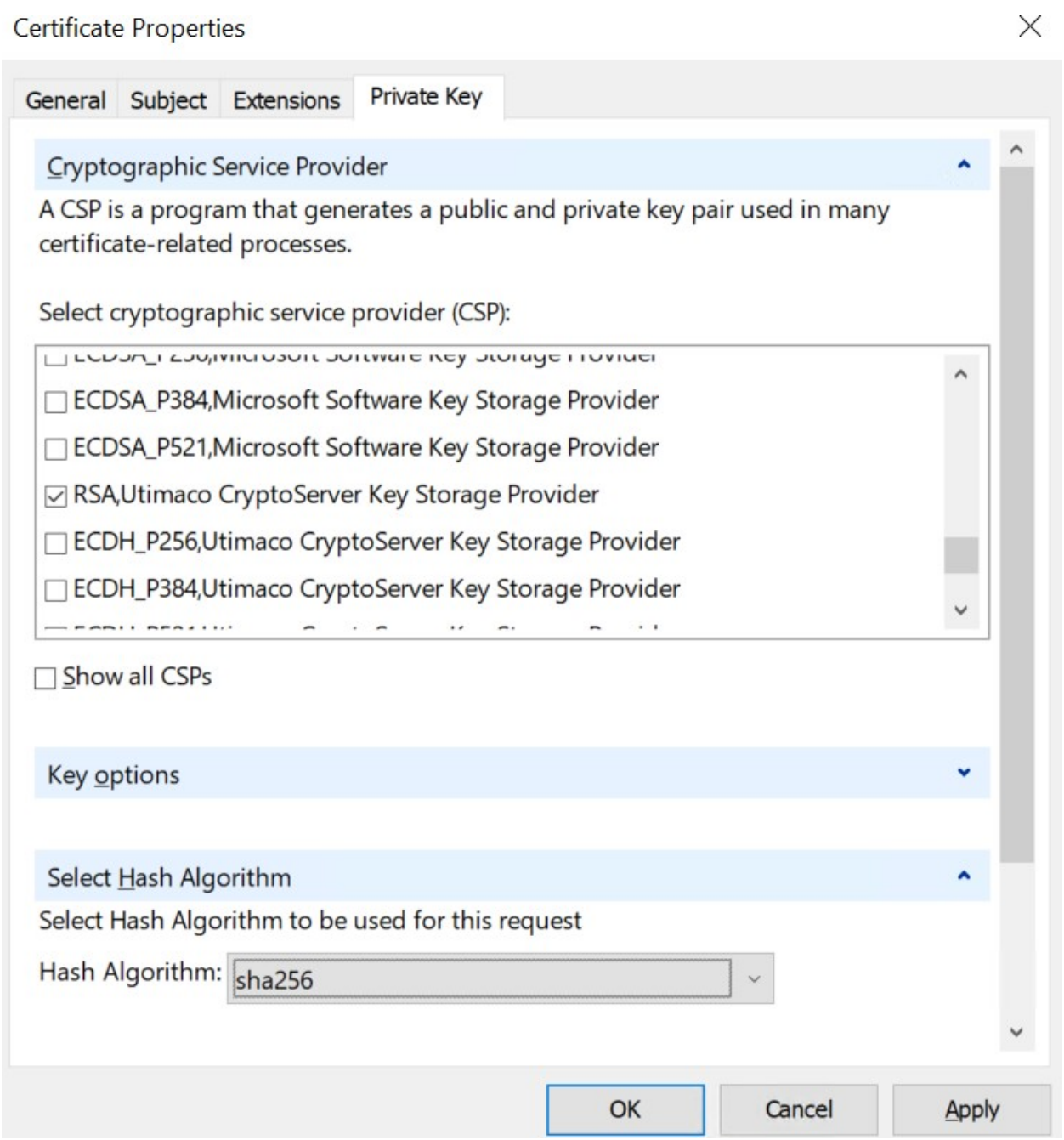


Figure 15: Certificate Properties - Private Key

11. Click Apply and OK
12. Check on HSM using below command that Certificate/Key is generated

›_ Console

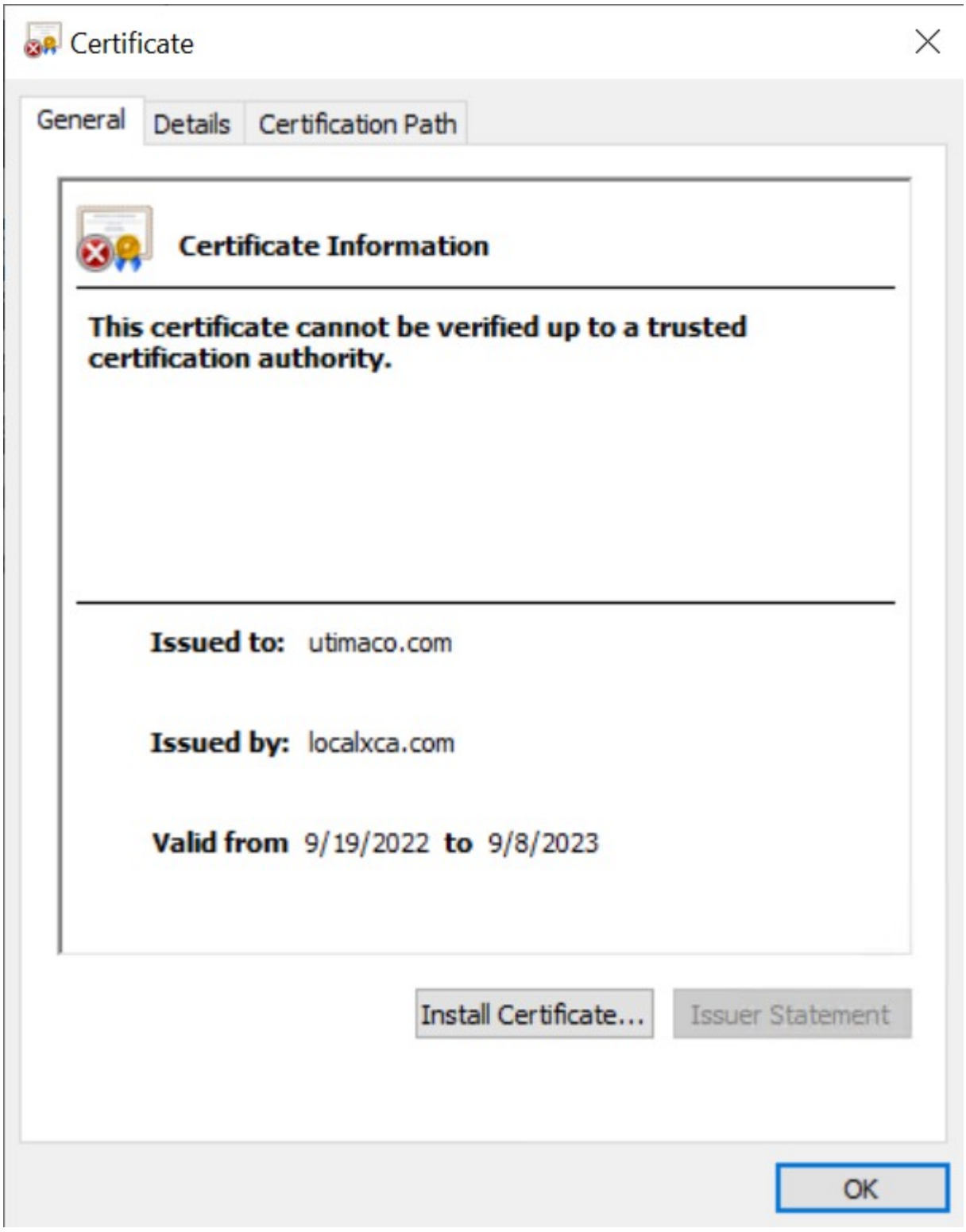
```
C:\>cngtool ListKeys
```

```
C:\>cngtool ListKeys

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

Provider          : Utimaco CryptoServer Key Storage Provider
Device            : 288@10.44.223.141
Group             : IISUser
Mode              : Internal Key Storage

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

Index  AlgId        Size   Group           Name                                Spec
-------------------------------------------------------------------------------------
1      RSA          2048   IISUser         te-a5506c38-c53d-4d60-b811-5f0252d51ff6 0
2      RSA          2048   IISUser         TESTSKEY123                         0
3      ECDSA_P256   256    IISUser         te-ab6198f7-cce5-4b4f-a8d6-557a7a0a1c71 0
```

Figure 16: Key Listing

2.9 Get Certificate Signed by CA

1. Submit the CSR file to a CA. The CA authenticates the request and returns a signed certificate or a certificate chain
2. Copy the signed certificate to IIS server



2.10 Install the Certificate

Figure 17: Certificate Properties

To make the certificate available for use in IIS, run the following command:

›_ Console

```
C:\ certreq --accept IISCertSigned.cer
```

Where IISCertSigned.cer is the signed certificate provided by the CA.

Install CA certificate in Trusted Root Certificate Authorities if root CA is not installed before installing IIS SSL certificate.

```
C:\>CertReq -Accept -machine IISCertSigned.cer
Installed Certificate:
  Serial Number: 291143aa32c40f1d
  Subject: CN=utimaco, C=IN, E=support@utimaco.com, L=pune, O=utimaco, OU=QA, S=MH
  NotBefore: 9/30/2022 7:06 AM
  NotAfter: 9/8/2023 11:14 AM
  Thumbprint: 91be409cf6545fa6170b932770abed8589a15378
```

Figure 18: Certreq command Output Window

2.11 Bind the certificate with a Secure IIS Web Server

1. Go to Start > Internet Information Service Manager
2. Select the hostname, then double-click Server Certificates and verify the certificate you accepted in the previous step is listed

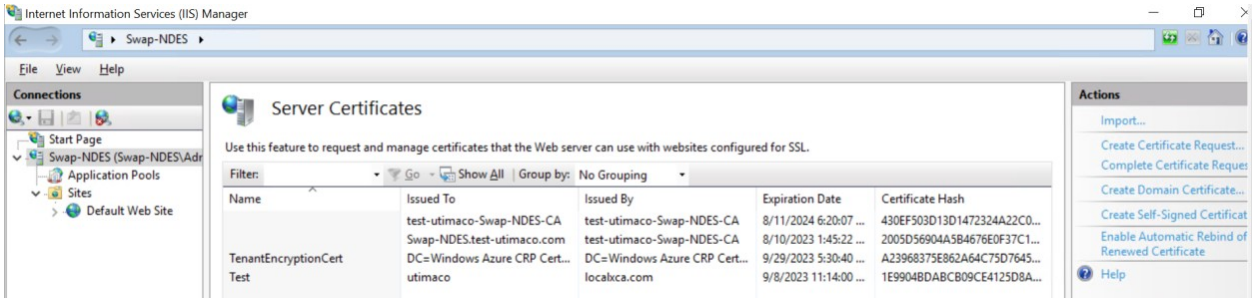


Figure 19: IIS Manager Dashboard

3. Click Default website under Sites on the left-hand side of the IIS Manager screen

4. Select Bindings link on the right-hand side of the IIS Manager
5. On the Site Bindings screen, select Add
6. Select the protocol as HTTPS and select the certificate from the SSL Certificate drop-down list

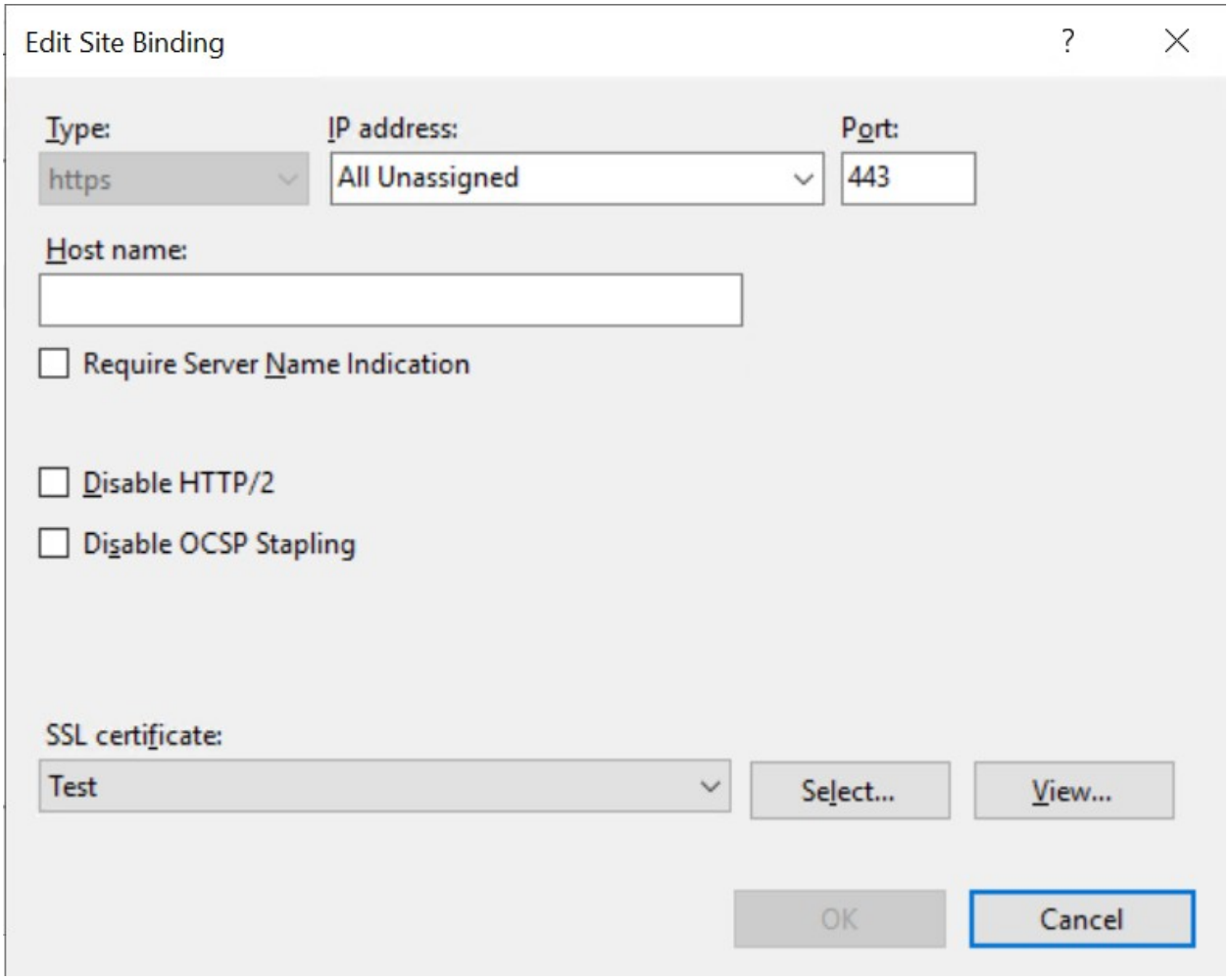


Figure 20: Site Binding wizard

7. Select OK to complete the certificate binding for SSL connection
8. Select Close on the Site Bindings screen
9. Restart the IIS server
10. Open https://<IIS_Server_IP>:443 in any of the browser
11. Verify that the page is accessible over https

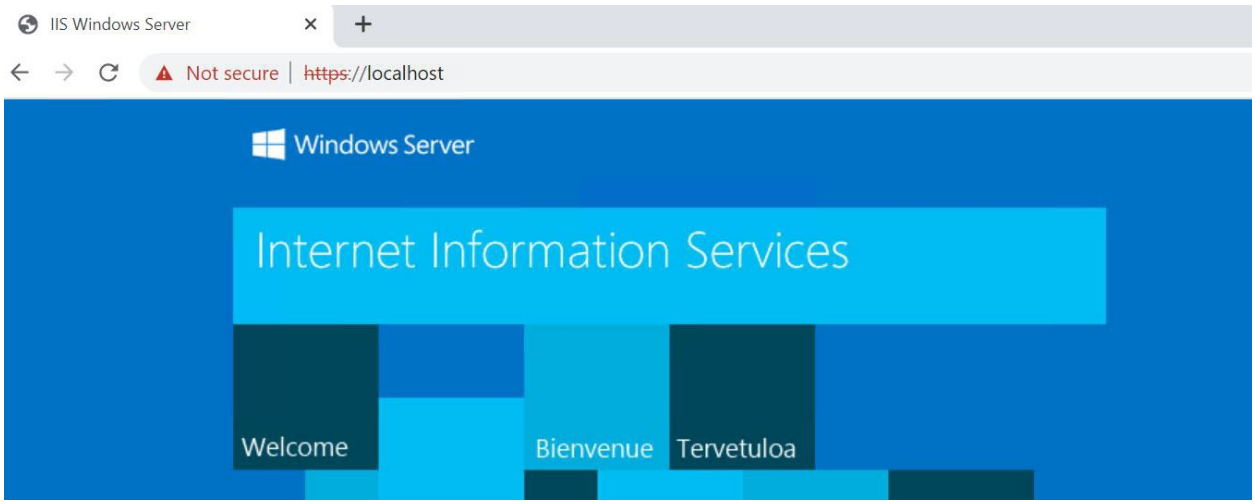


Figure 21: Site Binding wizard

This completes the integration of MS IIS with Utimaco HSM.

3 Troubleshooting

Error	*Diagnosis*
This site is not secure	Click on Go on to the webpage (not recommended)
Webpage not found	IIS service is not running, start it from services.msc. Also check if the certificate is configured properly for SSL.

Table 6: List of Error and its Diagnosis

4 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/

5 References

Reference	*Title/Company*	*Document No.*
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH	M011-0008-en
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSP11Tool2]	CryptoServer_p11tool2_Manual.pdf	2012-0004
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[CSLAN5]	CryptoServerLAN_Manual_Systemadministrators.pdf	2018-0004