Microsoft

Internet Information Services (IIS)

10.0

Integration Guide

u.trust GP HSM Se-Series

6.1.1

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 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	1.0.1
Date	2025-09-23
Status	PUBLISHED
Document No.	IG-2025-0027

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco to facilitate secure web server encryption practices. It outlines the integration of Microsoft Internet Information Services (IIS) with Utimaco's Hardware Security Module (HSM), enabling robust key management and enhanced protection of SSL/TLS private keys.

1.1 About This Guide

This guide describes how to integrate Microsoft Internet Information Services (IIS) with Utimaco HSM to enable secure key management for web server encryption operations. The primary objectives of this integration are:

- Strengthen data protection by securely managing SSL/TLS private keys within the Utimaco HSM.
- Enable IIS functionality using external key management to support compliance and enhance the security of HTTPS communications.

This guide walks through the required configuration steps, including HSM initialization, certificate enrollment, IIS binding setup, and secure key usage for TLS operations using SecurityServer.

1.2 Target Audience

This guide is intended for Microsoft IIS administrators and Utimaco HSM administrators.

1.3 Purpose of the Integration

The purpose of integrating Microsoft IIS with Utimaco HSM is to establish a secure and centralized key management solution for protecting private keys used in HTTPS communications. This integration ensures that SSL/TLS keys are generated, stored, and managed within a certified hardware-based environment, significantly reducing the risk of unauthorized access, key compromise, or data breaches.

1.4 Abbreviations

Abbreviation	Meaning
HSM	Hardware Security Module
IIS	Internet Information Services
CA	Certificate Authority
CNG	Cryptography API Next Generation
CSADM	CryptoServer Command-line Administration Tool
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
JRE	Java Runtime Environment
MBK	Master Backup Key
GUI	Graphical User Interface
CXI	Cryptographic eXtended Interface
HMAC	Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Prorocol

Abbreviation	Meaning
LAN	Local Area Network
PCIe	PCI Express Interface
PIN	Personal Identification Number
RSA	Rivest-Shamir-Adleman
SSL	Secure Socket Layer

Table 1: Abbreviations

1.5 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	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

Table 2: Document Conventions

We use special icons 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.

2 Product Overview

2.1 Overview of Microsoft IIS

Microsoft Internet Information Services (IIS) for Windows Server is a flexible, secure, and manageable web server platform for hosting websites, services, and applications. IIS supports a wide range of web technologies, including static content, dynamic applications, and media streaming.

IIS uses authentication, authorization, and SSL/TLS encryption to secure data transmitted between clients and servers. It provides a modular architecture that allows administrators to enable only the necessary components, improving performance and reducing the attack surface.

Key components of IIS include:
• Application Pools: Isolated environments for running web applications independently.
• Bindings: Configuration settings that associate websites with IP addresses, ports, and certificates.
• Modules: Pluggable features that handle specific tasks such as request filtering, compression, and logging.

IIS enables secure and scalable hosting for enterprise-grade web services. It helps protect data in transit (also called data on the wire) and ensures reliable delivery of web content across diverse environments

2.2 Overview of 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.

2.3 Joint Value Proposition

Integrating Microsoft IIS with Utimaco HSM offers a secure and compliant solution for protecting cryptographic keys used in web server communications. Microsoft IIS provides robust support

for SSL/TLS encryption to secure data in transit, while Utimaco HSM ensures that private keys are generated and stored in a tamper-resistant hardware environment.

3 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 the required Software.

3.1 Tested Versions

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

Operating System	IIS Version	Utimaco Security Server Version	Utimaco HSM
Windows Server 2022	10.0	6.1.1	u.trust GP HSM Se-Series
Windows Server 2025	10.0	6.1.1	u.trust GP HSM Se-Series

Table 3: Tested Versions

3.2 Hardware and Software Requirements

3.2.1 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	u.trust GP HSM Se-Series LAN with firmware SecurityServer 6.1.1 or higher
Utimaco PCI-e HSM	u.trust GP HSM Se-Series PCI-e with firmware SecurityServer 6.1.1 or higher

Table 4: Hardware Requirements

3.2.2 Software Requirements

Software	Software Requirements
HSM Interfaces	CryptoServer CSP/CNG Provider
Microsoft IIS	10.0
JRE 8	Java Runtime Environment 8

Table 5: Software Requirements

3.3 Prerequisites

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

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

4 Installation and Configuration

4.1 Setting Up Utimaco SecurityServer Software

4.1.1 Creating HSM Users

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

4.1.2 Creating a Crypto User

Crypto user with a permission level of 00000002 must be created using encrypted passwords. In this guide, a user with permission level 00000002, assigned to the CXI_GROUP IISUser, and secured with an HMAC password will be created.

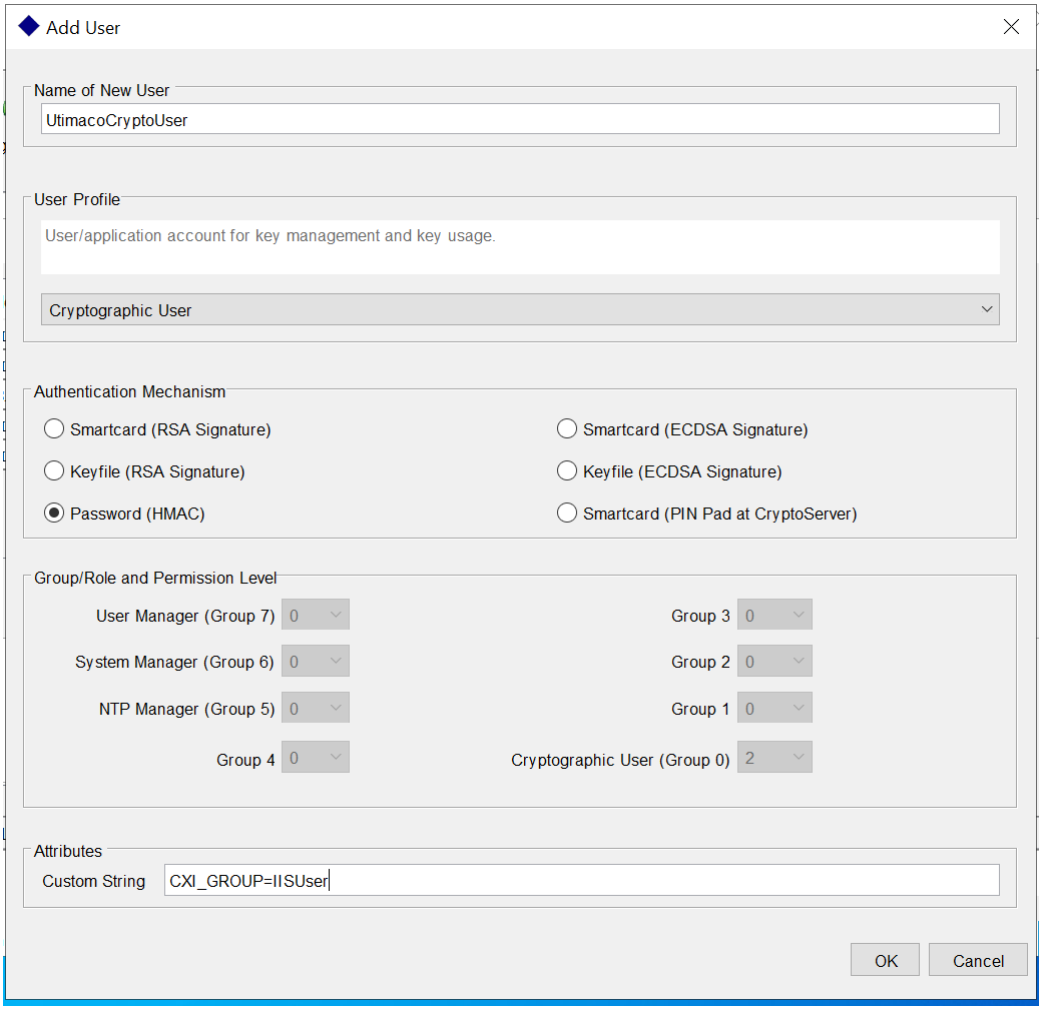

Figure 1 : Creating CryptoUser

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.

4.2 Setting up Microsoft IIS

4.2.1 Install Microsoft IIS

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

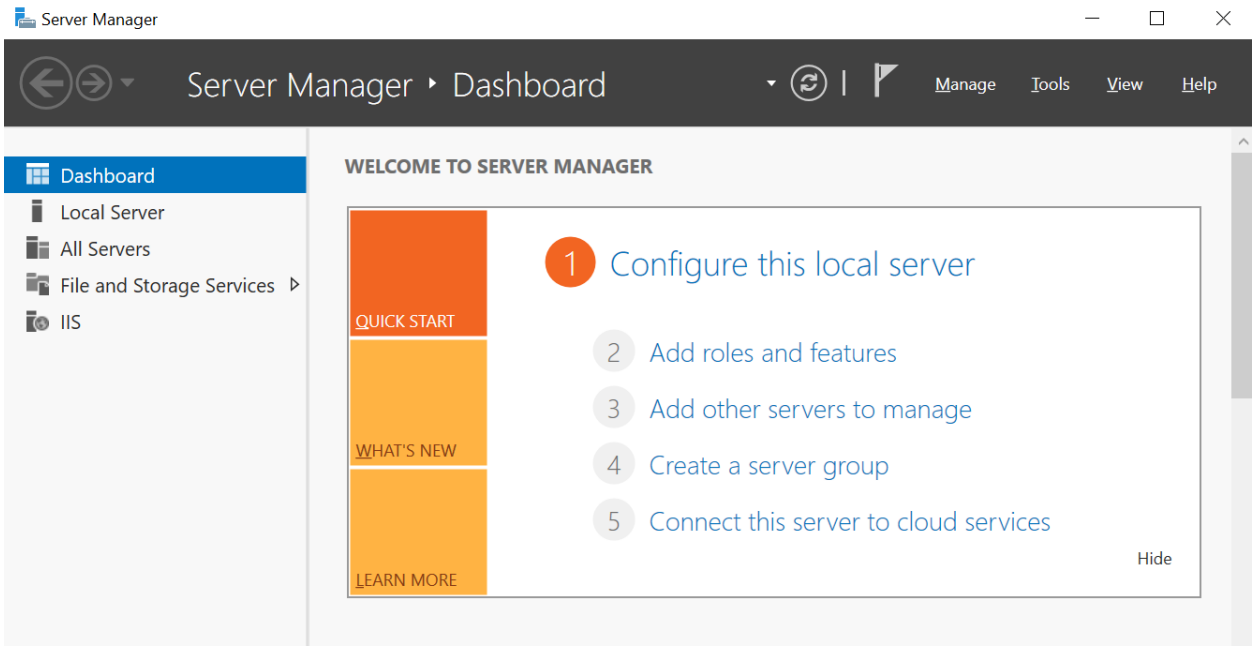

Figure 2 : Server Manager Dashboard

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

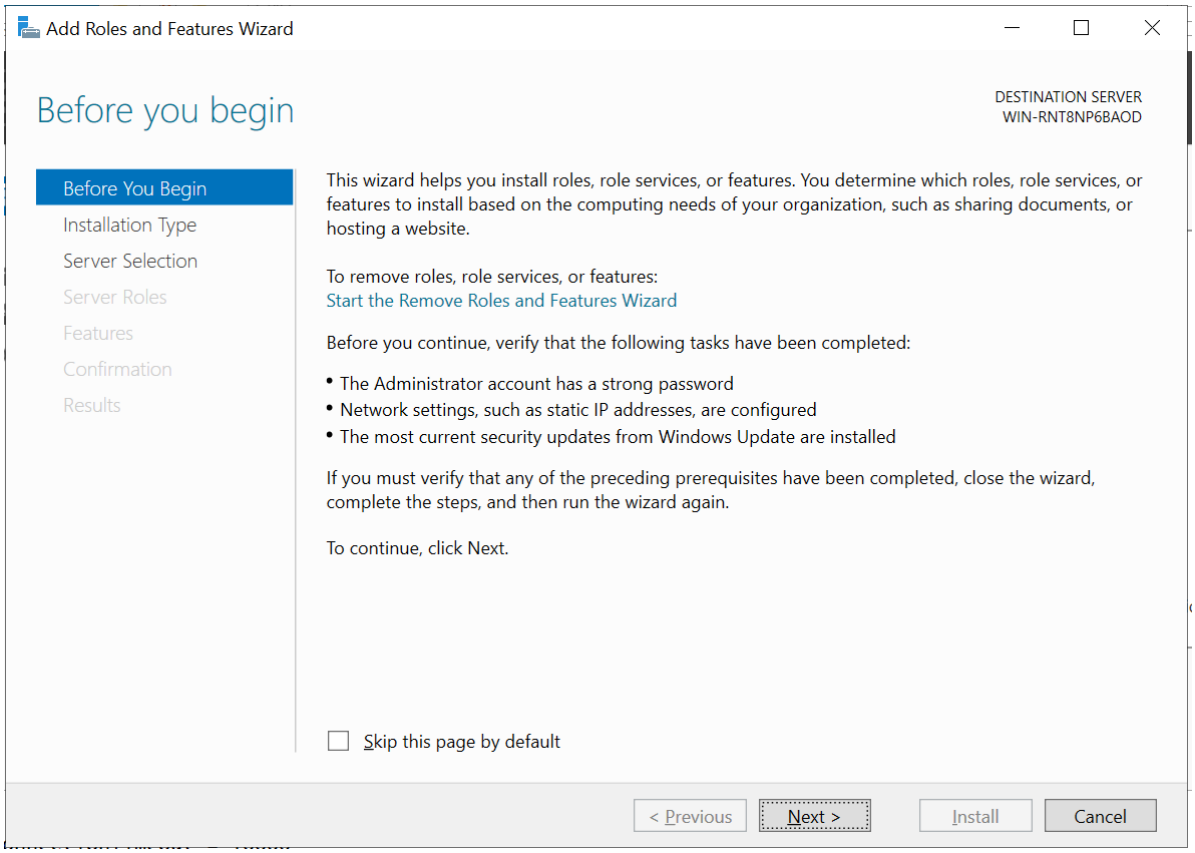

Figure 3 : Add Roles and Features Wizard

4. On the Select installation type screen, ensure the default selection of **Role-based or feature-based Installation** is selected and select **Next**

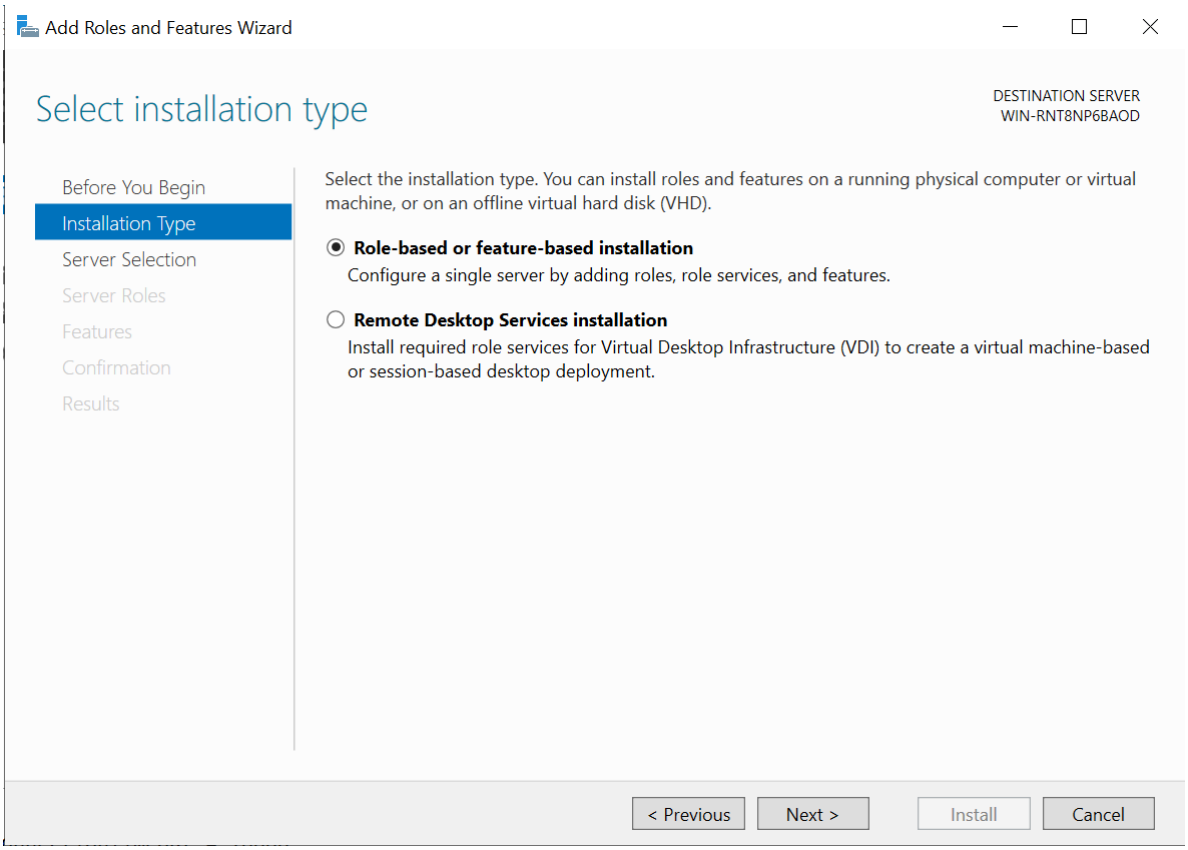

Figure 4 : Installation Type window

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

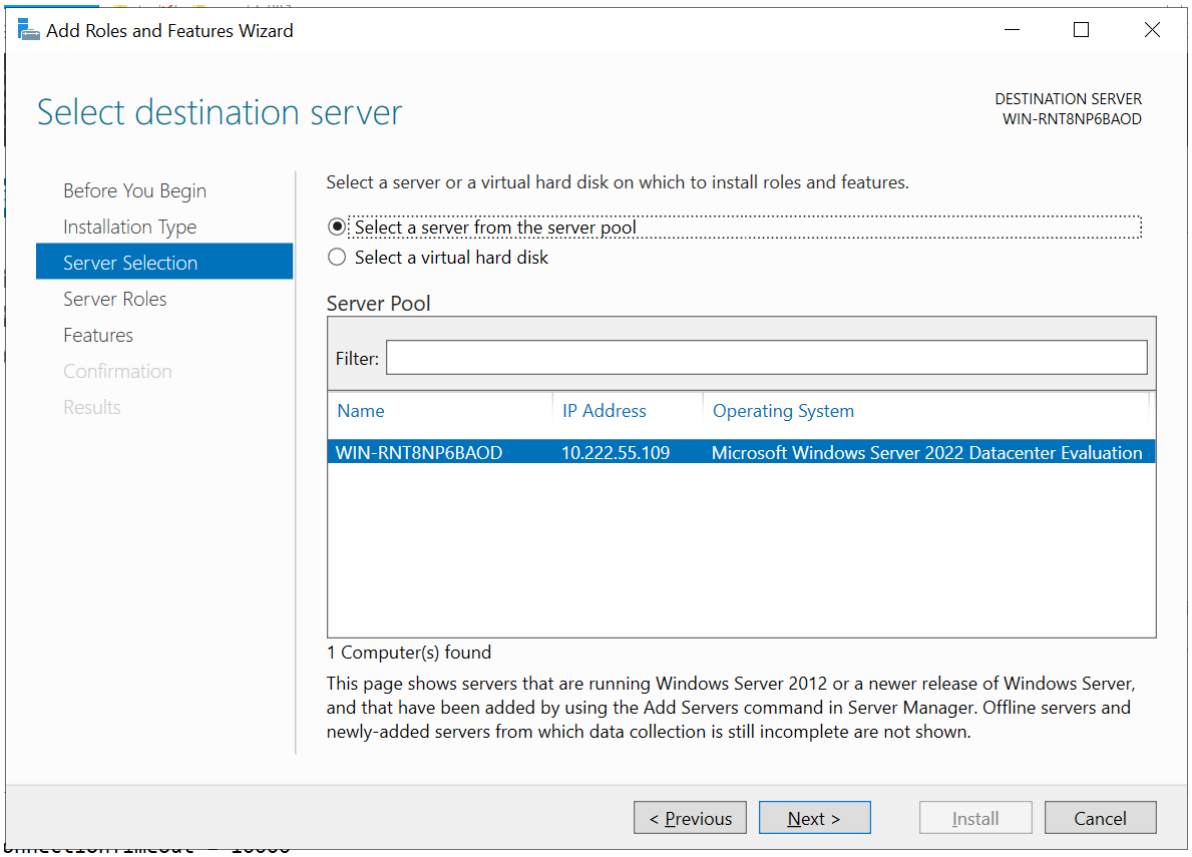

Figure 5 : Destination Server wizard

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

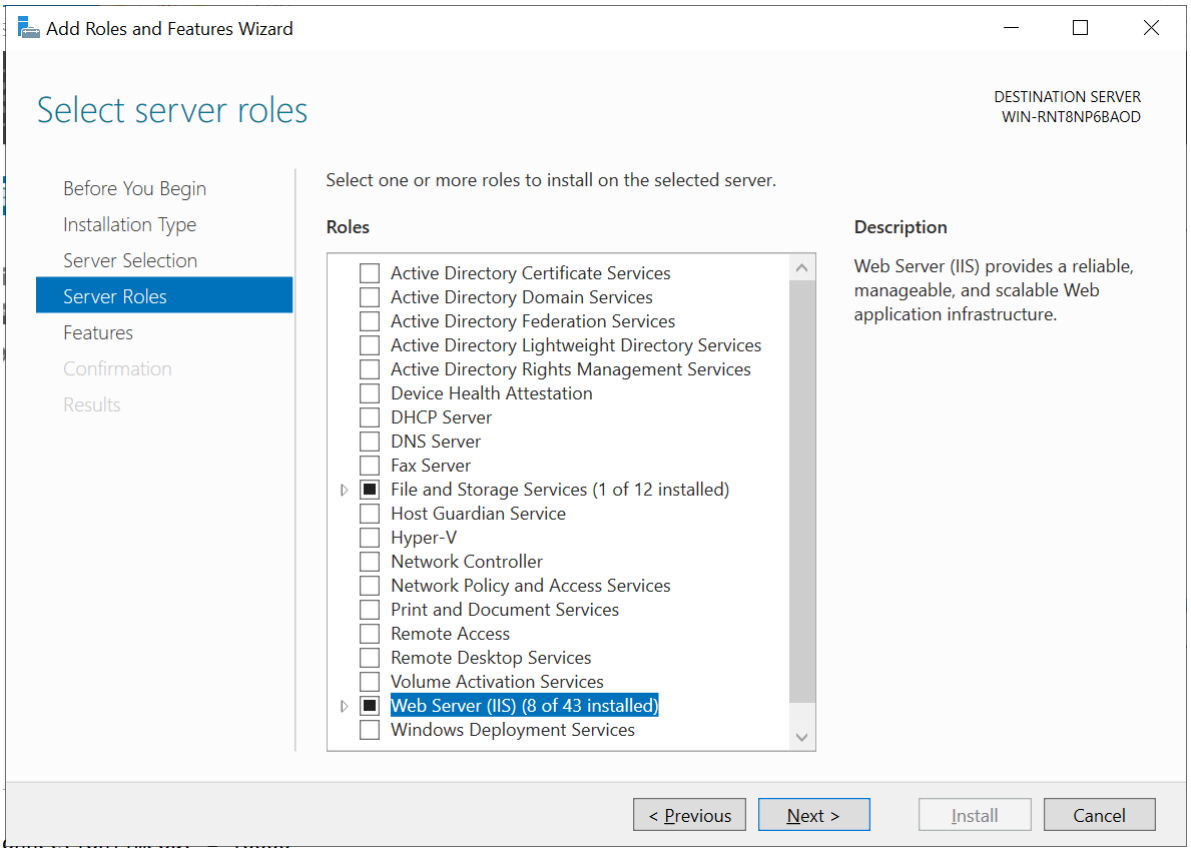

Figure 6 : Select Server Roles

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**
12. Once the installation completes, select **Close**

4.2.2 Setting up the CSP/CNG Provider

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.

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`

1. Open the `cs_cng.cfg` file with an appropriate text editor
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 "Utimaco25"

cs_cng.cfg

Login = UtimacoCryptoUser,HMACPwd=Utimaco25

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

4.2.2.1 Testing Connection

To enumerate providers, use the following command:

```
> cngtool EnumProvider
```

```
C:\Users\Administrator>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
Utimaco CryptoServer Key Storage Provider
Windows Client Key Protection Provider
```

Figure 7 : Providers list

To get the provider information, use the following command:

```
> cngtool ProviderInfo
```

```
C:\Users\Administrator>cngtool ProviderInfo

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

Provider          : Utimaco CryptoServer Key Storage Provider
Device            : 3001@localhost
Group             : IISUser
Mode              : Internal Key Storage

------------------------------------------------------------
Name              : Utimaco CryptoServer Key Storage Provider
Version           : 0x06010100
Impl.-Type        : 0x00000011
MaxNameLength     : 0x00000104
Device            : 3001@localhost
Group             : IISUser
Mode              : Internal Key Storage

C:\Users\Administrator>
```

Figure 8 : Provider Info

5 Integration Steps

5.1 Configuration on Microsoft IIS

5.1.1 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

5.1.1.1 Generate CSR by certreq Command Line Tool

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

```
> 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

request.inf

```
[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:

```
> 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.

5.1.1.2 Generate CSR by GUI Tool

1. Open Run and use `certlm.msc` command

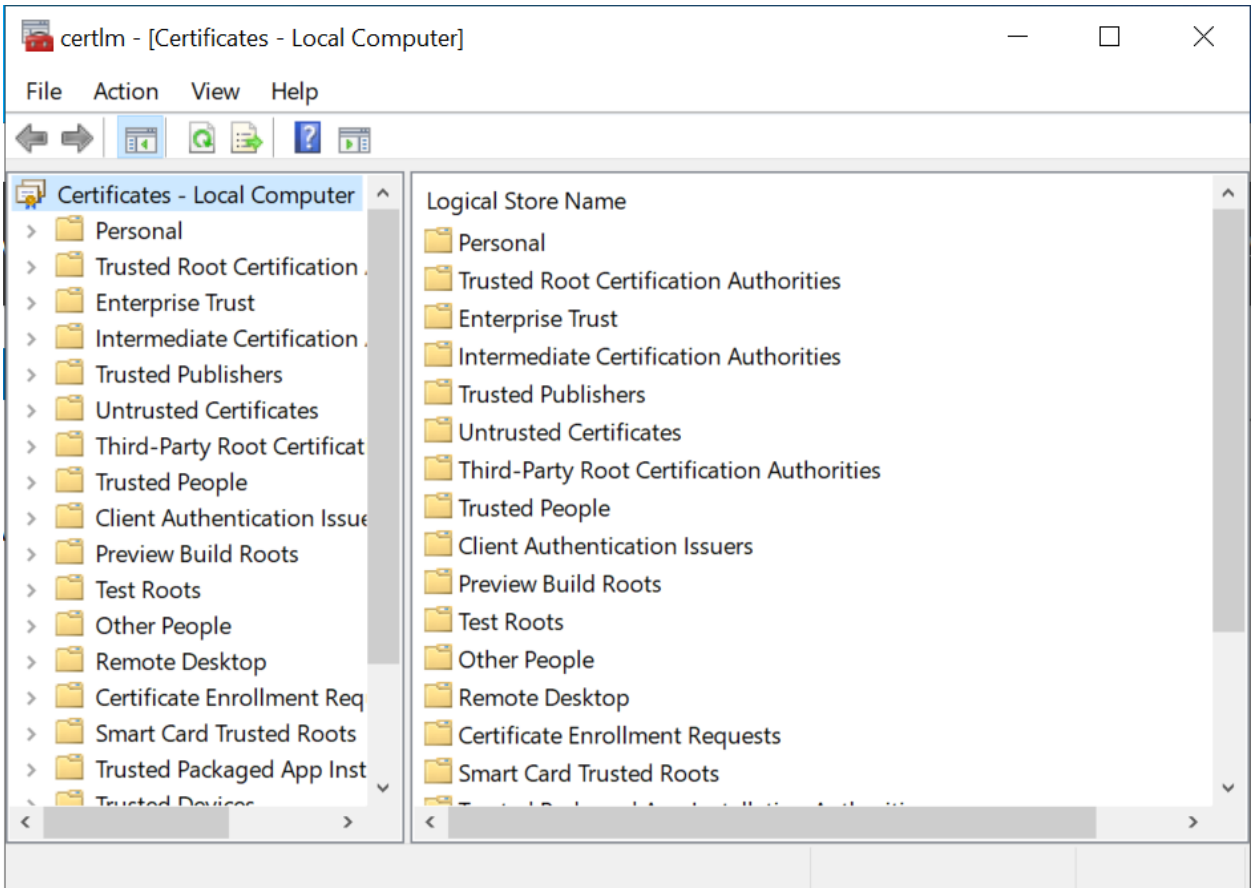

Figure 9 : Local Computer - Certificates

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

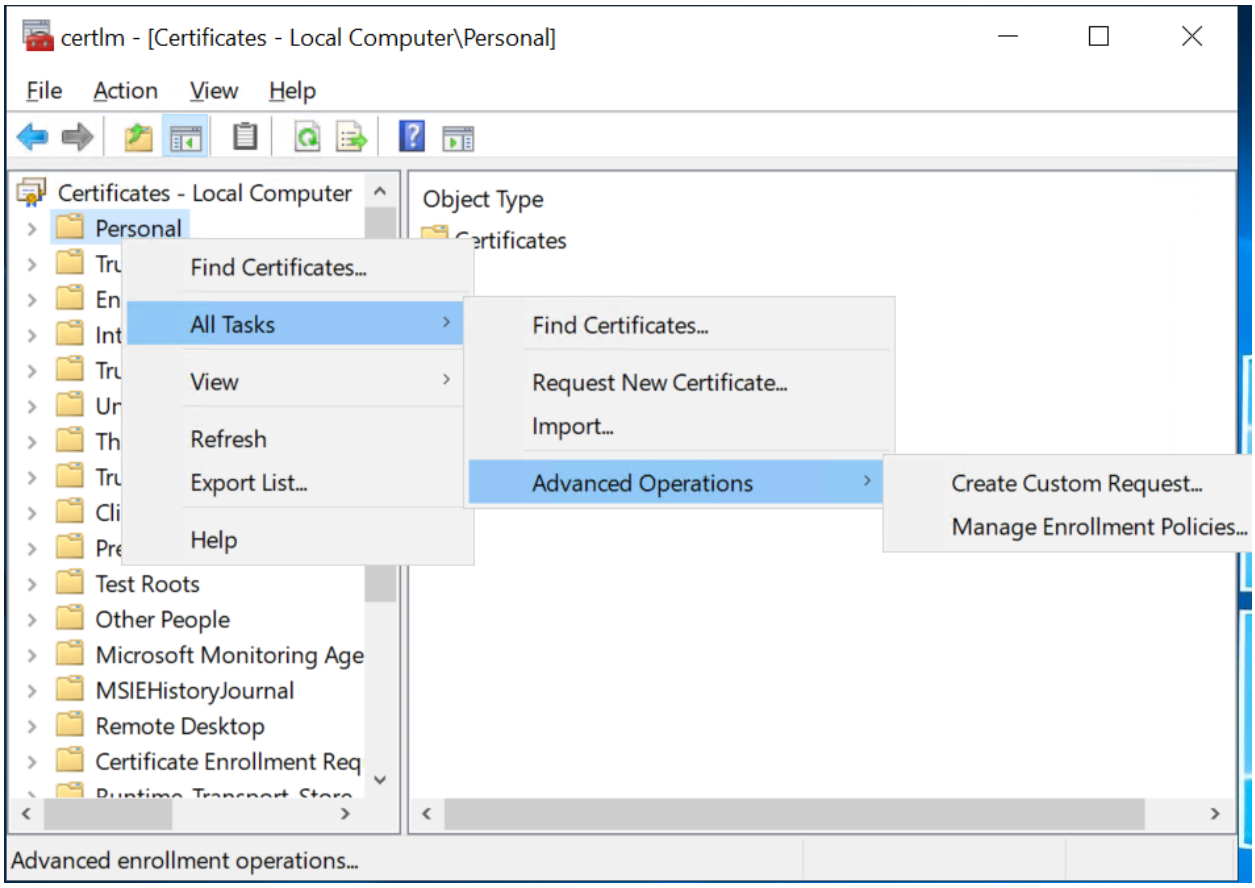

Figure 10 : Create Custom Request

3. Click **Next** button on Before you begin wizard screen
4. Click **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**

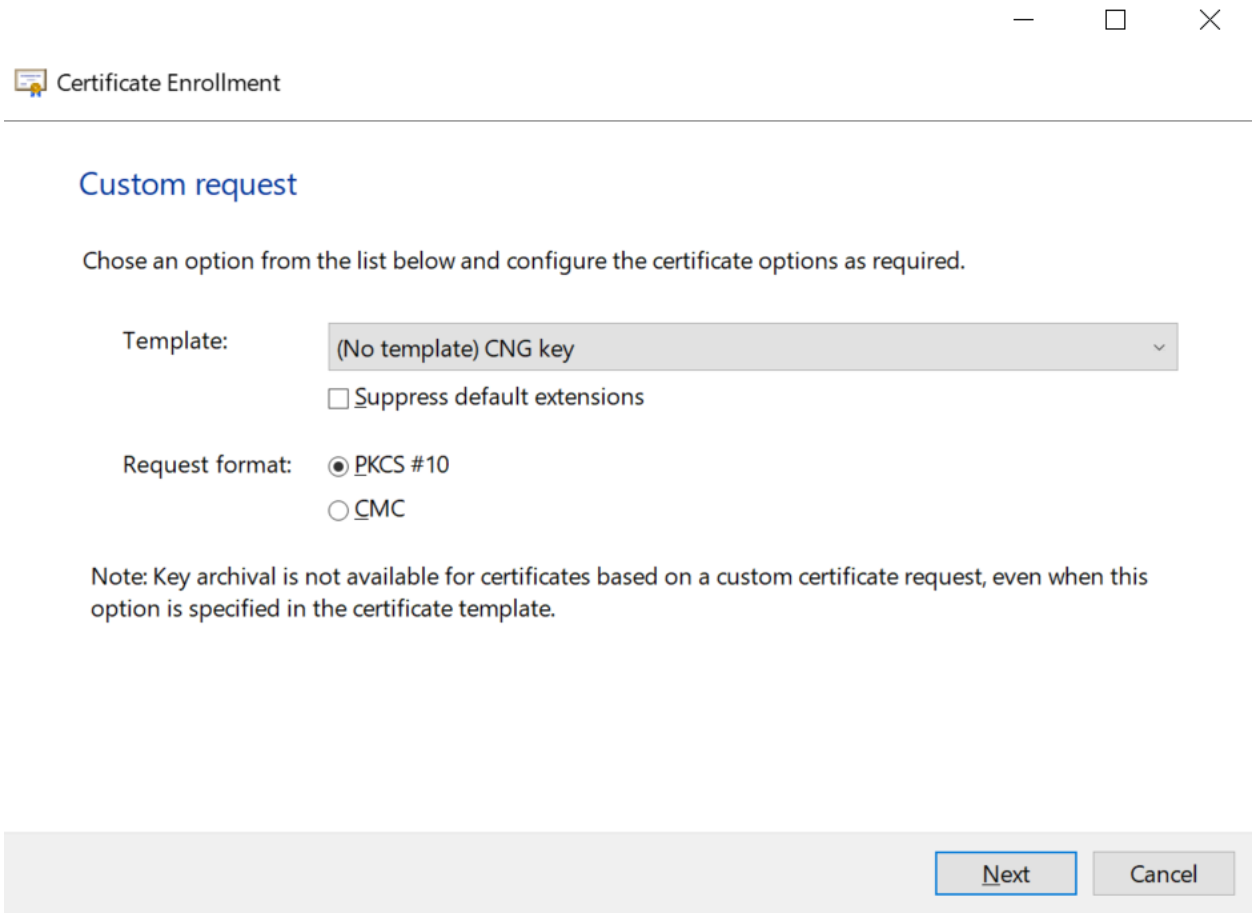

Figure 11 : Certificate Enrollment - Custom request

6. Select **Details** and click on **Properties** button

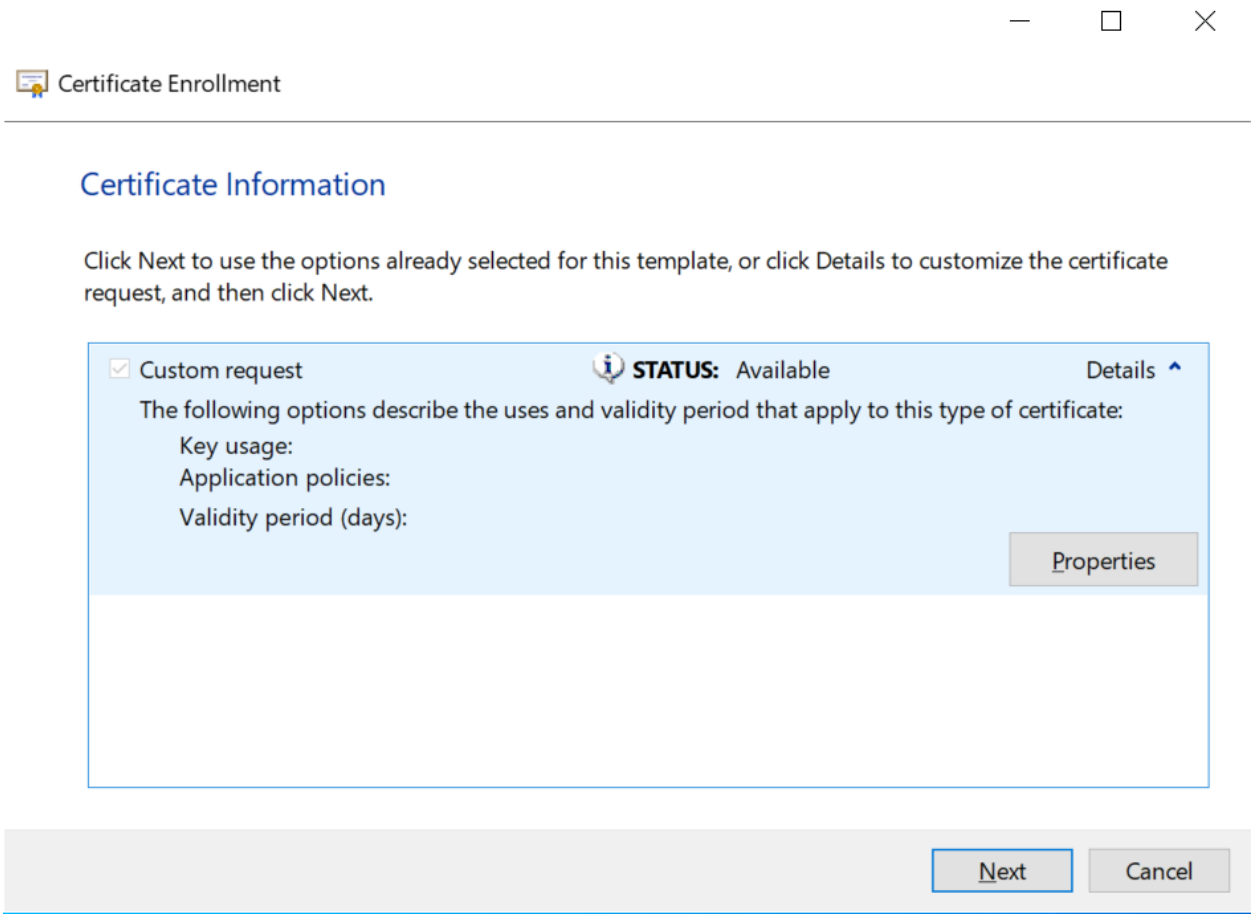

Figure 12 : Certificate Information

7. On Certificate Properties, Assign **Friendly name** and **Description**

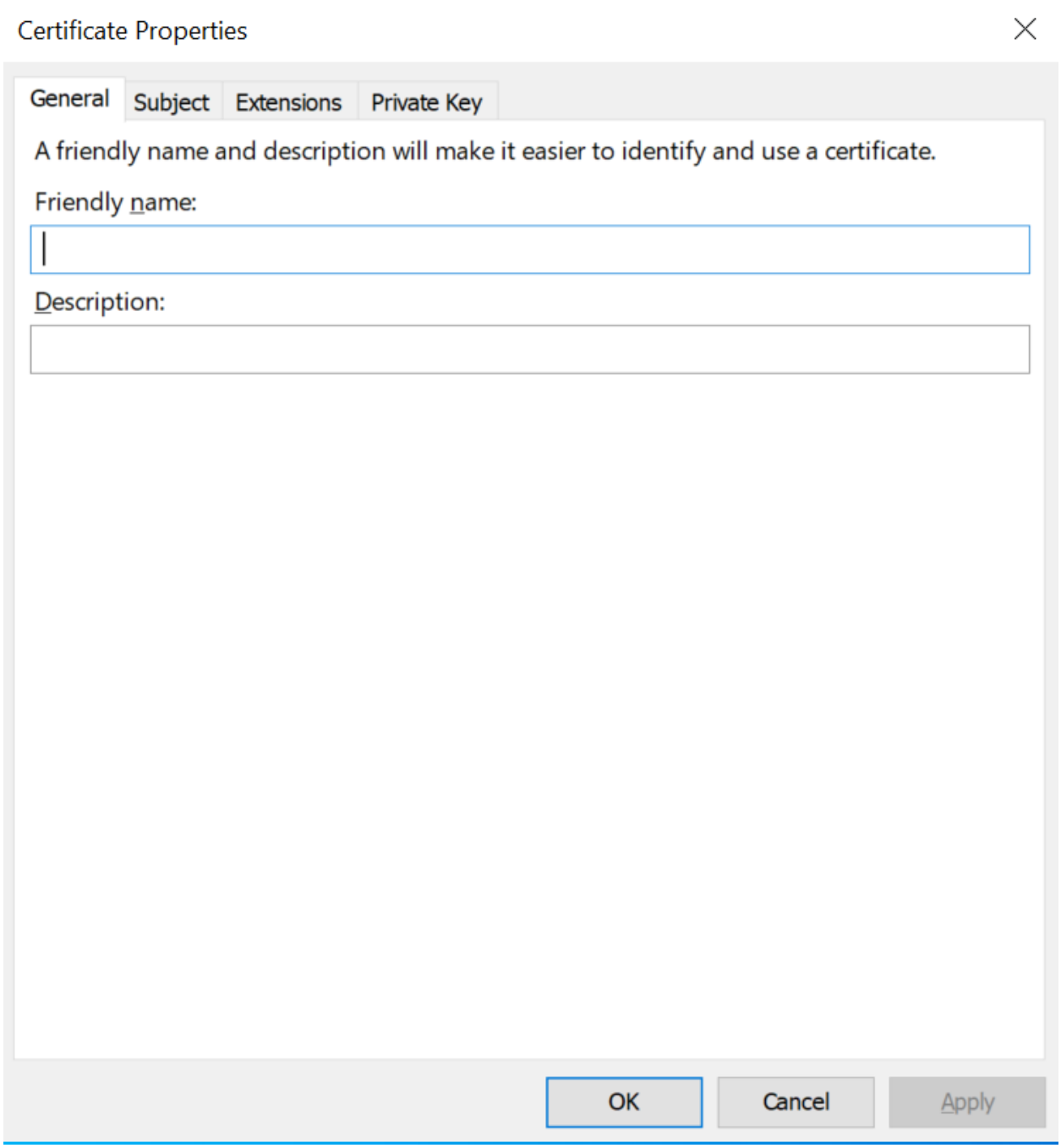

Figure 13 : Certificate Properties - Friendly Name and Description

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.,

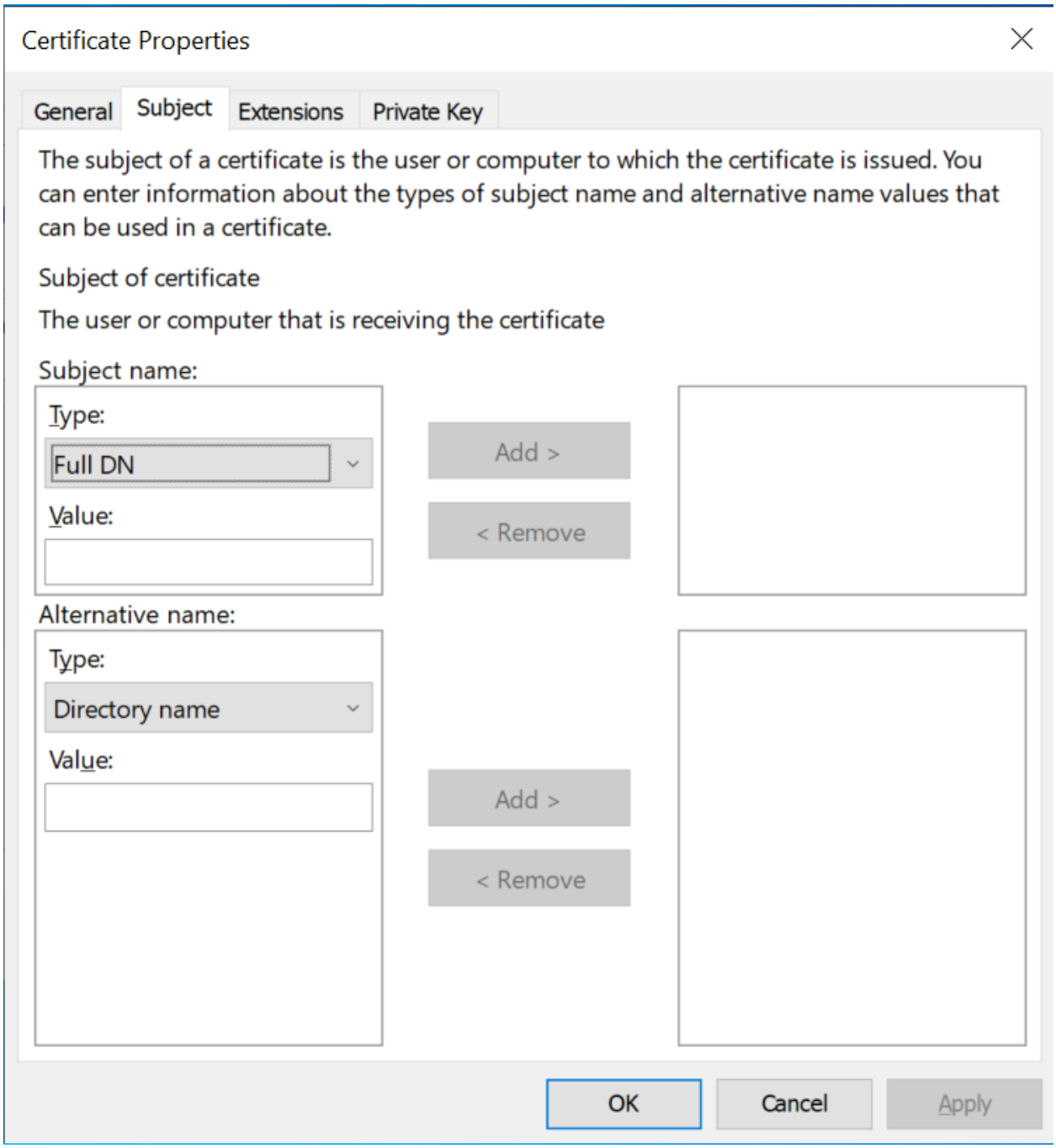

Figure 14 : Certificate Properties – Subject

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**

If RSA, Utimaco CryptoServer is not available by default, enable Show all CSPs checkbox

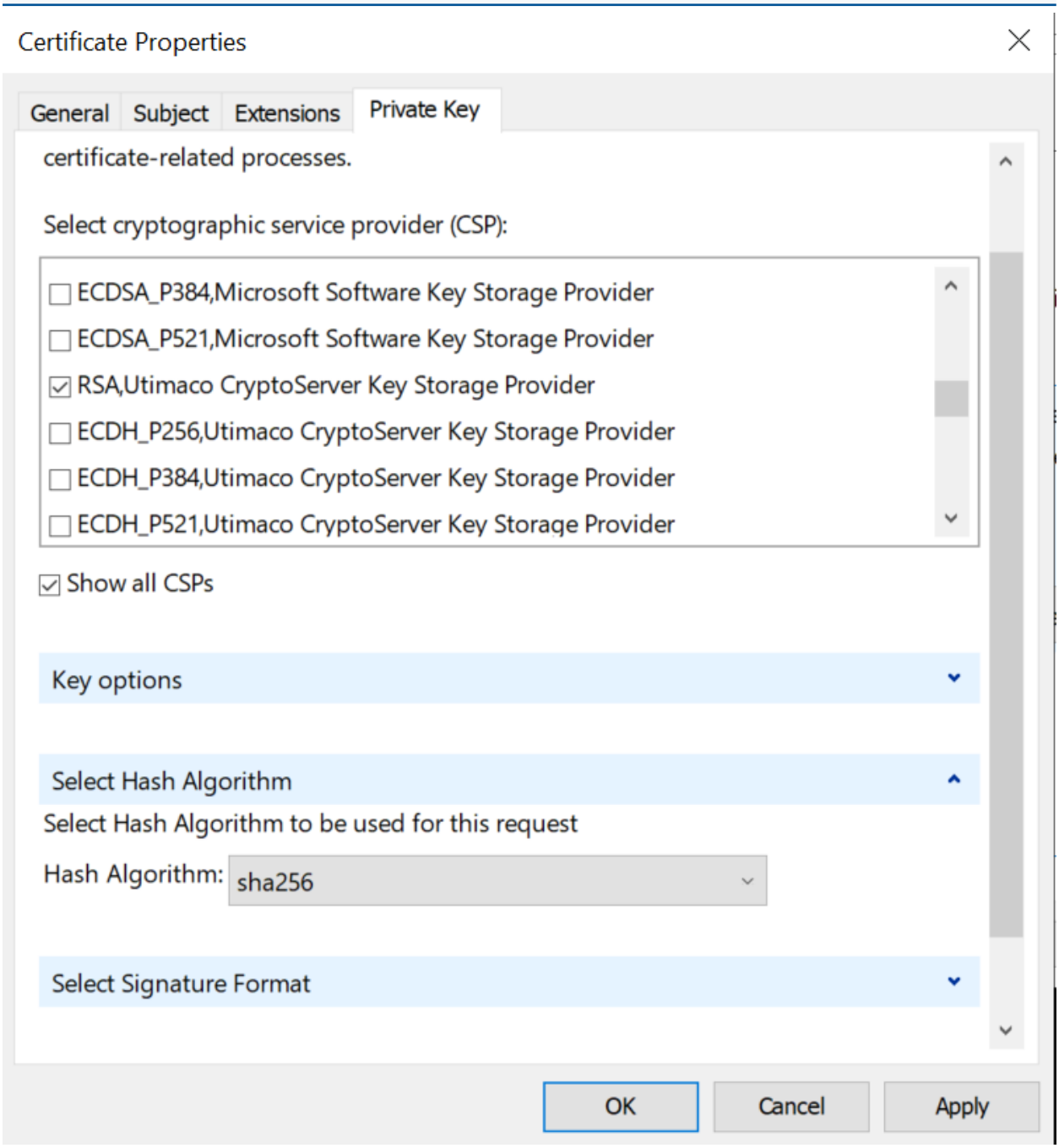

Figure 15 : Certificate Properties - Private Key

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

```
> cngtool ListKeys
```

```
C:\Users\Administrator>cngtool listkeys

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

Provider          : Utimaco CryptoServer Key Storage Provider
Device            : 3001@localhost
Group             : IISUser
Mode              : Internal Key Storage

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

Index  AlgId        Size   Group           Name                                Spec
-------------------------------------------------------------------------------------
1      RSA          2048   IISUser         tq-34f600cd-6ef4-4d53-acf1-edcb842a4f2f 0
```

Figure 16 : Key Listing

5.1.2 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

5.1.3 Install the Certificate

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

```
> 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 IISCertSigned.crt
Installed Certificate:
  Serial Number: 23
  Subject: CN=utimaco.com, OU=IISServer, O=UtimacoCom, L=testing, S=MH, C=IN
  NotBefore: 8/24/2025 1:42 PM
  NotAfter: 6/8/2035 1:42 PM
  Thumbprint: 2e5e76efe748b3f71be427ebf41ca8df80070a59
```

Figure 17 : Certreq command Output Window

5.1.4 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 that the certificate you accepted in the previous step is listed

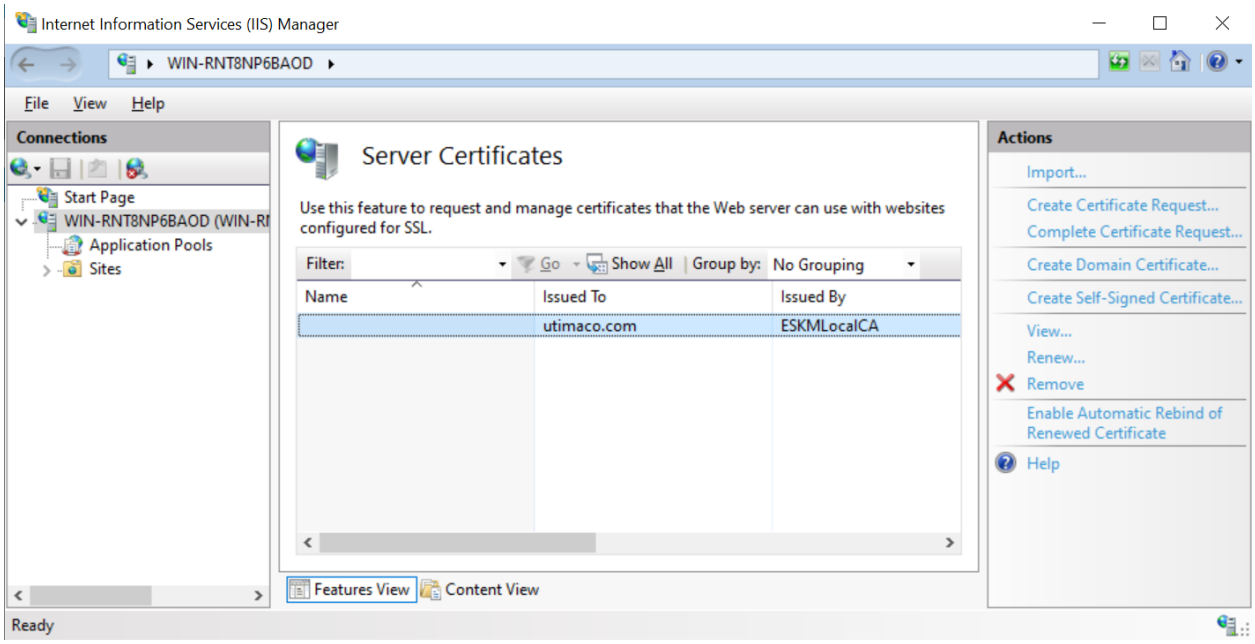

Figure 18 : IIS Manager Dashboard

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

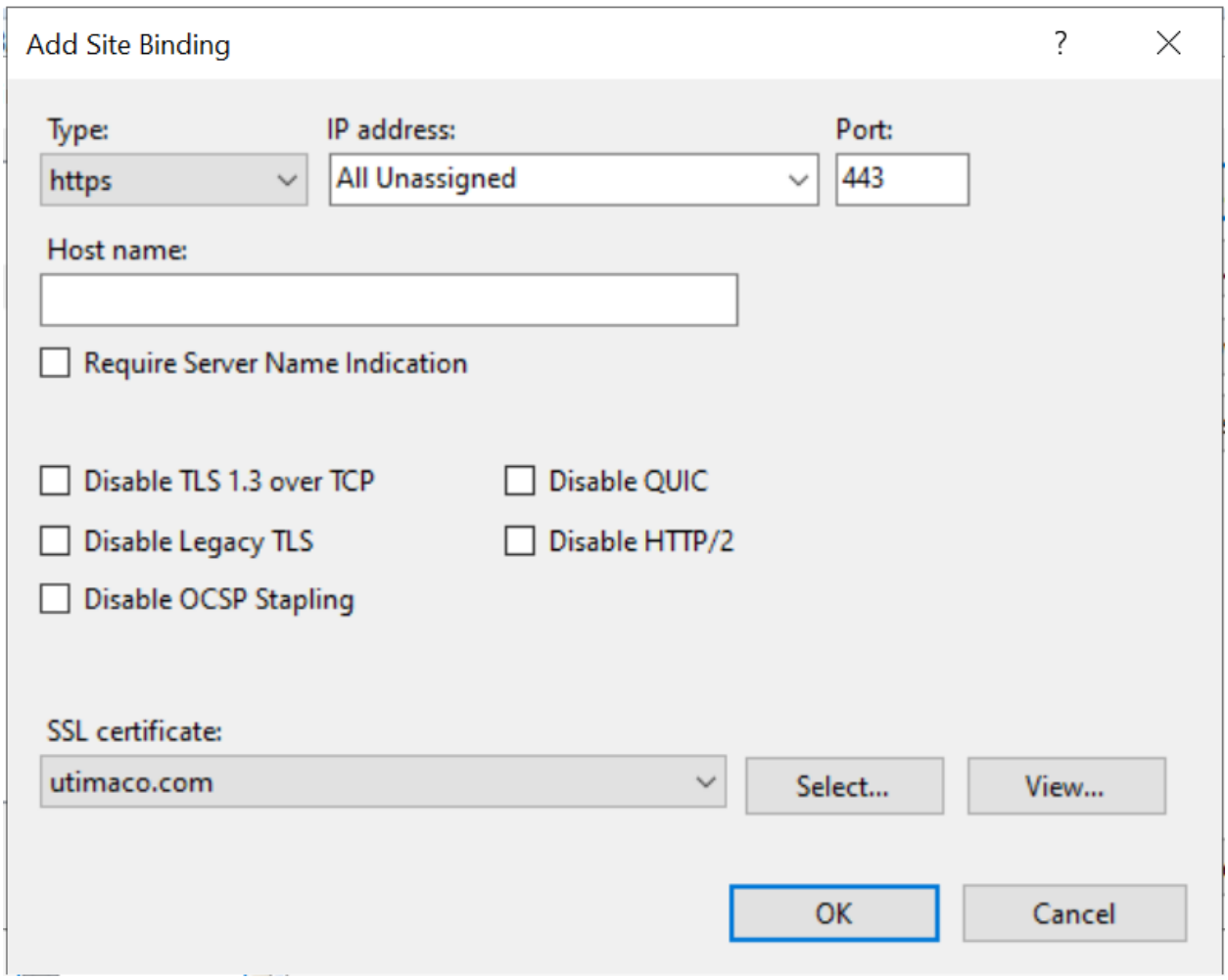

Figure 19 : Site Binding wizard

7. Select **OK** to complete the certificate binding for SSL connection
8. Select **Close** on the Site Bindings screen
9. Restart the IIS server

This completes the integration of Microsoft IIS with Utimaco HSM.

6 Verification and Testing

1. Open *<https://<IIS_Server_IP>>:443* in any of the browser
2. Verify that the page is accessible over https, and verify the certificate used for https is the same that was installed earlier

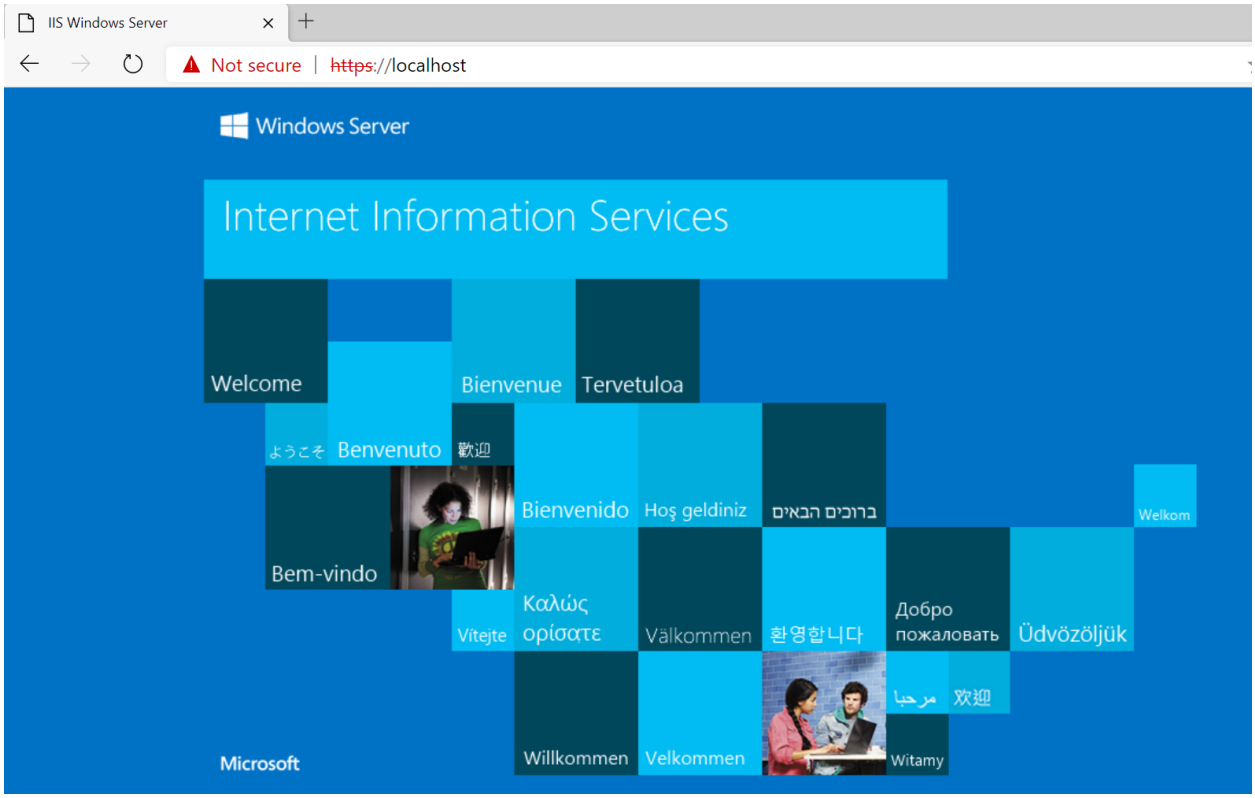

Figure 20 : HTTPS Webpage

7 Troubleshooting

7.1 Common issues and how to resolve them

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 Errors and Diagnosis

7.2 Log locations and interpretation

Understanding log storage locations is critical for effective troubleshooting. Below are the key log file paths relevant to IIS and Utimaco HSM integration on Windows Server.

- Log file name: `cs2cng.log`
- Location: `C:\ProgramData\Utimaco\CNG\log` or as defined in the configuration file `cs_cng.cfg`

8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Germanusstr. 4
52080 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

9 Appendices

9.1 References (links to external docs)

Title	Document Number
utrust_Anchor_LAN_V5_Operating_Manual	2021-0039
utrust_Anchor_PCIe_Operating_Manual	2020-0042
CryptoServerLAN_V5_Operating_Manual	2018-0004
CryptoServerPCIe_CSe-Series_Operating_Manual	M013-0002-en
CryptoServerPCIe_Se-Series_Gen2_Operating_Manual	M015-0001-en

Table 7: References