Microsoft

Active Directory Federation Service (AD FS)

AD FS 4

Integration Guide

CryptoServer HSM

4.45.5.0

utimaco®

Imprint

Copyright 2026	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	2026-06-12
Status	PUBLISHED
Document No.	IG-2026-0052

Table of Contents

1 Introduction 5
1.1 About This Guide 5
1.1.1 Target Audience for This Guide 5
1.1.2 Document Conventions 5
1.1.3 Abbreviations 6
2 Overview 9
2.1 Microsoft AD FS 9
2.2 Utimaco CryptoServer HSM 9
3 Integration Requirements and Prerequisites 10
3.1 Tested Versions 10
3.2 Software Requirements 10
3.3 Hardware Requirements 11
3.4 Prerequisites 11
4 Configuring the Utimaco CSP-CNG Provider 13
4.1 Introduction and Prerequisites 13
4.2 Creating HSM Users 13
4.2.1 Creating a Key Manager User 13
4.2.2 Creating a Crypto User 14
4.3 Setting up the CSP/CNG Provider 16
4.3.1 Testing Connection 18
5 Integrating Microsoft AD FS on Windows 2019 Server 19
5.1 Create Certificate Template for SSL Certificate, Token Signing Certificate and Token Decryption Certificate for AD FS 19
5.2 Issue the Created AD FS Certificate Template 25
5.3 Generate SSL Certificate, Token Signing Certificate and Token Decryption Certificate 27
5.4 Provide Full User Permission for the Private Keys of the Certificates to Generated Certificate 33
5.5 Install AD FS 34
5.6 Create a GMSA Account 40
5.7 Configure AD FS Service 41
5.8 Add Token Certificate from AD FS Manager 49
5.8.1 Add a Token Signing Certificate 49

5.8.2 Set Token Signing Certificate as Primary 51
5.8.3 Add Token Decryption Certificate 52
5.8.4 Set Token Decryption Certificate as Primary 53
5.9 Verify the AD FS Server is Operational and Accessible Through the URL 54
5.9.1 Verify the SSO Operation of AD FS Server 55
6 Troubleshooting 58
7 Further Information 59
8 References 60
9 Contact and Support Information 61

1 Introduction

This guide is a part of the information and support provided by Utimaco. Additional documents 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 on Utimaco's website at https://utimaco.com/.

1.1 About This Guide

This guide provides an integration explaining how to integrate an Utimaco CryptoServer Hardware Security Module (HSM) with Microsoft Active Directory Federation Service (AD FS). Utimaco HSM securely stores and protect the SSL Certificate Keys, Token Signing keys and Token Decryption keys used by AD FS.

1.1.1 Target Audience for This Guide

This guide is intended for administrators of Microsoft AD FS and of Utimaco HSMs.

1.1.2 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 1: 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.

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
AD	Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Service
CD	Compact Disc
CNG	Cryptography API Next Generation
CSADM	CryptoServer Command-line Administration Tool

Abbreviation	Meaning
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
GUI	Graphical User Interface
HSM	Hardware Security Module
IIS	Internet Information Services
IP	Internet Protocol
LAN	Local Area Network
MMC	Microsoft Management Console
OS	Operating System
PKI	Public Key Infrastructure
PCIe	PCI Express Interface
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer
SSO	Single Sign On
UPN	User Principal Name

Abbreviation	Meaning
URL	Uniform Resource Locator
VM	Virtual Machine
XML	Extensible Markup Language

Table 2: List of abbreviations

2 Overview

2.1 Microsoft AD FS

Active Directory Federation Service (AD FS) enables Federated Identity and Access Management by securely sharing digital identity and entitlements rights across security and enterprise boundaries. AD FS extends the ability to use single sign-on functionality that is available within a single security or enterprise boundary to Internet-facing applications to enable customers, partners, and suppliers a streamlined user experience while accessing the web-based applications of an organization.

Federation servers in AD FS require Token signing certificate and Token decryption certificate. Token signing certificates are standard X509 certificates that are used to securely sign all tokens that the federation server issues. Token decryption certificates are standard X509 certificates that are used to decrypt any incoming tokens. The private keys of these certificates are stored on Utimaco HSM.

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.

3 Integration Requirements and Prerequisites

Ensure 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 AD FS.

Operating System	Service	Utimaco Security Server Version	Utimaco HSM
Windows Server 2019	Microsoft AD FS	SecurityServer 4.45.5	CryptoServer CSe-Series/Se-Series

Table 3: List of tested versions

3.2 Software Requirements

Software	Software Requirements
AD FS	AD FS 4
JAVA	1.8.0_351
HSM Interface	CryptoServer CSP/CNG Provider

Table 4: List of software requirements

3.3 Hardware 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 5: List of hardware requirements

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

3.4 Prerequisites

Before you begin, please ensure that:

- The CryptoServer is set up and configured. Refer to the CryptoServer documentation to set up the HSM.
- The MBK is created and stored onto each HSM. Refer to the CryptoServer documentation to set up the MBK.
- The CryptoServer Default Admin has been replaced with a new admin user.
- The operating system used is listed in Tested Versions.
- The SecurityServer used is listed in Tested Version.
- For demonstration purpose following machines have been used:
    - One system with AD DS and AD CS role installed on it. It will be used as a domain controller and certificate authority. You can also use your existing domain controller and certificate authority.
    - Second system joined in domain for AD FS server.
- Java version 8 or above has been installed on the AD FS server.
- An admin user is set up, as it is required for installing software.

- The CSP/CNG library is set up and configured on the AD FS server as per the environment. Refer the CryptoServer documentation to set up and configure the library for the CryptoServer.
- Port 443 is allowed through the Firewall.
- You familiarize yourself with the AD FS documents and setup process.

4 Configuring the Utimaco CSP-CNG Provider

4.1 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 a second-generation cryptographic interface, developed by Microsoft. It offers updated cryptographic algorithms and is intended as 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, and 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.

4.2 Creating HSM Users

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

4.2.1 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 the "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.

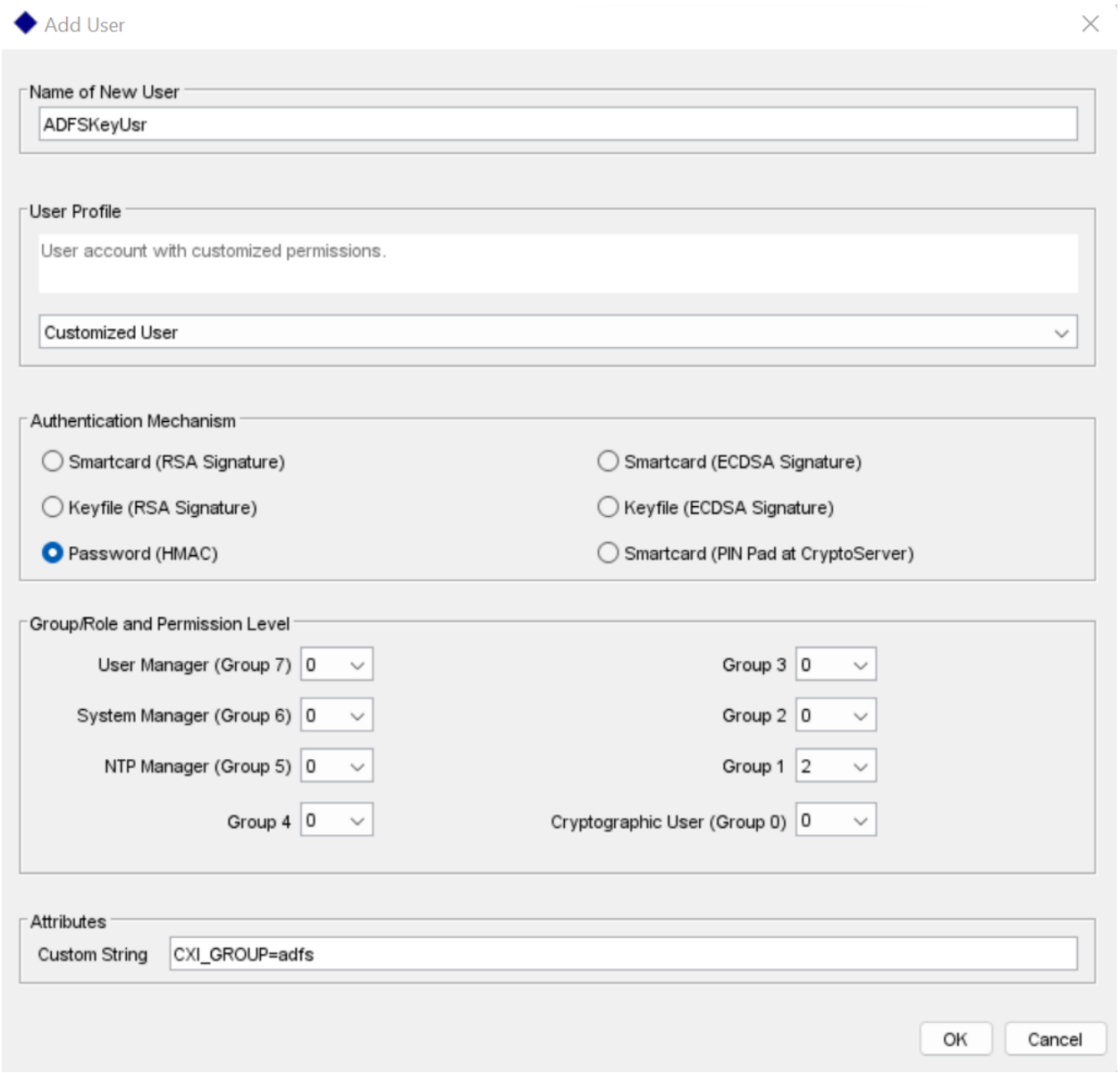

Figure 1 : Creating a Key Manager user

4.2.2 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** "**adfs**" and **HMAC** password will be created.

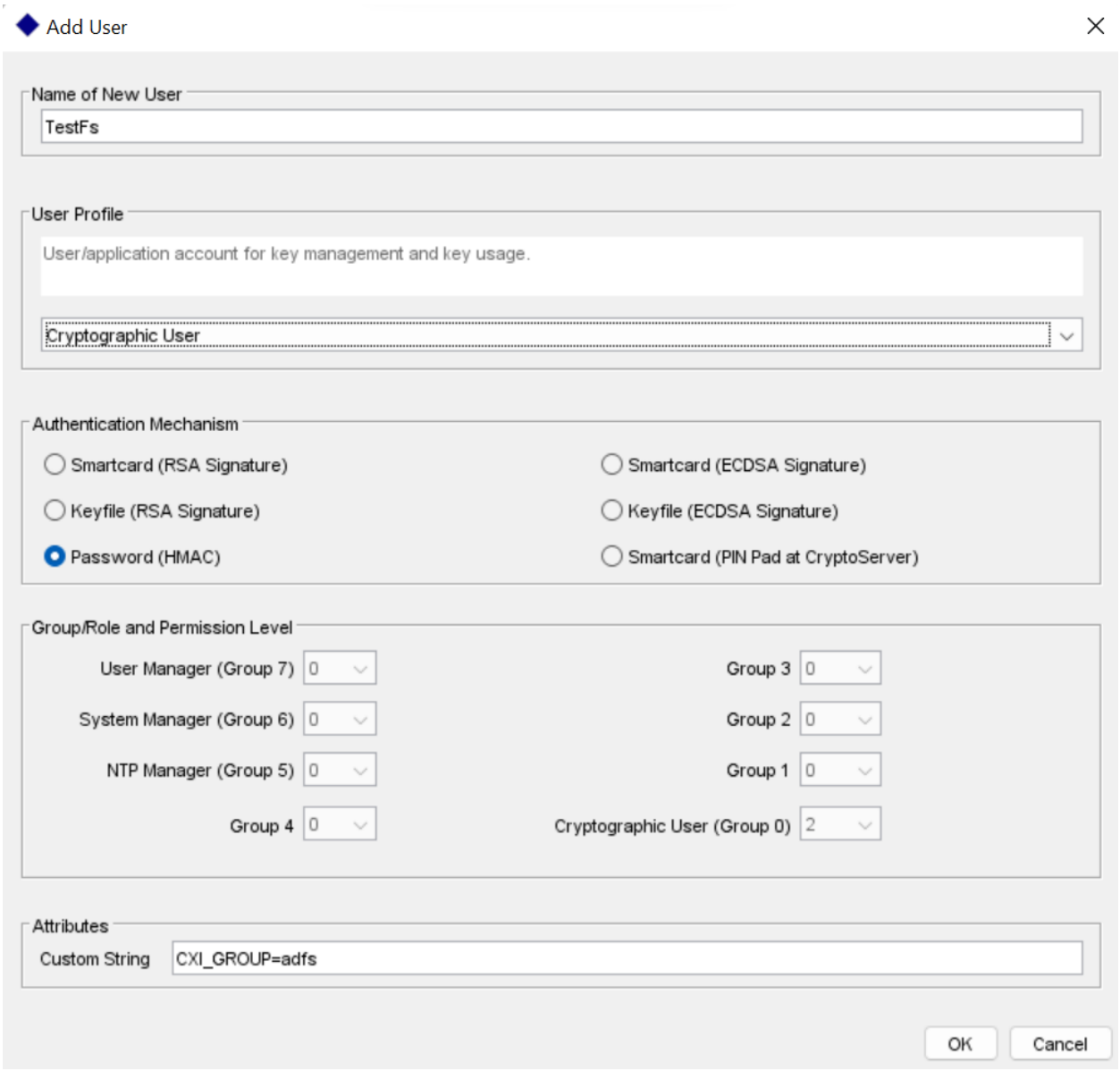

Figure 2 : Creating a Crypto User

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

4.3 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
```

3. Set the Login. In this case, the name of the Cryptographic User is **TestFs** with an HMAC password **123456**.

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.

›_ cs_cng.cfg

```
Login = TestFs,HMACPwd=123456
```

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 to the 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 = adfs

# 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

4.3.1 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 : adfs

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 : adfs

Mode : Internal Key Storage
```

5 Integrating Microsoft AD FS on Windows 2019 Server

5.1 Create Certificate Template for SSL Certificate, Token Signing Certificate and Token Decryption Certificate for AD FS

You need to create a certificate template that will be used for the SSL, Token Signing, and Token Decryption certificates.

1. Log in to the Certificate Authority server as a domain administrator.
2. Select **Start**, click on **Run** then type MMC and click on **OK**.
3. MMC Console window populates, select **File** and select **Add/Remove Snap-in…** .
4. From the Add or Remove Snap-Ins dialog box, find and select the **Certificates and Certificate Authority snap-in** under the **Available snap-ins** section.
5. Click **Add**, select **Computer Account**, and click **Next**.
6. Select **Local Computer** and click on **Finish**.

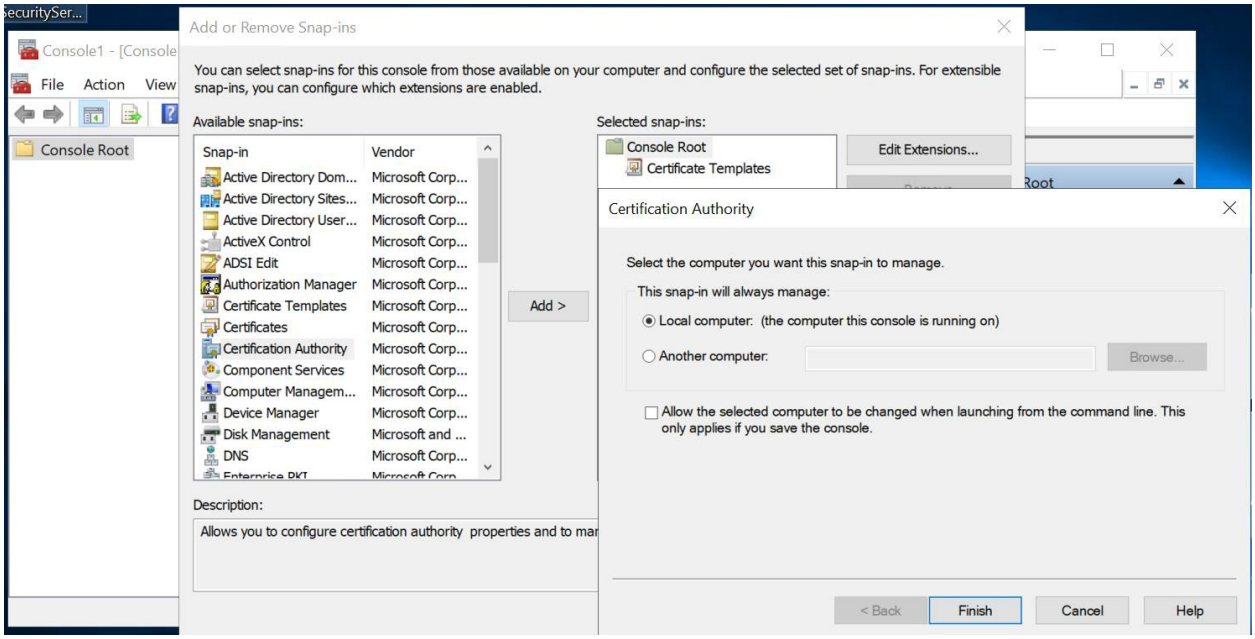

Figure 3 : Certificate authority selection wizard

7. Open **Certificate Template** and duplicate the **Web Server** template and name it as ADFSCertificateTemplate from **General** tab.

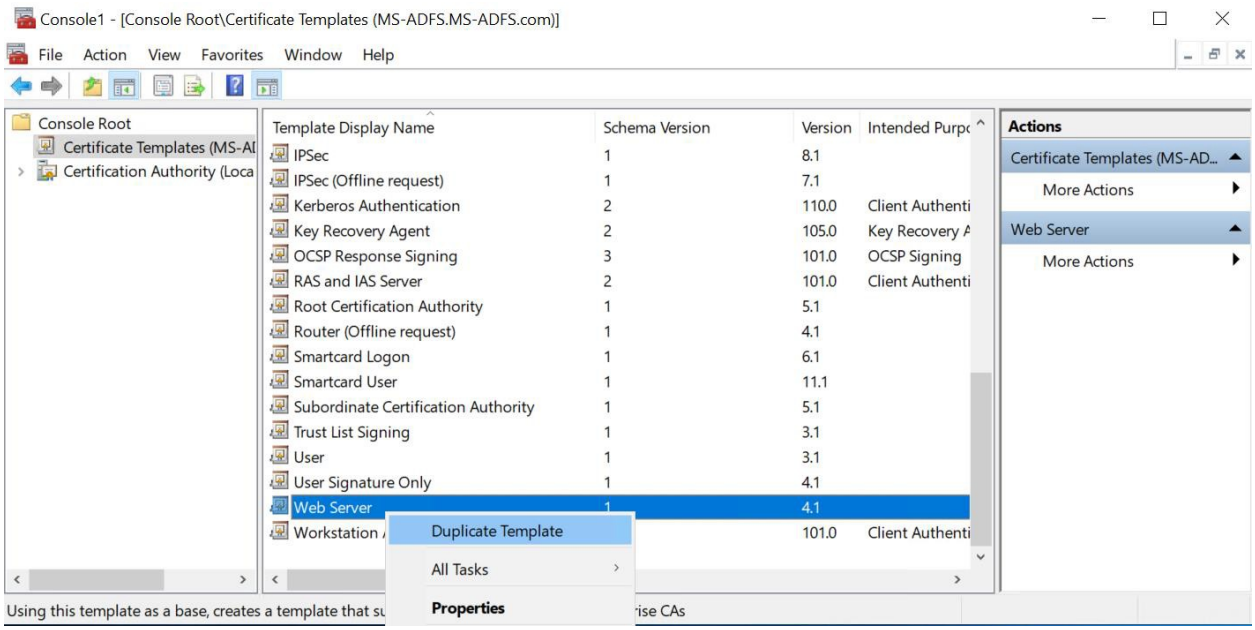

Figure 4 : Certificate template wizard

8. Go to the **Compatibility** tab and select the appropriate Windows Server. For example, the Windows 2016 server as below.

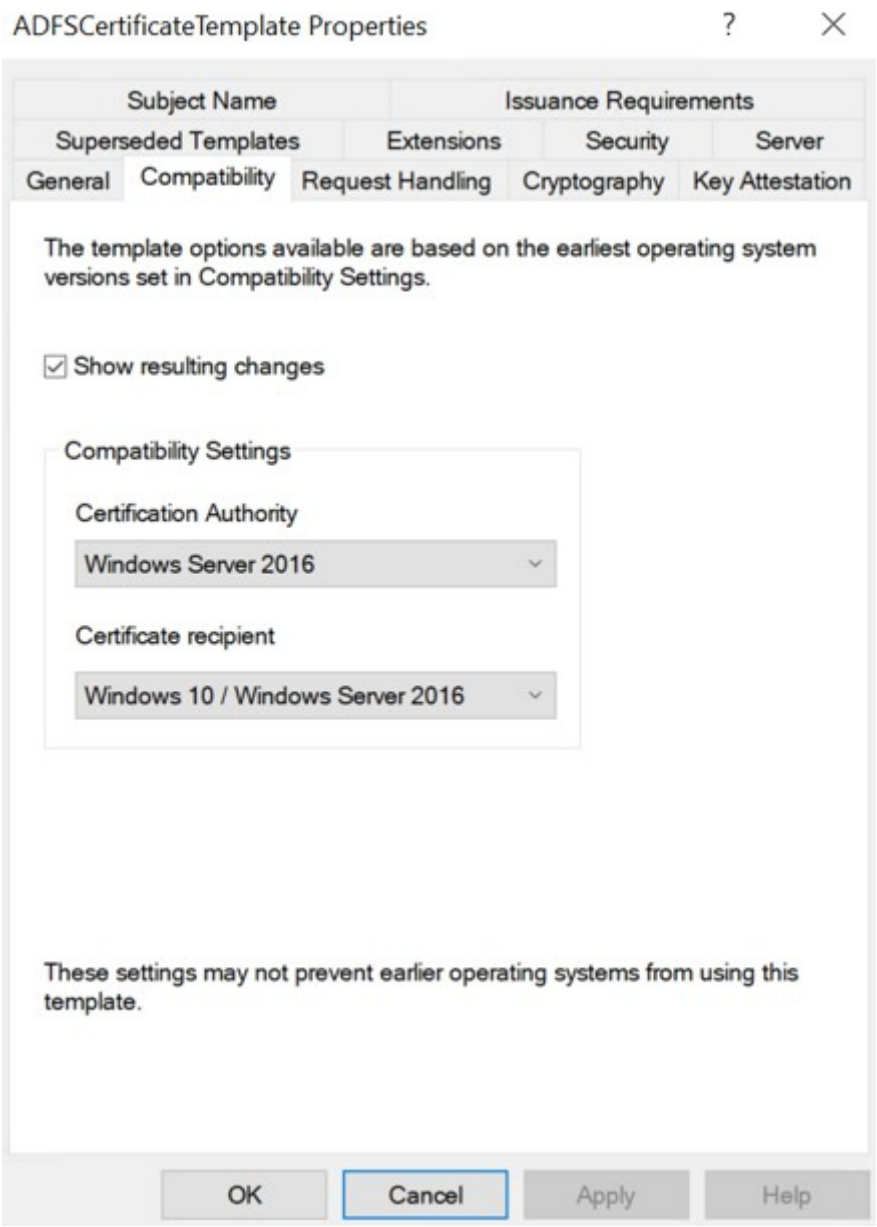

Figure 5 : AD FS certificate template properties wizard

9. Go to the **Cryptographic** tab and select the **Provider Category**, **Algorithm name** and **Minimum key size**. Select **Requests must use one of the following providers** option and check **Utimaco Cryptoserver Key Storage Provider**, as below.

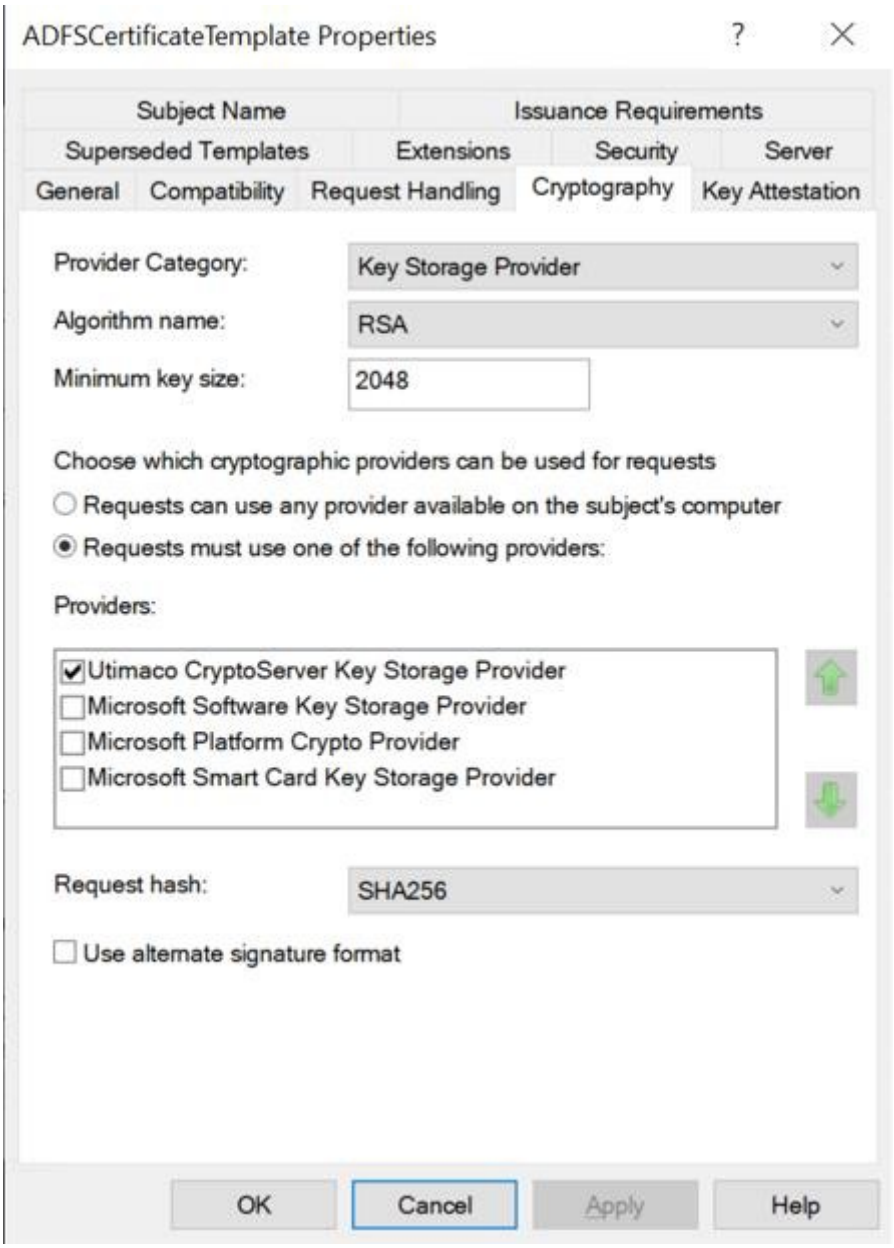

Figure 6 : AD FS certificate template properties wizard

If you are using an existing CA, make sure to install the SecurityServer software on it. This will add Utimaco Cryptoserver Key Storage Provider to the providers list, as shown above.

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

10. Go to the **Subject Name** tab and make sure to uncheck **E-mail name** option, and check the **User principal name (UPN)** option.

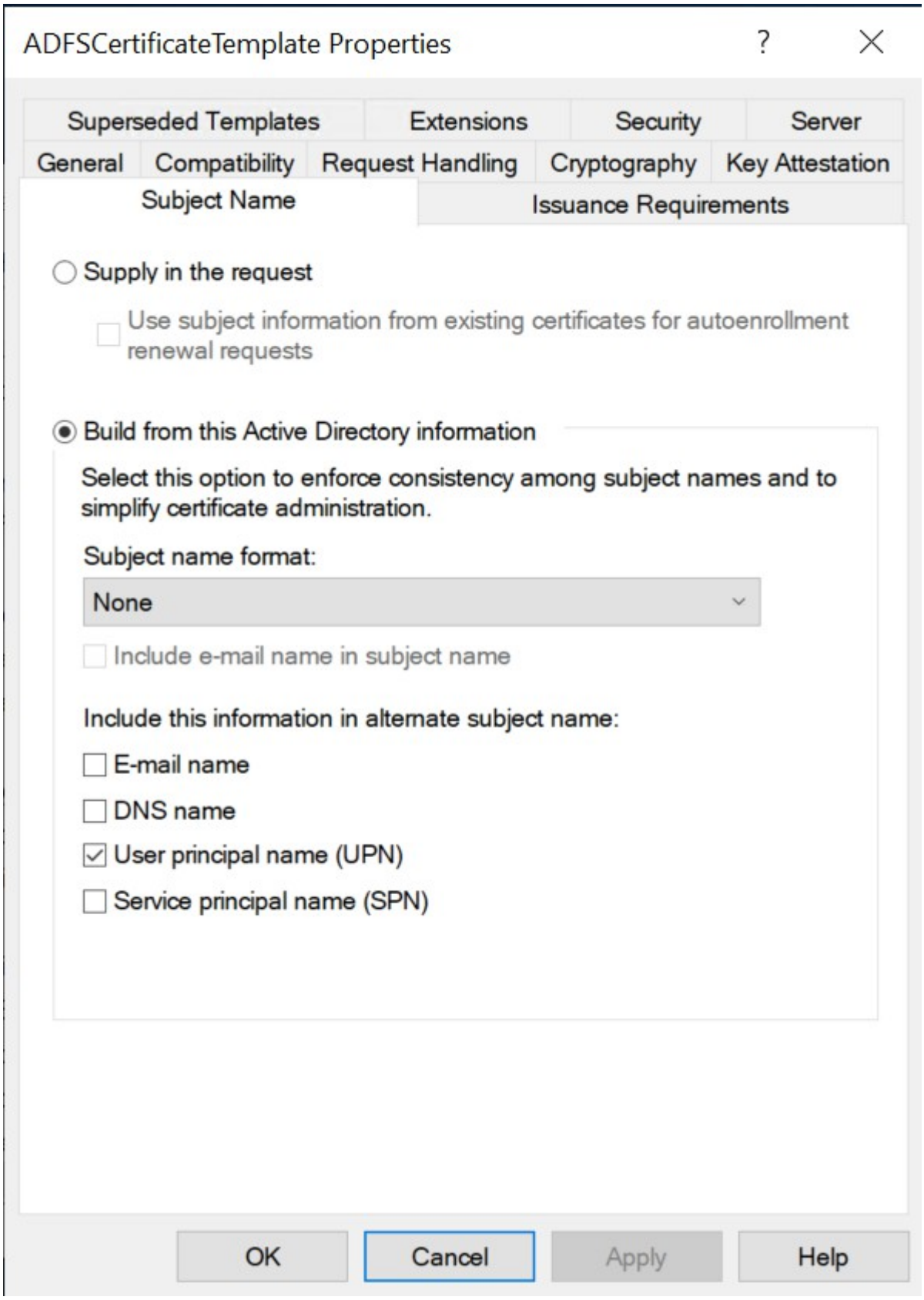

Figure 7 : AD FS properties wizard

11. Go to the **Security** tab and add domain computer, NETWORK SERVICE and IIS_IUSRS in **Groups** and username, provide the read, enroll permissions. Then click on **Apply** and **OK**.

You can see the ADFSCertificateTemplate has been created under the certificate template.

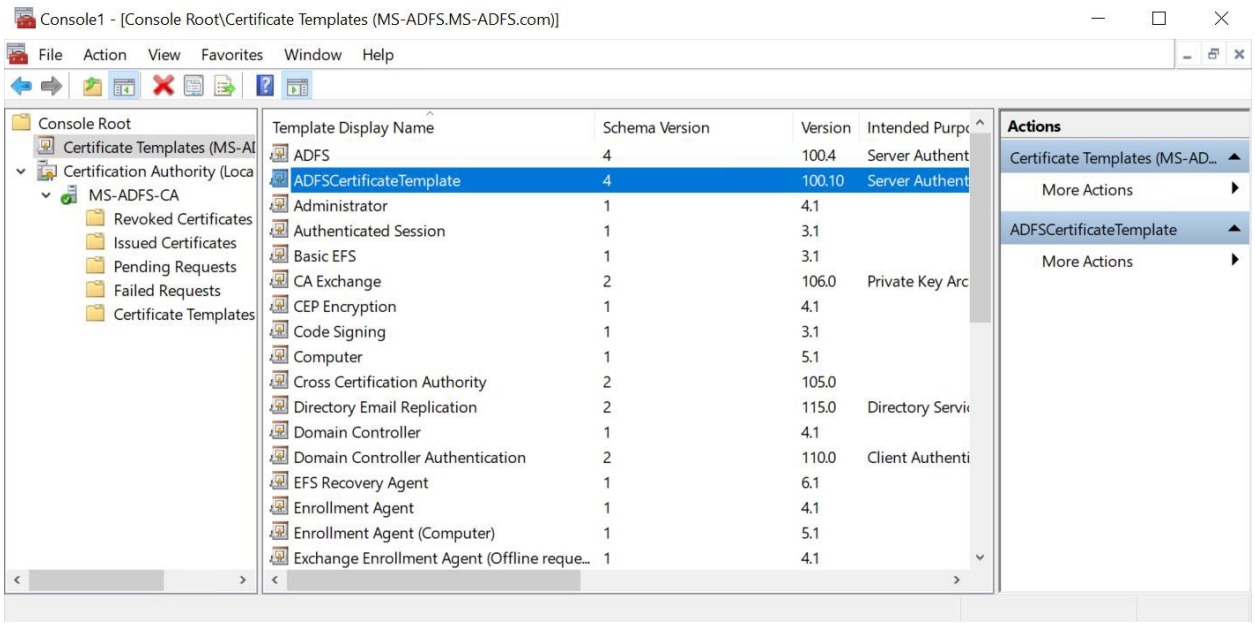

Figure 8 : MMC console

5.2 Issue the Created AD FS Certificate Template

1. For issuing the certificate template on certificate authority, open the **Certificate Authority** option added from the mmc console or go to **Run** and type “certlm.msc”.
2. **Certificate Authority** window gets populated, then expand it.
3. Right-click on the **Certificate Template** option and select **New**. Then select **Certificate Template to Issue**.

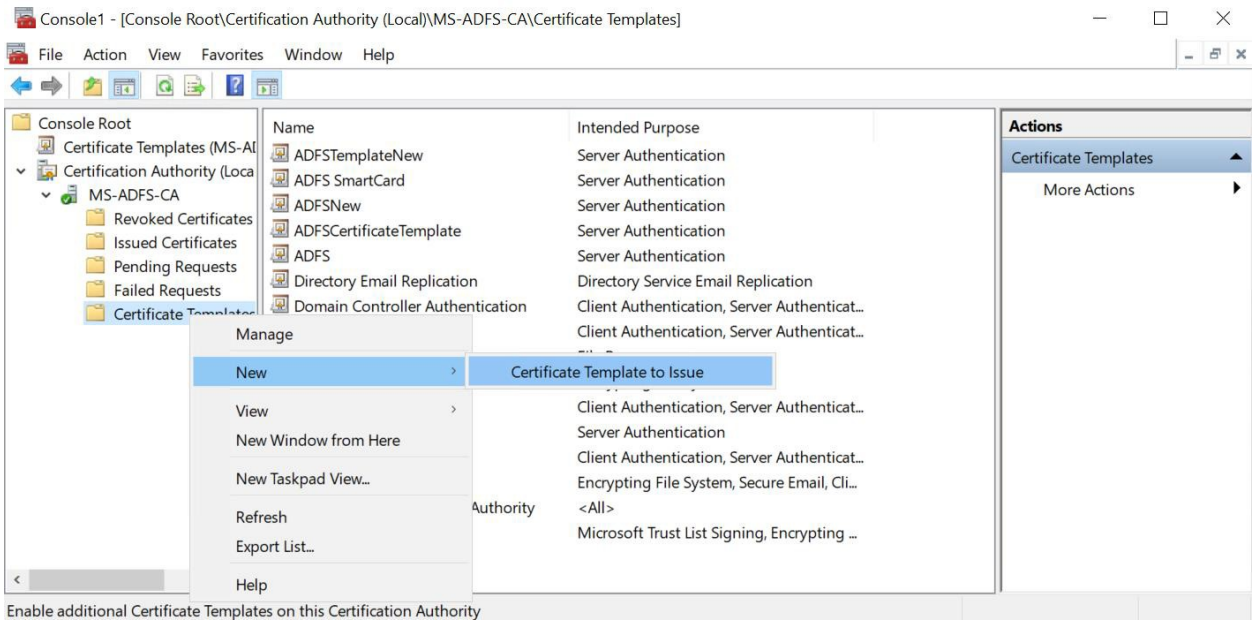

Figure 9 : Certificate authority wizard

4. **Enable Certificate Templates** window gets populated, where you need to select **ADFSCertificateTemplate** and click on the **OK** button.

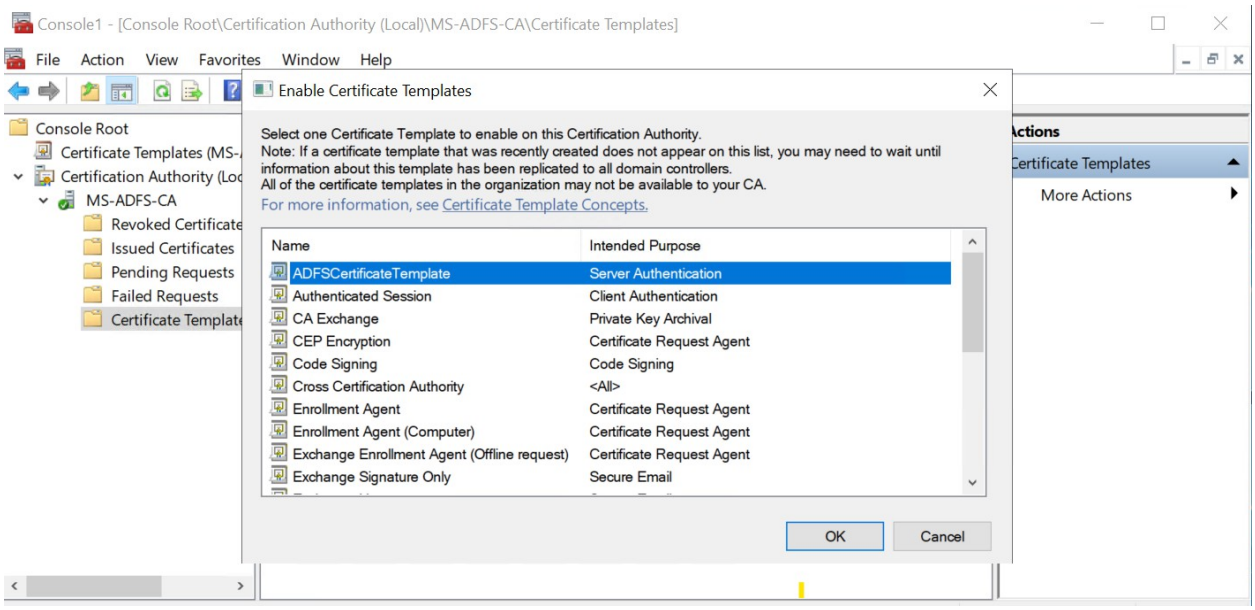

Figure 10 : Enable certificate template wizard

5. After clicking on the **OK** button, the **Issued Certificate** option it will show and ADFSCertificateTemplate has been issued.

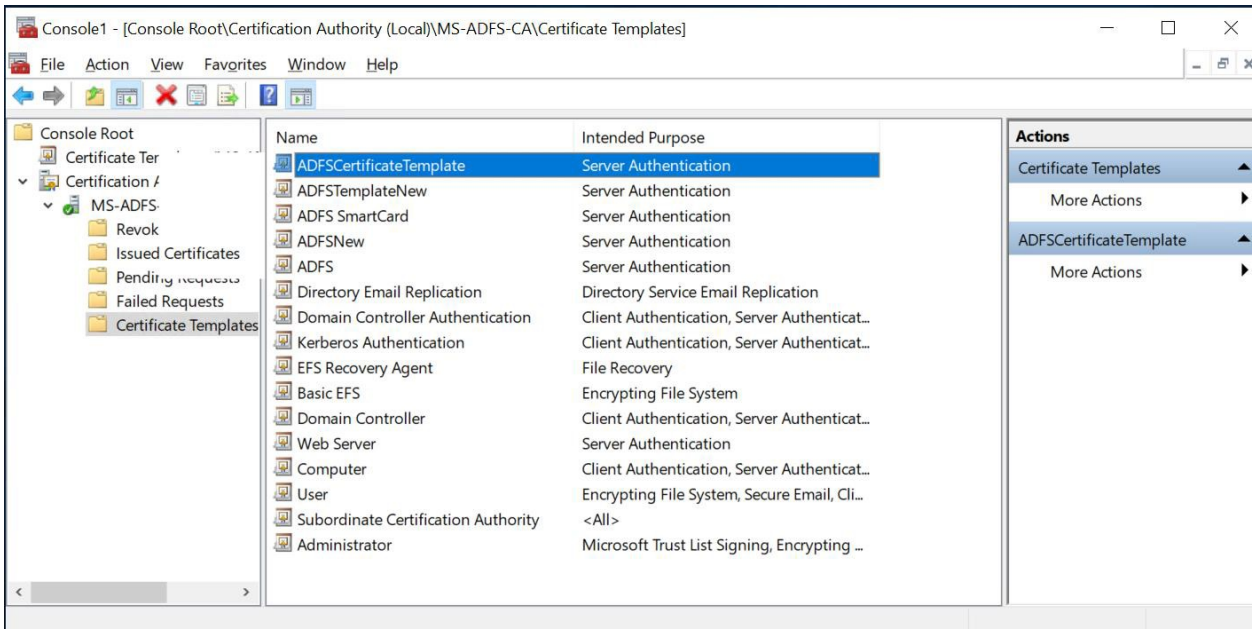

Figure 11 : Certificate template wizard

5.3 Generate SSL Certificate, Token Signing Certificate and Token Decryption Certificate

1. Add the AD FS server to domain if not added.
2. Log in to the AD FS server as a domain administrator.
3. Open **Start** and **Run**, then type “certlm.msc”. This will open the certificate for the **Local Computer**.
4. Go to **Personal** and right-click on **All Tasks**. Then, select **Request New Certificate**.

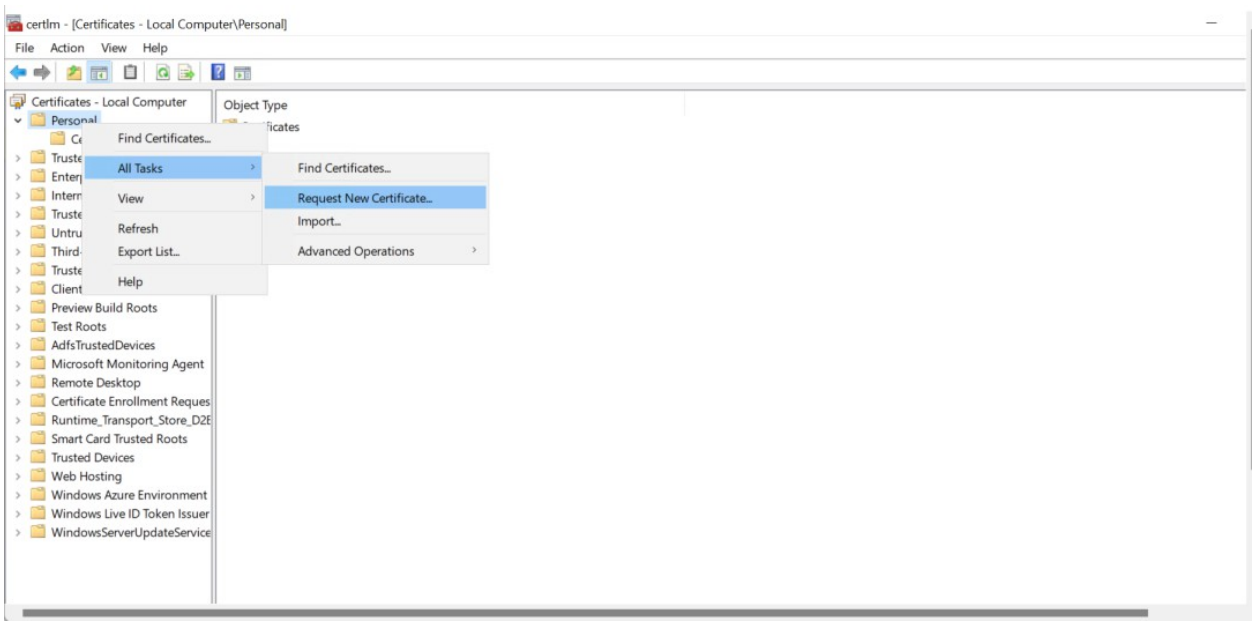

Figure 12 : Certificate console

5. Click **Next**, **Select Active Directory Enrollment Policy**, then click on the down arrow button. The certificate template that you have configured, the ADFSCertificateTemplate, will be displayed.

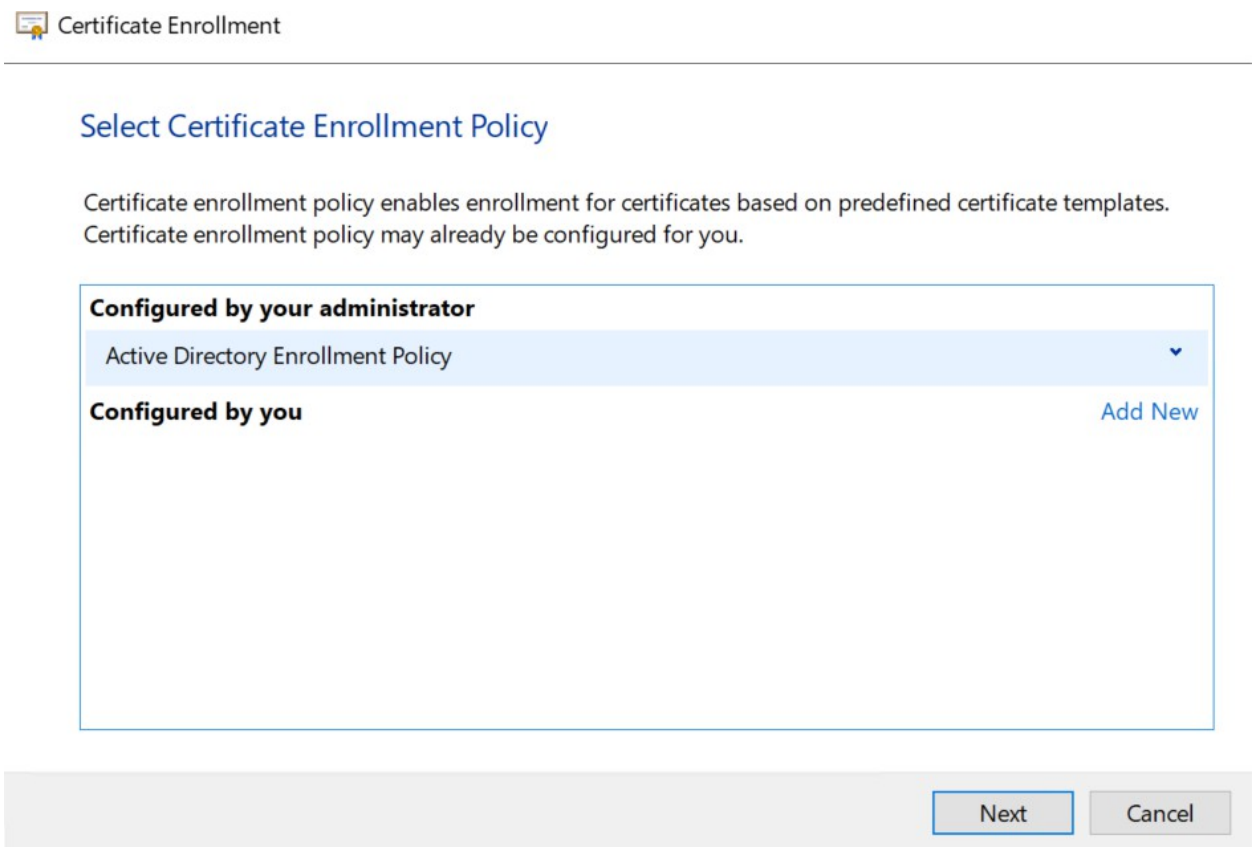

Figure 13 : Certificate enrollment

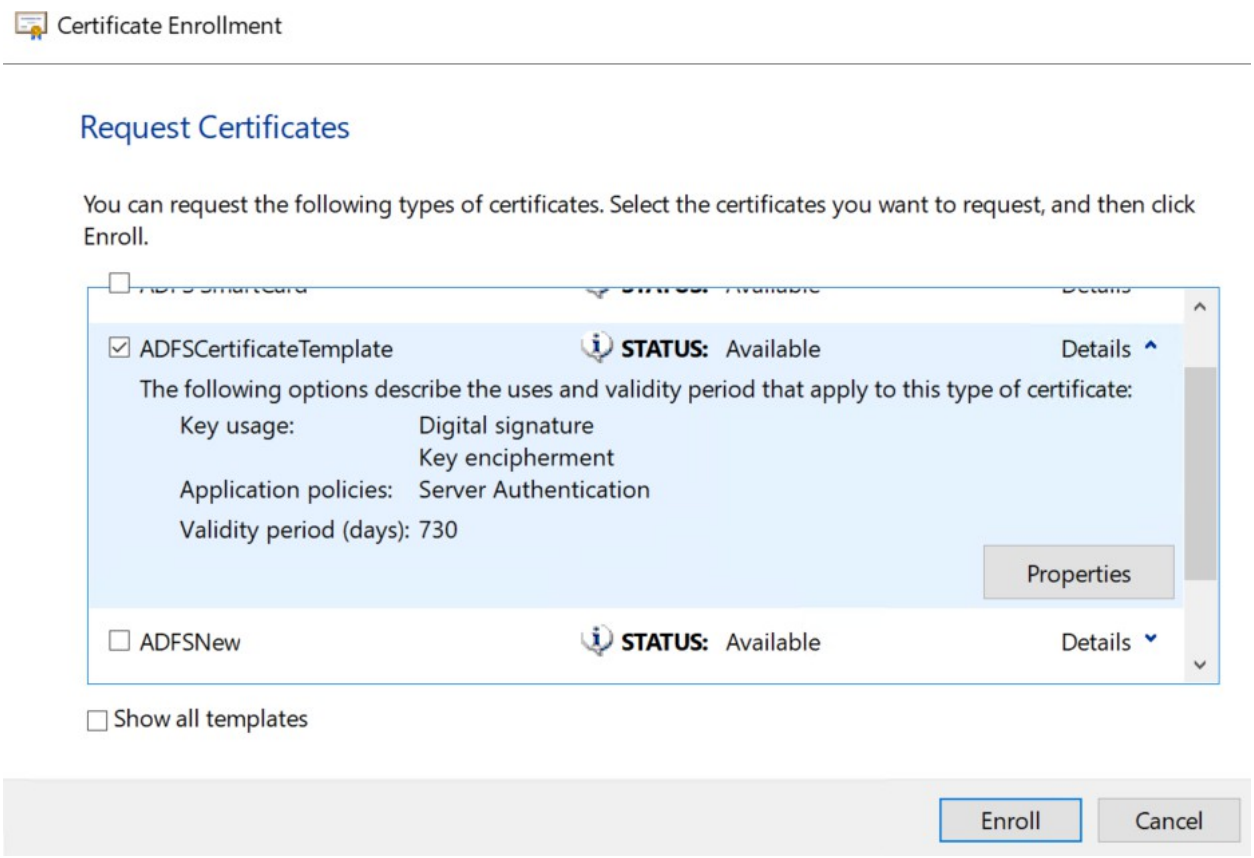

Figure 14 : Certificate enrollment

6. Click on **Properties** of the certificate template.
7. The **Certificate Properties** will open. Provide the details for the certificate.
8. Click on the **Private Key** tab and make sure that **RSA, Utimaco CryptoServer Key Storage Provider** is selected.

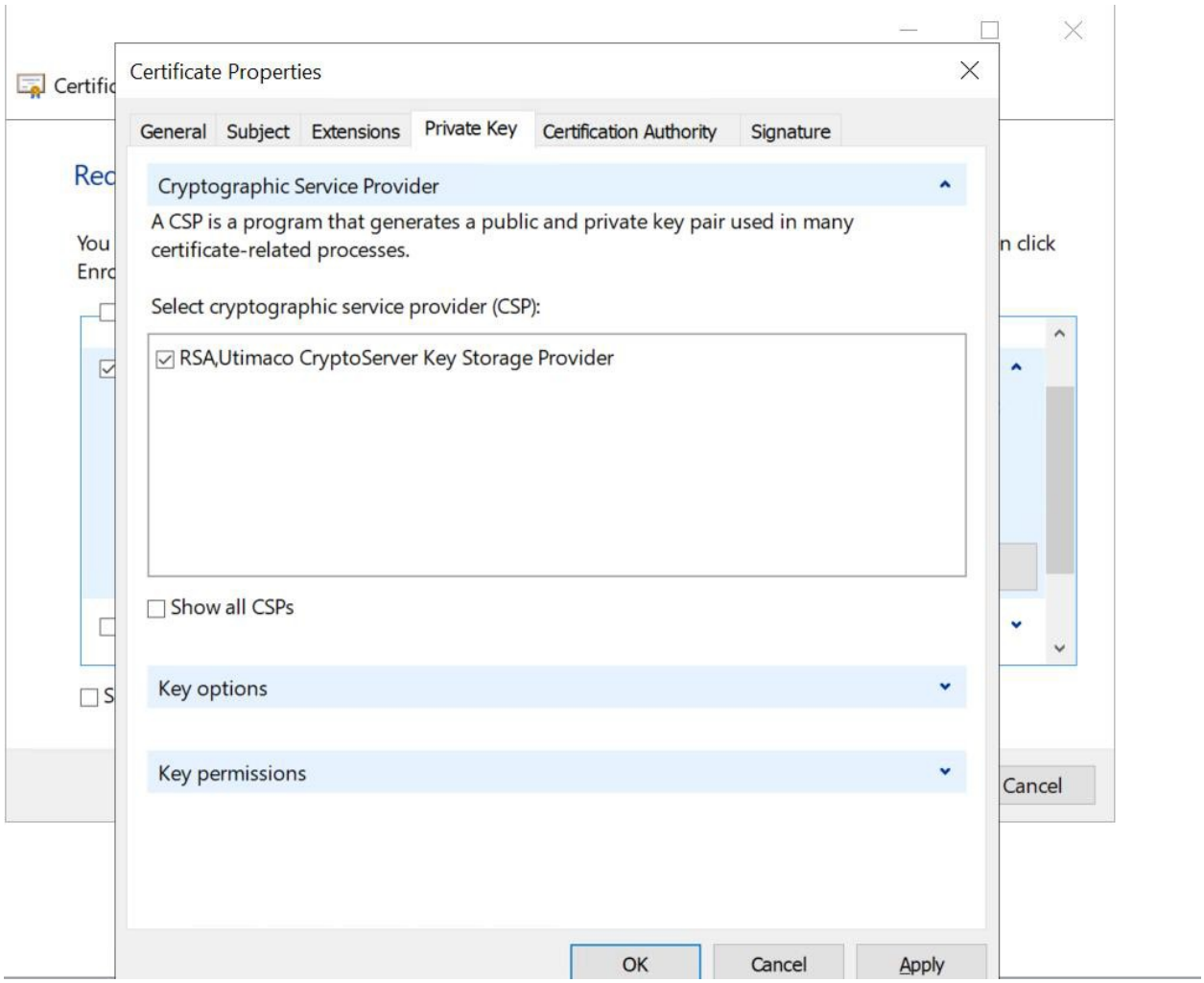

Figure 15 : Certificate properties

9. Click **apply** and **OK**.
10. Click **Enroll** to enroll the SSL certificate. Click on **Finish**.

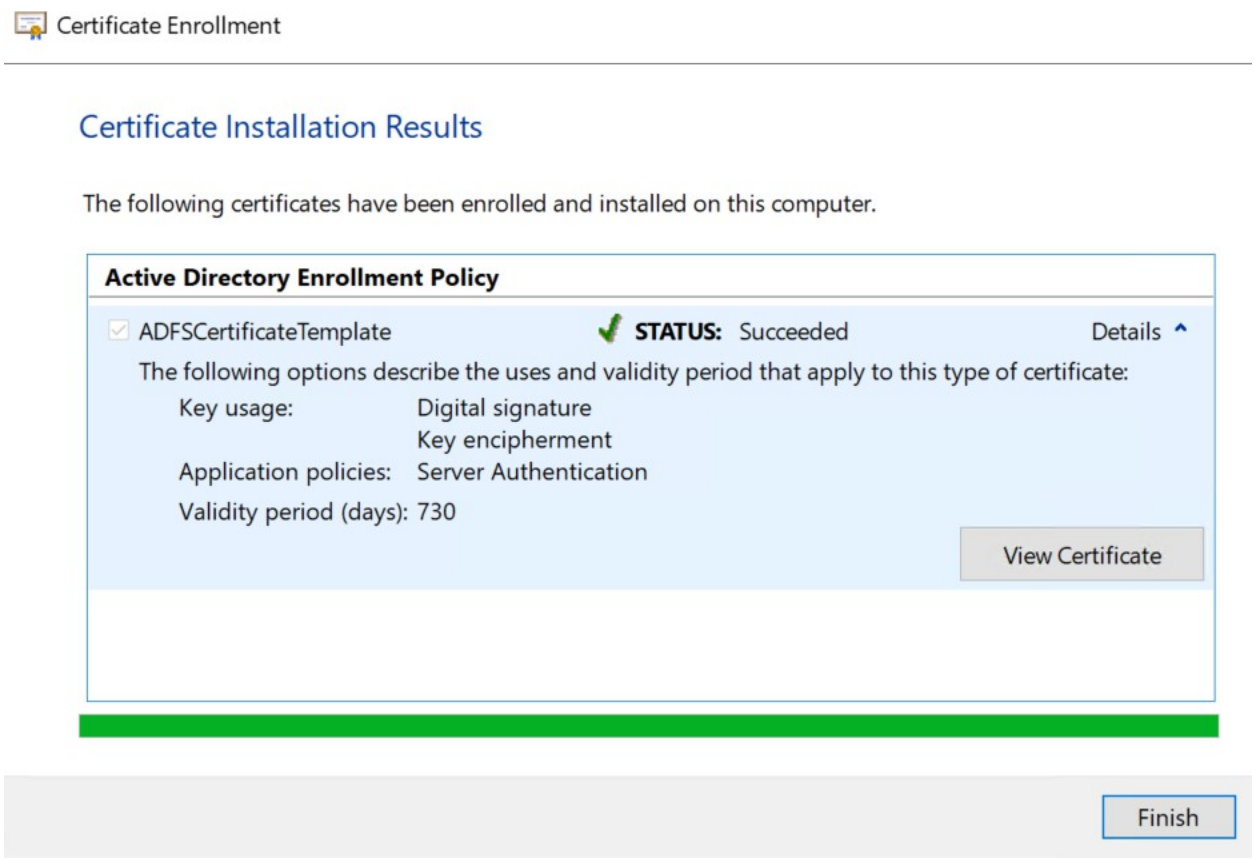

Figure 16 : Certificate installation results

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

11. Repeat the above steps to generate the **Token Signing Certificate** and the **Token Decryption Certificate**.

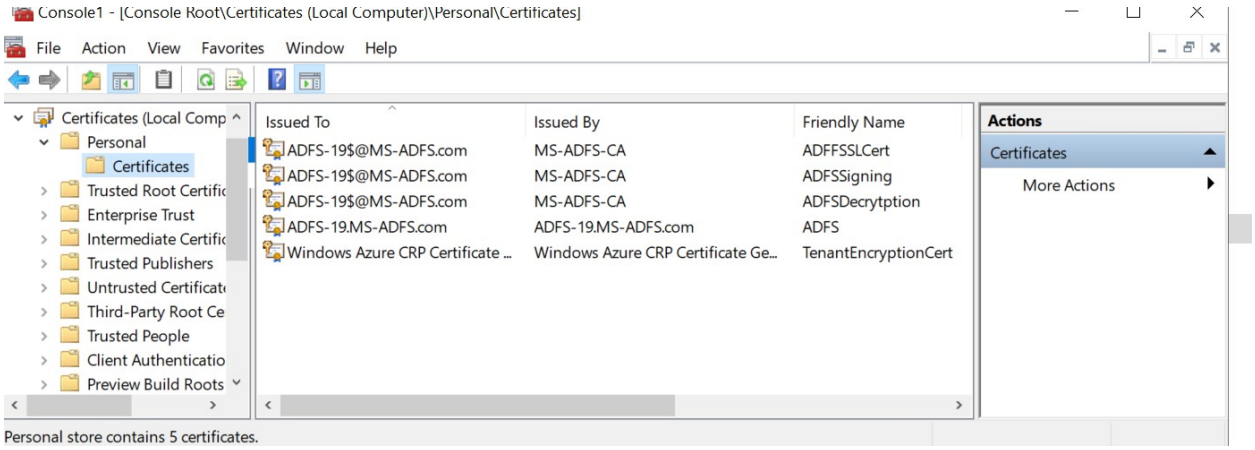

Figure 17 : Certificate window

5.4 Provide Full User Permission for the Private Keys of the Certificates to Generated Certificate

1. Open **Start** and **Run** on the AD FS server. Then, type “certlm.msc”. This will open the certificate for the **Local** computer.

2. Right-click on your SSL certificate that you have enrolled. Then, select **All Tasks > Manage Private Keys**.

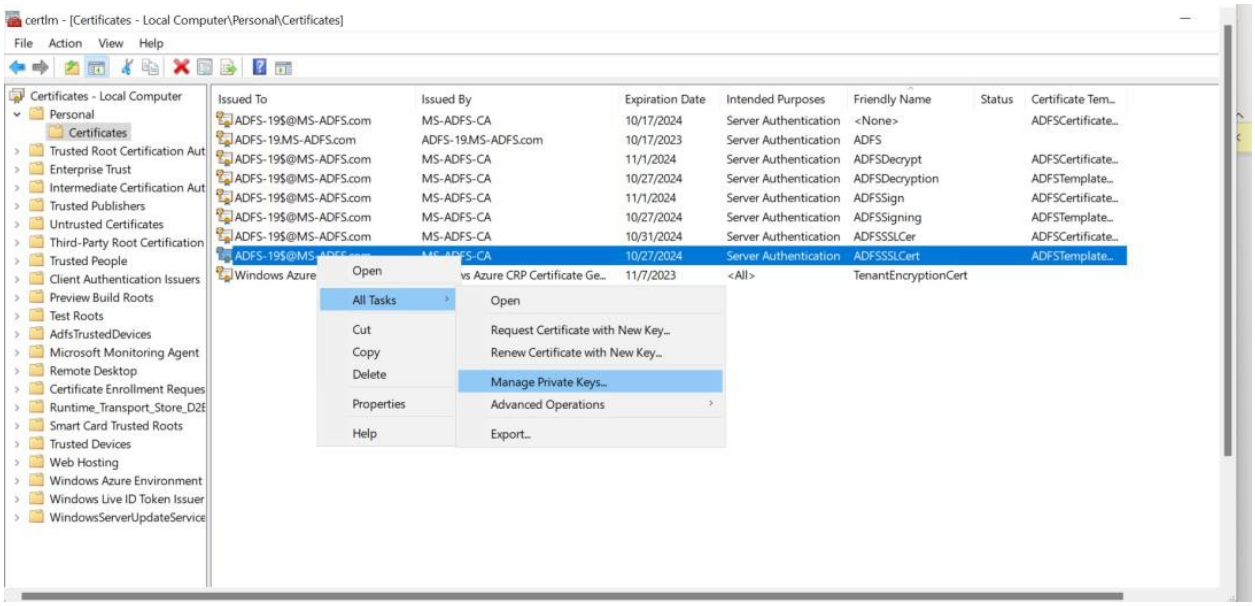

Figure 18 : Certificate window

3. Select **Add > Object Types > Select Service Accounts > Locate and select your ADFS service account**. Grant full control.

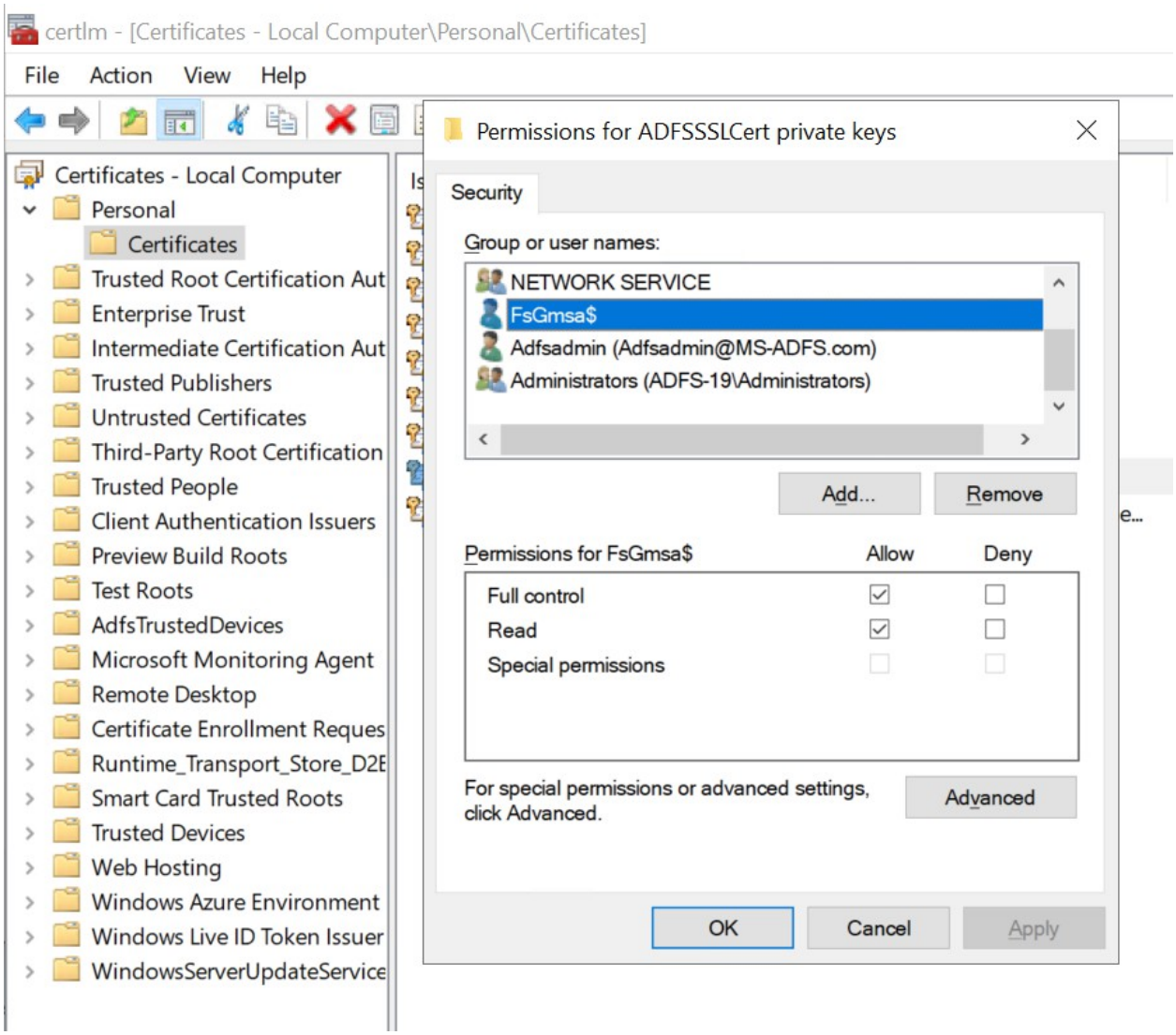

Figure 19 : Permissions for ADFSSSLCert private keys

Once you click on **OK**, it will provide permissions for private keys of the certificate. Similarly, follow the above process to provide permissions for the Token Singing Certificate and the Token Decryption Certificate Private Keys.

5.5 Install AD FS

1. Log in to AD FS Server as a domain administrator.

2. Go to the server manager and select **Add Role and Feature**.

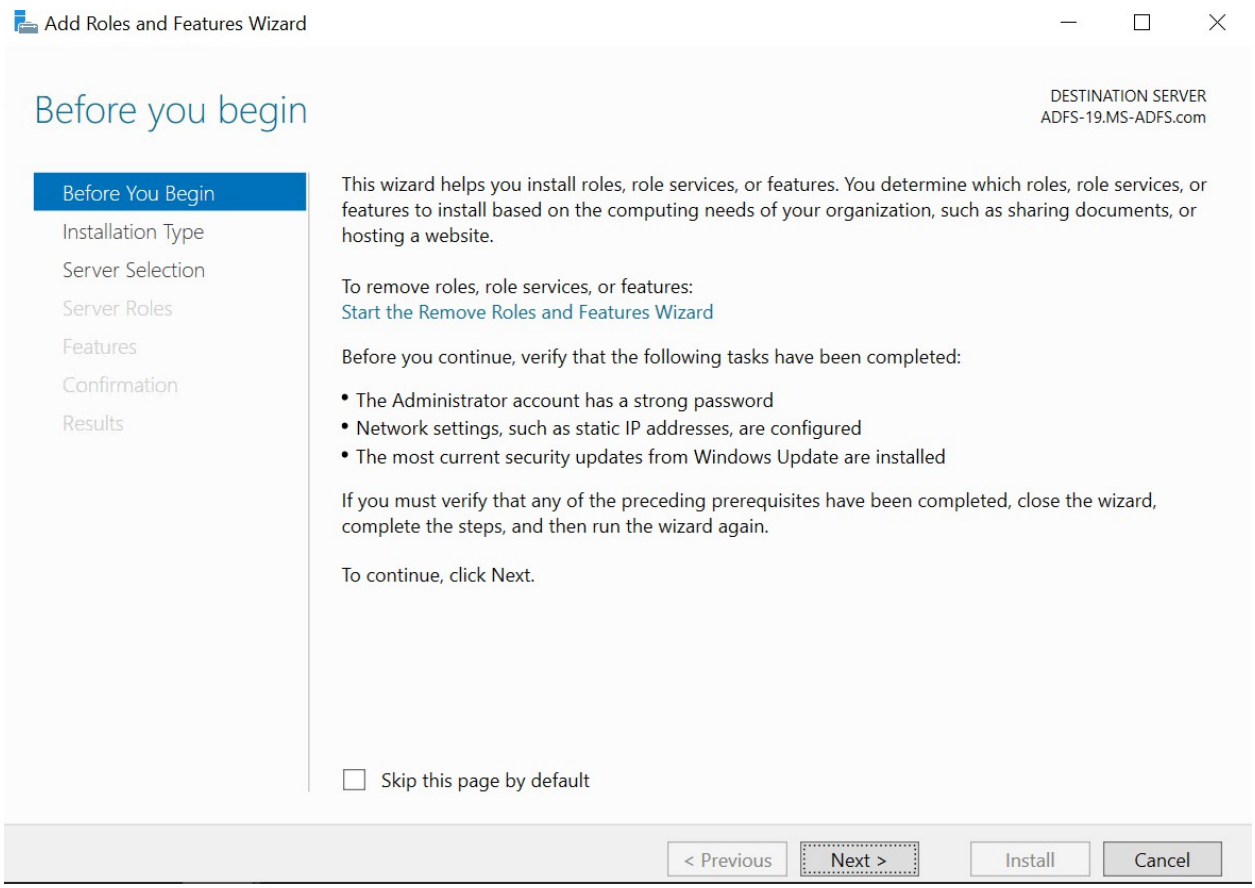

Figure 20 : Server manager dashboard

3. Select the server from pool.

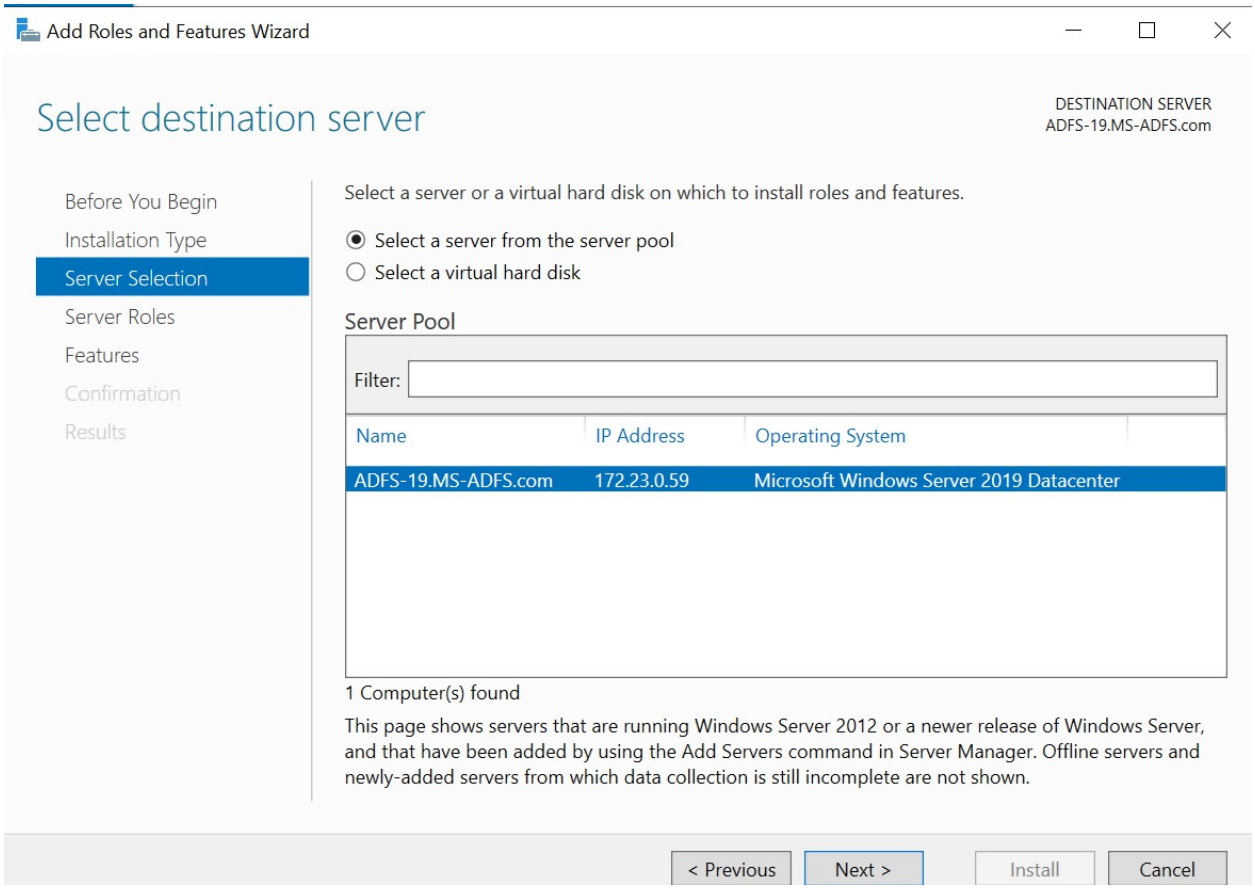

Figure 21 : Add Roles and Features Wizard

4. Select **Active Directory Federation Services** and click on **Next**.

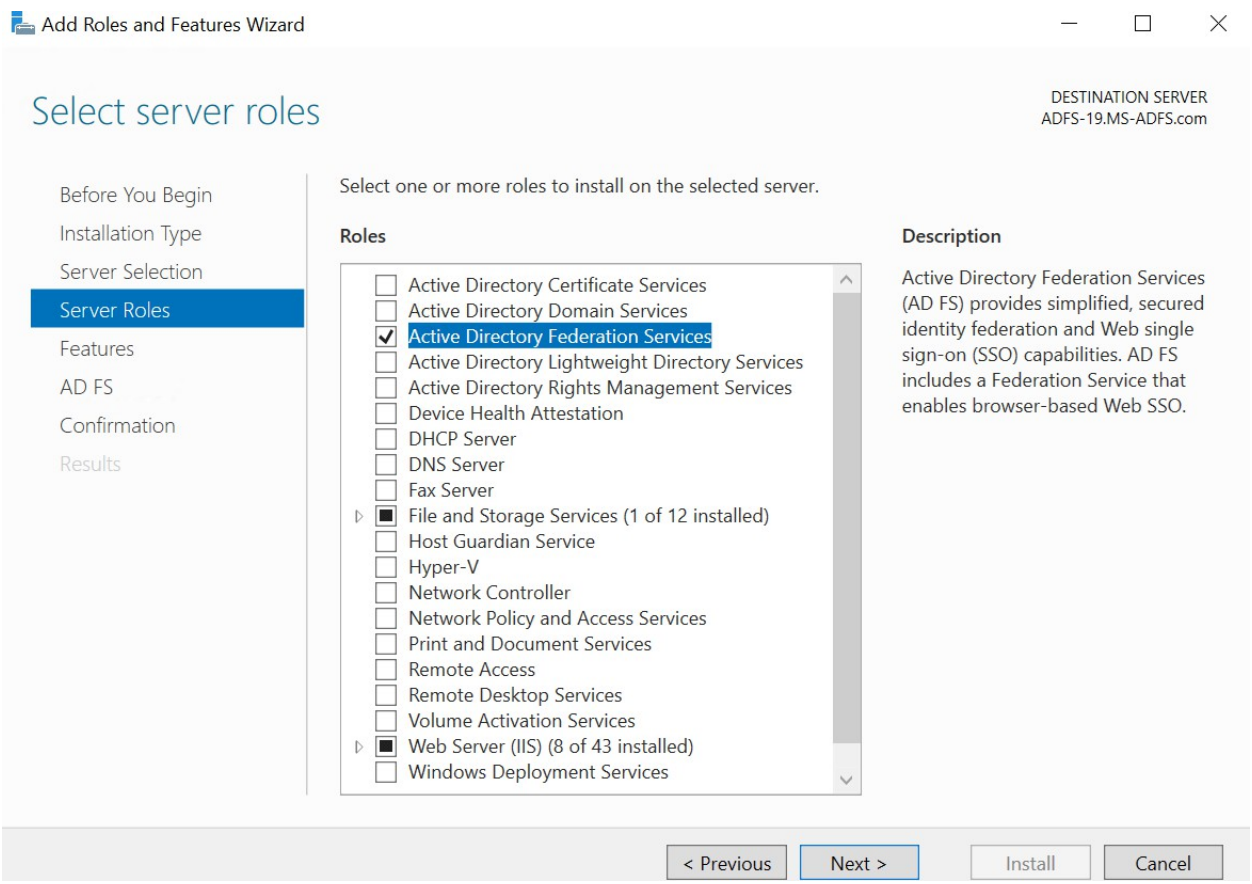

Figure 22 : Select server roles

5. Click on **Next**. Click on the **Next** button again.

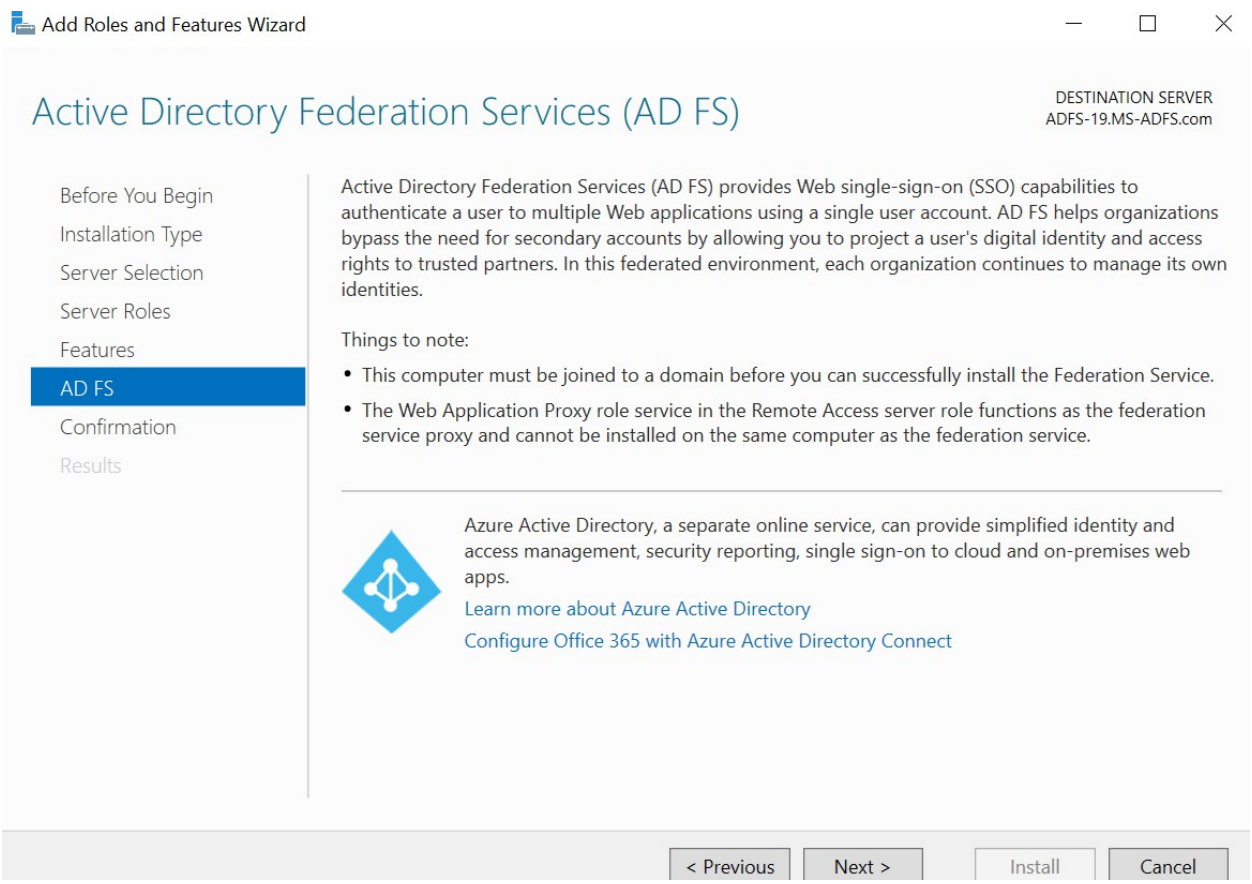

Figure 23 : AD FS wizard

6. Select the checkbox **Restart the destination servers automatically if required**. Click on **Install**.

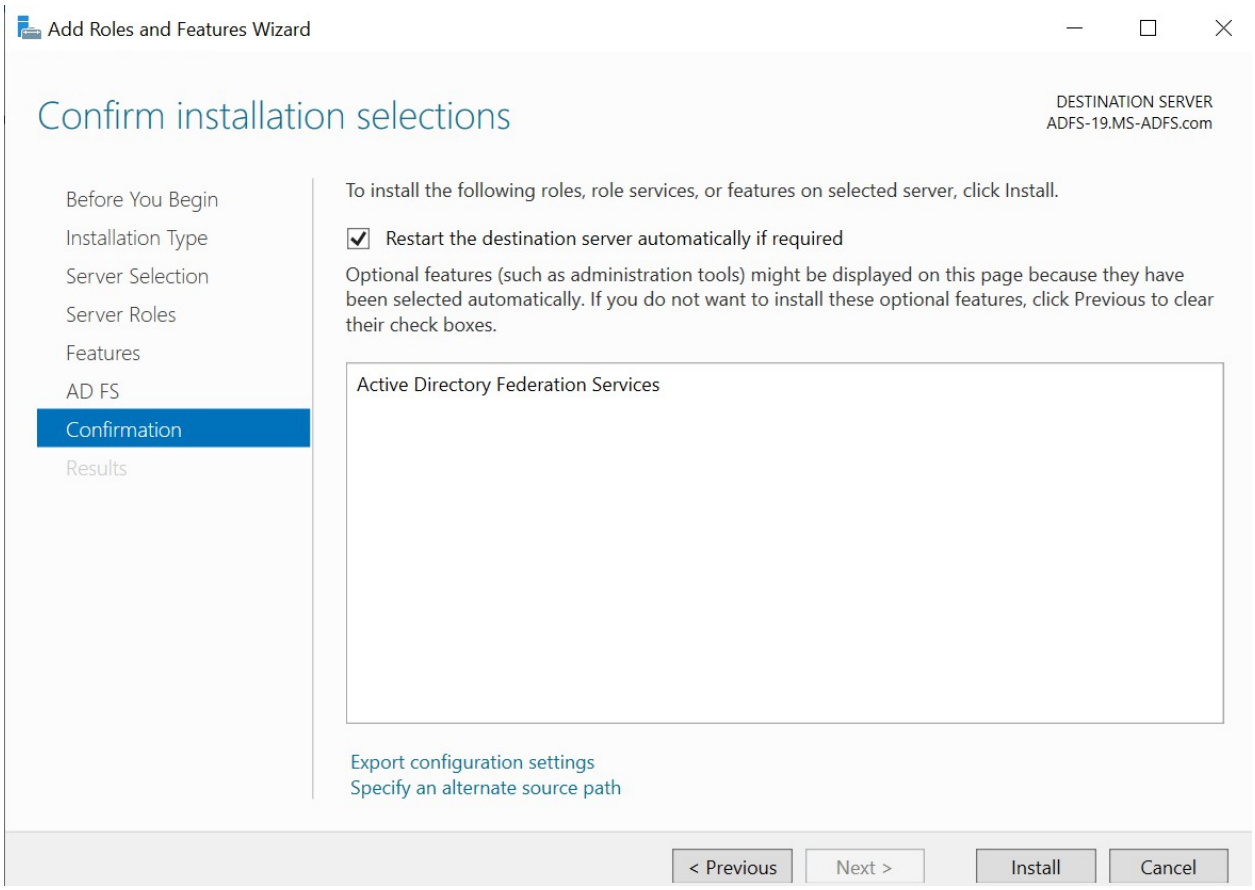

Figure 24 : Confirmation wizard

7. Wait until the installation is completed.

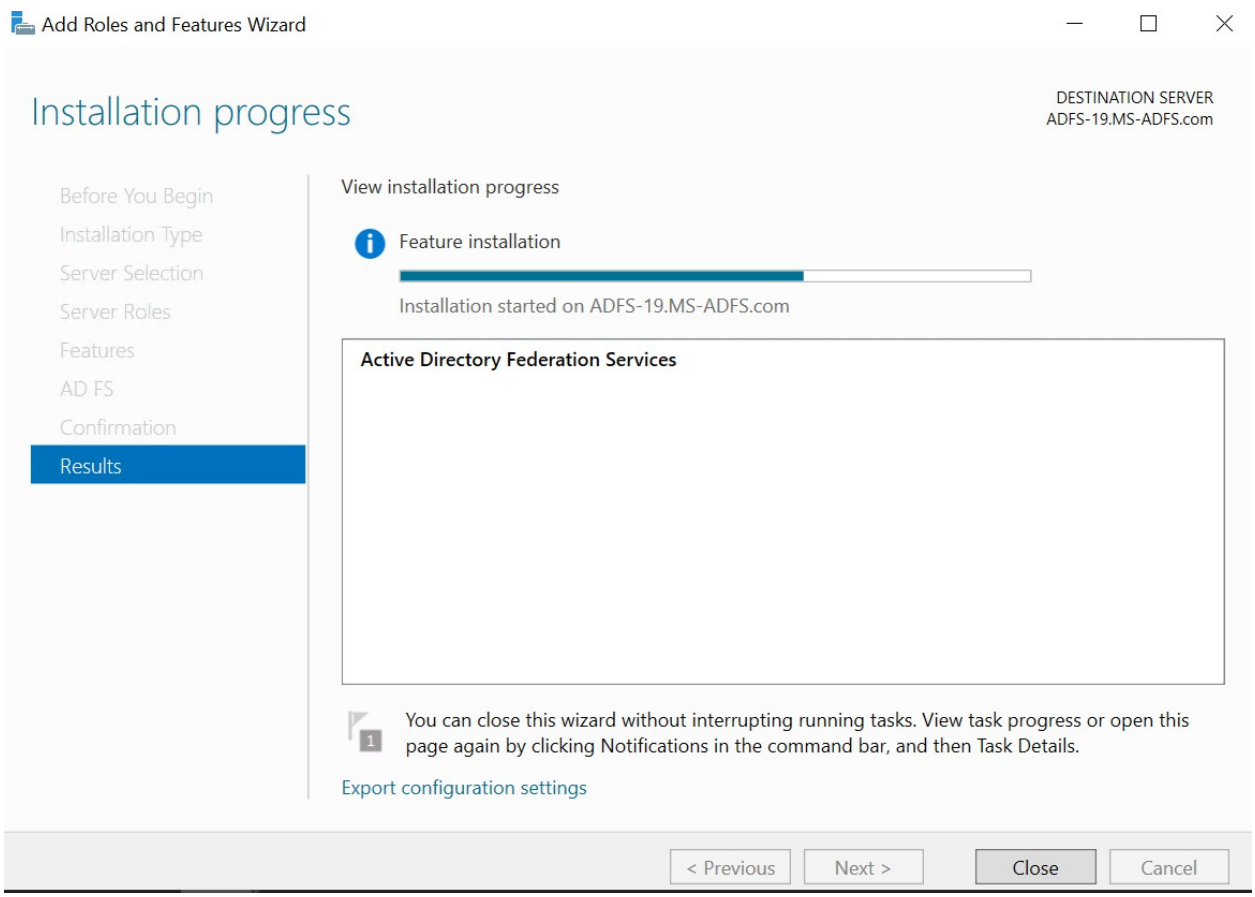

Figure 25 : Results wizard

5.6 Create a GMSA Account

The Group Managed Service Account (GMSA) account is required during the Active Directory Federation Services (AD FS) installation and configuration.

To create a GMSA account open a Windows PowerShell command window and type:

›_ PowerShell

```
C:\> Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

C:\> New-ADServiceAccount FsGmsa -DNSHostName MS-ADFS.com -
ServicePrincipalNames http/MS-ADFS.com
```

```
PS C:\> Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

Guid
----
2ee3b2b3-1f7e-9393-e04e-9686ceb42811


PS C:\> New-ADServiceAccount FsGmsa -DNSHostName MS-ADFS.com -ServicePrincipalNames http/MS-ADFS.com
PS C:\>
```

Figure 26 : Create a GSMA account

5.7 Configure AD FS Service

1. Once installation is completed, click on the **Configure the federation service on this server** option.

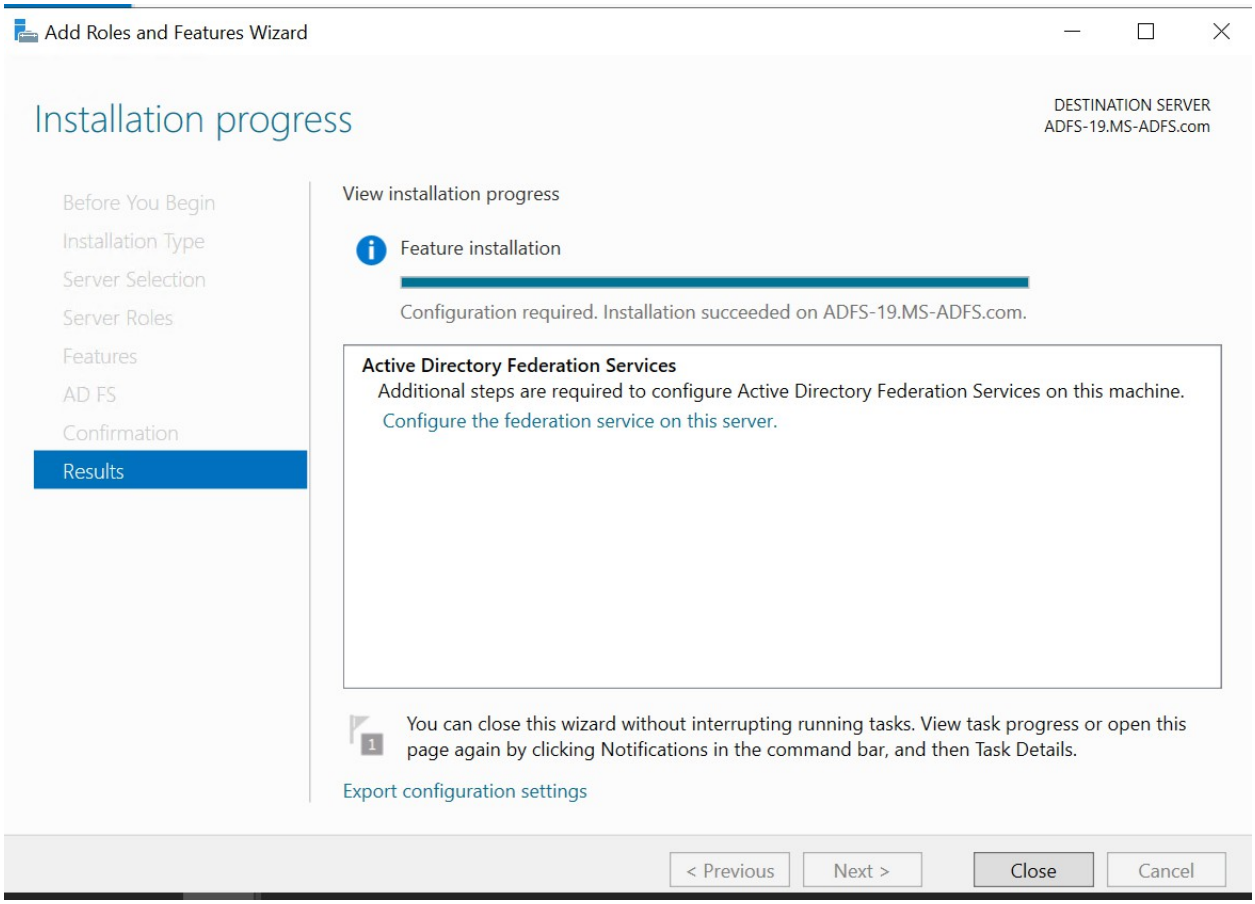

Figure 27 : Post-deployment configuration wizard

2. Select **Create the first federation server in a federation server farm** radio button.

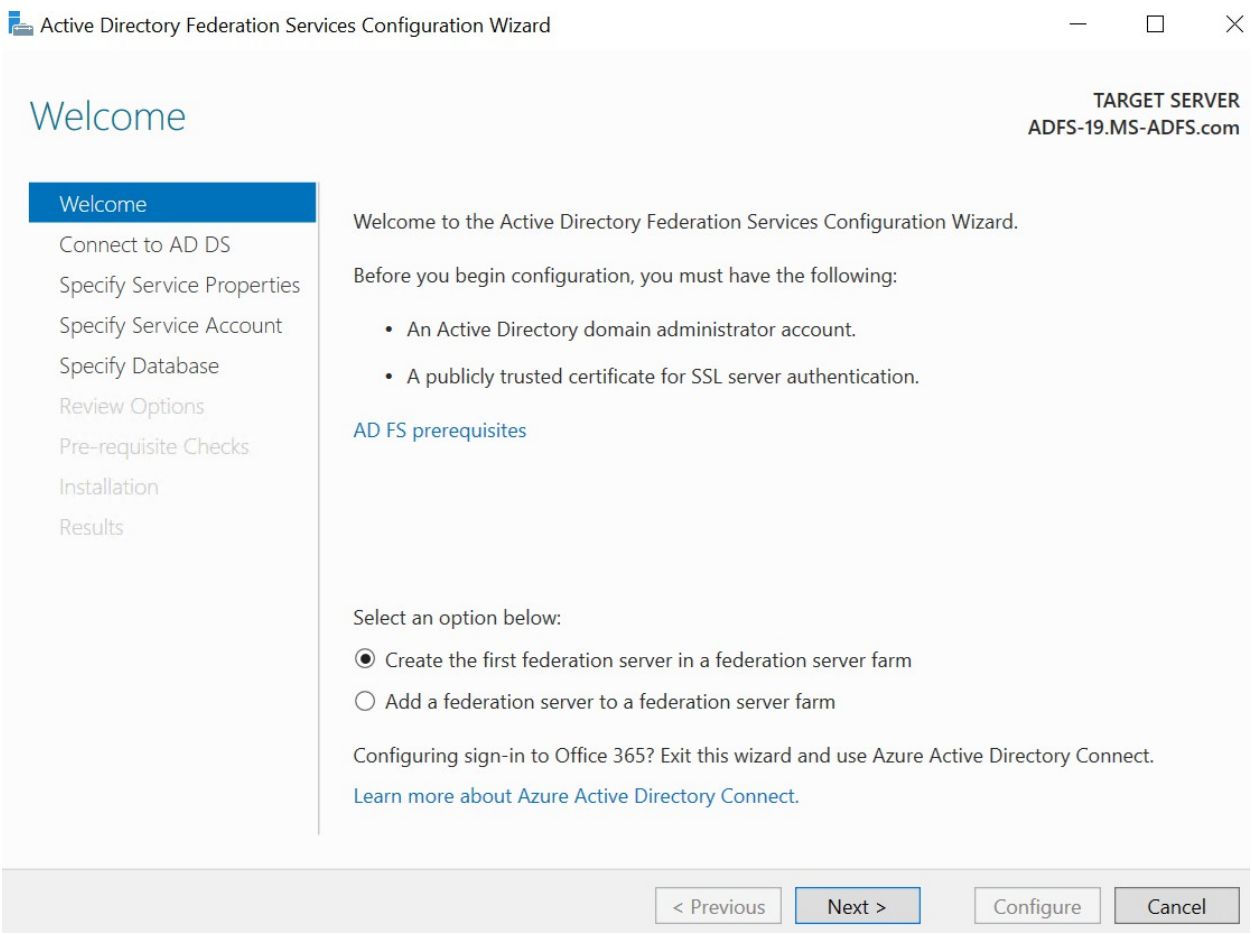

Figure 28 : Welcome wizard

3. Select the system user with domain credentials.

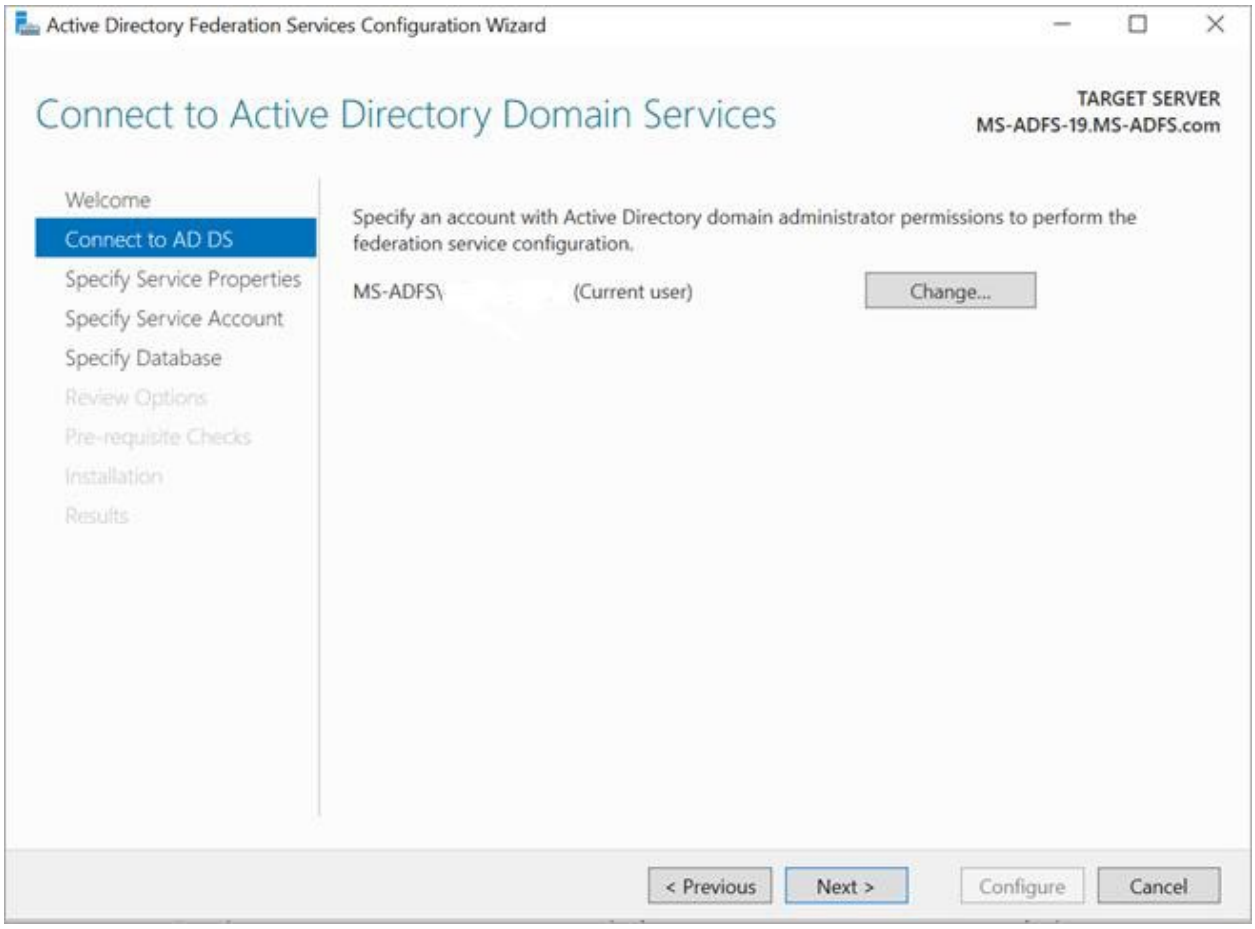

Figure 29 : Connect to AD DS wizard

Make sure this user has full permissions on for the private keys of the certificates that you have generated.

4. Browse the SSL certificate that you have generated earlier.
5. Use the appropriate domain user account to proceed further.

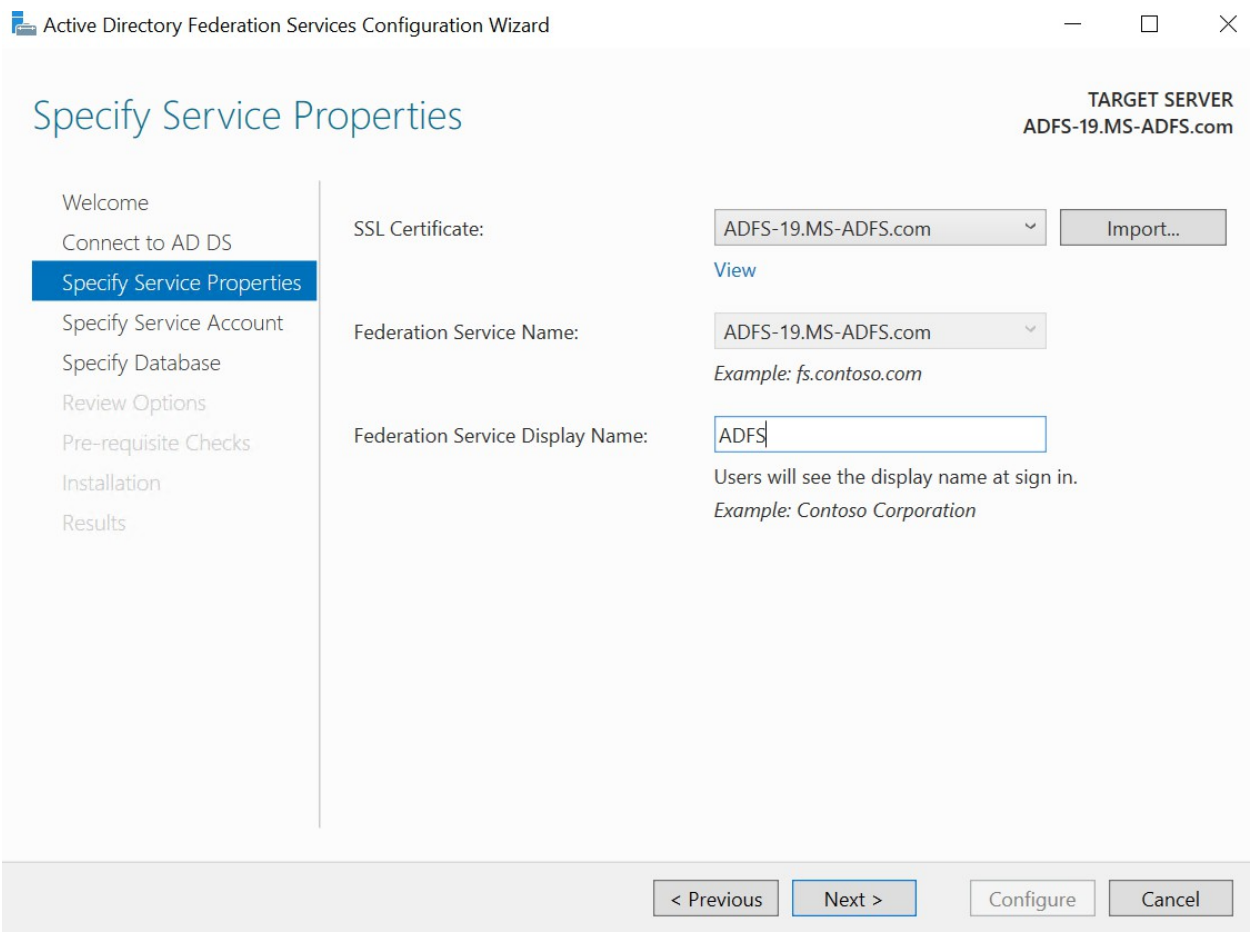

Figure 30 : Specify Service Properties wizard

6. Click on the **Next** button.
7. Select **Use an existing domain user account or group Managed Service Account**.

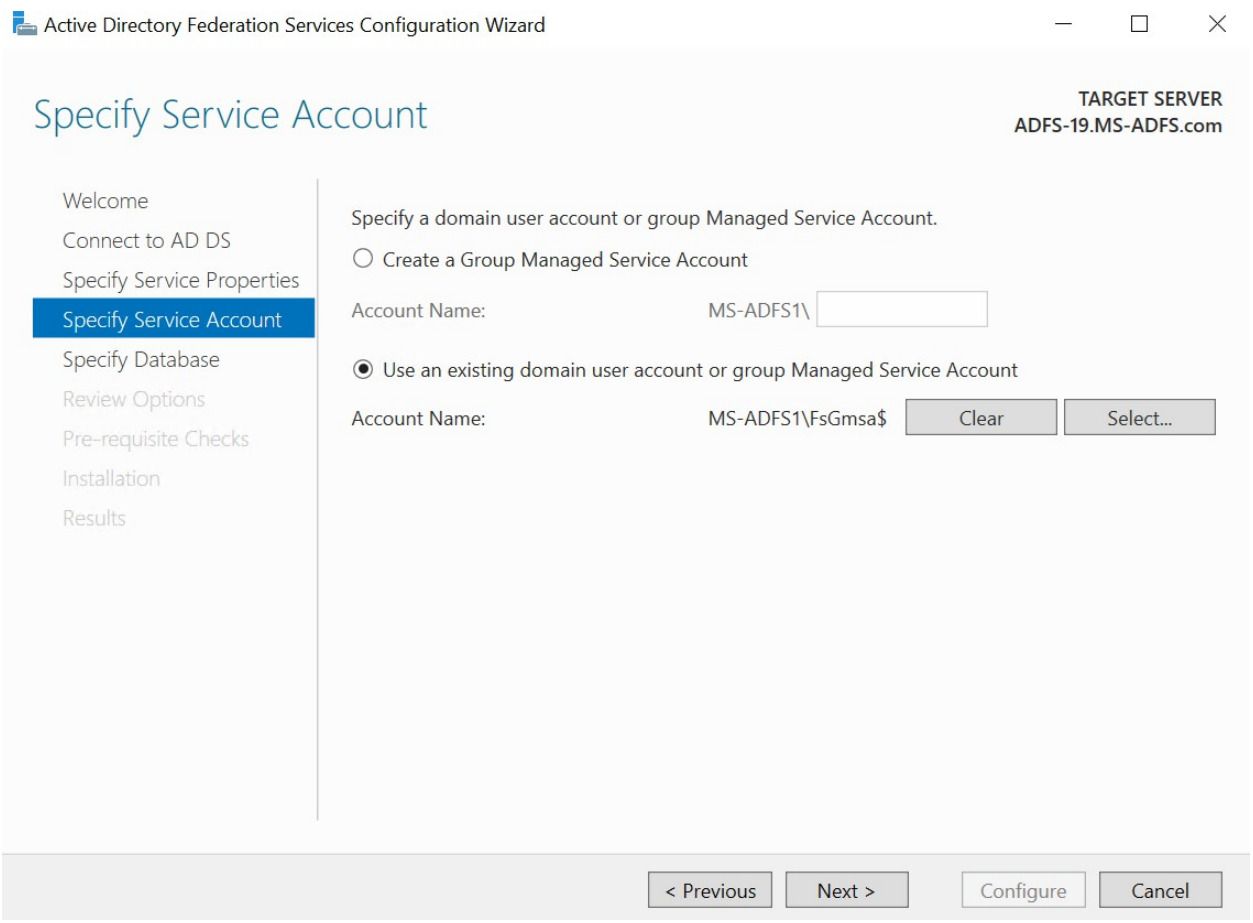

Figure 31 : Specify Service Account wizard

8. Select the radio button **Create a database on this server using Windows Internal Database**. Alternatively, you can also use SQL Server if you have it installed and running.

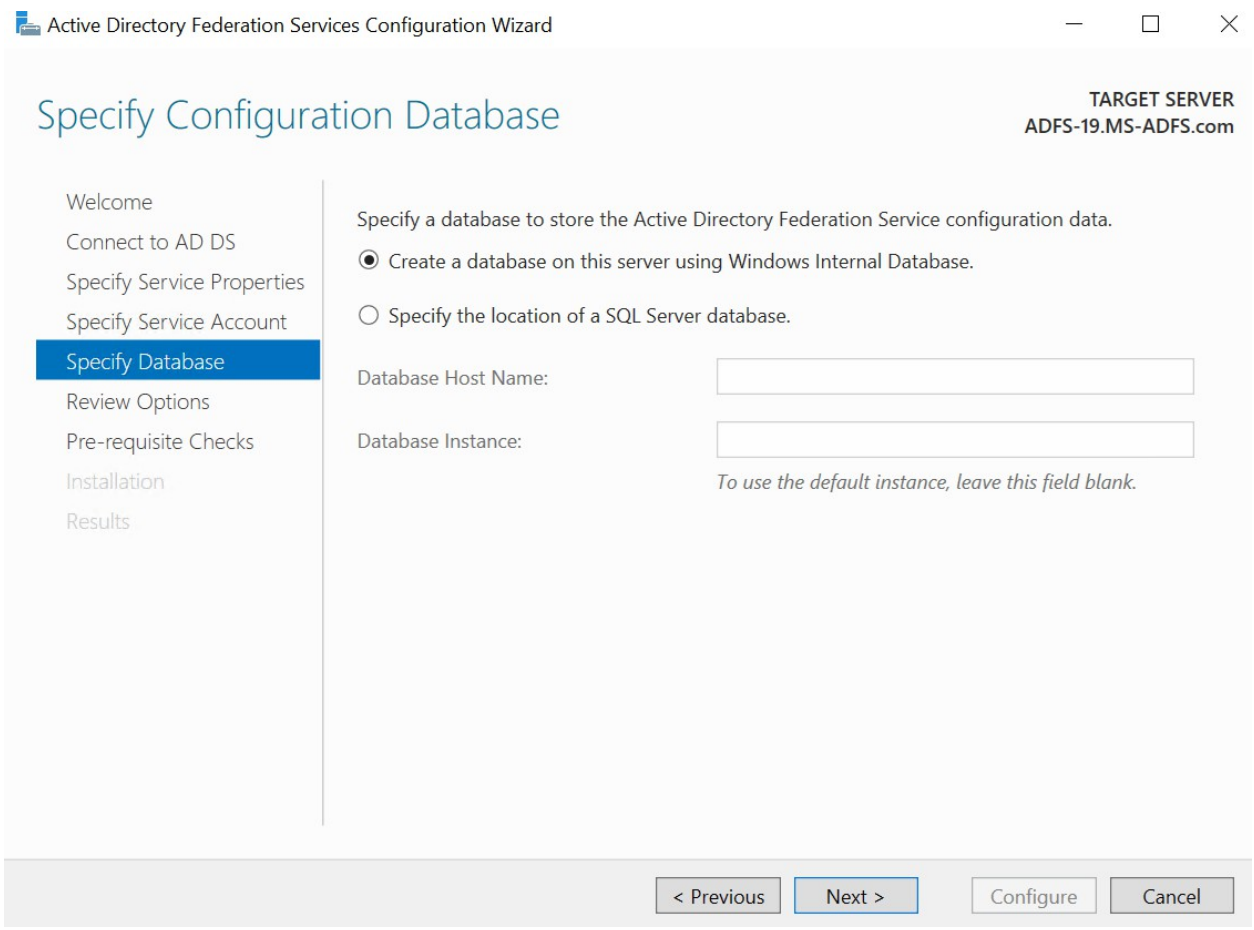

Figure 32 : Specify Configuration Database wizard

9. Click on the **Next** button.
10. Review the configuration settings and click on the **Next** button.

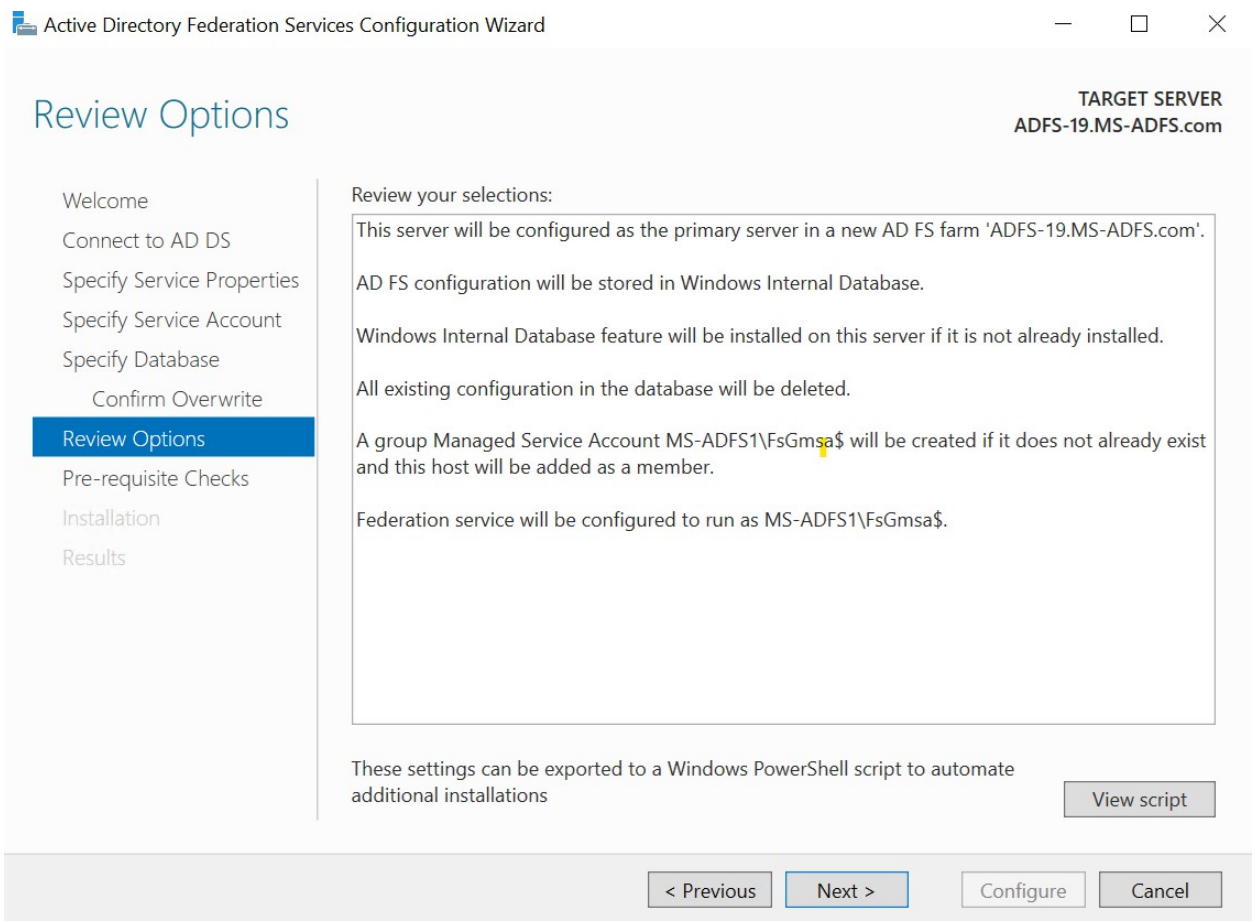

Figure 33 : Review Options wizard

11. Once all the prerequisites are checked and passed, the below message will be shown. Then, click on the **Configure** button for the final configuration.

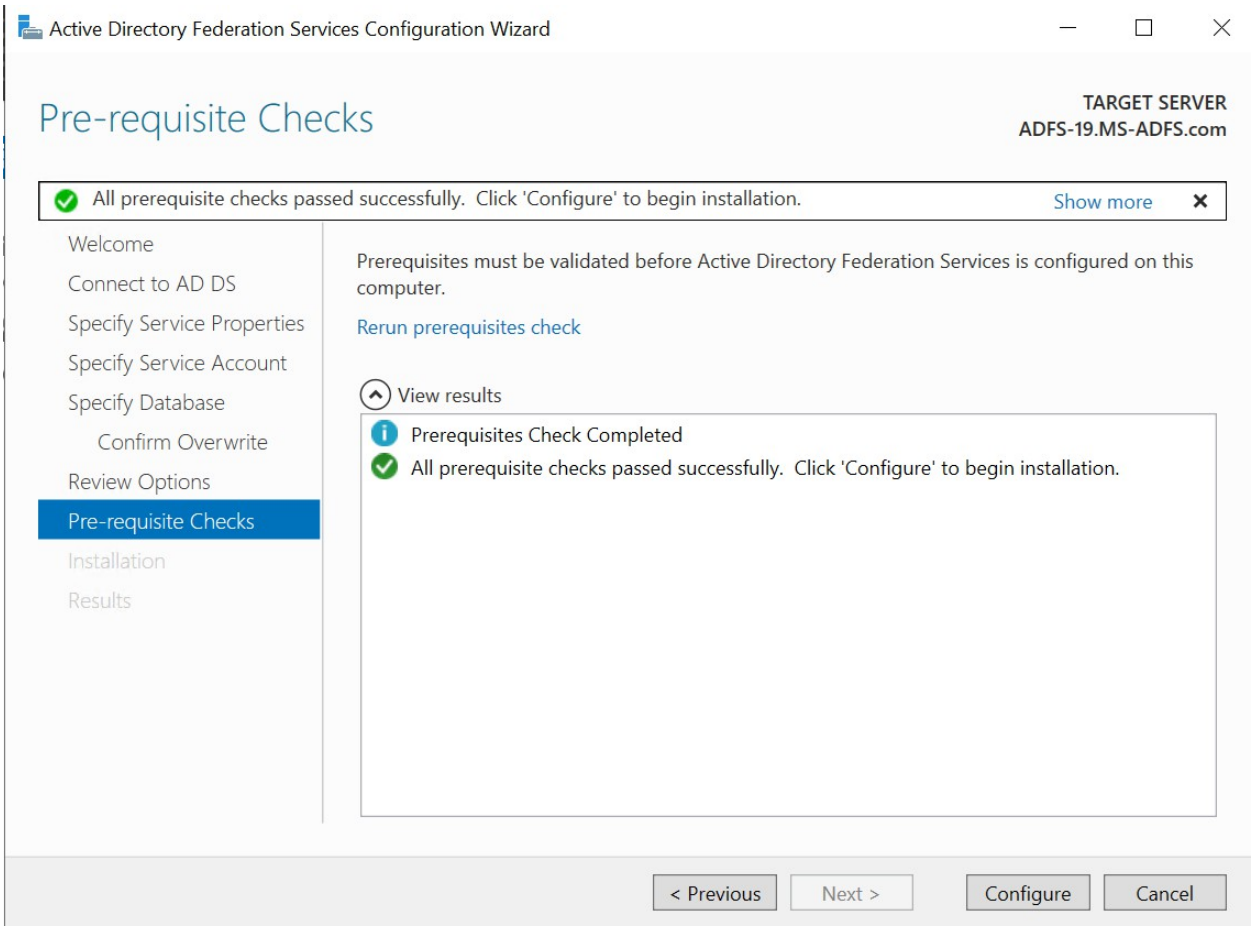

Figure 34 : Pre-requisite Checks wizard

12. After the installation is completed, the below message will be shown. Click on **Close**.

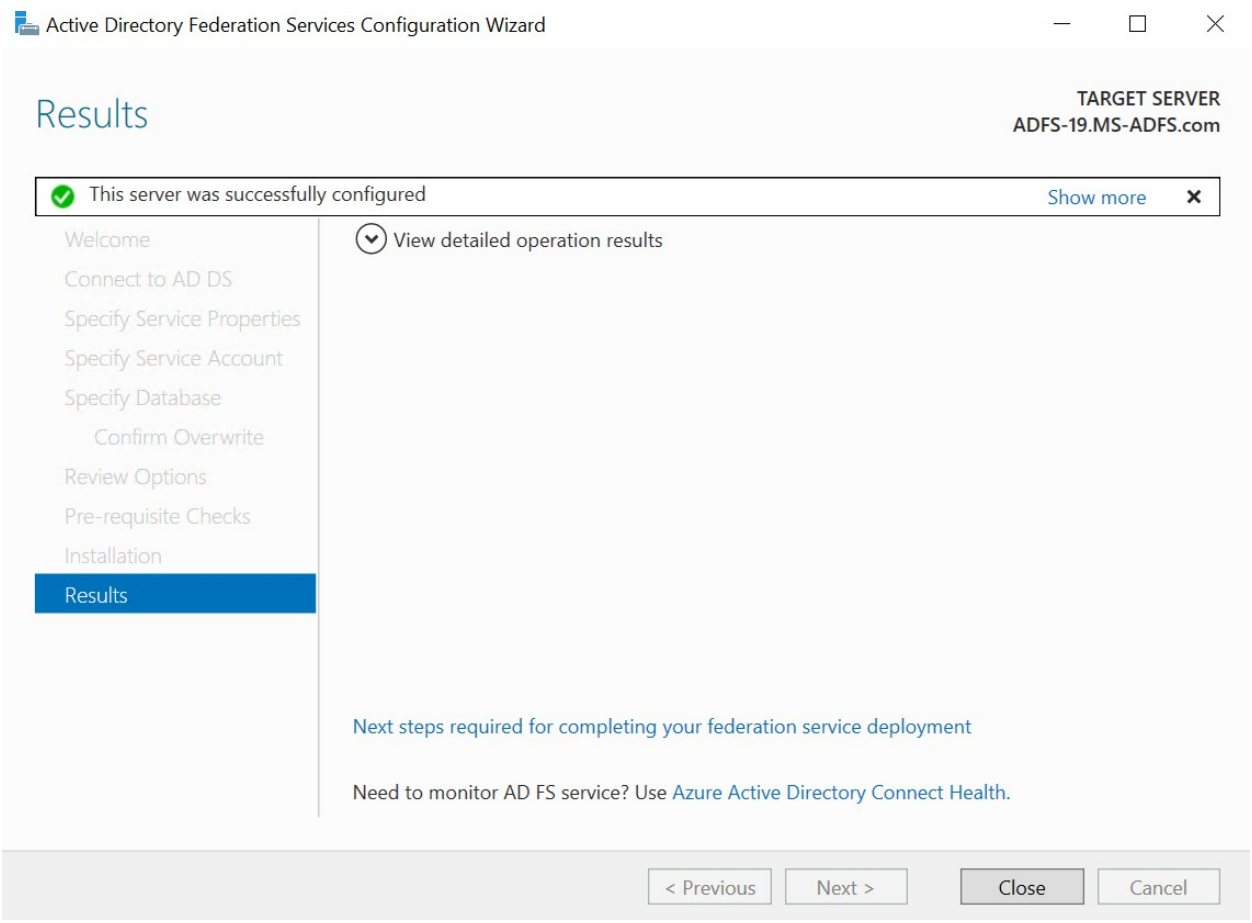

Figure 35 : Results wizard

5.8 Add Token Certificate from AD FS Manager

5.8.1 Add a Token Signing Certificate

Use the following steps to add the token-signing certificate to the AD FS Management snap-in.

1. Open PowerShell and run the following: `Set-ADFSProperties -AutoCertificateRollover $false`.

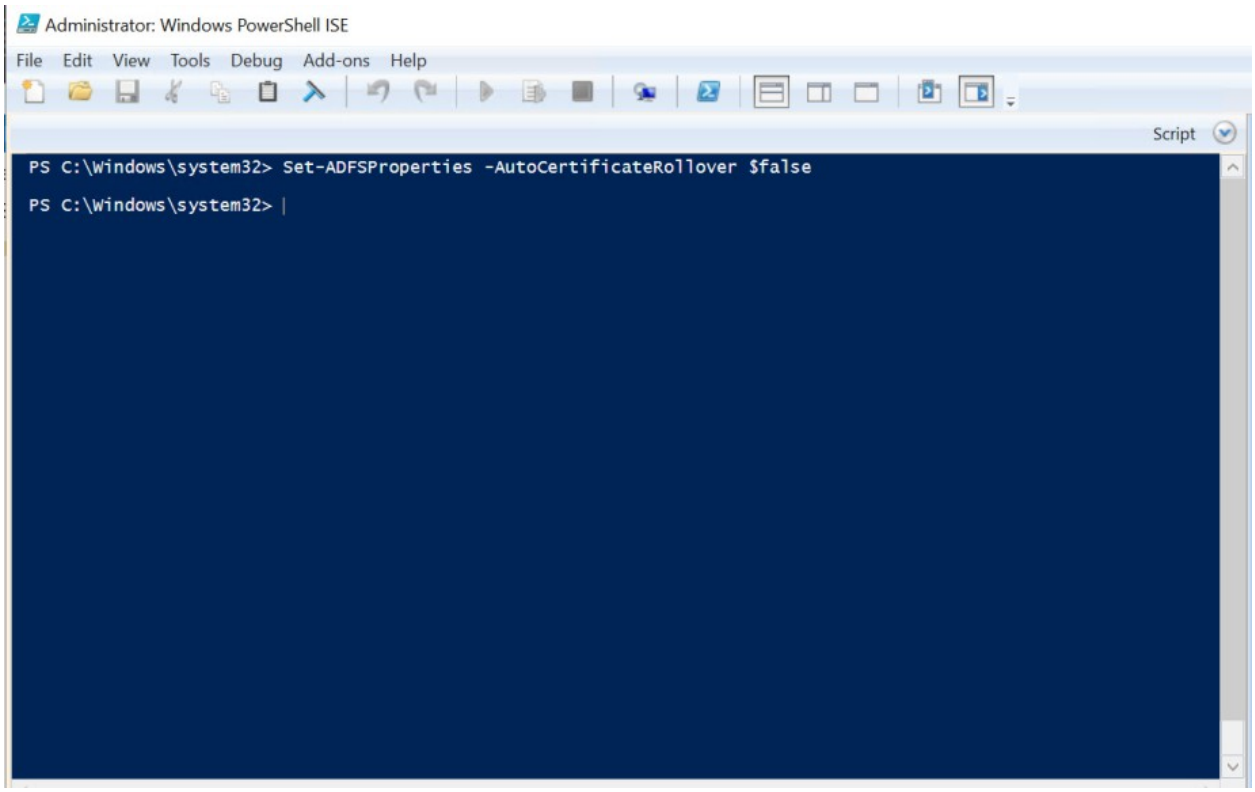

Figure 36 : PowerShell console

AutoCertificateRollover is not supported with Utimaco HSM, and its value needs to be set as false. If AutoCertificateRollover is set to false, AD FS will not automatically generate or start using new token-signing or token-decrypting certificates. You will have to perform these tasks manually. Once you have allowed enough time for your federation partners to consume your new certificate (either they pull your federation metadata or you send them the public key of your new certificate), you must promote the secondary certificate to primary certificate.

2. On the **Start** screen, type “AD FS Management”, and press **ENTER**.
3. In the console, double-click on **Service**, and then click on **Certificates**.
4. In the **Actions** pane, click the **Add Token-Signing Certificate** link.
5. In the **Browse for Certificate** file dialog box, navigate to the certificate file that you have created previously, the Token Signing Certificate. Select the certificate file, and click **Open**.

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

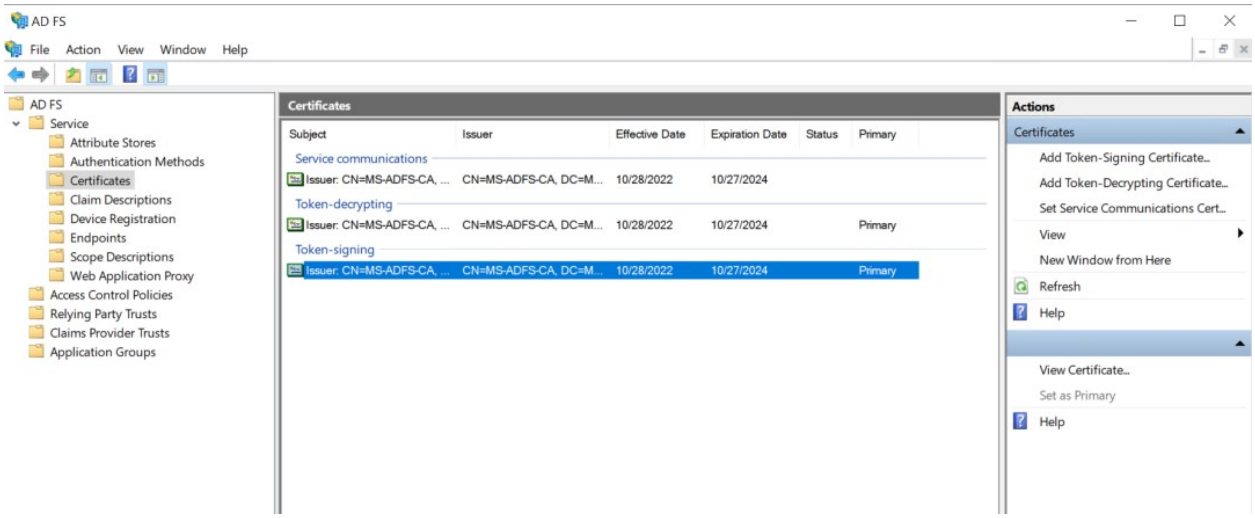

Figure 37 : Add the token-signing certificate

5.8.2 Set Token Signing Certificate as Primary

If the certificate which you have added as the token-signing certificate has been set to secondary, you need to change it to primary, as shown below.

1. Right-click on the **Token-signing** certificate and select **Set as Primary**.

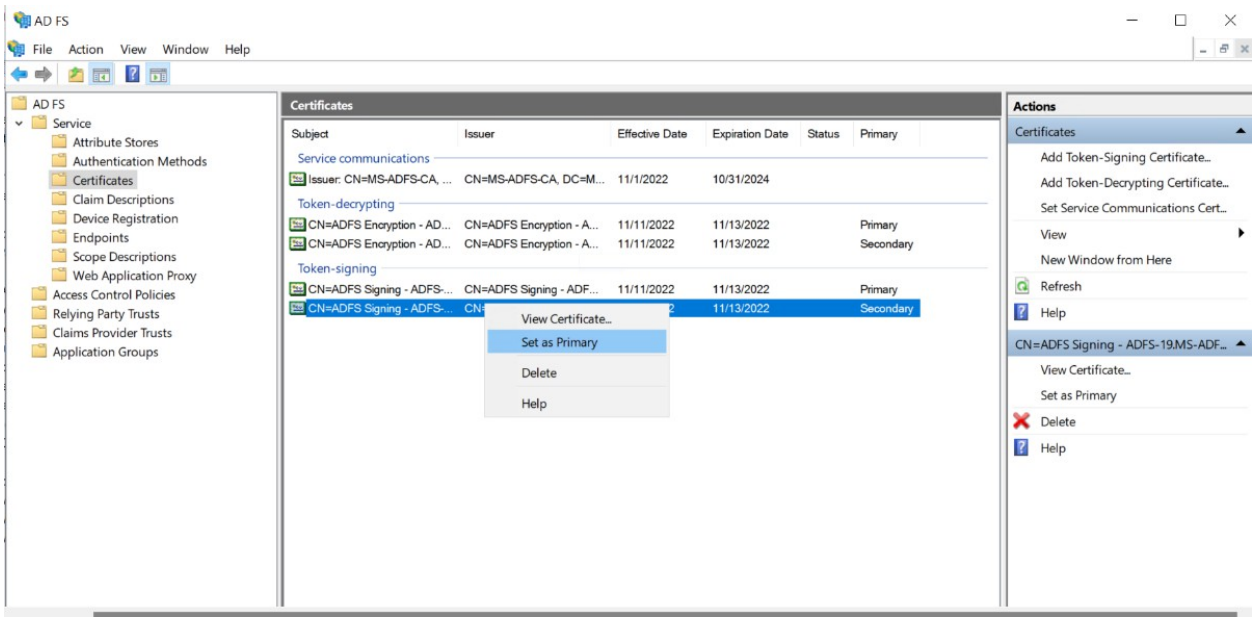

Figure 38 : AD FS management console

Certificates used for token-signing are critical to the stability of the Federation Service. Because loss or unplanned removal of any certificates configured for this purpose can disrupt service, you should back up any certificates configured for this purpose.

5.8.3 Add Token Decryption Certificate

To add a token-decrypting certificate:

1. On the **Start** screen, type “AD FS Management” and press **ENTER**.
2. In the console tree, double-click **Service**, and click **Certificates**.
3. In the **Actions** pane, click the **Add Token-Decrypting Certificate** link.
4. In the **Browse for Certificate** file dialog box, navigate to the certificate file that you have created previously, the Token Decryption Certificate, and select the certificate file. Then, click **Open**.

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

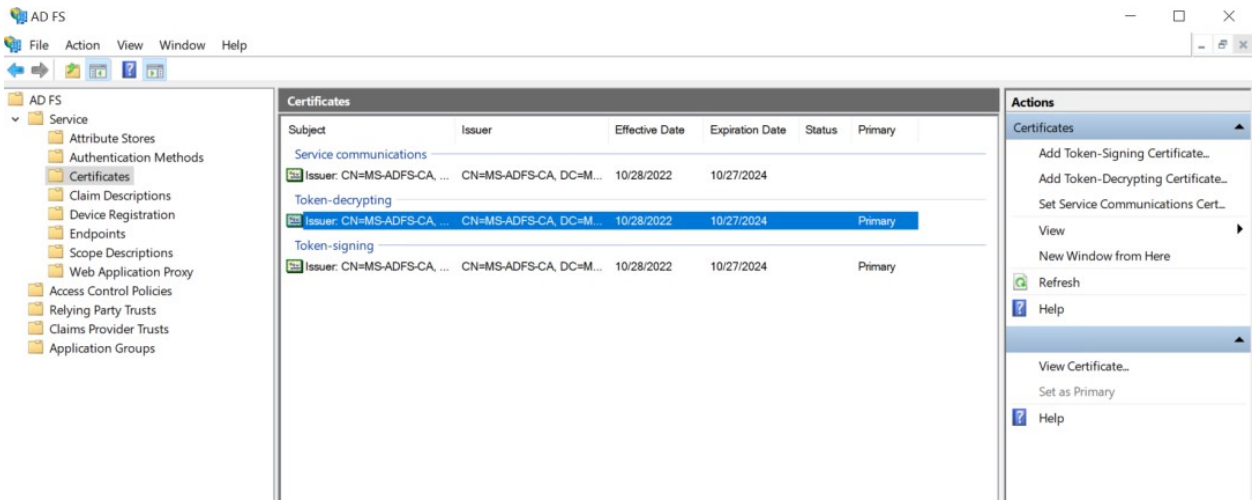

Figure 39 : Add a token-decryption certificate

5.8.4 Set Token Decryption Certificate as Primary

If the certificate which you have added as a Token Decryption Certificate has been set as secondary, you need to change it to primary as shown below.

1. Right-click on **Token-decrypting** certificate and select **Set as Primary**.

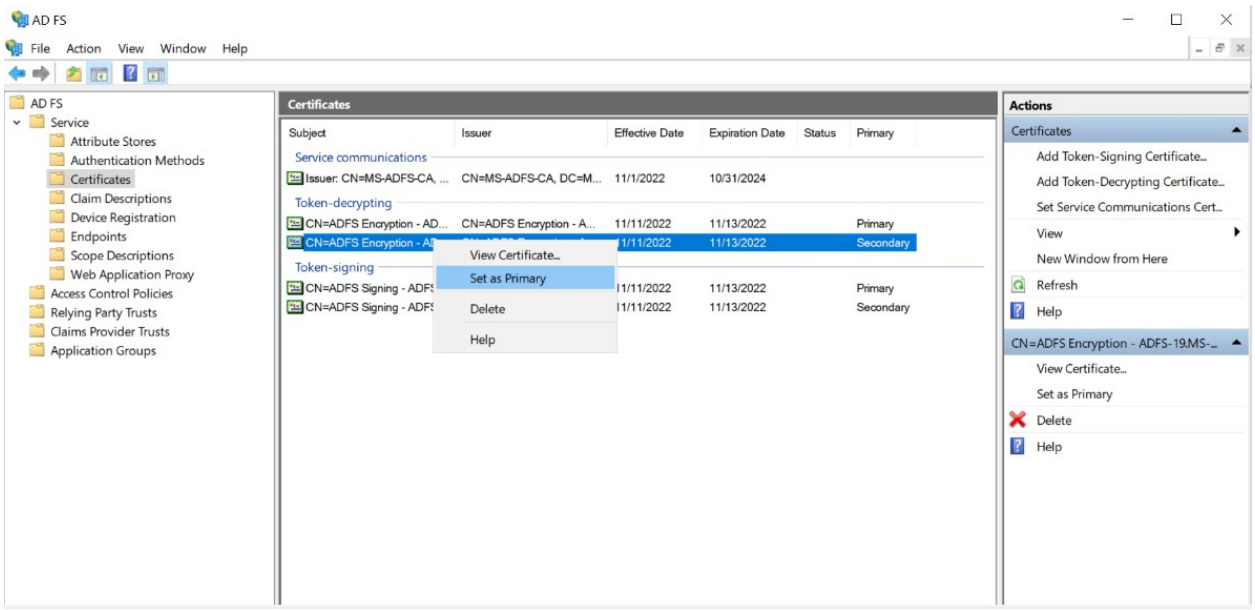

Figure 40 : AD FS management console

Certificates used for token-decrypting are critical to the stability of the Federation Service. Because loss or unplanned removal of any certificates configured for this purpose can disrupt service, you should back up any certificates configured for this purpose.

5.9 Verify the AD FS Server is Operational and Accessible Through the URL

Once you successfully add the token encryption and decryption certificates, you must restart the AD FS Services by following the steps below.

1. Go to **Start**, then Administrative tools select services. Then, select **Active directory federation service** and restart it.

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

2. To verify that the Internet Information Services (IIS) is configured correctly, on the federation server log on to a client computer that is located in the same forest as the federation server.
3. Open a browser window. In the address bar, type the federation server's host name, and then append `/adfs/fs/federationserverservice.asmx` to it for the new federation server. For example: https://<adfs_server>/adfs/fs/federationserverservice.asmx.
4. Press the **ENTER** button, and complete the next procedure on the federation server computer. If you see the message 'There is a problem with this website's security certificate', click **Continue** to this website.
5. The expected output is a display of XML with the service description document. If this page appears, IIS on the federation server is operational.

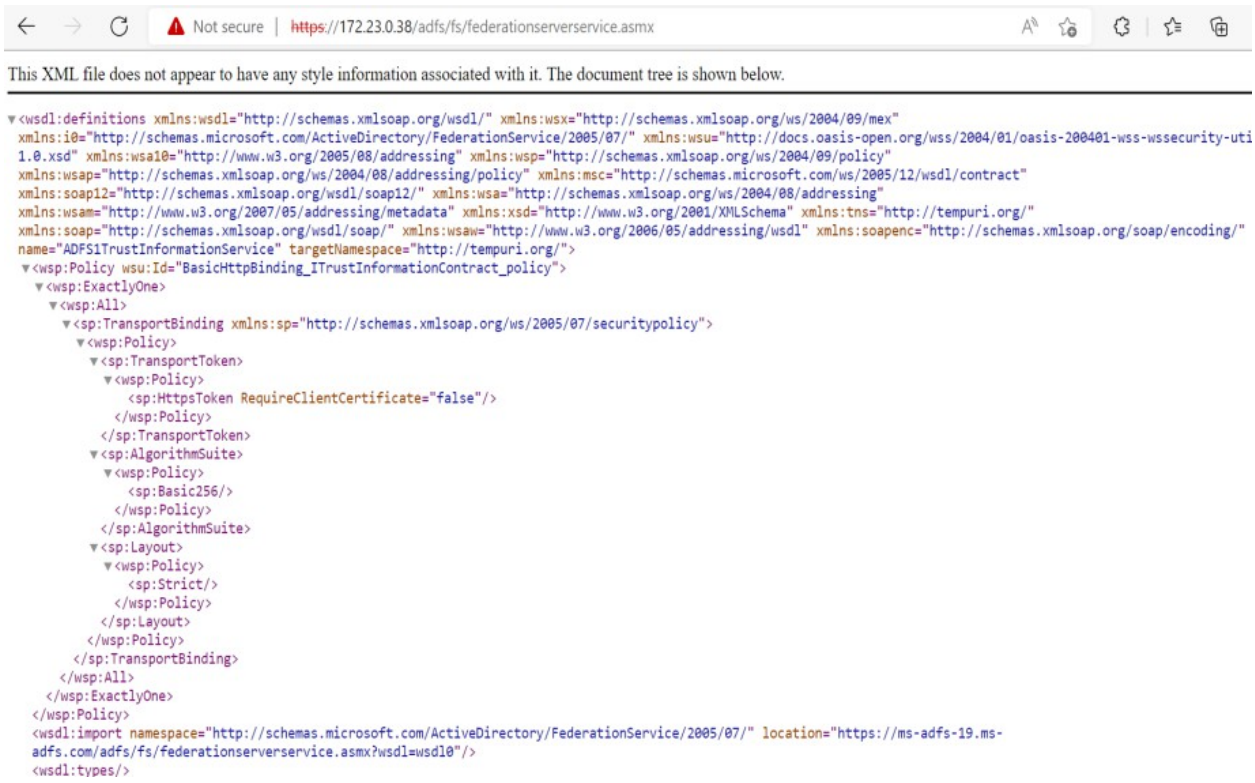

Figure 41 : Federation server verification window

5.9.1 Verify the SSO Operation of AD FS Server

1. Use the following PowerShell command on your AD FS server to enable the Sing Sign on.

›_ PowerShell

```
C:\> Set-AdfsProperties -EnableIdpInitiatedSignOnPage $True
```

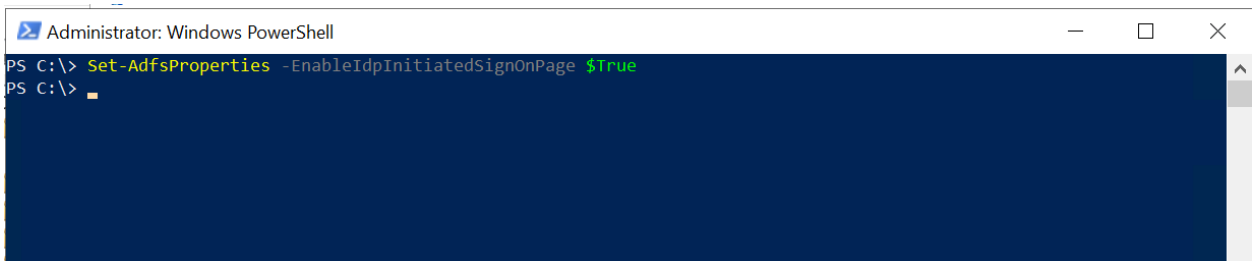

Figure 42 : PowerShell console

2. Open a browser window.
    a. In Internet Explorer, select **Tools**, and then select **Internet Options**.
    b. Select **Security** tab.
    c. Select **Local intranet zone** then click on **Sites**.
    d. Select **Advanced**.
    e. Add the above URL from **Add this website to the zone** option.
    f. Select **Add**, select **Close**, and then select **OK**.
    g. Select the **Advanced** tab. Scroll down and verify that under **Security Enable Integrated Windows Authentication** is checked.
    h. Select **OK** to close the **Internet Options** dialog box.
3. Go to the browser's setting and enable to Java script in order to access the above URL.
4. In the address bar, type the federation server's host name, and then append `/adfs/ls/idpinitiatedsignon.html`. For example: https://<adfs_server>/adfs/ls/idpinitiatedsignon.html.
5. Once the URL is accessible, it will ask for sign in and provide the login credentials. Click **Sign In**.

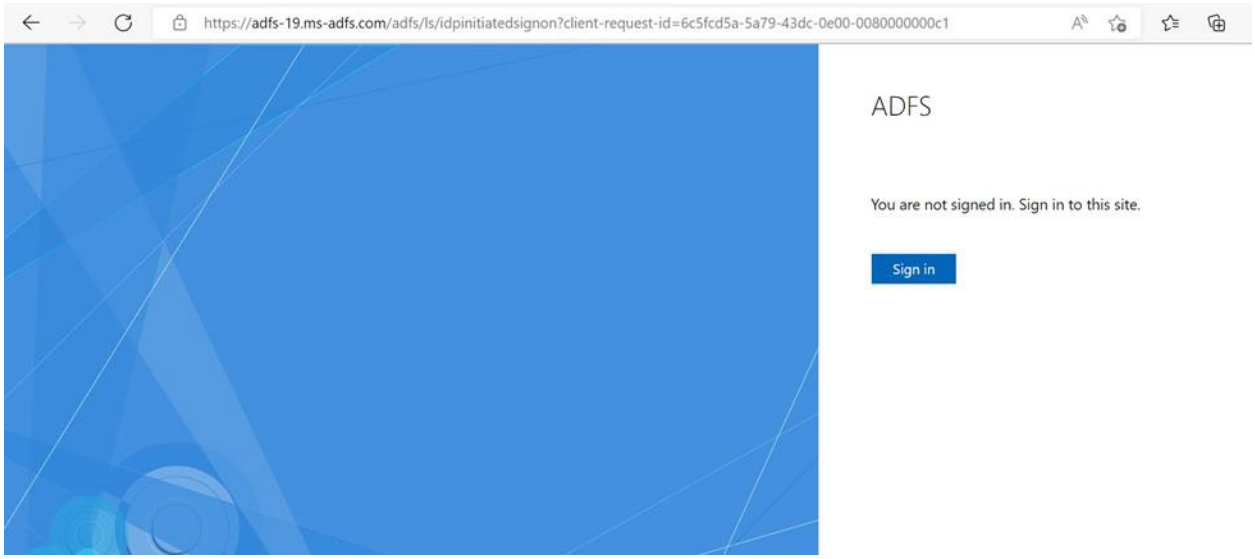

Figure 43 : Microsoft AD FS SSO sign-in page

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

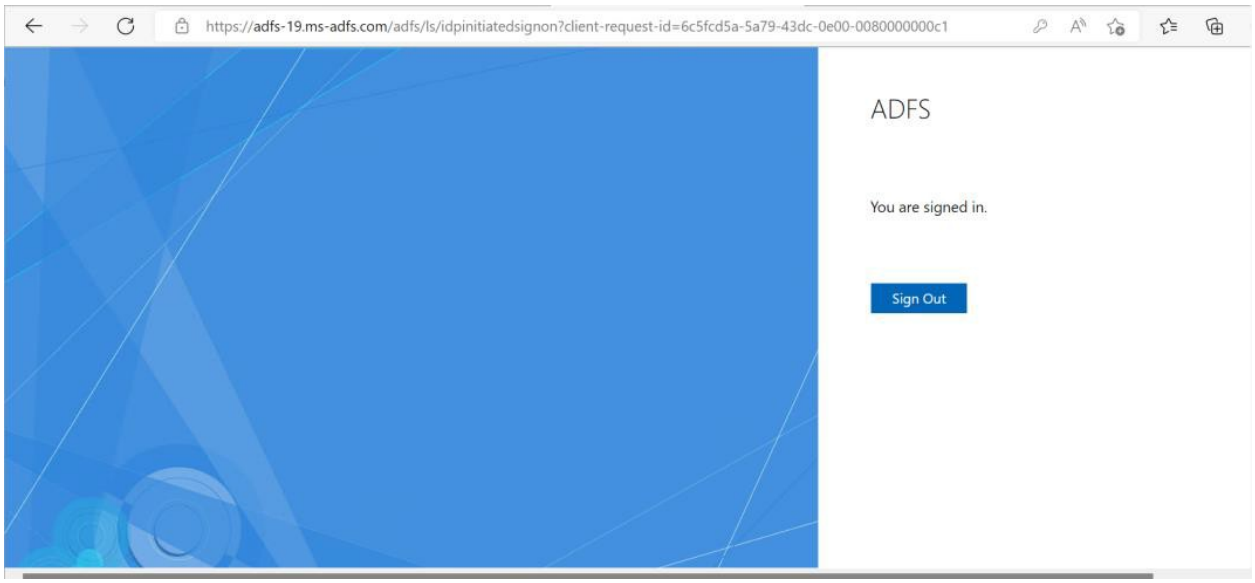

Figure 44 : SSO login page

This completes the integration of ADFS with Utimaco HSM.

6 Troubleshooting

Error	Diagnosis
The service did not respond to the start or control request in a timely fashion.	Make sure that AD FS service isproperly installed and running on your server/machine.
Windows could not start the Active Directory Federation Service on Local Computer. Error 1064: An exception occurred in the service when handling the control request	Restarted the AD FS service Start the Net.Tcp Listener Adapter service.
https://172.23.0.38/adfs/ls/idpinitiatedsignon.ht ml link not working	1. From powershell check if the EnableIdpInitiatedSignonPage parameter is false. If it is, change it to true. 2. Set-AdfsProperties -EnableIdpInitiatedSignonPage $true 3. Also, enable Javascript from browser.

Table 6: List of errors and their diagnoses

7 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: http://hsm.utimaco.com.

8 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer_csadm_Manual/Utimaco IS GmbH	2009-0003
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSP-CNG]	CryptoServer_Manual_CSP_CNG.pdf	2008-0002
[CSLAN5]	CryptoServerLAN_Manual_Systemadministrators.pdf	2018-0004

Table 7: References

9 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
Krefelder Str. 220
52070 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.