Microsoft CSP/CNG

Integration Guide

CryptoServer HSM

4.10

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	2026-05-29
Status	PUBLISHED
Document No.	IG-2026-0051

Table of Contents

1 Introduction

Most of today's corporate IT environments use Microsoft Operating Systems and their Active Directory. Microsoft provides different features to secure the infrastructure by various roles and services. The main task of all these applications is to store private keys. By default, these are located on the hard drive of the system and are thus not protected from attacks. Hardware Security Modules (HSMs) are used to provide a secure storage environment for the keys by employing physical and logical security measures.

This integration guide provides an explanation of the methods in which an HSM can be integrated with various features of Microsoft Server Operating Systems.

1.1 Certificate Authority

A Certification Authority (CA) is a point of trust in your IT environment. The keys of this CA must be protected with the highest available methods, but must also be accessible to an organization's security officer(s) (SO) in the most convenient way. A security officer, for example, uses a CA to generate digital user certificates and certificates for computer management. If anyone has access to the root certificate, they are able to set up an identical CA. For this purpose, Utimaco is able to protect the keys from misuse. The keys are generated inside secure and protected memory of the Utimaco HSM. From the CNG key storage provider perspective, the generation of the keys is completely transparent.

1.2 Online Certificate Status Protocol Service (OCSP)

The Online Certificate Status Protocol (OCSP) is a protocol used to determine whether a certificate has been revoked by the issuing CA. When a certificate is received by SSL/TLS, the client checks the certificate revocation lists (CRLs) of the publisher to determine whether a certificate is still valid. These lists are not suitable for a quick check, however, because they can be large and need to be downloaded from the issuer. Therefore, systems using OCSP obtain the status of a specific certificate from the publisher that will use an OCSP Responder, to provide the up-to-date status of the certificate being checked.

1.3 Host Guardian Service (HGS)

With Windows Server 2016, Microsoft publishes a new security feature for Hyper-V; the so called Host Guardian Service. In addition to protecting hosts or other virtual machines from a virtual

machine (VM) running malicious software, it is also necessary to protect virtual machines from a compromised host.

To protect against compromised fabric, Windows Server 2016 Hyper-V introduces “shielded” VMs. A shielded VM is a generation 2 VM (supported on Windows Server 2012 and later) that has a virtual TPM, is encrypted using BitLocker and can only run on healthy and approved hosts in the fabric. Shielded VMs and guarded fabric enable cloud service providers or enterprise private cloud administrators to provide a more secure environment for tenant VMs. A guarded fabric consists of:

- 1 Host Guardian Service (HGS) cluster.
- 1 or more guarded hosts.
- A set of shielded virtual machines.

When a tenant creates shielded VMs that run on a guarded fabric, the Hyper-V hosts and the shielded VMs themselves are protected by the HGS. The HGS provides two distinct services: attestation and key protection. The attestation service ensures only trusted Hyper-V hosts can run shielded VMs, while the key protection service provides the keys necessary to power them on and to share them with other guarded hosts. The keys which are used by the key protection service can be securely stored in the HSM. This prevents even Administrators with full access to the system from running shielded VMs on a non-guarded fabric.

1.4 Rights Management Services (RMS)

Active Directory Rights Management Services (AD RMS) and the AD RMS client enables the improvement of the security strategy of a company by protecting information through persistent usage policies. These policies are always applied to data even when moved. Using AD RMS, it is possible to prevent sensitive information (such as financial reports, product specifications, customer data, and confidential e-mails) from deliberately or accidentally falling into the wrong hands.

Providing an AD RMS system gives organizations the following benefits:

1. Protection of confidential information.

   Applications such as word processors, e-mail clients, and industry applications can be activated for AD RMS to protect sensitive information. Users can define who is allowed to open, change, print, forward, or perform other actions related to the information.

Organizations can create custom templates for usage guidelines (such as “Confidential - WriteProtected”) that can be applied directly to the information.

1. Durable protection.

AD RMS improves existing, perimeter-based security solutions (such as firewalls and access control lists for optimized protection of information) by locking the usage rights in the document itself. Thus, it is possible to control how the information itself is used after being opened by a particular user.

1. Flexible and customizable technology.

Independent software vendors (ISVs) and developers can enable applications for AD RMS. Information protection cna therefore be extended into server-based solutions that can include, for example, document and data record management, e-mail gateways and archiving systems, automated workflows and content audits.

2 Utimaco CSP/CNG Installation

The following chapter describes how to install Utimaco CSP/CNG on the Windows Server. If you need detailed information about installation and usage of Utimaco CSP/CNG, please have look at our CNG documentation, located in the product CD at `\Documentation\Crypto_APIs\CSP-CNG\CryptoServer_Manual_CSP_CNG.pdf`.

2.1 Hardware and Software Requirements

The following hardware and software versions are tested:

HSM Model (tested)

Utimaco CryptoServer Se-Series,

Utimaco CryptoServer Se-Gen2-Series

Utimaco CryptoServer CSe-Series

HSM Firmware

Utimaco SecurityServer Product CD 4.10 or higher

OS

Windows Server 2012 R2

Windows Server 2016

The general configuration of the CSP/CNG API differs since product CD 4.10. Please check the CNG API documentation on the product CD 4.10 as well.

2.2 Installation and Configuration of Utimaco Providers

The CryptoServer installer software CryptoServerSetup-X.XX.X.X.exe, which you can find on the delivered product CD, automatically copies the necessary files and registers the provider. The CSP/CNG Interface must be selected when running the installer.

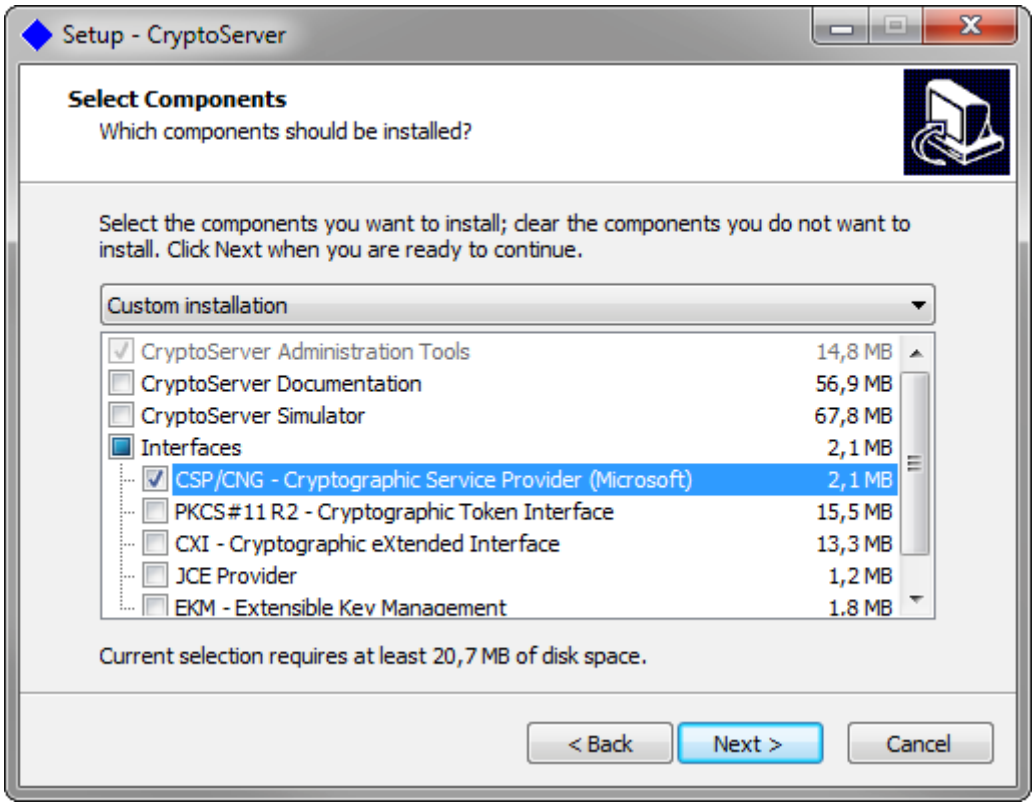

Figure 1 : CryptoServer Setup - Components Selection

It is recommended to use a separate machine for the simulator. You can reach the simulator with 3001@<IP-ADDRESS>. If you want to use the simulator on the same machine, please select the CryptoServer Simulator as well when running the installer.

If not already done, generate a new cryptographic user (level 2 in group 0) with rights in the required CXI group. Open the configuration file for the CSP/CNG provider. The environment variable `CS_CNG_CFG` contains the path and name of the configuration file. It is set by default during the host software installation to `C:\ProgramData\Utimaco\CNG\cs_cng.cfg`. Edit this file for your installation. Most important parameters are described here. You can find a detailed description about all parameters in the document CryptoServer_Manual_CSP_CNG.pdf, located in the product CD at `\Documentation\Crypto_APIs\CSP-CNG\CryptoServer_Manual_CSP_CNG.pdf`.

Parameter	Description
KeysExternal	Specifies the type of the key storage: internal or external. This setting is of type Boolean. If `KeysExternal = true`, the keys are only read and written from/to an external key storage, i.e., a key database outside the CryptoServer and protected with the Master Backup Key of the CryptoServer. If `KeysExternal = false`, the keys are only read and written from/to the internal key database of the CryptoServer.
KeyStore	Specifies the path to the external key storage (default `C:\ProgramData\Utimaco\CNG\keys`). This parameter shall be set if `KeysExternal = true.` The directory must be created by the user and be given appropriate rights. The filename of the key storage is appended automatically by the CNG provider.
ExportPolicy	Defines which export properties cannot be set by a CNG user. **0**: CSP keys are exportable as plaintext. **1**: CSP keys can be exported when wrapped with another key. **2**: CSP key export is denied completely.

Parameter	Description
Group	Defines the key group, which is assigned to new keys and to which keys shall belong in order to be accessible to the CryptoServer CSP/CNG provider.
Device	Specifies the device address of the CryptoServer device to connect to the CSP/CNG provider. This parameter can only specify a single device address per statement. There might be multiple `Device=` statements in the CSP/CNG provider configuration file. The first `Device=` statement defines the default device. A connection to the next device(s) is automatically requested if the previous one(s) does not respond. Valid device specifiers: `Device=PCI:0` for a CryptoServer PCIe plug-in card. `Device=3001@127.0.0.1` for the CryptoServer Simulator. `Device=<IPv4 or IPv6 address>` for a CryptoServer LAN appliance.

Parameter	Description
Login	Specifies the authentication credentials for the CryptoServer CNG-user, who is the only user permitted to generate and access cryptographic keys. The exact syntax of the different authentication types is described in the following subchapter.

2.2.1 Authentication Mechanisms of Login Parameter

2.2.1.1 HMAC password

Login = "username,password"

2.2.1.2 RSA Signature

- stored in a keyfile:

Login = "username,RSASign=filename#password"

- stored in a smartcard; PIN pad is connected to the host computer:

Login = "username,RSASign=:cs2:cyb:USB0#PIN" for REINER SCT cyber Jack

Login = "username,RSASign=:cs2:cjo:USB0#PIN" for REINER SCT cyber Jack One

Login = "username,RSASign=:cs2:auto:USB0#PIN" for both pin pads

- stored in a smartcard; PIN pad is is directly connected to the CryptoServer:

Login = "username,RSASC=:cs2:cyb:USB0#PIN" for REINER SCT cyber Jack

Login = "username,RSASC=:cs2:cjo:USB0#PIN" for REINER SCT cyber Jack One

Login = "username,RSASC=:cs2:auto:USB0#PIN" for both pin pads

2.2.1.3 ECDSA Signature

- stored in a keyfile:

Login = "username,ECDSA=filename#password"

- stored in a smartcard; PIN pad is connected to the host computer:

Login = "username,ECDSA=:cs2:cyb:USB0#PIN" for REINER SCT cyber Jack

Login = "username,ECDSA=:cs2:cjo:USB0#PIN" for REINER SCT cyber Jack One

Login = "username,ECDSA=:cs2:auto:USB0#PIN" for both pin pads

Optionally, the PIN for smartcard authentication can be given with a preceding # for automatic login. If the PIN is not present, the user must enter it via the keyboard of the PIN pad, e.g. Login = "username,RSASign=:cs2:cyb:USB0".

2.3 Checking the Installation

You can test the configuration with `cngtool`. If you get something similar to the following output, everything works fine. Otherwise you must check your configuration.

›_ Console

```
C:\> cngtool listkeys
------------------------------------------------------------
Provider          : Utimaco CryptoServer Key Storage Provider
Device            : 192.168.0.1
Group             : CNG
Mode              : Internal Key Storage
------------------------------------------------------------
Index  AlgId       Size  Group       Name        Spec
------------------------------------------------------------
```

3 Utimaco CSP/CNG Migrations

In some cases, it is necessary to migrate from a software to a hardware provider, or from an older installation to the new CNG version. This chapter describes the following cases:

- Migration from Microsoft Software Provider to Utimaco CNG Provider 2.x.
- Migration from Utimaco CSP/CNG Provider 1.x to Utimaco CSP/CNG Provider 2.x.

3.1 Microsoft Software Provider to Utimaco CNG Provider 2.x

This part describes the scenario where a user of the Microsoft Software Provider wants to migrate the existing keys into the Utimaco CryptoServer using the Utimaco CNG Provider 2.x.

There are two ways to migrate an existing CA. Either use the existing certificate in the new key storage provider, or use the existing private key and renew the certificate. In general, to migrate ADCS to Utimaco CNG, complete the following steps:

1. Back up the CA and configuration.
2. Install the CryptoServer hardware.
3. Install the CryptoServer software.
4. Import the private key to your CryptoServer HSM.
5. Reconfigure the CA.
6. Test and clean up the procedures.

In this guide, only the reusing of an existing certificate is described.

3.1.1 Back up the CA and configuration

For migrating the CA, it could be required to remove the complete ADCS role. Therefore, it is necessary and recommended to create a backup of the certificate database, the CA registry settings, and the CA certificate with the private key of the CA. To do so, we refer to the guidelines provided in the Microsoft TechNet database. In the following, example is shown for a backup of a CA.

1. Open a PowerShell with administrator rights and create a directory for the backup at your preferred location.

2. Back up the certification database.

›_ PowerShell

```
PS C:\> certutil -backupdb C:\backupCA
```

3. Back up the private key and the CA certificate. Enter a secure password as the symmetric key to protect the PKCS#12 file.

›_ PowerShell

```
PS C:\> certutil -backupKey C:\backupCA
Enter new password:
Confirm new password:
```

4. Back up the CA registry settings.

›_ PowerShell

```
PS C:\> reg export HKLM\SYSTEM\CurrentControlSet\services\CertSvc \
C:\backupCA\CAregistry.reg
```

5. Stop the CA service.

›_ PowerShell

```
PS C:\> Stop-service certsvc
```

3.1.2 Install CryptoServer Hardware

For the installation and setup of the CryptoServer hardware, please refer to:

1. CryptoServerPCIe_Se-Series_Gen2_Operating_Manual.pdf.
2. CryptoServerPCIe_Se-Series_Operating_Manual.pdf.
3. CryptoServerPCIe_CSe-Series_Operating_Manual.pdf.
4. CryptoServerLAN_V4_Operating_Manual.pdf.

3.1.3 Install CryptoServer Software

Install the CryptoServer software as described in: Utimaco CSP/CNG Installation.

3.1.4 Import the Private Key to the CryptoServer HSM

Before changing the ADCS role configuration to use the CryptoServer, it is necessary to import the private key into the HSM. Please perform the following steps.

1. Open a PowerShell with administrator rights.
2. Import the private key by using the Utimaco command line tool `cngtool` where `<CA-Name>` is the name of your certificate authority. You will be asked for a passphrase. The passphrase is for the decryption key of the PKCS#12 file you set earlier.

›_ PowerShell

```
PS C:\stuff> cngtool Provider="Utimaco CryptoServer Key Storage
Provider" Name=<CA-Name> spec=0 export=deny password=ask
importkey="<Your CA cert/key PFX file>"
```

3. Now you can check if the import was performed correctly.

›_ PowerShell

```
PS C:\stuff> cngtool listkeys
------------------------------------------------------------
Provider           : Utimaco CryptoServer Key Storage Provider
Device             : 192.168.0.1
Group              : cng
Mode               : Internal Key Storage
------------------------------------------------------------
Index  AlgId       Size  Group             Name               Spec
-------------------------------------------------------------------
1      RSA         4096 UTIMACO-HSM-CA     UTIMACO-HSM-CA      0
```

If you use the internal key storage of the HSM, and you have a cluster of HSMs, you have to synchronize the `CXIKEY.db` manually.

3.1.5 Reconfigure the CA

The next steps reconfigure the CA while maintaining the existing certificate. In this case it is necessary to link the existing certificate with the new CNG key storage provider. Before reconfiguring the CA it is recommended to delete the existing private key in the old storage provider. To do so, carry out the following steps.

1. Open a PowerShell with administrator rights.
2. Get the details of your CA certificates, by using the Microsoft command line tool `certutil –store my <Your CA common name>` and make a note of the value for Cert Hash.

›_ PowerShell

```
PS C:\>certutil -store my UTIMACO-HSM-CA
my "Personal"
================ Certificate 0 ================
Serial Number: 43ef6081aa8b6bac45ef49ccb278684c
Issuer: CN=UTIMACO-HSM-CA, DC=utimaco, DC=local
NotBefore: 10.12.2015 10:09
NotAfter: 10.12.2020 10:19
Subject: CN=UTIMACO-HSM-CA, DC=utimaco, DC=local
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 6b 17 b8 1e ea db 70 d6 c2 a0 51 36 de ed 14 f5 4c 9b
...
Key Container = UTIMACO-HSM-CA
Unique container name:
084d751dc1f9bd60ae27b5b68c2b7a67_43b39732-c78b...
Provider = Microsoft Base Cryptographic Provider v1.0
Signature test passed
CertUtil: -store command completed successfully.
```

3. Delete the existing CA certificate and private key.

    a. Change the path to the local certificate store.

›_ PowerShell

```
PS C:\> cd cert:\localmachine\my
```

    b. Using the value for Cert Hash that you noted down in step 2, run the following command to delete the certificate and private key from the local machine.

›_ PowerShell

```
PS Cert:\localmachine\my> Del -deletekey
6b17b81eeadb70d6c2a05136de...
```

c. Repeat the previous step for all CA certificates that were identified when you ran the `certutil` command.

4. Migrate the CA certificate to the Utimaco CNG provider by running the following command:

›_ PowerShell

```
PS C:\> certutil -csp "Utimaco Cryptoserver Key Storage Provider"
-importpfx <Your CA cert/key PFX file>
```

5. Link the existing CA certificate with the private key in the new key storage by using the Microsoft command line tool `certutil -f -repairstore -csp "Utimaco Cryptoserver Key Storage Provider" my <Cert Hash>`.

›_ PowerShell

```
PS C:\> certutil -f -repairstore -csp "Utimaco Cryptoserver Key \
Storage Provider" my 6b17b81eeadb70d6c2a05136de...
my "Personal"
================ Certificate 0 ================
Serial Number: 43ef6081aa8b6bac45ef49ccb278684c
Issuer: CN=UTIMACO-HSM-CA, DC=utimaco, DC=local
NotBefore: 10.12.2015 10:09
NotAfter: 10.12.2020 10:19
Subject: CN=UTIMACO-HSM-CA, DC=utimaco, DC=local
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 6b 17 b8 1e ea db 70 d6 c2 a0 51 36 de ed 14 f5 4c 9b
...
Key Container = UTIMACO-HSM-CA
Unique container name: 20091850E4CF622C2FB19079CC36CF82
Provider = Utimaco CryptoServer Key Storage Provider
Private key is NOT exportable
Encryption test passed
Signature test passed
CertUtil: -repairstore command completed successfully.
```

6. Import registry settings for the CSP.

a. Create a registry file named `Csp.reg` that has the following values, and replace `<Your CA Common Name>` with your CA common name:

Csp.cfg

```
[HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Your
CA Common Name>\CSP]
"ProviderType"=dword:00000000
"Provider"="Utimaco Cryptoserver Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGHashAlgorithm"="SHA1"
```

b. Before you save the file, confirm that you are using `SHA1` by running one of the following commands:

i. In case the old CA used a CSP provider:

›_ PowerShell

```
PS C:\> certutil –v –getreg ca\csp\HashAlgorithm
HashAlgorithm REG_DWORD = 8004 (32772)
CALG_SHA1
Algorithm Class: 0x8000(4) ALG_CLASS_HASH
Algorithm Type: 0x0(0) ALG_TYPE_ANY
Algorithm Sub-id: 0x4(4) ALG_SID_SHA1
CertUtil: -getreg command completed successfully.
```

If you do not see `SHA1` in your output, modify the `CNGHashAlgorithm` key value in the file to have the appropriate name.

ii. In case the old CA used a CNG provider:

›_ PowerShell

```
PS C:\> certutil -v -getreg ca\csp\CNGHashAlgorithm
CNGHashAlgorithm REG_SZ = SHA256
CertUtil: -getreg command completed successfully.
```

If you do not see `SHA1` in your output, modify the `CNGHashAlgorithm` key value in the file to have the appropriate name.

c. Save the file and then run it.

›_ PowerShell

```
PS C:\backupCA> .\Csp.reg
```

7. Import registry settings for the CSP encryption settings.

a. Create a registry file named `EncryptionCsp.reg` that has the following values, and replace `<Your CA Common Name>` with your CA common name:

```
[HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Your
CA Common Name>\EncryptionCSP]
"ProviderType"=dword:00000000
"Provider"="Utimaco Cryptoserver Key Storage Provider"
"CNGPublicKeyAlgorithm"="RSA"
"CNGEncryptionAlgorithm"="3DES"
"MachineKeyset"=dword:00000001
"SymmetricKeySize"=dword:000000a8
```

b. Before you save the file, confirm that you are using `3DES` by running one of the following commands:

i. In case the old CA used a CSP provider:

›_ PowerShell

```
PS C:\> certutil –v –getreg ca\encryptioncsp\EncryptionAlgorithm
EncryptionAlgorithm REG_DWORD = 6603 (26115)
CALG_3DES
Algorithm Class: 0x6000(3) ALG_CLASS_DATA_ENCRYPT
Algorithm Type: 0x600(3) ALG_TYPE_BLOCK
Algorithm Sub-id: 0x3(3) ALG_SID_3DES
CertUtil: -getreg command completed successfully.
```

If you do not see `3DES` in your output, modify the `CNGEncryptionAlgorithm` key value in the file to have the appropriate name.

ii. In case the old CA used a CNG provider:

›_ PowerShell

```
PS C:\> certutil –v –getreg
ca\encryptioncsp\CNGEncryptionAlgorithm
CNGEncryptionAlgorithm REG_SZ = 3DES
CertUtil: -getreg command completed successfully.
```

If you do not see `3DES` in your output, modify the `CNGEncryptionAlgorithm` key value in the file to have the appropriate name.

c. Save the file and then run it.

›_ PowerShell

```
PS C:\backupCA> ./EncryptionCsp.reg
```

8. Optional but strongly recommended: Change the CA hash algorithm to SHA-2 family, for example SHA256.

›_ PowerShell

```
PS C:\> certutil -setreg ca\csp\CNGHashAlgorithm SHA256
New Value:
CNGHashAlgorithm REG_SZ = SHA256
CertUtil: -setreg command completed successfully.
```

9. Start the CA service again.

›_ PowerShell

```
PS C:\> Start-Service CertSvc
```

3.1.6 Test and Cleanup Procedures

After the migration has been completed you should verify that everything works correctly.

1. Run the following command on the CA to verify that CA service is up and ready to receive requests.

›_ PowerShell

```
PS C:\> certutil –ping
Connecting to HSM-CA.utimaco.local\UTIMACO-HSM-CA ...
Server "UTIMACO-HSM-CA" ICertRequest2 interface is alive (16ms)
CertUtil: -ping command completed successfully.
```

2. Run the command `certutil –store my <Your CA Common Name>` on the CA to verify that the CA is configured with the correct key and provider.

›_ PowerShell

```
PS C:\> certutil -store my UTIMACO-HSM-CA
my "Personal"
================ Certificate 0 ================
Serial Number: 1ee7e741878151a947b6a1771ec46152
Issuer: CN=UTIMACO-HSM-CA, DC=utimaco, DC=local
NotBefore: 10.12.2015 15:59
NotAfter: 10.12.2020 16:09
Subject: CN=UTIMACO-HSM-CA, DC=utimaco, DC=local
Certificate Template Name (Certificate Type): CA
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Template: CA, Root Certification Authority
Cert Hash(sha1): ce cd da 29 05 31 04 82 d0 e0 c7 8c 9f 30 6a fa f0 89
...
Key Container = UTIMACO-HSM-CA
Unique container name: D0A70AB53D75E80677291C6100C2A996
Provider = Utimaco CryptoServer Key Storage Provider
Signature test passed
CertUtil: -store command completed successfully.
```

3. Request and issue a certificate for a user or computer and inspect the resulting certificate details to verify that the certificate shows the correct signature algorithm and signature hash algorithm.

4. Verify that the certificate revocation list can be published and has the correct signature algorithm and signature hash algorithm. Publish the certificate revocation list (CRL) and check the correct signature algorithm by running the following commands on the CA. Please replace `<Your CA Common Name>` with your CA Common Name.

›_ PowerShell

```
PS C:\> certutil –crl
CertUtil: -CRL command completed successfully.
PS C:\> certutil C:\Windows\System32\CertSrv\CertEnroll\
<Your CA Common Name>.crl | findstr /spi algorithm
Signature Algorithm:
Algorithm ObjectId: 1.2.840.113549.1.1.13 sha512RSA
Algorithm Parameters:
Signature Algorithm:
Algorithm ObjectId: 1.2.840.113549.1.1.13 sha512RSA
Algorithm Parameters:
```

If everything works correctly, the migration is completed. Clean up all created exported files and backups used during this migration.

Before you go into production mode, be sure that you remove the backup of the PKCS#12 file from every unsecure data storage.

3.2 Utimaco CSP/CNG Provider 1.x to Utimaco CSP/CNG Provider 2.x

You can find all migration steps and information in our API documentation located in the product CD at `\Documentation\Crypto_APIs\CSP-CNG\CryptoServer_Manual_CSP_CNG.pdf`. This documentation describes all steps to migrate from CSP 1.x to CSP 2.x respectively CNG 1.x to CNG 2.x. If you want to migrate from CSP 1.x to CNG 2.x please contact our support.

4 Active Directory Certificate Service (ADCS)

Before you can integrate the Utimaco CryptoServer with the Microsoft Windows Server Certification Authority, complete the Utimaco CSP/CNG Installation.

4.1 Install Microsoft Windows Server Active Directory Certificate Services

In this guide, we describe how to install ADCS via PowerShell. Thus, you can use this guide for GUI as well as core installations. For other methods of installing ADCS, please check the Microsoft TechNet website.

Managing the private key ACL is not possible in a pure core installation of Microsoft Windows Server. Please follow the instructions to install ADCS.

1. Open a PowerShell with administrator rights.
2. Install the new role **Adcs-Cert-Authority**.

›_ PowerShell

```
PS C:\>Install-WindowsFeature Adcs-Cert-Authority
-IncludeManagementTools
```

3. Now, install the certification authority. Adjust all parameters to your installation. A complete description about all the parameters can be found in the TechNet documentation library.

```
Parameter Set: NewKeyParameterSet
Install-AdcsCertificationAuthority
[-AllowAdministratorInteraction]
[-CACommonName <String>
[-CADistinguishedNameSuffix <String> ]
[-CAType <CAType> ]
[-Credential <PSCredential> ]
[-CryptoProviderName <String> ]
[-DatabaseDirectory <String> ]
[-Force]
[-HashAlgorithmName <String> ]
[-IgnoreUnicode]
[-KeyLength <Int32> ]
[-LogDirectory <String> ]
[-OutputCertRequestFile <String> ]
[-OverwriteExistingCAinDS]
[-OverwriteExistingDatabase]
[-OverwriteExistingKey]
[-ParentCA <String> ]
[-ValidityPeriod <ValidityPeriod> ]
[-ValidityPeriodUnits <Int32> ]
[-Confirm]
[-WhatIf]
[ <CommonParameters>]
```

In this case we install ADCS with a new key and a new certificate. The following command is an example of how to install ADCS.

Be sure that you use one of the following Utimaco providers:

- 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.

›_ PowerShell

```
PS C:\>Install-AdcsCertificationAuthority -AllowAdministratorInteraction
-CACommonName rootca.hsm.local -CAType EnterpriseRootCA
-CryptoProviderName "RSA#Utimaco Cryptoserver Key Storage Provider"
-HashAlgorithmName SHA512 -KeyLength 4096 -ValidityPeriod Years
-ValidityPeriodUnits 5
```

4. Start the certificate authority service.

›_ PowerShell

```
PS C:\>Start-Service CertSvc
```

4.1.1 Testing and cleanup procedures

After the installation has been completed, you should verify that everything works correctly.

1. Run the following command on the CA to verify that the CA service is up and ready to receive requests.

```
PS C:\> Certutil -ping
Connecting to Win2k12RootCA.hsm.local\rootca.hsm.local ...
Server "rootca.hsm.local" ICertRequest2 interface is alive (15ms)
CertUtil: -ping command completed successfully.
```

2. Run the command `Certutil –store my *` on the CA to verify that the CA is configured for the correct key and provider.

```
PS C:\> certutil -store my *
my "Personal"
================ Certificate 0 ================
Serial Number: 62cb8d6fb4f3b2ac4b8880b2d743166b
Issuer: CN=rootca.hsm.local, DC=hsm, DC=local
NotBefore: 29.03.2017 12:56
NotAfter: 29.03.2022 13:05
Subject: CN=rootca.hsm.local, DC=hsm, DC=local
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): bc 14 ec b1 12 d0 f4 39 db ce 35 50 75 70 ...
Key Container = rootca.hsm.local
Unique container name: D2E5CD8E1AB51DA3B1DE7ACEB0657635
Provider = Utimaco CryptoServer Key Storage Provider
Private key is NOT plain text exportable
Signature test passed
CertUtil: -store command completed successfully.
```

3. Request and issue a certificate for a user or computer, and inspect the resulting certificate details to verify that the certificate shows the correct signature algorithm and signature hash algorithm.

If everything works correctly, the installation is completed.

5 Host Guardian Service

This document will instruct how to integrate the Utimaco CryptoServer into the Microsoft Host Guardian Service.

This guide introduces mainly the configuration steps relevant to the Utimaco CryptoServer. Further information about the complete deployment is available here: https://aka.ms/ShieldedVMs.

5.1 Install Microsoft Host Guardian Service 2016

The first step is to add the HGS role by using the Server Manager or by running the following command in a PowerShell Console:

›_ PowerShell

```
PS C:\> Install-WindowsFeature -Name HostGuardianServiceRole
-IncludeManagementTools -Restart
```

After this, you can install the HGS. It can be installed it in its own new forest or in an existing bastion forest. For more information about it check the complete integration description in Microsoft TechNet.

In the following example we are using an existing forest. Install the HGS using the following command:

›_ PowerShell

```
PS C:\> Install-HgsServer -HgsDomainName 'relecloud.com' -Restart
```

You need to configure the Host Guardian Service with two certificates for encryption and signing purposes. Generate these certificates in your preferred way but be sure that you generated these certificates with the key storage provider; Utimaco CryptoServer Key Storage Provider. One way to generate these certificates is to generate new certificate templates for computer certificates where you define Utimaco CryptoServer Key Storage Provider as the only key storage provider

which can be used in this template. Then you create two files, one each for encryption and for signing, similar to the following example:

```
[NewRequest]
Subject = "CN=HGSencryption.relecloud.com"
Exportable = FALSE
HashAlgorithm = sha256
KeyAlgorithm = RSA
KeyLength = 2048
KeySpec = 1
KeyUsage = 0x01
MachineKeySet = True
ProviderName = "Utimaco CryptoServer Key Storage Provider"
RequestType = PKCS10
SMIME = FALSE
FriendlyName = "HGSencryption"
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.1 ;Server Authentication
OID = 1.3.6.1.5.5.7.3.2 ;Client Authentication
[RequestAttributes]
CertificateTemplate = "Host-Guardian-Server-Certs"
```

```
[NewRequest]
Subject = "CN=HGSsigning.relecloud.com"
Exportable = FALSE
HashAlgorithm = sha256
KeyAlgorithm = RSA
KeyLength = 2048
KeySpec = 1
KeyUsage = 0x80
MachineKeySet = True
ProviderName = "Utimaco CryptoServer Key Storage Provider"
RequestType = PKCS10
SMIME = FALSE
FriendlyName = "HGSsigning"
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.1 ;Server Authentication
OID = 1.3.6.1.5.5.7.3.2 ;Client Authentication
[RequestAttributes]
CertificateTemplate = "Host-Guardian-Server-Certs"
```

Then create a new request of both INF files.

›_ PowerShell

```
Certreq –new RequestPolicy.inf CertReq.req
```

Send/Copy both request files to your certificate authority, and submit these requests.

›_ PowerShell

```
Certreq –submit –config FQDN_CA\CA_Name CertReq.req CertResponse.cer
```

If the requests are submitted, you will get two certificates. Copy these certificates back to your HGS server and accept these certificates.

›_ PowerShell

```
Certreq –accept –config FQDN_CA\CA_Name CertResponse.cer
```

You can check your keys stored inside the HSM with the following command:

›_ PowerShell

```
PS C:\> cngtool listkeys
```

You should see two keys, one for each certificate. This shows that the HGS is secured with the Utimaco CryptoServer.

In the last configuration step you have to initalize the HGS service. You need the thumbprints of both certificates to do this.

›_ PowerShell

```
PS C:\> $Certs = Get-ChildItem Cert:\LocalMachine\My\ -dnsname HGS*
PS C:\> $Certs
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint Subject
---------- -------
4D3F4E749E37B73090C6655FB69A0B7AAA12CF1C CN=HGSsigning.relecloud.com
0F8EAF6A23AD9E0A913A73630CE9D9BCEFD23944 CN=HGSencryption.relecloud.com
PS C:\> $signing = $Certs[0].Thumbprint
PS C:\> $encryption = $Certs[1].Thumbprint
```

Now, you can initialize the HGS service with the following command.

›_ PowerShell

```
PS C:\var> Initialize-HgsServer -HgsServiceName tpmHGS
-SigningCertificateThumbprint $signing -EncryptionCertificateThumbprint
$encryption -TrustTpm
```

Run the Local Machine Certificate Management Console (certlm.msc). Locate the encryption and signing certificates under the **Personal** folder, right-click each of them in turn and verify (or add the permission if necessary to) the service account (e.g. HGSSVC_276CF$) to the list of **Groups and Users** permitted to manage the private keys. **Allow Read** is the only needed permission.

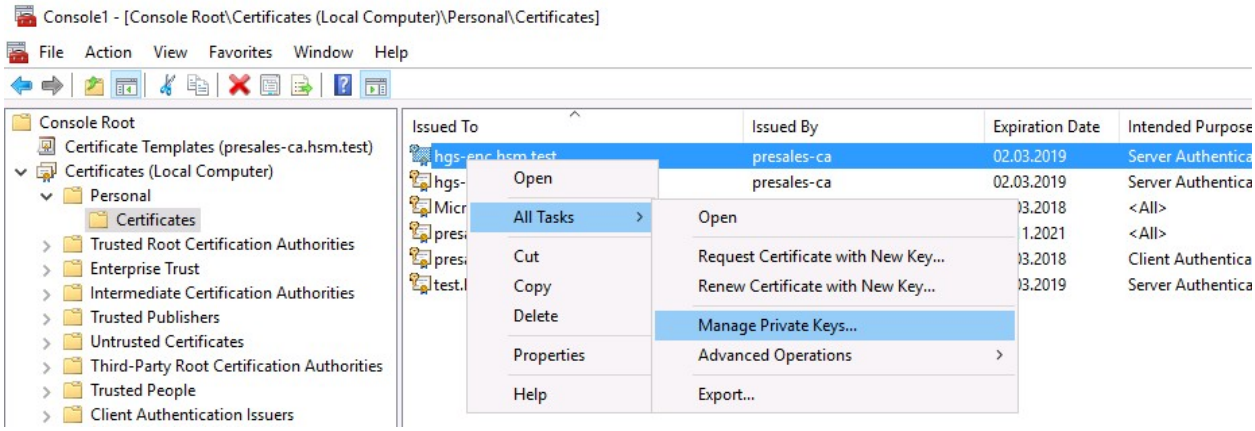

Figure 2 : Menu of Manage Private Keys

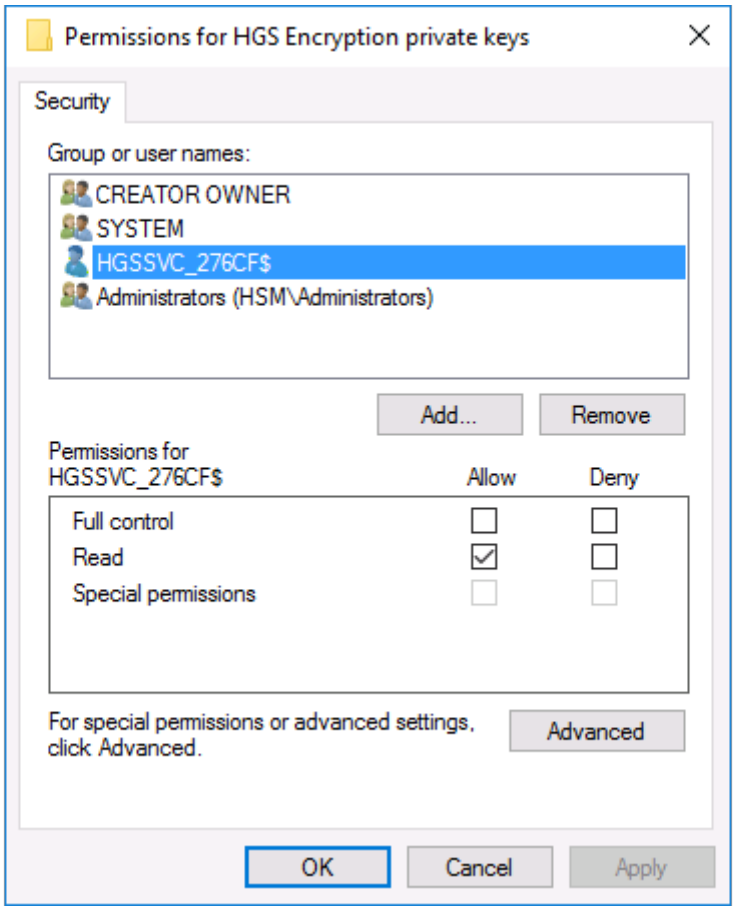

Figure 3 : Security Tab with Permissions for HGS Private Keys

To confirm KPS has access to the private keys of your encryption and signing certificates, run the HGS diagnostics using `Get-HgsTrace`. If any tests fail, be sure to remedy the identified problems before continuing to configure any additional nodes.

›_ PowerShell

```
PS C:\> Get-HgsTrace -RunDiagnostics
```

For any further installation and configuration steps, please refer to the complete TechNet deployment guide which can be found at https://aka.ms/ShieldedVMs.

6 Online Certificate Status Protocol Service

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

6.1 Prepare Certificate Template for OCSP Signing

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

1. Open the **Certificate Authority Manager**.
2. Open the **Certificate Templates Console** by right-clicking on the folder **Certificate Templates** and **Manage**.

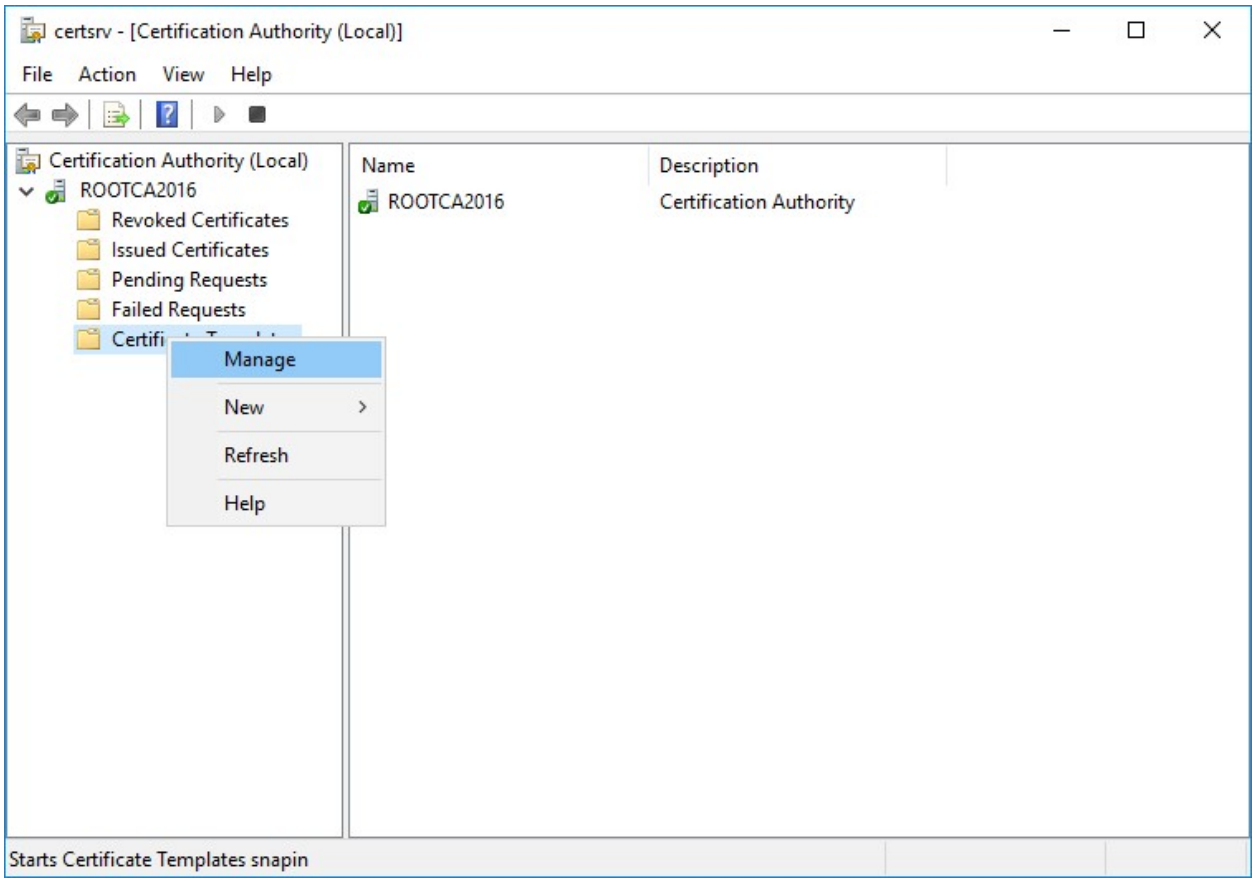

Figure 4 : Manage Certificate Templates

3. Locate the **OCSP Response Signing Certificate**, and click on **Duplicate Template**.

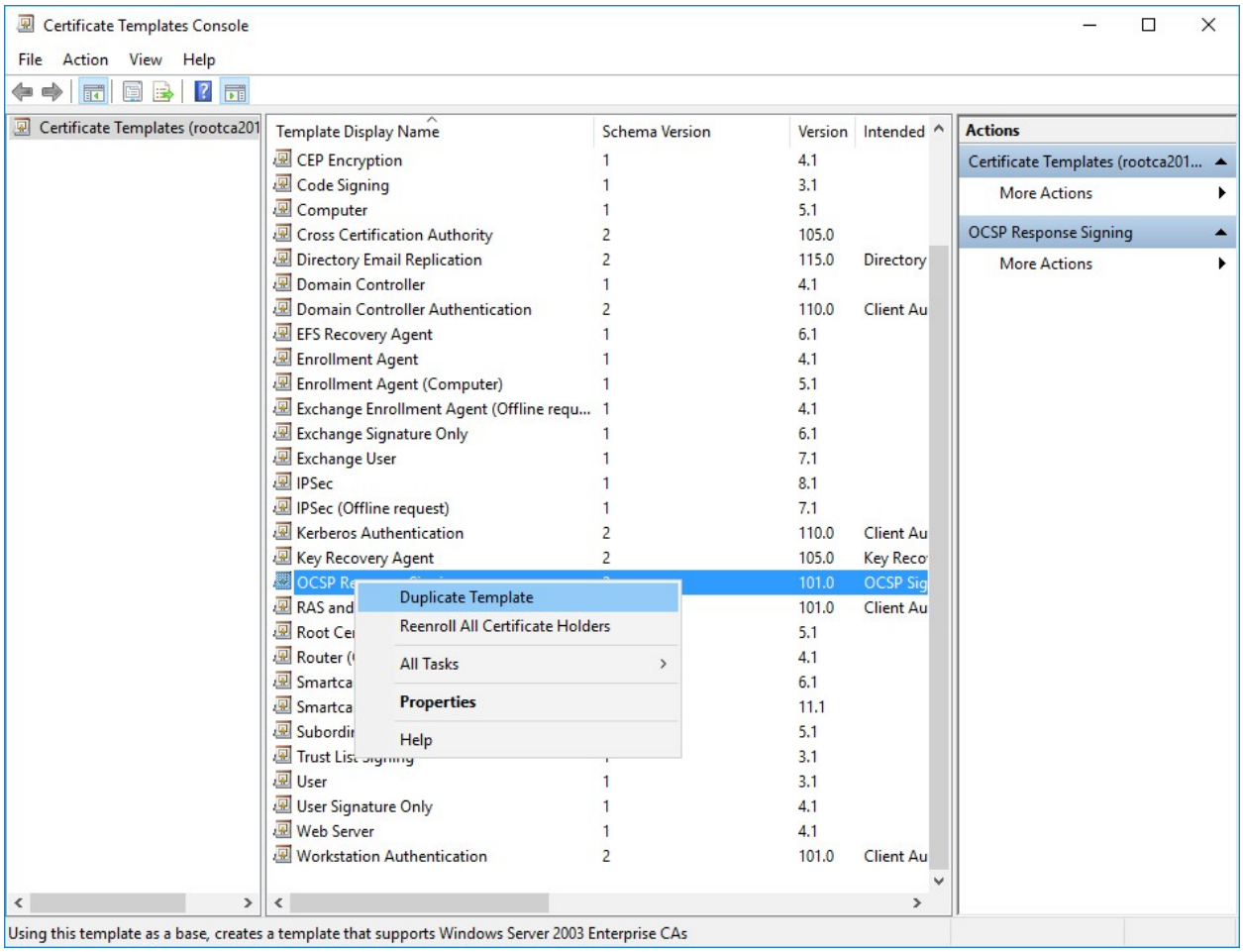

Figure 5 : Duplicate a Certificate Template

4. It is advisable to change this certificate template to reflect your requirements. The following steps are the minimum changes necessary.

    a. In the **General** tab, change the **Template display name** and the **Template name**.

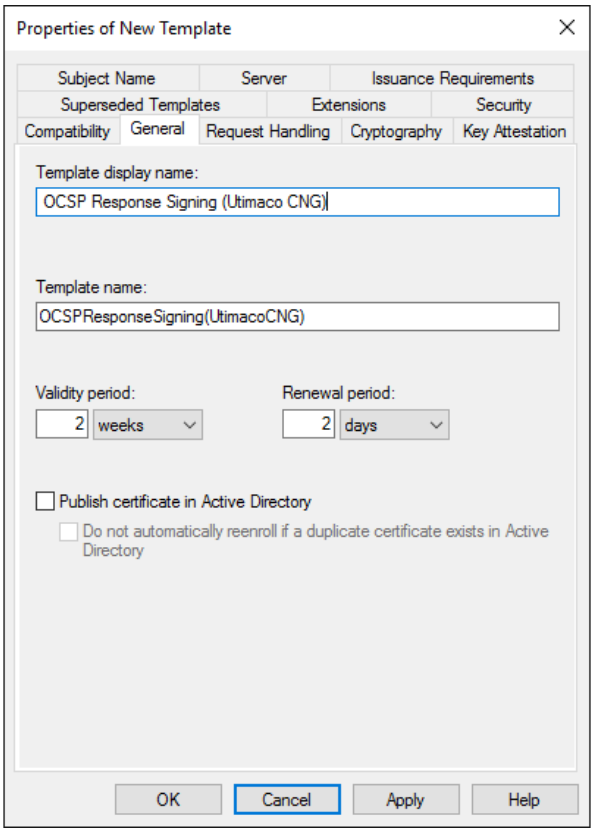

Figure 6 : General Tab of Properties of New Template

b. In the **Cryptography** tab, change the **Provider Category** to **Key Storage Provider**, and check only the **Utimaco CryptoServer Key Storage Provider**.

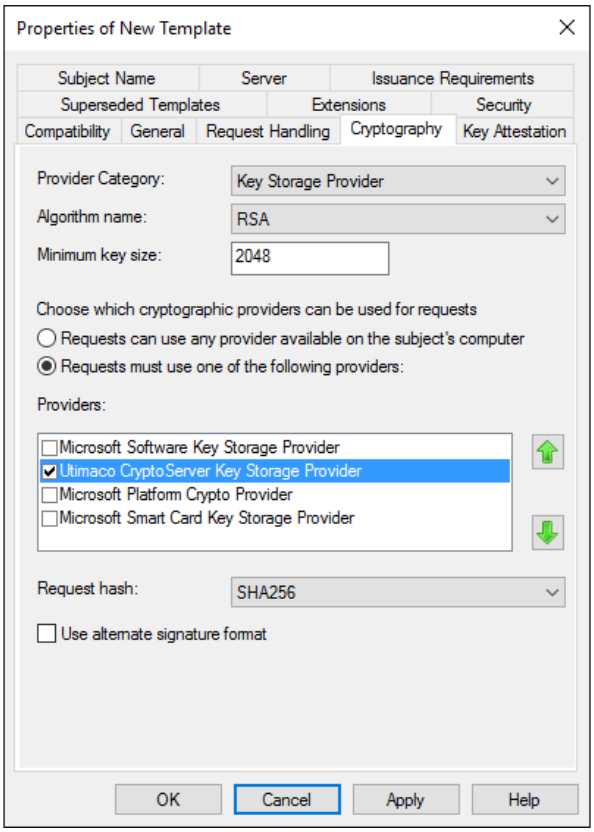

Figure 7 : Cryptography Tab of Properties of New Template

c. In the **Security** tab, add all OCSP servers that will be hosting the OCSP service. Grant the server read and enroll rights.

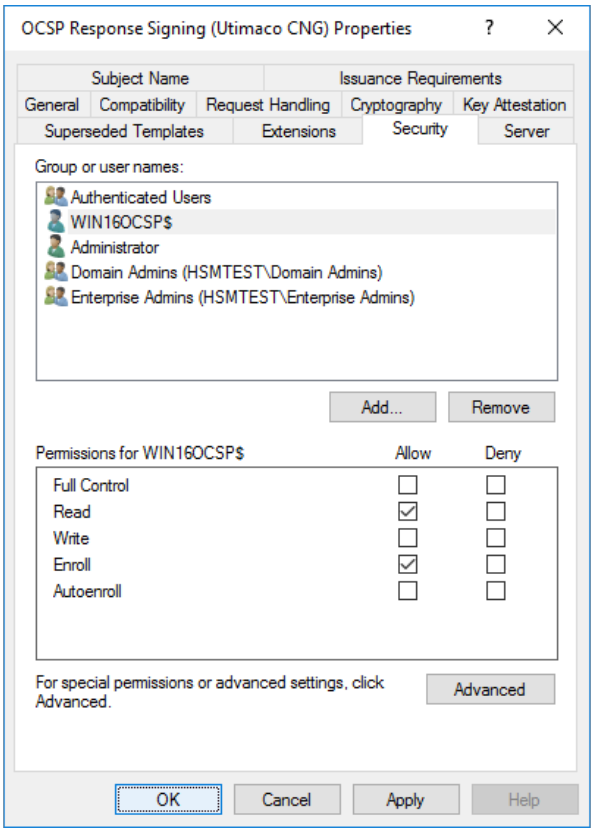

Figure 8 : Security Tab of Properties of New Template

5. After finishing the configuration of the certificate template, confirm with **OK** . Then activate the OCSP certificate template.

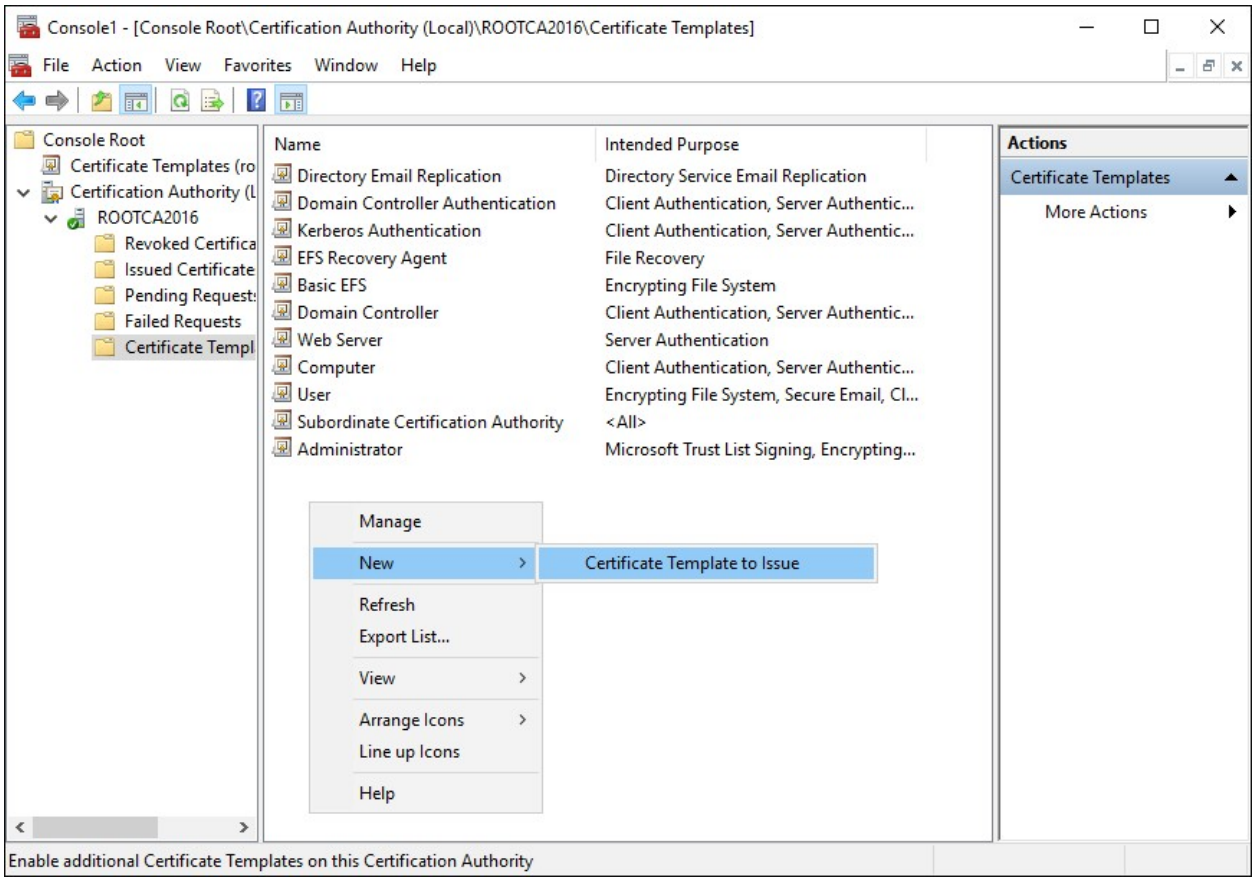

Figure 9 : Certificate Template to Issue

6. Select the newly created certificate template and confirm with **OK**.

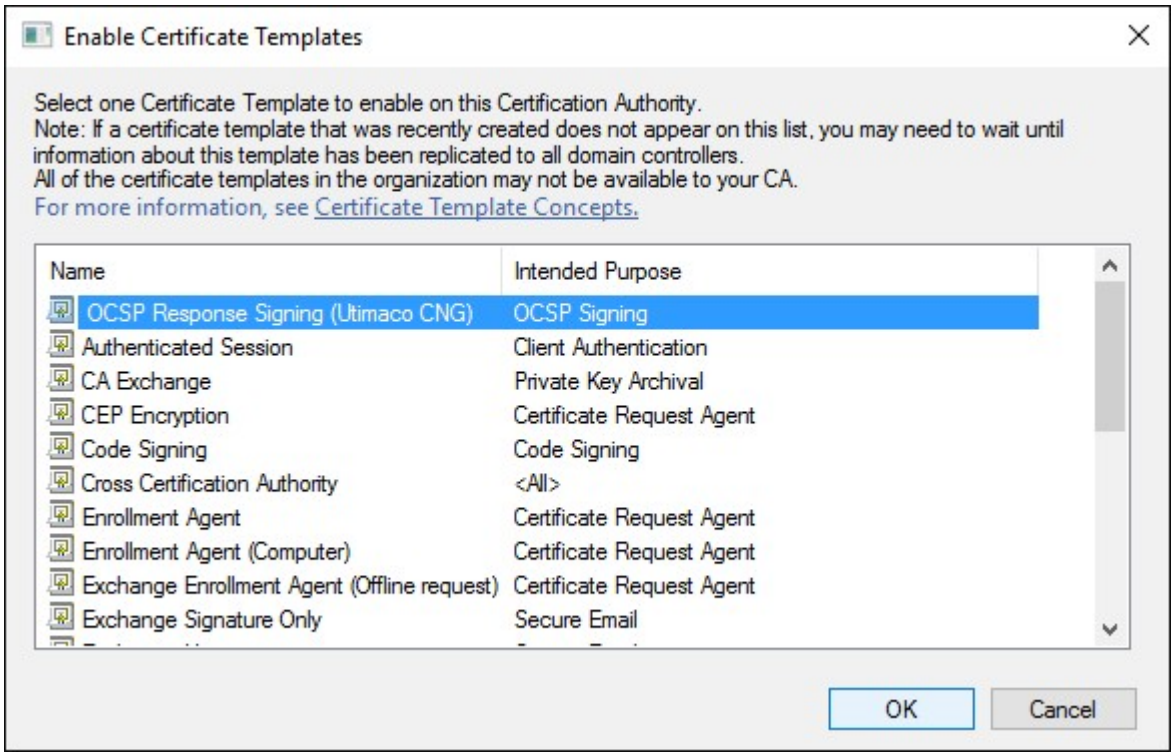

Figure 10 : Enable Certificate Templates

6.2 CA Configuration

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

1. Now, you have to configure the extensions of your CA. Open the properties of your certificate server.

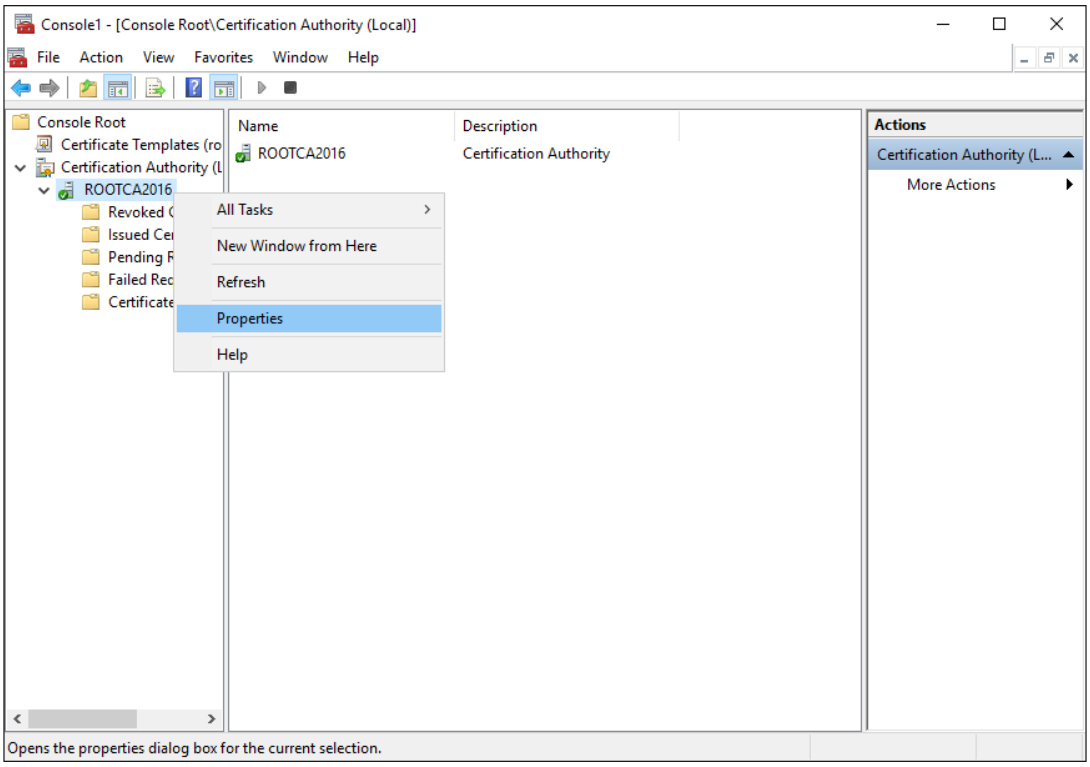

Figure 11 : Properties of a Certification Authority

2. 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>/ocsp`. Select the URL previously entered and tick **Include in the online certificate status protocol (OCSP) extension**.

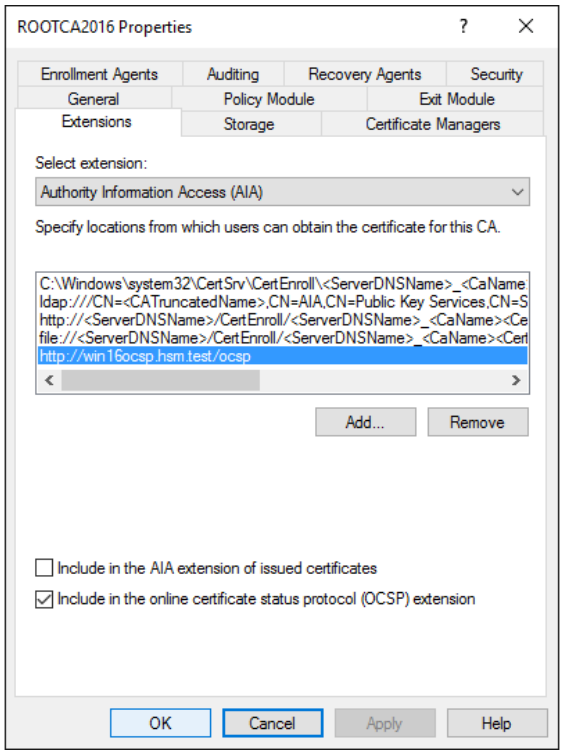

Figure 12 : Extensions Tab of the Certification Authority Properties

6.3 Install and Configure Online Responder

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

1. Open a PowerShell with administrator rights.
2. Add the OCSP role.

›_ PowerShell

```
PS C:\>Install-WindowsFeature Adcs-Online-Cert
```

3. Install and enable the Online Responder service.

›_ PowerShell

```
PS C:\>Install-AdcsOnlineResponder
```

6.4 Make a Revocation Configuration

To use OCSP you have to create a new revocation configuration.

1. Launch the **Online Responder Management console**.
2. Click on **Revocation Configuration**, and then **Action → Add Revocation Configuration**.
3. Enter a name for your configuration.

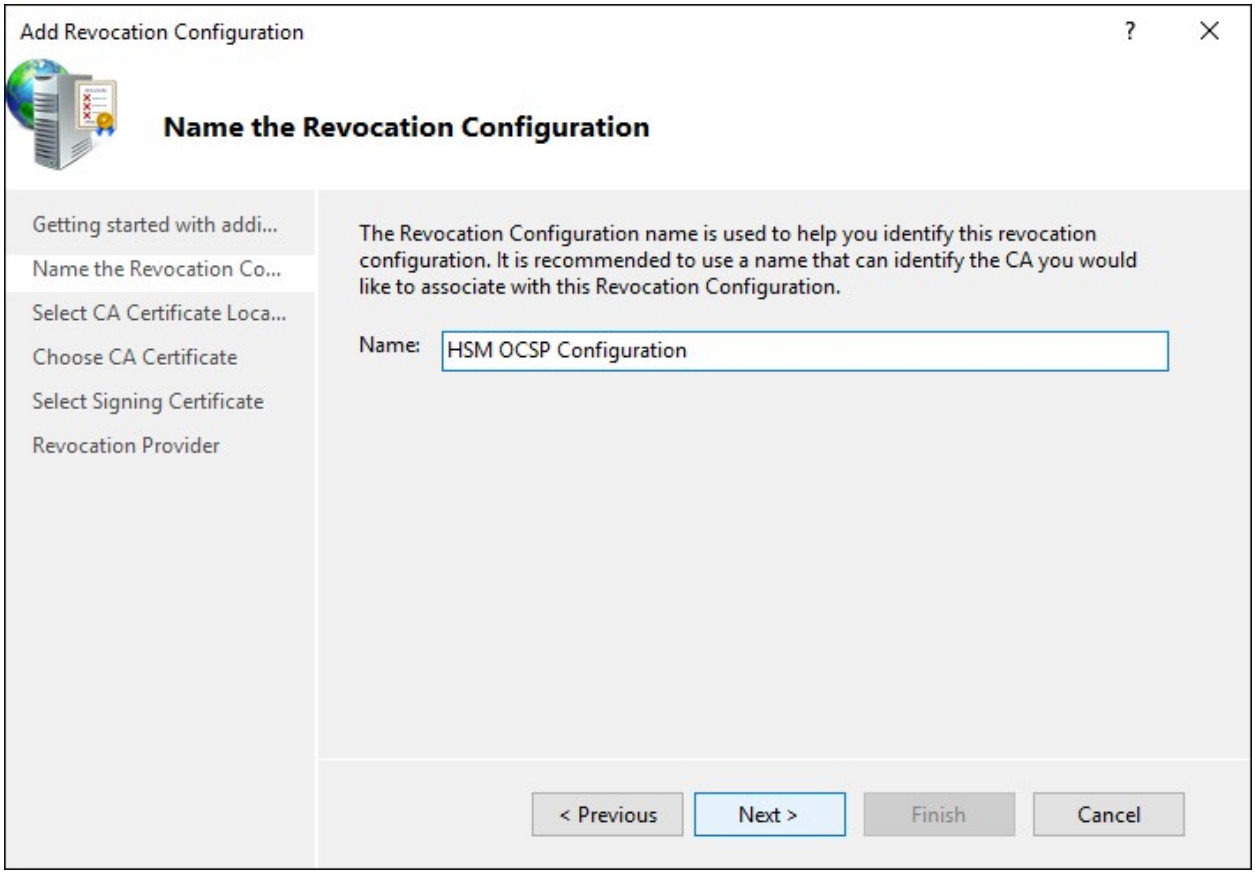

Figure 13 : Add Revocation Configuration Wizard - Name the Revocation Configuration

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

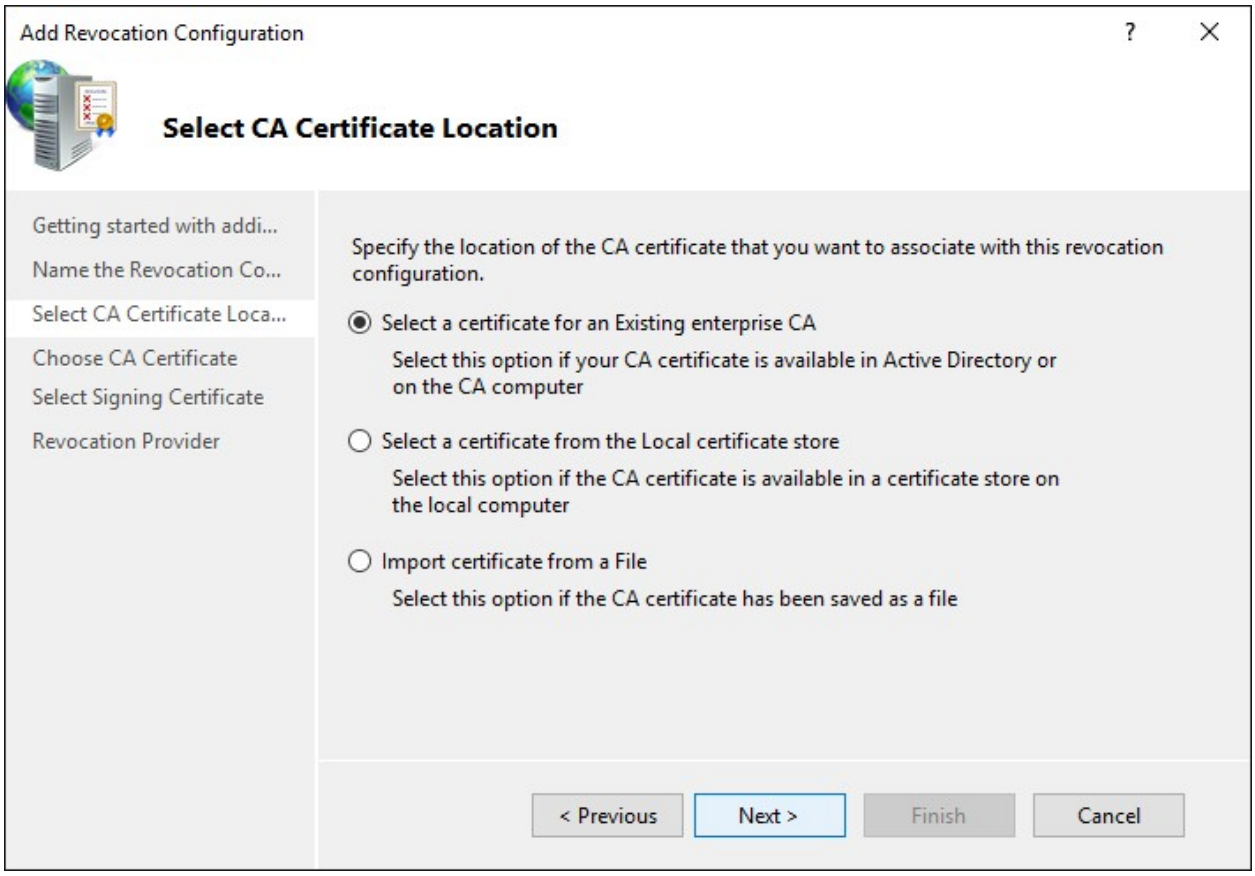

Figure 14 : Add Revocation Configuration Wizard - Select CA Certificate Location

5. Select the OCSP certificate template created earlier.

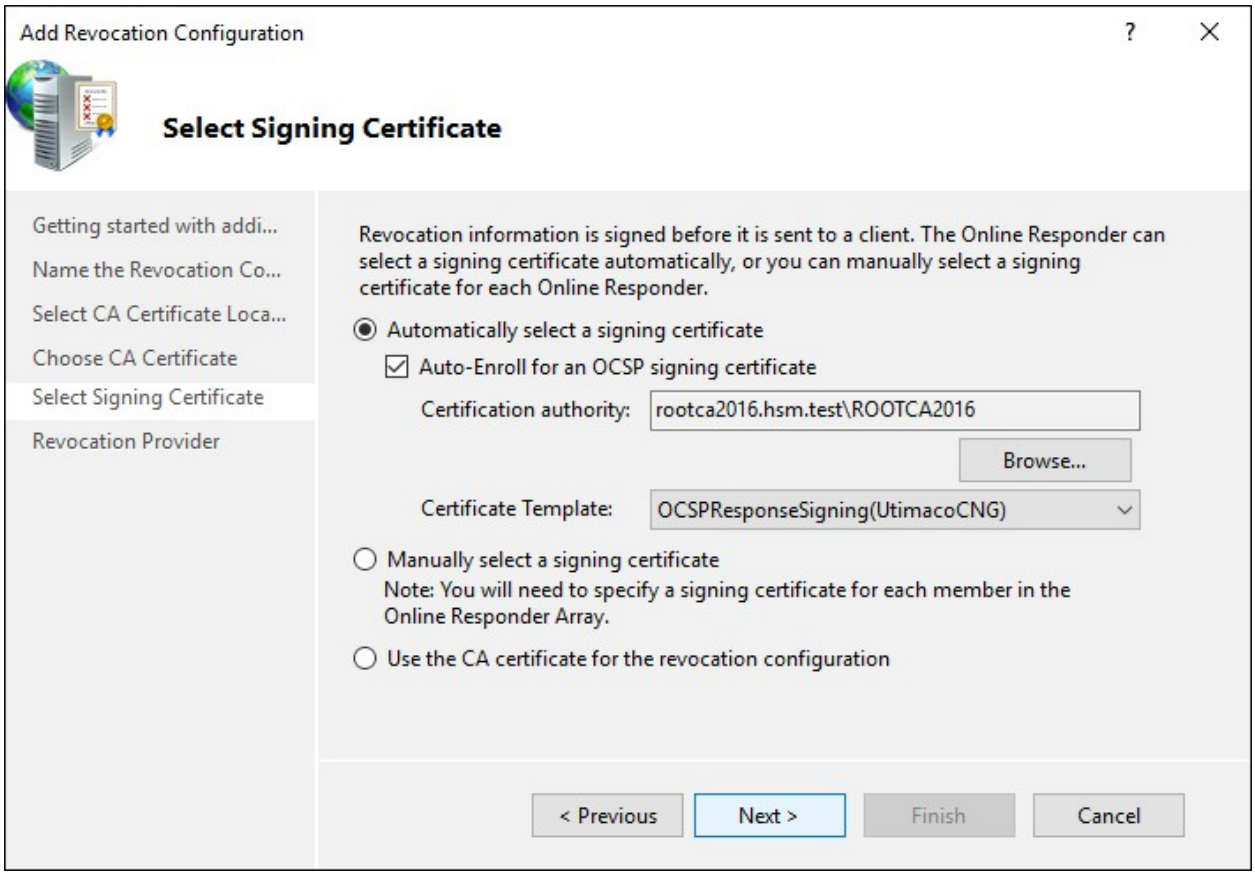

Figure 15 : Add Revocation Configuration Wizard - Select Signing Certificate

6. 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.

7. Once you have set up the Revocation Configuration, you should have the status **Working** as below.

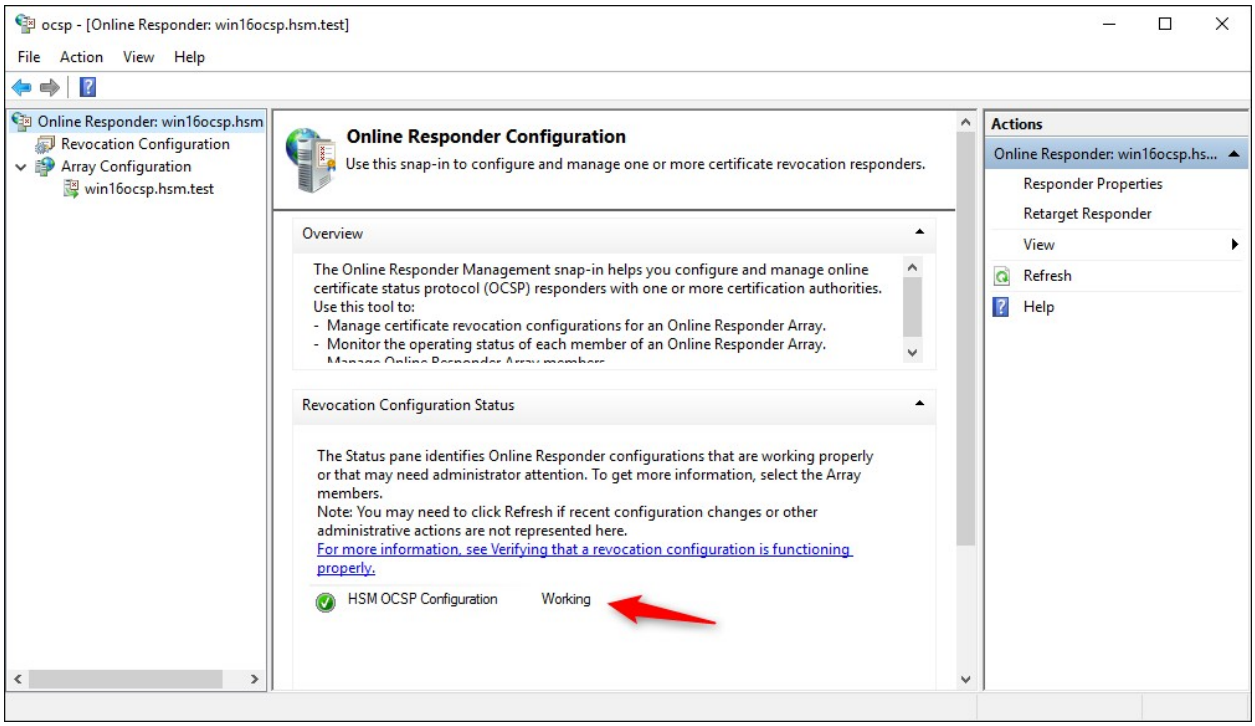

Figure 16 : Check OCSP Service

8. You can check if the key of 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, you can be assured that your Online Responder Service is using the Utimaco CryptoServer HSM correctly.

›_ PowerShell

```
PS C:\>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
```

6.5 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 as shown below.

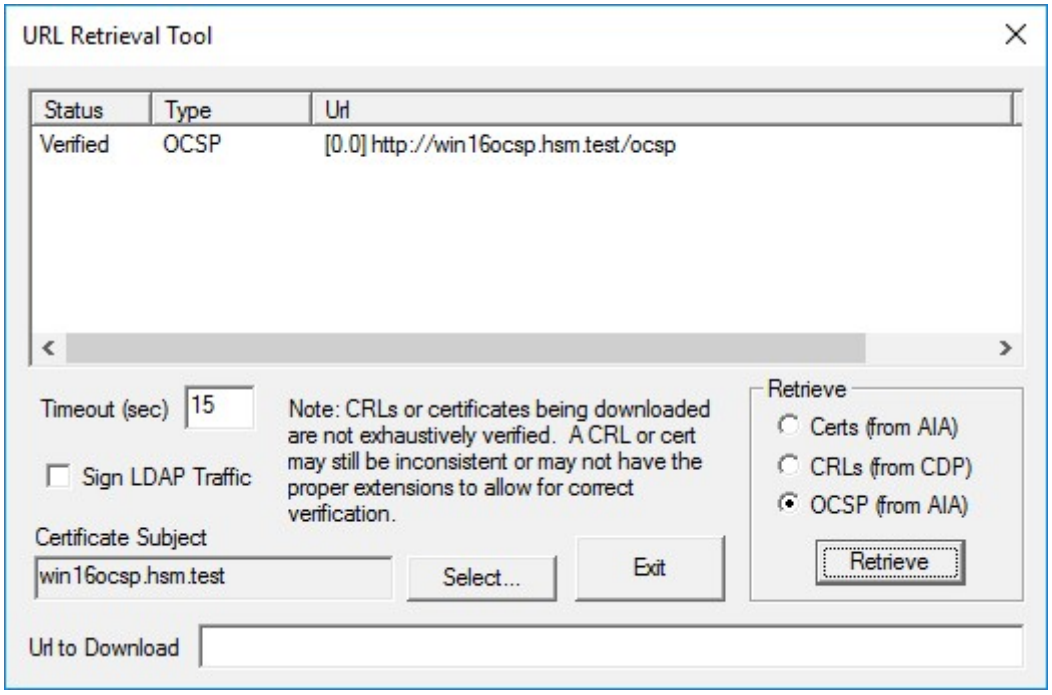

Figure 17 : URL Retrieval Tool

Select **OCSP** and click on **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 click again on **Retrieve** now, the status should change to **Revoked**.

7 Rights Management Services

This chapter describes how to add the Active Directory Rights Management Services role and how to configure it with the Utimaco CryptoServer. For any further configuration refer to the Microsoft TechNet website.

Before you can integrate the Utimaco CryptoServer with Microsoft Active Directory Rights Management Services, complete the Utimaco CSP/CNG Installation.

7.1 Install the Active Directory Rights Management Services

1. Add the Active Directory Rights Management Services (AD-RMS) role to your system. To do this, open the Server Manager and select **Manage → Add Roles and Features**.

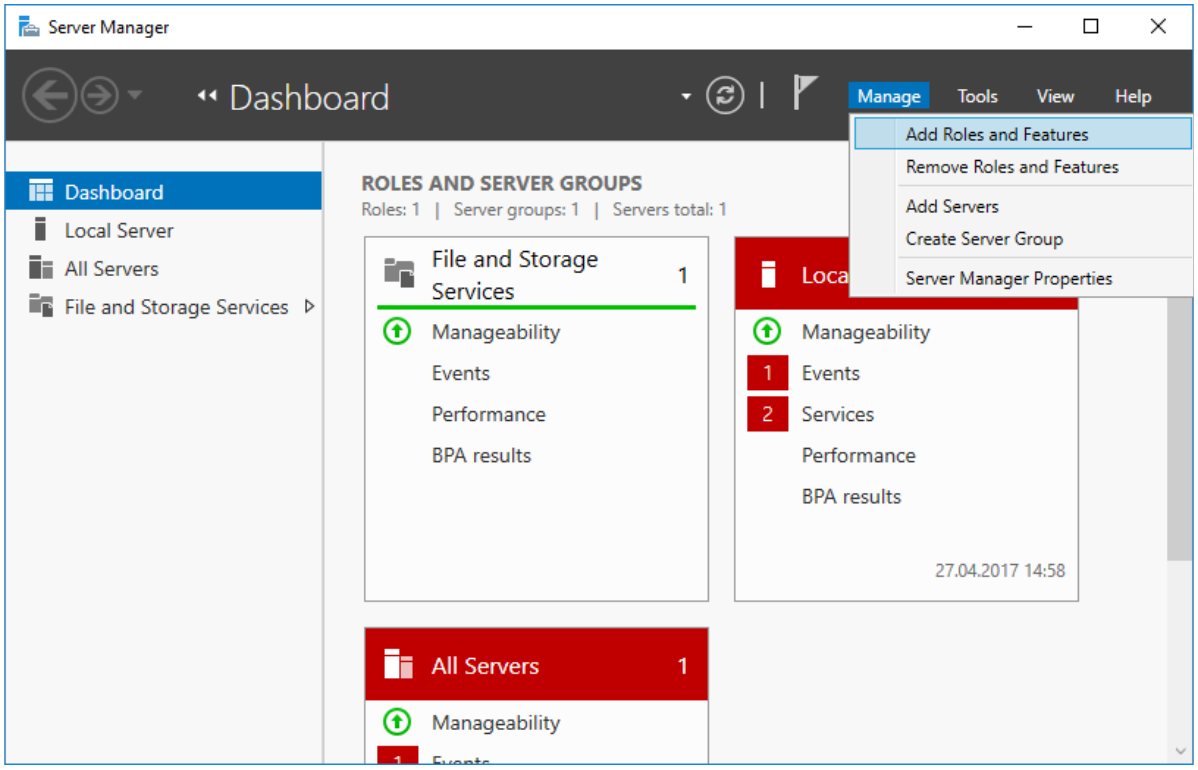

Figure 18 : Server Manager - Add Roles and Features

2. In the step **Server Roles**, in the **Add Roles and Features Wizard**, select the role **Active Directory Rights Management Services**.

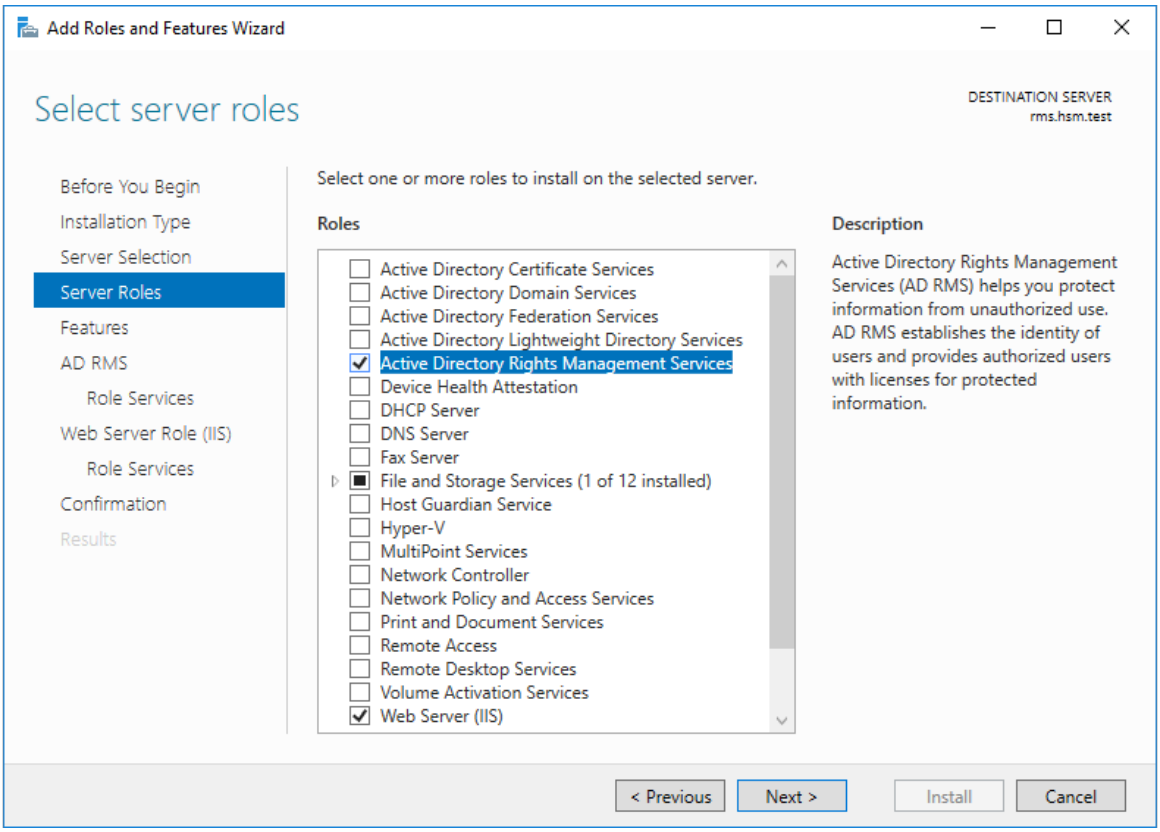

Figure 19 : Add Roles and Features Wizard - Server Roles

3. Use the wizard depending on your requirements. At the end of this wizard, click on **Install** to trigger the installation of AD-RMS.

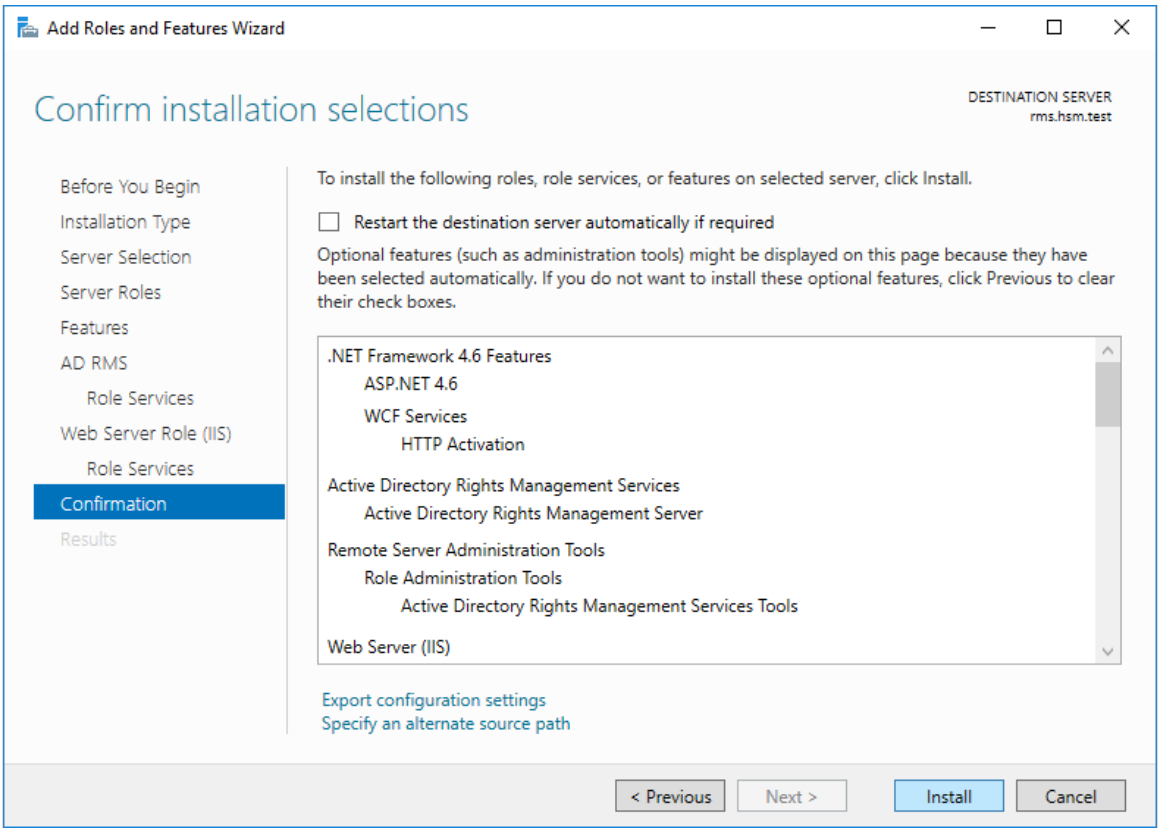

Figure 20 : Add Roles and Features Wizard - Confirmation

4. As soon as the installation is finished, you can click on **Close** and proceed with the initial configuration.

7.2 Initial Configuration of Active Directory Rights Management Services

The following example only describes a basic configuration and should be adjusted to your requirements.

1. In the **Server Manager** Window, the flag shows a warning after the installation. Select the flag and click on **Perform additional configuration**.

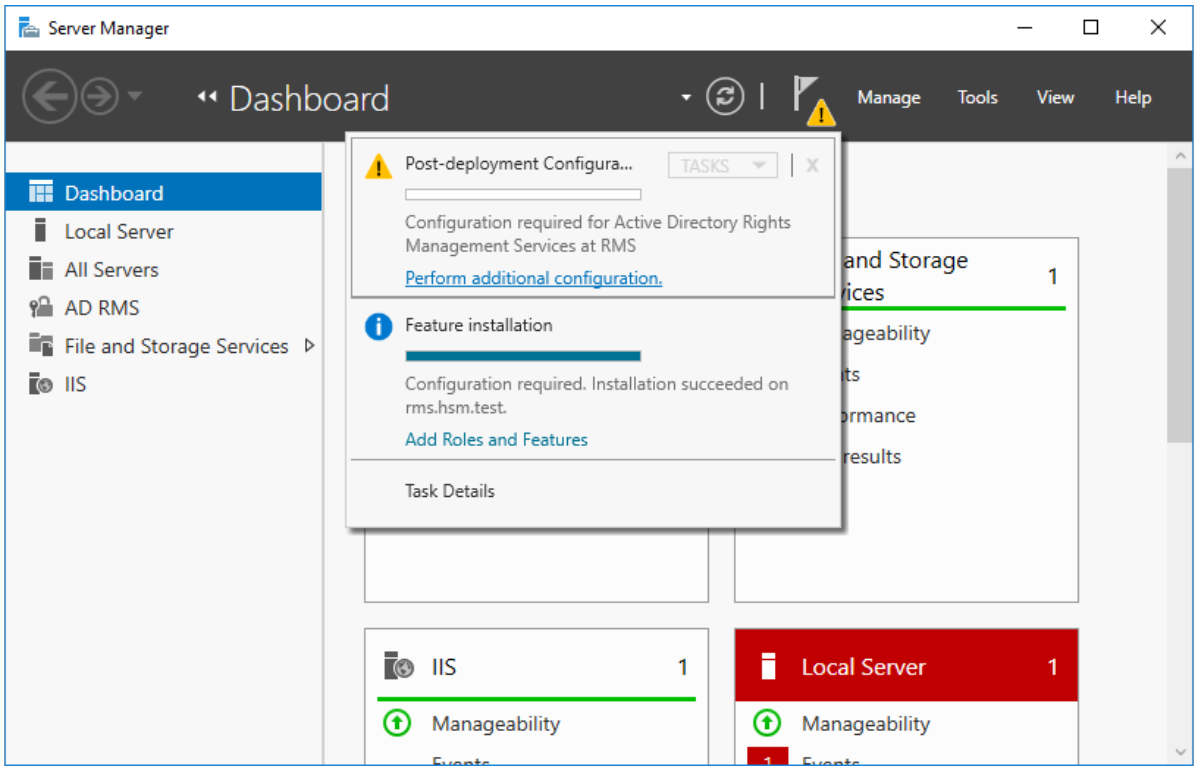

Figure 21 : Server Manager - Post-deployment Configuration of AD RMS

2. In the **AD RMS Configuration** Wizard, go through the single configuration steps. It is important that you select **Cryptographic Mode 2 (RSA 2048-bit-keys/SHA-256 hashes)** in the step **Cryptographic Mode**.

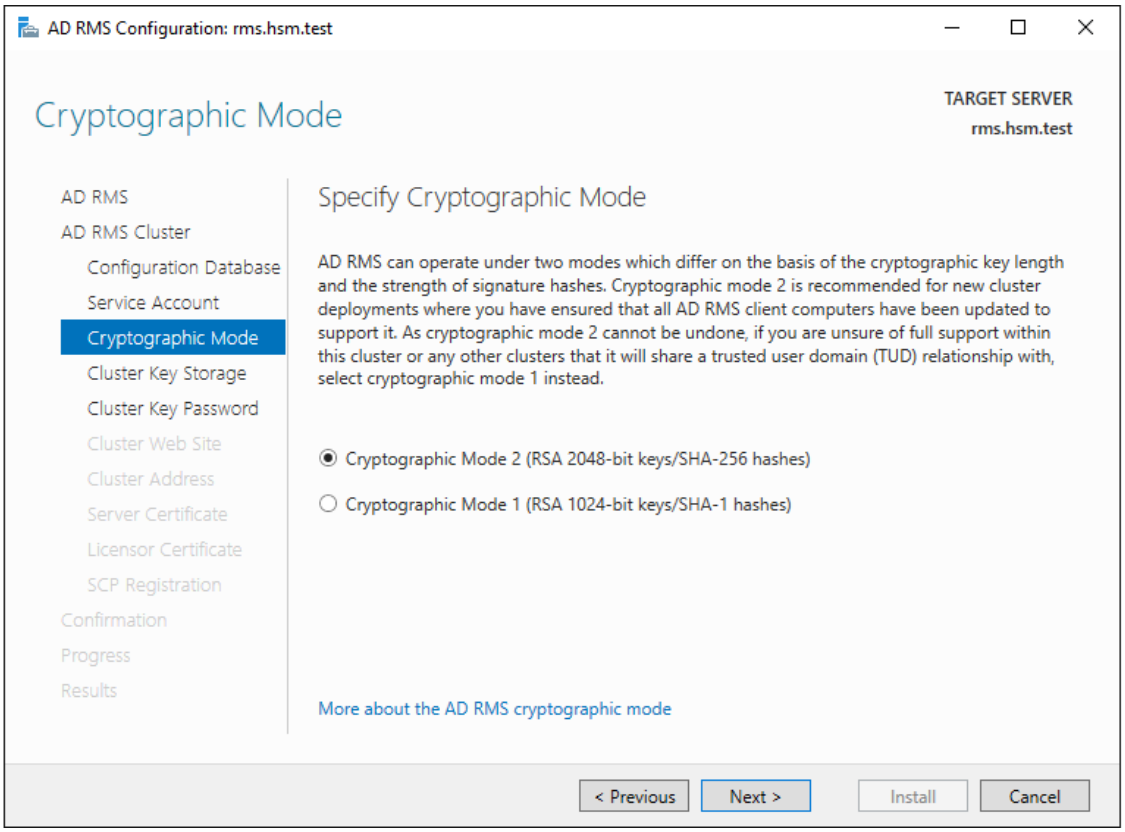

Figure 22 : AD RMS Configuration - Cryptographic Mode

3. In the step **Cluster Key Storage**, select the option **Use CSP key storage**.

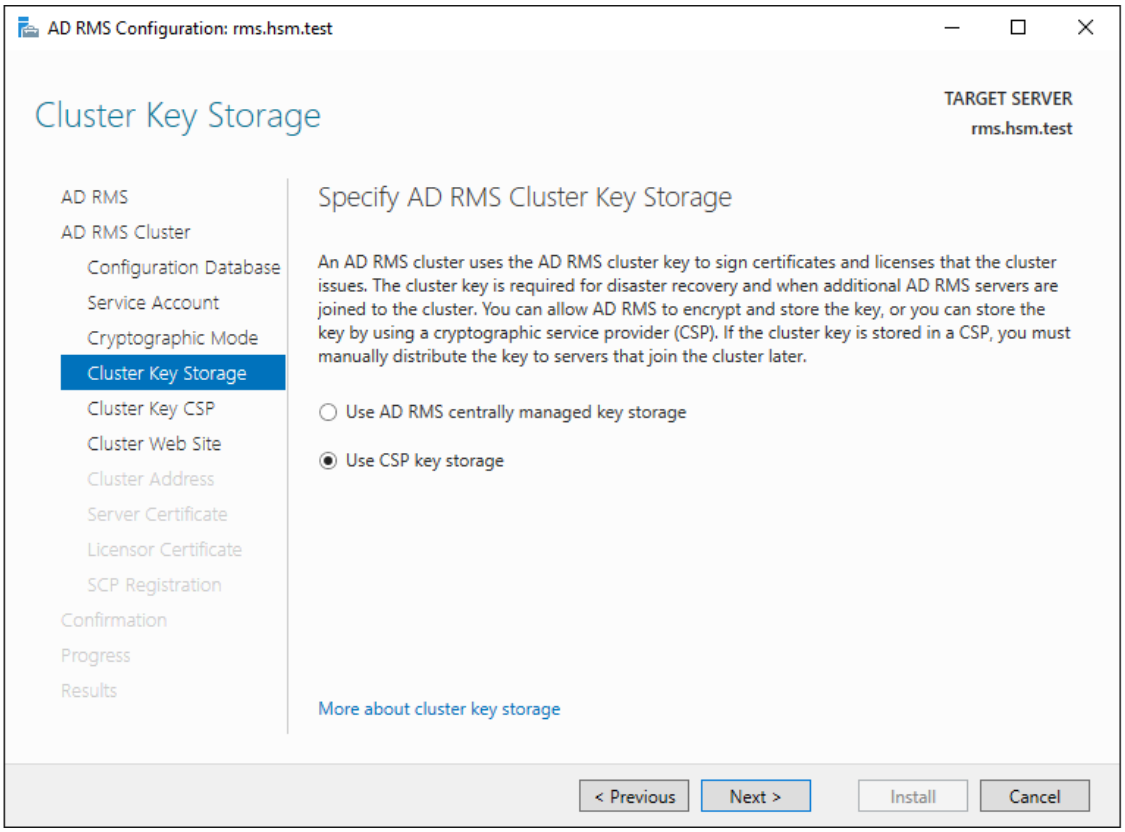

Figure 23 : AD RMS Configuration - Cluster Key Storage

4. In the step **Cluster Key CSP**, select the CSP **Utimaco CryptoServer RSA and AES CSP**. If you want to use an existing key in the HSM, you can select one. If you want to create a new key, select the option **Create a new key with the selected CSP (recommended)**.

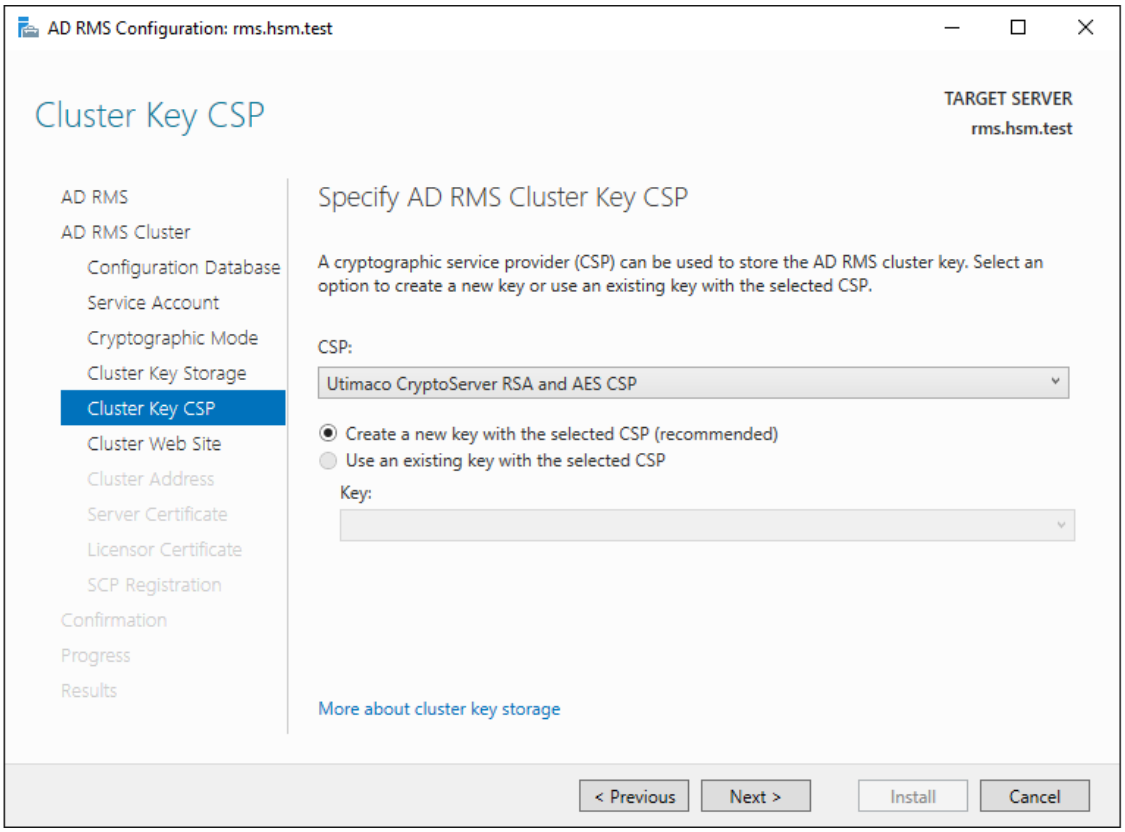

Figure 24 : AD RMS Configuration - Cluster Key CSP

5. At the end of the wizard, please check your configuration. If everything is satisfactory, click on **Install**.

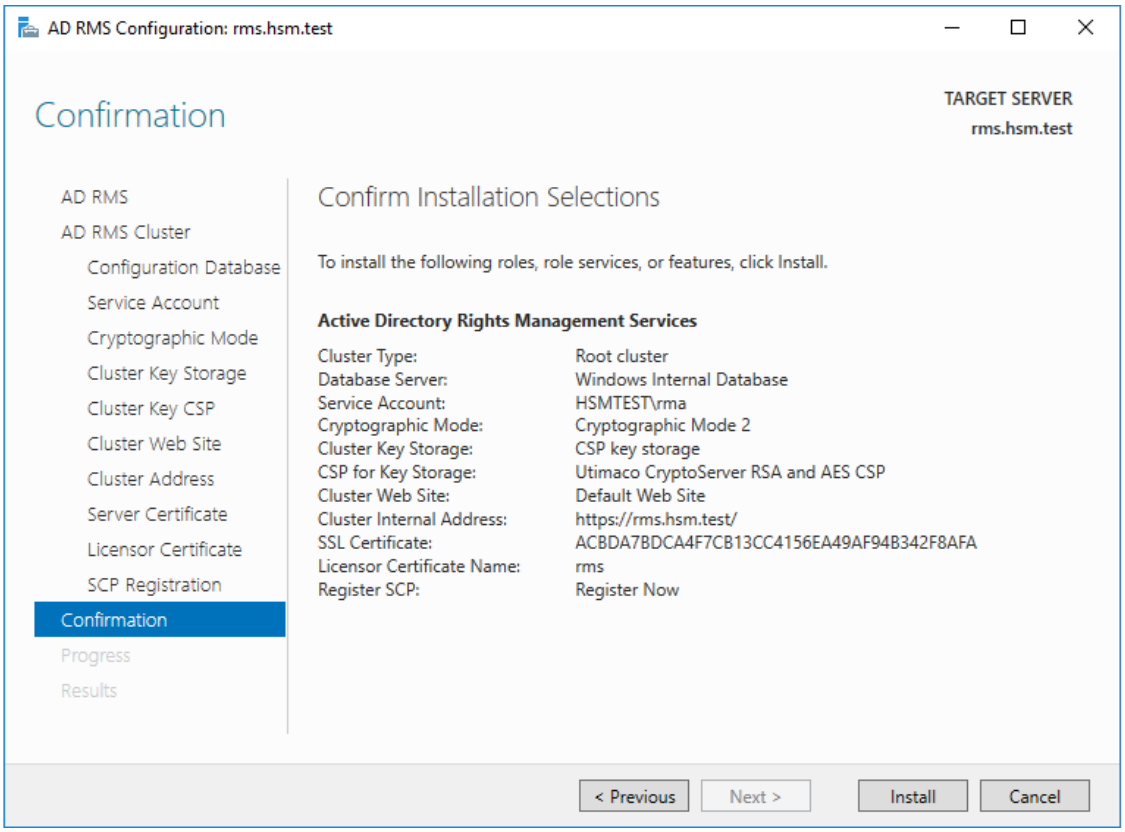

Figure 25 : AD RMS Configuration - Confirmation

6. If the configuration was successful, you will get a confirmation that the role AD RMS was installed successfully.

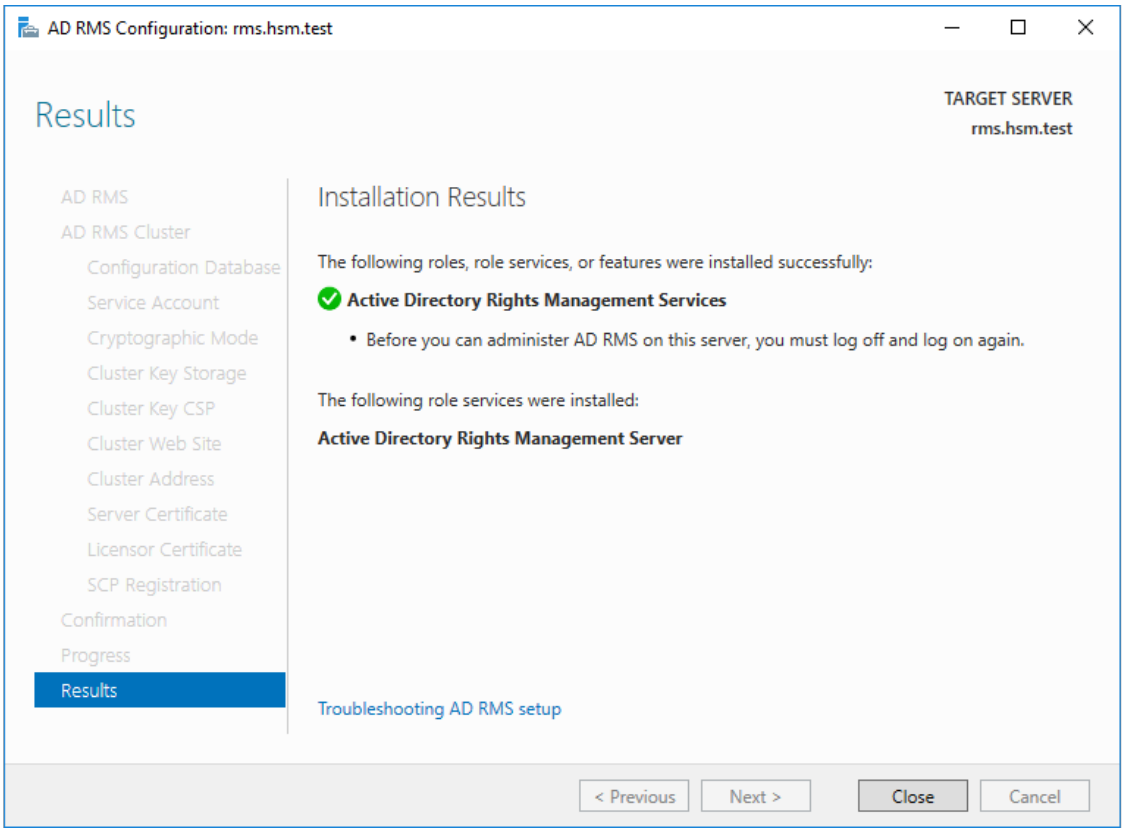

Figure 26 : AD RMS Configuration - Results

7. You can now check if the key has been created and stored successfully in the HSM. To do this, start the PowerShell command line interface and issue the command `cngtool listkeys`. If you see a key similar to the following output, the key is stored and available inside the HSM.

```
PS C:\> cngtool listkeys
------------------------------------------------------------
Provider : Utimaco CryptoServer Key Storage Provider
Device : 10.17.72.53
Group : RMS
Mode : External Key Storage
------------------------------------------------------------
Index AlgId Size Group Name Spec
------------------------------------------------------------------
1 RSA 2048 RMS _DRMS:Mode2:MS-GUID:{b8c4c...8f741} 1
```

For any further configuration for AD RMS refer to the Microsoft TechNet website.

8 Further Information

This document is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the documentation directory.

All of the Utimaco CryptoServer documentation is also available at the Utimaco IS GmbH website: Utimaco | Data Protection & Secure Payments On-Prem and as a Service.

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.

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.