nCIPHER

www.ncipher.com

Microsoft AD CS and OCSP

Integration Guide for Microsoft Windows Server 2008 R2

Version: 1.3

Date: Tuesday, June 25, 2019

Contents

1 Introduction

1.1 This product

Microsoft Active Directory Certificate Services (AD CS) provides the functionality for creating and installing a Certificate Authority (CA). The CA acts as a trusted third-party that certifies the identity of clients to anyone who receives a digitally signed message. The CA may issue, revoke, and manage digital certificates.

The Online Responder is a Microsoft Windows Service that implements the Online Certificate Status Protocol (OCSP) by decoding revocation status requests for specific certificates. The service provides up-to-date validation of certificates, and sends back a signed response containing the requested certificate status information. OCSP is used to provide real-time information about a certificate's status.

The CA uses the HSM to protect its private key. The HSM is also used for important operations such as key generating, certificate signing, and CRL signing. The HSM can be setup to protect the CA's private key to Federal Information Processing Standards (FIPS) 140-2 level 2 or level 3 securities. The HSM gives an additional level of security where smart cards have been used to protect the key. When using smart cards an operator must be present to insert the Operator Card Set (OCS) into the smart card reader to issue a new certificate or access the CA's private key.

Throughout this guide, the term HSM refers to nShield® Solo™ modules (nShield PCIe and Solo XC), nShield Connect™, and nShield Edge™ products.

1.1.1 Product configuration

We have successfully tested the integration between the HSM and the AD CS in the following configurations:

Operating system	ADCS version	OCSP version	nShield Security World Software version	nShield Solo support	nShield Connect Support	nShield Edge support
Microsoft Windows Server 2008 R2 Enterprise SP1	6.1	1.0	11.60	Yes	Yes	Yes
Microsoft Windows Server 2008 64-bit SP2	6.0	1.0	11.60	Yes	Yes	Yes

Operating system	ADCS version	OCSP version	nShield Security World Software version	nShield Solo support	nShield Connect Support	nShield Edge support
Microsoft Windows Server 2008 32-bit SP2	6.0	1.0	11.60	Yes	Yes	Yes

1.1.2 Supported nCipher functionality

Soft Cards	No	Key Management	Yes	FIPS 140-2 level 3	Yes
Key Recovery	Yes	Module-only Key	Yes	K-of-N Card Set	Yes
Load Balancing	Yes	Key Import	Yes	Fail Over	Yes

CA failover clustering is only supported with network attached HSMs (nShield Connect) for Windows Server 2008 Enterprise R2 SP1.

1.1.3 Requirements

Before installing the software, we recommend that you familiarize yourself with the AD CS and OCSP documentation and setup processes, and that you have the nCipher HSM documentation available.

We also recommend that there is an agreed organizational Certificate Practices Statement and Security Policy/Procedure in place covering administration of the HSM. In particular, these documents should specify the following aspects of HSM administration:

- The number and quorum of Administrator Cards in the Administrator Card Set (ACS), and the policy for managing these cards.
- Whether the application keys are protected by the module or an OCS.
- The number and quorum of Operator Cards in the OCS, and the policy for managing these cards.
- Whether the Security World should be compliant with FIPS 140-2 level 3.
- Key attributes such as the key size and time-out.
- Whether there is any need for auditing key usage.
- Whether to use the nCipher Cryptographic Service Providers for Cryptographic API: Next Generation (CNG) or CryptoAPI (CAPI).

We recommend that you use CNG for full access to available features and better integration with Windows Server 2008 and Windows Server 2008 R2.

1.2 This guide

This guide describes how to set up and configure AD CS and OCSP with nCipher nShield Hardware Security Module (HSM). We have thoroughly tested the instructions, which provide a straightforward integration process. There may be other untested ways to achieve interoperability. This guide might not cover every step of the hardware and software setup process.

This guide assumes that you have read your HSM documentation and that you are familiar with this and the setup process for AD CS and OCSP.

1.3 More information

For more information about the HSM, refer to the *User Guide* for the HSM.

For more information about OS support, contact your Microsoft sales representative or nCipher Support.

For more information about installing the AD CS and OCSP, refer to the Microsoft documentation.

For more information about contacting nCipher, see *Addresses* at the end of this guide.

Additional documentation produced to support your nCipher product is in the document directory of the CD-ROM or DVD-ROM for that product.

2 Procedures

To set up and configure the AD CS and OCSP with an HSM:

1. "Install the HSM" below.
2. "Install the software and create or share the Security World" below.
3. "Install and configure AD CS" on the facing page.
4. "Configure auto-enrollment group policy for a domain" on page 10.
5. "Configure the nCipher nShield HSM with Certificate Services" on page 10.
6. "Configure Certificate Enrollment to use CA templates" on page 12.
7. "Set up key use counting" on page 13.
8. "CA Backup, migrate and restore" on page 15.
9. "Install OCSP" on page 21
10. "Configure the CA to issue an OCSP Response Signing Certificate" on page 21.
11. "Set up a revocation configuration" on page 24.
12. "Verify that OCSP works correctly" on page 25.
13. "Uninstall AD CS and OCSP" on page 27.

This chapter describes these procedures.

2.1 Install the HSM

Install the HSM using the instructions in the *Hardware Installation Guide* for the HSM. We recommend that you install the HSM before configuring the Security World software, and before installing and configuring AD CS and OCSP.

2.2 Install the software and create or share the Security World

To install the Security World Software and create the Security World:

1. Install the latest version of the Security World Software as described in the *User Guide* for the HSM.

   

   We recommend that you always uninstall any existing Security World Software before installing the new Security World software.

2. Initialize a Security World as described in the *User Guide* for the HSM.

   

   You can also use the CSP Install Wizard or the CNG Configuration Wizard to create a Security World for nShield Solo and Edge HSMs. For nShield Connect, we recommend that you use the front panel user interface to create the Security World.

3. Register the Cryptographic Service Providers that you intend to use.

For CAPI on 64-bit Windows, both 32-bit and 64-bit CSP Install Wizards are available. If you intend to use the nCipher CAPI CSPs from both 32-bit and 64-bit applications, or if you are unsure, run both wizards. The CNG Configuration Wizard registers the nCipher CNG Providers for use by both 32-bit and 64-bit applications where relevant. For detailed information on registering the nCipher CAPI CSPs or CNG Providers, refer to the *User Guide* for the HSM.

4. If you are installing OCSP on a different server to the CA, install the Security World Software on both servers, as described in the *User Guide* for the HSMs, and share the Security Worlds by copying the %KMDATA% file from the CA server to the OCSP server. See the *User Guide* for more information.

2.3 Install and configure AD CS

To install and configure Microsoft Active Directory Certificate Services:

1. Select `Start > Administrative Tools > Server Manager`.
2. Right-click `Roles` on the left-hand side, and select `Add Roles`. The `Add Roles Wizard` window appears.
3. On the `Before You Begin` screen, click `Next`.
4. In the control panel, select `Active Directory Certificate Services` and click `Next` twice.
5. The `Select Role Services` window appears. Ensure that `Certification Authority` is selected.
6. To be able to submit certificate requests using a Web interface, ensure that `Certification Authority Web Enrollment` is selected.
7. Click `Next`. The `Specify Setup Type` window appears.
8. Select the appropriate Certification Authority (CA) setup type for your requirements:
   - `Enterprise`.
   - `Standalone`.

   

   If your machine is not a member of an Active Directory domain, only `Standalone` is available.

9. Click `Next`. The `Specify CA Type` window appears.
10. Select the type of CA for your requirements:
    - `Root`.
    - `Subordinate`.

    

    If your CA is to be the only CA, select `Root`. If you want to use multiple CAs, select `Root` or `Subordinate` according to where in the hierarchy this CA is to appear.

11. Click `Next`. The `Set Up Private Key` window appears.

12. Select the private key setup appropriate for your requirements:
    - For a typical installation, select `Create a new private key`.
    - If you have special requirements, such as Key Use counting, or if you are migrating from a previous CA, select `Use existing private key`.
13. Click `Next`. The `Configure Cryptography for CA` window appears.
14. If you have chosen to create a new private key, select a hash algorithm, cryptographic service provider and key character length.
15. Select `Allow administrator interaction when the private key is accessed by the CA`. Otherwise, you will not be prompted for authorization if necessary. Click `Next`.
16. As prompted, enter a name for the CA. Click `Next`.
17. As prompted, enter a certificate validity period. Click `Next`, and on `Configure Certificate Database` click `Next`.
18. Verify that the installation settings are correct, and click `Install`.
19. After installing AD CS, you must register nFast Server as a dependency of the CA service. This ensures that the nCipher CNG or CAPI CSPs are available for use before the CA starts up. Run the command: `>ncsvcdep -a certsvc`. By default, the `ncsvcdep.exe` utility is installed in the `%NFAST_HOME%\bin` directory.

2.3.1 Verify that the CA service has started successfully

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

```
>sc query certsvc
```

2.3.2 Configure auto-enrollment group policy for a domain

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

1. On the domain controller, click `Start > Administrative Tools > Group Policy Manager`.
2. Double-click `Group Policy Objects` in the forest and domain containing the Default Domain Policy Group Policy object (GPO) that you want to edit.
3. Right-click the `Default Domain Policy GPO`, and then click `Edit`.
4. In the `Group Policy Management Editor`, click `Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies`.
5. Double-click `Certificate Services Client - Auto-Enrollment`.
6. In `Configuration Model`, click `Enabled` to enable auto-enrollment.
7. Click `OK` to accept your changes and close the Editor.

2.3.3 Configure the nCipher nShield HSM with Certificate Services

2.3.3.1 Configure Certificate Services with a new key

To install the Certificate Server using the nCipher nCipher Key Storage Provider (KSP):

1. Install and configure the nCipher HSM hardware and software as described in the section above, "Install the software and create or share the Security World" on page 8.
2. Install Microsoft Active Directory Certificate Services and a CA as described in the section above, "Install and configure AD CS" on page 9, with the following settings:
   - In the `Setup Private Key` window, click `Create a new private key` and click `Next`.
   - In the `Configure Cryptography for CA` window, select the appropriate nCipher algorithm and hash algorithm.
   - Continue the CA setup as described above in the section "Install and configure AD CS" on page 9.

2.3.3.2 Configure Certificate Services using an existing private key

To install the Certificate Server using the nCipher KSP with an existing HSM private key:

1. Install and configure the nCipher HSM hardware and software as described in the section above, "Install the software and create or share the Security World" on page 8.
2. Install Microsoft Active Directory Certificate Services and a CA as described in the section above, *Install and configure AD CS* with the following settings:
   - In the `Setup Private Key` window, select `Create a new private key` and click`Next`.
   - Continue the further CA setup as described in the section above, "Install and configure AD CS" on page 9
3. In the `Set up Private Key` window, select `Use existing private key` and select an existing private key on this computer.
4. In the `Select Existing Key` window, click `Edit`.
5. In the `Edit Search Criteria` window, select the CSP that contains the created key. Delete the contents of the field `CA common name`, and click `Search`.
6. The search finds the existing private key. Select the key and click `Next`.
7. Select the appropriate hash algorithm.
8. Select `Allow administrator interaction when the private key is accessed by the CA` and click `Next`.
9. On the `CA name` window, click `Next`.
10. On the `Set validity period` window, click `Next`.
11. On the `Certificate database` window, click `Next`.
12. On the `Confirmation` window, click `Install` and wait for the installation to complete.
13. After successful installation, the `Results` window will be displayed. Click `Close`.
14. Verify that the CA service has successfully started by running the command:

```
>sc query certsvc
```

16. Verify the CA key by running the command:

```
>certutil -verifykeys
```

2.3.4 Configure Certificate Enrollment to use CA templates

To integrate the CA certificate enrolment functionality with a nCipher HSM generated CA private key:

1. Create a CA template that uses the nCipher KSP:
    a. Run `certtmpl.msc`.
    b. In the right-hand pane, right-click the `Administrator` template, and select `Duplicate Template`.
    c. Select `Windows Server 2008 Enterprise` and click `OK`. The `Properties` window opens showing the `General` tab.
    d. Click the `General` tab and in `Template display name`, type a name for the template.
    e. Click the `Request Handling` tab, and in `Purpose` select `Signature` and click `Yes` to confirm changes to the certificate purpose.
    f. Deselect `Allow private key to be exported`.
    g. Click the `Cryptography` tab.
    h. Select `Requests must use one of the following providers` and in `Providers`, select `nCipher Security World Key Storage Provider` only. Do not select any other provider.
    i. In `Algorithm Name`, select an ECC algorithm.
    j. In `Request Hash`, select a hash type.
    k. Click `Subject Name` tab and deselect `Include e-mail name in subject name` and deselect `E-mail name`.
    l. Click `OK` to save the template settings.
2. Run `certsrv.msc`.
3. In the left-hand pane, double-click the CA name.
4. Right-click the `Certificate Template` node and select `New > Certificate Template to Issue`.
5. Select the template you just created, and click `OK`.
6. Request a certificate based on the template:
    a. Run `certmgr.msc`.
    b. In the left-hand pane, right-click the `Personal` node, and select `All Tasks > Request New Certificate`.
    c. Click `Next` and `Next` to pass through the first two windows.
    d. Select the template that you created, and click `Enroll`.
    e. The nCipher Key Storage Provider window appears.
    f. Click `Next`.
    g. Select the type of protection you want to use, and click `Next`.

1. If OCS is selected, select the OCS from the `Card sets` pane, and click `Finish`.
2. If passphrase authentication is enabled, a prompt for passphrase appears.

7. Verify that the certificate is enrolled successfully.

   The enrollment wizard shows if the certificate enrollment was successful or failed. Use the `Details` button to check the main information.

2.3.5 Set up key use counting

Setting up key use counting is optional. The procedures described in this section do not apply to most setups. If you require key use counting, follow the procedures described in this section.

If you do not follow the procedures described in this section, key use counting is not installed. You cannot add key use counting to a key retrospectively.

2.3.5.1 Key use counter overview

The key use counter audits usage of the CA signing key. It maintains a count of how many times the key has been used. We recommend using the key use counter with a root CA that has a low volume of signings where the count can be logged immediately before servicing a signature request and after the signature request has been serviced. This ensures that any illicit use of the CA is revealed through discrepancies in the counter log.

You also need to remember the following information about the key use counter:

- The counter is in the NVRAM of the HSM.
- The counter is a 64-bit integer counter associated with a single private key.
- The counter is started at zero.
- If the maximum count is reached, the counter restarts at zero.
- The counter can exist only on one HSM. If more than one HSM is attached to the server, you must choose which HSM stores the counter.
- If the module firmware is upgraded, the counter value is lost.
- If the CA startup event in the Security log wrongly reports a usage count of zero for the signing key, see http://support.microsoft.com/kb/951721.

2.3.5.2 Key use counter increments

The key use counter increments depend on the type of CA (such as offline or online issuing) and the cryptographic operations that are executed by the CA to service a certificate signature request (CSR). The key counter is incremented by values that range from 0 to 3. The CA audit logs record the key use count whenever CA is started or stopped.

2.3.5.3 Install Certificate Services with key use counting

To install Certificate Services with key use counting:

1. If it is not already on your system installation, create the file **%SystemRoot%\capolicy.inf** (where *%SystemRoot%* is the system environment variable for the Windows installation folder, by default **C:\WINDOWS\capolicy.inf**) with the following content:

```
[Version]
 Signature="$Windows NT$"
 [certsrv_server]
 EnableKeyCounting=True
```

You must create the **capolicy.inf** file before Certificate Services is installed.

3. Install the CA using the HSM KSP.
4. Enable auditing for CA startup and shutdown.
5. Enable auditing for the CA service by running the command:

```
>certutil -setreg ca\auditfilter 1
```

7. Right-click the CA and click `Properties`.
8. Click the `Auditing` tab and check the box for `Start and stop Active Directory Certificate Services`.
9. Go to `Local Security Policy` from `Start->Administrative Tools-> Local Security Policy`.
10. Go to `Local Policy`. Expand it and select `Audit Policy`.
11. On the right-hand pane, double-click `Audit Object Access` and select `Success and Failure`.
12. Click `Apply` and then `OK`, then close the window.
13. Update the local security policies by opening a command prompt and running the command:

```
>gpupdate.exe /force
```

15. Restart the CA service to pick up the changes, by running the commands:

```
>net stop certsvc
>net start certsvc
```

17. Run `Eventvwr.exe`.
18. Select `Windows Logs > Security`.
19. Filter for event ID 4881 (CA startup event) or event ID 4880.
20. Verify the CA startup event shows the `PrivateKeyUsageCount` property with a corresponding value. Make a note of this value.

21. Restart the Certificate Server, by running the commands:

```
>net stop certsvc
>net start certsvc
```

23. Verify that the event viewer contains a new CA startup event (event ID 4881).
24. Verify that the `PrivateKeyUsageCount` property value has not changed.

2.3.6 CA Backup, migrate and restore

The most common scenario related to backup and restore for the CA and HSM is backup and migrate. This procedure describes backing up the CA/HSM data on an existing server and then restoring the CA/HSM data to a new server. It has been successfully tested in the following configurations:

- Windows Server 2003 SP2 Enterprise 64-bit (CAPI) to Windows Server 2008 R2 Enterprise (CNG)
- Windows Server 2008 SP2 Enterprise 64-bit (CNG) to Windows Server 2008 R2 Enterprise (CNG)
- Windows Server 2008 R2 Enterprise (CNG) to Windows Server 2008 R2 Enterprise (CNG) —RSA and ECDSA key types

If your existing CA is using a custom **`CAPolicy.inf`** file, you should copy the file to the new planned CA server. The **`CAPolicy.inf`** file is located in the **`%SystemRoot%`** directory, which is usually **`C:\Windows`**.

2.3.6.1 Backup and migrate an existing certificate and its associated private key

To back up the CA and HSM data on the existing server (machine #1), and then migrate the CA and HSM onto a new server (machine #2):

1. *On Machine #1:*

   Back up the CA database by running the command:

```
>certutil -config <CA_config_string> -backupdb <BackupDirectory>
```

4. Export the certificate on machine #1:
   a. Run `mmc`.
   b. In the console, navigate to `File > Add/Remove Snap-in`.
   c. Select the `Certificates` and click `Add`.
   d. The certificate snap-in windows opens. Select `Computer Account` and click `Next`.
   e. Keep the default selection, click `Finish` and then click `OK`.
   f. Navigate to the directory `Trusted Root Certificates > Certificates`.
   g. Right-click the CA certificate, and click `All Tasks->Export`.
   h. Click `Next`.

i. Select Base-64 encoded X.509 (.CER), and click `Next`.

j. Specify the path and file name to save the certificate, and click `Next`.

k. Click `Finish`.

l. Click `OK` to close the export success message.

5. Back up the contents of the nShield Security World data from the following location:`C:\ProgramData\nCipher\KeyManagement Data\local`.

6. Uninstall the CA from machine #1.

7. *On Machine #2:*

   Copy the backed-up nShield Security World data on the following path on machine #2:`C:\ProgramData\nCipher\KeyManagement Data\local`.

9. Load the Security World onto the HSM on machine #2, by running the command:

```
>new-world -l
```

   For more information, refer to the *User Guide* for the HSM.

12. Run the `CNG Configuration Wizard`. If selecting operator card set protection, do *not* check `Always use the wizard when creating or importing keys`.

13. Copy and install the X.509 certificate into the local user Trusted Root CA Store on machine #2:

    a. Right-click the certificate, and click `Install`.

    b. Click `Next`.

    1. Select `Place all certificates in the following store`, and click `Browse`.

    2. Select Trusted Root Certification Authorities, and click `OK`.

    3. Click `Next`.

    4. Click `Finish`.

    5. Click `OK` to close the import success message.

14. If you want to import your existing CAPI key into CNG then you only need to execute the following steps:

    a. Run the CNG Configuration Wizard. Identify the key file name that corresponds to the signing key in the named CAPI container, by running the following command:

```
>csputils -m -d -n <CAPI-CONTAINER-NAME>
```

    If you are unsure of the CAPI container name, run the following command:

```
>csputils -l -m
```

    This command produces output of the form:

```
Detailed report for container ID
#00c1deb83de30a7015e15e8e9e763742fc3e1d48
Filename: key_mscapi_container-
00c1deb83de30a7015e15e8e9e763742fc3e1d48
Container name: SAMPLE-CAPI-CONTAINER-CA
Container is a machine container.
CSP DLL name: ncsp.dll
Filename for signature key is
key_mscapi_eea3d453a94b8890f5fc4c2e920c93813ee6d5ee
Key was generated by the CSP
Key hash: eea3d453a94b8890f5fc4c2e920c93813ee6d5ee
Key is recoverable.
Key is cardset protected.
Cardset name: SampleCardset
Sharing parameters: 1 of 1 shares required.
Cardset hash: 22f94c0d459594b230da3255af46d7446af81d42
Cardset is non-persistent.
No key exchange key
```

The key hash from this output is required by cngimport:

h. Import the CAPI key into CNG:

```
>cngimport --import --machine-key --key=eea3d453a94b8890f5fc --appname=mscapi
<newkeyname>
```

j. Confirm that the key has been imported successfully by running the command:

```
>cnglist --list-keys
```

15. Install the certificate into `my store`, by running the following command from the console:

```
>certutil -addstore my <certificate name>
```

A success message appears.

18. Repair the certificate store by running the command:

```
>certutil -f -repairstore -csp "nCipher Security World Key Storage Provider" my "<cert
serial number>"
```

20. If the private key is protected by an OCS with passphrase, you need to execute the following:
    a. Set the environment variable `NFAST_NFKM_TOKENSFILE` as follows:

       Open a console with administrator privileges and run:

       ```
       >set NFAST_NFKM_TOKENSFILE=<absolute path to file>
       ```

       

       There must be no white space in the specified path and filename.

       Example:

       ```
       c:\preload\tokensfile
       ```

    f. Run the preload command from `C:\Program Files (x86)\nCipher\nfast\bin>` in the same console:

       ```
       >preload -m1 -c <cardset name> pause
       ```

    h. Open another console with administrator privileges and run the following command again:

       ```
       >set NFAST_NFKM_TOKENSFILE=<absolute path to file>
       ```

    j. Run `certutil -repairstore` with the certificate serial number. To find the certificate serial number:
       i. Open the certificate.
       ii. In the `Details` tab, click `Serial number`.
       iii. The serial number is shown. Copy it using `Ctrl+C`.
    k. In the same administrator command prompt, run the command:

       ```
       >certutil -f -repairstore -csp "nCipher Security World Key Storage Provider" my
       "<cert serial number>"
       ```

       A success message appears.
21. From the command prompt run `>servermanager.msc`. The server manager console will now appear. Server manager must be opened this way. Opening it through Windows will result in the certificate not being displayed in the CA configuration wizard.
22. Install and configure CA with the following settings:
    a. In the `Set Up Private Key` window, select `Use existing private key` and then `Select a certificate and use its associated private key`.

1. In `Certificates`, the imported certificate is shown. Select the certificate and select `Allow administrator interaction when the private key is accessed by the CA` and click `Next`.
2. In the `Certificate Database` window click `Next`.
3. In the `Confirmation` window click `Install`.

23. When the CA installation is complete, click `Close` in the installation results window.
24. Copy the backed-up CA database data onto machine #2.
25. Run the following command:

```
>certutil -shutdown
```

27. On machine #2, restore the CA database by running the command:

```
>Certutil.exe -f -restoredb <BackupDirectory>
```

29. Restart the CA by running the command:

```
>net start certsvc
```

31. Verify that the CA service has started successfully by running the following command:

```
>sc query certsvc
```

2.3.6.2 Back up and migrate an existing private key

To back up the CA and HSM data on the original server (machine #1), and then migrate the CA/HSM on a new server (machine #2):

1. *On Machine #1*:

   Back up the CA database by running the command:

```
>certutil -config <CA_config_string> -backupdb <BackupDirectory>
```

4. Back up the nShield Security World data and the private key, which are found in`C:\ProgramData\nCipher\Key Management Data\local`.

   For more information, refer to the *User Guide* for the HSM.

6. Uninstall the CA from machine #1.
7. *On Machine #2*:

   Copy the backed-up nShield Security World data and the private key to `C:\ProgramData\nCipher\Key Management Data\local` on machine #2.

9. Load the Security World onto the HSM on machine #2, by running the command:

```
>new-world -l
```

For more information, refer to the *User Guide* for the HSM.

12. On machine #2, run the CNG Configuration Wizard and select `Use existing security world`.
13. Install the CA using the nCipher Security World Key Storage Provider, with the following settings:
    a. In the `Add Roles Wizard`, in the `Set up Private Key` window, select `Use an existing private key` and select the option `Select an existing private key on this computer`. Click `Next`.
    b. In the `Select Key` window, click `Edit` and select the CSP that contains the created key
    c. Empty the search field and click `Search`.
    d. Select the key that you want to use for this CA, select the key that you generated on machine #1, and click `Next`.
    e. Select the appropriate hash algorithm, and then select `Allow administrator interaction when the private key is accessed by the CA`. Click `Next`.
    f. In the CA name window, click `Next`.
    g. In the `Set validity period` window, select the validity period for the certificate generated for this CA and click `Next`.
    h. In the `Certificate database` window, specify the certificate database location and click `Next`.
    i. In the `Confirmation` window, click `Install`.
    j. In the Installation Results window, click `Close`.
14. Copy the backed-up CA database data onto machine #2.
15. Run the following command:

```
>certutil -shutdown
```

17. On machine #2, restore the CA database by running the command:

```
>Certutil.exe -f -restoredb <BackupDirectory>
```

19. Restart the CA by running the command:

```
>net start certsvc
```

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

```
>sc query certsvc
```

2.4 Install OCSP

If you are installing OCSP on a different server from the CA, see "Install the software and create or share the Security World" on page 8 for instructions on sharing the Security World.

To install Online Responder Services:

1 From the `Start` menu, select `Administrative Tools > Server Manager`.

2 In the left pane, right-click `Roles` and click `Add Roles`.

3 On the `Before You Begin` screen, click `Next`.

4 On the `Select Server Roles` screen, select `Active Directory Certificate Services` and click `Next` twice.

5 In the `Select Role Services` section, select `Online Responder`. The `Add Role wizard` appears, prompting you to add role service and features required for Online Responder. Click on `Add required role service` and click `Next`.

6 On the `Web Server(IIS)` screen, click `Next`.

7 On the `Select role service to install for web server(IIS)` screen, keep the default selection and click `Next`.

8 On the `Confirm Installation Selections` screen, check that everything is correct and click `Install`.

9 Once the set-up is complete, check that there were no errors and click `Close`.

2.4.1 Configure the CA to issue an OCSP Response Signing Certificate

This section describes how to update the OCSP certificate template for use with the key storage provider CNG/MSCAPI. This scenario assumes you have an Enterprise CA installed.

2.4.1.1 Configure certificate templates for your test environment

1. Go to `Start > Run`.
2. In the run dialog type `mmc` and click `OK`.
3. In the mmc console that appears go to `File > Add/Remove Snap-in`
4. In the `Add or Remove Snap-Ins` dialog box that appears find and click the `Certificate Templates` snap-in.
5. Click `Add` and then click `OK`.
6. Under `Console Root` expand `Certificate Templates` snap-in. All the available certificate templates that you can make your CA issue are listed in the middle section.
7. Scroll down the list until you locate the `OCSP Response Signing` template. Right-click the `OCSP Response Signing template` and click `Properties`.
8. In the popup dialog that appears click the `Security` tab and click `Add`.

9. In the Select User, Computers, or Groups dialog that appears type the name of the machine that is hosting the Online Responder service.
10. Click OK.

    The machine is not immediately located. Another dialog appears.

12. In this dialog click Object Types and make sure the check box next to Computers is checked, and then click OK.
13. Re-enter machine name in the Select User, Computers, or Groups dialog if it is not already there and click OK.

    The machine hosting the Online Responder is added to the Group and user names area under the Security tab.

15. Click the machine name in the Group and user names area and under the Permissions area make sure that the Read, Enroll and Autoenroll check boxes are ticked. Click Apply and then Ok.
16. Click Request Handling tab and make sure that both Authorize additional service accounts to access the private key and Allow private key to be exported are disabled.
17. Click the Cryptography tab.
18. Select the algorithm, hash and key size you want to use from the Algorithm Name drop-down combo box. We recommend that you choose the same algorithm as your CA is using, although you can use any.
19. Below the combo box are two radio buttons:
    - Requests can use any provider on the clients machine
    - Requests must use one of the following providers

    Select the second option so that it becomes active.

21. Check the box that opens next to the nCipher Security World Key Storage Provider entry.
22. Click Apply and then OK.
23. Select the Subject Name tab.
24. The radio button Build this from Active Directory Information is selected. In this box there are 4 check boxes:
    - E-mail
    - DNS name
    - User principal name (UPN)
    - Service principal name (SPN)

    Make sure that only Service Principal Name (SPN) is checked. Uncheck any other checked boxes. Then click Apply and then OK.

2.4.2 Configure the CA to support the Online Responder service

1. Go to Start > Control Panel > Administrative Tools > Certification Authority.
2. Navigate to the Action menu and click Properties.
3. Select Extensions tab. In the Select extension list, click Authority Information Access (AIA).
4. Click Add and in the Add Location dialog box type under Location http://machinename/ocsp.

5. Click OK.
6. On the Extensions tab make sure that the URL that was just added to the locations area is highlighted. Then make sure the check boxes next to Include in the AIA extension of issued certificates and Include in the online certificate status protocol (OCSP) extension are ticked.
7. Click Apply and let the service restart and click OK.
8. In Certification Authority, right-click Certificate Templates, and then click New Certificate Templates to Issue.
9. In Enable Certificates Templates, select the OCSP Response Signing template and any other certificate templates that you configured previously, and then click OK.
10. Open Certificate Templates in the Certification Authority and verify that the modified certificate templates appear in the list.

2.4.3 Request a certificate from OCSP Response Signing template

1. Open the command prompt and run the following command:

```
>certutil -pulse
```

3. Go to Run, type mmc and click OK.
4. In the mmc console that appears, select File > Add/Remove Snap-in.
5. In the Add or Remove Snap-Ins pop-up dialog that appears, find the Certificates snap-in (under the Available snap-ins section).
6. Click the snap-in and click Add.
7. In the dialog that appears, check the Computer Account radio button, and then click Next.
8. In the Select Computer dialog, ensure that Local Computer is selected and click Finish.
9. Click OK.
10. Under the Console Root, expand the Certificates heading.
11. Select the Personal folder and expand it.
12. Right-click Certificates and select All Tasks > Request New Certificate.
13. On Before You Begin page, click Next.
14. On Select Certificate Enrollment Policy page, Click Next.
15. On Request Certificates page, select OCSP Response Signing template and click Enroll.
16. If you select the nCipher Key Storage Provider in the OCSP template, you will be prompted to create a new key. Click Next and select a method to protect the new key, then click Finish.

If your default protection mechanism is module-only protection, then you will not be prompted to create a new key.

17. On Certificate Installation Results page, select Finish.
18. Select the Personal folder and expand it.

19. Select the Certificates folder. In the middle pane, an OCSP certificate appears.
20. Right-click the certificate and click Properties.
21. Under the General tab in the dialog box that appears. Under Certificate Purposes select Enable Only for the following purposes.
22. Click Apply and then OK.

2.4.4 Modify the Online Responder service to use an nCipher nShield HSM

1. Select Start > Administrative Tools > Services..
2. Locate the Online Responder Service in the list of services.
3. Right-click the Online Responder Service and select Properties.
4. In the dialog box that appears select the Log on tab.
5. Under the Log on as heading, hover over the radio button next to Local System account and click. The heading Allow service to interact with desktop becomes active with a check box next to it.
6. Select the check box.
7. Click Apply and then OK.
8. From the Services window, right-click Online Responder Service and restart the service.

2.4.5 Set up a revocation configuration

A revocation configuration is needed to respond to status requests about certificates that have been issued by a specific CA. Revocation configuration settings include:

- The CA certificate.
- The signing certificate for the online responder.
- The locations that clients can send their requests to.

To set up a revocation configuration:

1. Select Start > Administrative Tools > Online Responder Management..
2. In the left-hand pane click Revocation Configuration.
3. In the right-hand pane under Actions click Add Revocation Configuration.
4. Click Next on the Getting started with adding a revocation configuration section.
5. In the Name the Revocation Configuration section, type a name for the configuration in the text box. (For this example we use Test). Then click Next.
6. In the Select CA Certificate Location section ensure that the Select a certificate for an Existing enterprise CA radio button is checked and click Next.
7. Under the Choose CA Certificate section ensure that the Browse CA certificates published in Active Directory radio button is selected and then click Browse.
8. In the Select Certification Authority dialog box that opens select the CA and click OKthen Next.
9. In the Select Signing Certificate section ignore the default settings and make sure the Manually select a signing certificate radio button is selected. Click Next.

10. If you are installing OCSP on a different server to the CA:
    a. On the Revocation Provider section click on Provider tab. It will open Revocation Provider Properties.
    b. Under Base CRLs click on Add.
    c. Enter **http://<OCSP hostname>/ocsp/<CA-name>.crl** in the Open URL dialog box and click OK.
    d. Under Base CRLs select the above URL, click Move Up button and then click OK.
    e. Copy **crl** files from the **c:\Windows\System32\certsrv\CertEnroll** folder of the CA server to the **C:\Windows\SystemData\ocsp** folder of the OCSP server.
11. In the Revocation Provider window, click Finish. A dialog box opens stating Executing the specified action.... Let this finish.
12. When the wizard completes, the status of the Online Responder is shown in the Revocation Configuration Status box as Bad Signing Certificate on Array Controller.
13. To fix this, click Array Configuration in the left-hand pane and expand it.
14. In the directory tree, click the machine name that is being used.
15. The revocation configuration that you just created is listed in the middle section, in this case Test.
16. In the right-hand pane, click Assign a signing certificate.
17. Click the certificate that you set up earlier and is listed in the dialog box that opens. Click OK.
18. Go back to the Revocation Configuration pane and right-click the revocation configuration you created (in this case Test) and then click Edit Properties.
19. A Properties for Revocation Configuration: Test pane opens. Three tabs are available:
    - Local CRL
    - Revocation Provider
    - Signing

    Click the Signing tab.
21. Uncheck the Do not prompt for credentials for cryptographic operations check box and click OK.
22. Go back to Online Responder Management, go to Actions and click Refresh.
23. In the left-hand pane click Online Responder: Computer Name and check that the Revocation Configuration Status shows as Working.

2.4.6 Verify that OCSP works correctly

2.4.6.1 Generate a certificate request

1. Open Notepad and create a file called rsa.inf with contents similar to the following on your local C drive:

```
[Version]
Signature = "$Windows NT$"
```

```
[NewRequest]
Subject = "CN=TEST-CA"
HashAlgorithm = SHA512
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "nCipher Security World Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
RequestType = PKCS10
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.1
[Extensions]
1.3.6.1.5.5.7.48.1.5 = Empty
```

In the file above replace the subject with your CA common name.

4. Go to your local directory and check it contains the file `rsa.inf`.
5. From the command prompt navigate to your local C drive and add:

```
>Certreq –new rsa.inf rsa.req
```

7. Check that `rsa.req` is listed in the directory.
8. In the command line run the command:

```
>certreq –submit –attrib –CertificateTemplate:WebServer rsa.req
```

10. Click `OK` to select the CA certificate and save it as `rsa.cer` in your local directory.
11. Navigate to the directory where you saved the certificate and look for `rsa.cer`.

2.4.6.2 Retrieve information about the certificate's AIA, CRLs, and OCSP

1. To check that clients can still obtain revocation data in the command prompt, navigate to the folder where the certificate is stored, then type:

```
>Certutil –url rsa.cer
```

The URL Retrieval Tool appears.

4. Select `Certs (from AIA)`.
5. Click `Retrieve`.

   The list contains the verified Certificate and its URL.

7. Select `CRLs (from CDP)`.
8. Click `Retrieve`.

9. The list contains the verified status, type of the CRL and its URL.
10. Select `OCSP (from AIA)`.
11. Click `Retrieve`.
12. The list contains the Verified OCSP URL.
13. Click `Exit`.

2.4.6.3 Verify the OCSP Server is Active

1. To check details about the certificate and its CA configuration in the command prompt, navigate to the folder wher the certificate is stored, then type:

```
>Certutil -verify rsa.cer > rsa.txt
```

3. Open the text file `rsa.txt`.The last few lines should be as follows:

```
Verified Issuance Policies: None
Verified Application Policies:
 1.3.6.1.5.5.7.3.1 Server Authentication
Leaf certificate revocation check passed
CertUtil: -verify command completed successfully.
```

This shows that the OCSP Server is working correctly and there were no errors.

2.5 Uninstall AD CS and OCSP

To uninstall AD CS and OCSP:

1. Open `Server Manager`.
2. Select `Roles > Remove Roles`. The Remove Roles Wizard opens.
3. Click `Next`.
4. Deselect `Active Directory Certificate Services and Online Responder`, and click `Next`.
5. Restart the machine when prompted.

3 Troubleshooting

The following table provides troubleshooting guidelines.

Problem	Cause	Resolution
Online Responder reports `Bad Signing Certificate on Array Controller`.	This error occurs when the CA certificate is stale or cannot be located by the Online Responder client.	Ensure that the steps above have been correctly carried out. Also, ensure that the CA is correctly configured and that a valid CA certificate exists for OCSP Signing.
Using certutil —url <certnamehere.cer> and selecting `Certs (from AIA)` shows an entry in the list called AIA with `Failed` next to it.	This error occurs when Certificate Authority Web Enrolment is not installed on the CA.	Install Certificate Authority Web Enrolment on the CA machine. Go to `Server Manager`. Expand the `Roles` section (in the left-hand section) and click `Active Directory Certificate Services`. In the bottom right-hand section, click `Add Role Services` and select `Certificate Authority Web Enrolment`.
Using the certreq —new <.req file here> command returns an Invalid Provider Specified error.	This error occurs when the CSPs are not installed and set up on the client machine or not set up correctly.	Ensure that the nCipher CAPI CSP and nCipher CNG CSP providers are correctly installed and set. (Do this by running the CSP Install Wizard and CNG Configuration Wizard under nCipher in the Start menu).
When using the CAPI or CNG wizard to access a private key protected by an OCS with password, you are prompted multiple times to enter the password.	This error is due to a problem in Windows Server 2008R2.	To prevent this from happening, download and install the hotfix available at the following location: http://support.microsoft.com/kb/2740017/EN-US

Contact Us

Web site:	https://www.ncipher.com
Support:	https://help.ncipher.com
Email Support:	support@ncipher.com
Online documentation:	Available from the Support site listed above.

You can also contact our Support teams by telephone, using the following numbers:

Europe, Middle East, and Africa

United Kingdom:	+44 1223 622444 One Station Square Cambridge CB1 2GA UK

Americas

Toll Free:	+1 833 425 1990
Fort Lauderdale:	+1 954 953 5229 Sawgrass Commerce Center – A Suite 130, 13800 NW 14 Street Sunrise FL 33323 USA

Asia Pacific

Australia:	+61 8 9126 9070 World Trade Centre Northbank Wharf Siddeley St Melbourne VIC 3005 Australia
Japan:	+81 50 3196 4994
Hong Kong:	+852 3008 3188 10/F, V-Point, 18 Tang Lung Street Causeway Bay Hong Kong

www.ncipher.com

About nCipher Security

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security, a leader in the general purpose hardware security module (HSM) market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. www.ncipher.com

Search: nCipher Security

TRUST. INTEGRITY. CONTROL