Microsoft AD CS

nShield® HSM Integration Guide

2026-06-15

Member of
Microsoft Intelligent
Security Association

Microsoft Security

Table of Contents

Chapter 1. Introduction

This guide describes how to integrate an nShield Hardware Security Module (HSM) with Microsoft Active Directory Certificate Services (AD CS) and how to set up a root Certificate Authority (CA). It also demonstrates CRL-based testing for the validation of certificate revocations, and optional set up procedures for the Online Responder.

Microsoft AD CS provides the functionality for creating and installing a 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 CA uses the Entrust nShield HSM to protect their private keys. The CA also uses the HSM for important operations such as key generation, certificate signing, and CRL signing. The nShield HSM can be configured to protect the private keys and meet FIPS 140-2 Level 2 or Level 3.

Instructions in this guide are given both for Microsoft Windows Server Enterprise and Server Core. Server Core is a minimalistic installation option of Windows Server. Server Core does not include a GUI, it is designed to be managed remotely through the command line, PowerShell, or from another computer via a remote GUI tool. In addition to this Server Core, the installation does not include all the Windows Server roles and services included in the Standard and Datacenter editions. These roles and services must be configured and managed from a remote computer. Wherever a step in this guide is different for Windows Server Enterprise and Windows Server Core, instructions are provided for both.

1.1. Product configurations

Entrust has successfully tested integrating nShield HSM integration with Microsoft Windows Server 2016 (Standard, Datacenter, and Server Core editions), Microsoft Windows Server 2019, 2022, and 2025, and Microsoft AD CS in the following configurations:

Microsoft Windows Server	nShield HSM	nShield Security World Software	nShield Security World Firmware
2016 2019 2022 2025	Solo XC Connect XC	12.60.3 12.60.7 12.60.11 12.70.4 12.71.0 12.80.4 13.3.2 13.4.5 13.6.3 13.6.5 13.6.8 13.6.12 13.6.14	12.50.11 (FIPS 140-2 certified) 12.72.1, 12.72.3 and 12.72.4 (FIPS 140-2 certified)
2016 2019 2022 2025	nShield 5c	13.3.2 13.4.5 13.6.3 13.6.5 13.6.8 13.6.12 13.6.14	13.4.5 (FIPS 140-3 certified)
2022	Edge	12.80.4	12.72.0 (FIPS 140-2 certified)

1.2. Supported nShield functionality

Feature	Support	Feature	Support
Softcards	Yes	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

Feature	Support	Feature	Support
Fail over	Yes	Mixed Estate	Yes

CA failover clustering is only supported with network attached HSMs (nShield Connect).

1.3. Requirements

Before installing these products, read the associated documentation:

- For the nShield HSM, read the *Installation Guide* and *User Guide* for the HSM.
- Microsoft AD CS and OCSP documentation (https://docs.microsoft.com).

Entrust also recommends that you have an agreed organizational Certificate Policy and Certificate Practice Statement, and a Security Policy or Procedure in place covering administration of the PKI and 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, Softcard, 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 nShield Cryptographic Service Providers for Microsoft Cryptographic API: Next Generation (CNG) or CryptoAPI (CAPI).
- Whether to initialize the nShield Security World as Recoverable. This is highly recommended and is the default option when initializing a Security World.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Entrust recommends that you use CNG for full access to available features and better integration with Microsoft Windows Server editions.

1.4. More information

For more information about OS support, contact your Microsoft sales representative or Entrust nShield Support, https://nshieldsupport.entrust.com.

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

Chapter 2. Environment setup procedures

2.1. Install the HSM

Install the HSM using the instructions in the *Installation Guide* for the nShield HSM.

Entrust recommends that you install the HSM before you configure the Security World software and before you install and configure AD CS.

If you already have an HSM installed and a Security World configured, proceed to install AD CS.

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. Entrust recommends that you 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 will be using this Security World when you are installing and registering either CSP or CNG providers.

3. Register the CSPs that you intend to use:
   - Windows Server Enterprise:

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

   - Windows Server Core:

     ```
     > cnginstall --install
     > cngregister
     > capingwizard
     ```

4. If you are going to use Key Counting using the nShield CNG/KSP with the CA, you

need to create a `CAPolicy.inf` file in the `%Windows%` directory before installing the CA role, and set a registry value. The Registry container is `HKLM\Software\nCipher\CryptoNG\` and the Registry Key is `UseCountEnabled` which must be set to 1. See Install Certificate Services.

5. If you are intending to use Module protection, pool mode can be configured using the relevant CNG or CAPI wizards. To enable pool mode using the CNG wizard:

   a. Launch the **CNG configuration** wizard, and select the **Enable HSM Pool Mode** screen.

   b. Select the **Enable HSM Pool Mode for CNG Providers** option.

   To enable pool mode using the CSP wizards:

   a. Select **32bit CSP install** wizard or **64bit CSP install** wizard (depending on the platform in use).

   b. Launch the **32bit CSP install** wizard or the **64bit CSP install** wizard, and select the **Enable HSM Pool Mode** screen. Select the **Enable HSM Pool Mode for CAPI Providers** option.

Chapter 3. AD CS Procedures

3.1. Install and configure AD CS with Windows Server Enterprise

If you are using Windows Server Core, see Install and configure AD CS with Windows Server Core.

To create an AD-integrated CA, that is, an Enterprise CA, an account with Enterprise Administrator level privileges is required for the role configuration.

1. Join the domain.
2. Select **Start > Server Manager** to open Server Manager.
3. Select **Manage**, then select **Add Roles & Features**. The **Before you begin** window opens. Select **Next**.
4. On the **Select installation type** window, make sure the default **Role or Feature Based Installation** is selected. Select **Next**.
5. On **Server selection**, select a server from the server pool. Select **Next**.
6. On the **Select server roles** window, select the **Active Directory Certificate Services** role.
7. When prompted to install Remote Server Administration Tools, select **Add Features**. Select **Next**.
8. On the **Select features** window, select **Next**.
9. On the **Active Directory Certificate Services** window, select **Next**.
10. On the **Select role services** window, the **Certification Authority** role is selected by default. Select **Next**.
11. On the **Confirm installation selections** window, verify the information, then select **Install**.
12. When the installation is complete, select the **Configure Active Directory Certificate Services** on the destination server link.
13. On the **Credentials** window, make sure that **Administrator's credentials** is displayed in the **Credentials** box. If not, select **Change** and specify the appropriate credentials. Select **Next**.
14. On the **Role Services** window, select **Certification Authority**. This is the only available selection when the certification authority role is installed on the server. Select **Next**.
15. On the **Setup Type** window, select the appropriate CA setup type for your

requirements. Select **Next**.

16. On the **CA Type** window, **Root CA** is selected by default. Select **Next**.
17. On the **Private Key** window, leave the default selection to **Create a new private key** selected. Select **Next**.
18. On the **Cryptography for CA** window, select the appropriate nShield cryptographic provider along with the key type, key length and suitable hash algorithm:
    - RSA #nCipher Security World Key Storage Provider
    - ECDSA_P256 #nCipher Security World Key Storage Provider
    - ECDSA_P384 #nCipher Security World Key Storage Provider
    - ECDSA_P521 #nCipher Security World Key Storage Provider

    If OCS or Softcard protection is used, select the **Allow administrator interaction when the private key is accessed by the CA** option.
19. Select **Next**.
20. On the **CA Name** window, give the appropriate CA name. Select **Next**.
21. On the **Validity Period** window, enter the number of years for the certificate to be valid. Select **Next**.
22. On the **CA Database** window, leave the default locations for the database and database log files. Select **Next**.
23. On the **Confirmation** window, select **Configure**.
24. If you select **nCipher cryptographic service provider** on the **Cryptography for CA** window, the **nCipher key storage provider-create a key** wizard prompts you to create a new key. Select **Next** and **OK**. Select a way to protect the new key. Select **Next**.

If either Softcard or OCS (token) protection was chosen when the CSP /CNG providers were installed using the wizards, you will be prompted to either enter Softcard Passphrase / PIN or present the OCS and credential. There will be no prompt if Module protection was chosen.

If you are using a FIPS 140-2 Level 3 Security World, you will need to present either a card from the ACS or OCS for FIPS authorization before the AD CS key can be generated, irrespective of your chosen protection method.

25. When the passphrase(s) has been successfully presented, close the wizard.

The **Progress** window opens during the configuration processing, then the **Results** window opens. Select **Close**. If the **Installation**

> **progress** window is still open, select **Close** on that window also.

26. Register `nFast Server` as a dependency of AD CS with the `ncsvcdep` tool in the `nfast/bin` directory; this is needed as the nShield service must have started before CA, otherwise the nShield CNG providers will fail.

    Run the command:

    ```
    >ncsvcdep -a certsvc
    ```

27. Verify that the CA service has started successfully by running the following command on the command line. Use **Windows key + R** to open the **Run** dialog, and type `cmd` to open the command prompt.

    Run the command:

    ```
    >sc query certsvc
    ```

    Output:

    ```
    SERVICE_NAME        : certsvc
    TYPE                : 110 WIN32_OWN_PROCESS (interactive)
    STATE               : 4 RUNNING
    (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE     : 0 (0x0)
    SERVICE_EXIT_CODE   : 0 (0x0)
    CHECKPOINT          : 0x0
    WAIT_HINT           : 0x0
    ```

3.2. Install and configure AD CS with Windows Server Core

If you are using Windows Server Enterprise, see Install and configure AD CS with Windows Server Enterprise.

1. Join the domain by running the command:

   ```
   > netdom join $(hostname) /domain:<full_DNS_domain_name> /userd:<user_name> /passwordd:<password>
   ```

2. Restart the machine after joining the domain by running the command:

   ```
   > shutdown /r /t 0
   ```

3. Enable WOW64 if you are working with 32-bit applications.

4. Run PowerShell as admin user.
5. Install CA binaries via PowerShell, by running the command:

```
> Add-windowsfeature ADCS-Cert-Authority --IncludeManagementTools
```

6. Configure CA via PowerShell, by running the command:

```
> Install-AdcsCertificationAuthority –AllowAdministratorInteraction –caType EnterpriseRootCA
–CryptoProviderName ECDSA_P256#HSM_KSP_NAME –KeyLength 256 –HashAlgorithmName SHA256
```

   Example:

```
> Install-AdcsCertificationAuthority –AllowAdministratorInteraction –caCommonName "Fips-128-Module-CA-1"
–caType EnterpriseRootCA –CryptoProviderName "RSA#nCipher Security World Key Storage Provider" –KeyLength
2048 –HashAlgorithmName SHA256
```

7. When the confirmation message appears, type **A** and press **Enter**.

3.2.1. 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
```

The expected output is:

```
SERVICE_NAME        : certsvc
TYPE                : 110 WIN32_OWN_PROCESS (interactive)
STATE               : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE     : 0 (0x0)
SERVICE_EXIT_CODE   : 0 (0x0)
CHECKPOINT          : 0x0
WAIT_HINT           : 0x0
```

3.3. Configure auto-enrollment group policy for a domain

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

1. On the domain controller, select **Start > Administrative Tools > Group Policy Management**.
2. Select **Forest**, then select your Domain and expand it.

3. Double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy Group Policy object (GPO)** that you want to edit.
4. Right-click the **Default Domain Policy GPO**, then select **Edit**.
5. In the **Group Policy Management Editor**, select **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
6. Double-click **Certificate Services Client - Auto-Enrollment**.
7. In **Configuration Model**, select **Enabled to enable auto-enrollment**. Select the following options:
    - Renew expired certificates, update pending certificates, remove and revoke certificates.
    - Update certificates that use certificate template.
8. Select **Apply** and **OK** to accept your changes and close the Editor.

3.4. Configure the HSM with Certificate Services

3.4.1. Configure Certificate Services with a new key

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

1. Install and configure the HSM hardware and software as described in Install Security World.
2. Install Microsoft Active Directory Certificate Services as described in Install and configure AD CS with Windows Server Enterprise, with the following settings:
    - In the **Private Key** window, select **Create a new private key**. Select **Next**.
    - Continue the CA setup as described in the section Install and configure AD CS with Windows Server Enterprise.

3.4.2. Configure Certificate Services using an existing private key

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

1. Install and configure the HSM hardware and software as described in .
2. Install Microsoft Active Directory Certificate Services as described in Install and configure AD CS with Windows Server Enterprise.
3. In the **Private Key** window, select **Use existing private key**, then **Select an existing private key on this computer**. Select **Next**.

4. In the **Select Existing Key** window, select **Change**.
5. In the **Change Cryptographic Provider** window, select the CSP that contains the created key. Delete the contents of the **CA common name** field, then select **Search**. The search finds the existing private key. Select the key, then select **Allow administrator interaction when the private key is accessed by the CA**. Select **Next**.
6. In the **Cryptography for CA** window, select the appropriate hash algorithm. Select **Next**.
7. In the **CA Name** window, select **Next**.
8. In the **Validity Period** window, specify the validity period. Select **Next**.
9. In the **CA Database** window, specify the certificate database locations and certificate database log locations. Select **Next**.
10. In the **Confirmation** window, select **Configure**.
11. Wait for the configuration to complete. After successful completion, close the **AD CS configuration** window.
12. Verify that the CA service has successfully started by running the command:

```
> sc query certsvc
```

13. Verify the CA key by running the command:

```
> certutil -verifykeys
```

3.5. Configure Certificate Enrollment to use CA templates on the AD CS Server

This section describes how to create certificate templates when the private key is managed using an HSM. All subscribers who enroll for a certificate based on such a template must have a client connection to the HSM.

If a CA installed on Windows Server Core is managed remotely, the snap-ins in this section must be run on a separate machine with GUI capabilities.

To integrate the CA certificate enrollment functionality with a CA private key generated by an nShield HSM:

1. Create a CA template that uses the nShield HSM KSP:
   a. Run `certtmpl.msc`.

b. Right-click the **Administrator** template, then select **Duplicate Template**. The **Properties** window opens, showing **Compatibility** tab.

c. Select **Windows Server 2016 Under Certificate Authority and Certificate Recipient** drop-down box.

d. Select the **General** tab. In **Template Display Name**, type a name for the template.

e. Select the **Request Handling** tab, and in **Purpose**, select **Signature** and deselect **Allow private key to be exported.**

f. Select the **Cryptography** tab and in the **Provider** category select **Key storage provider**.

g. In **Algorithm Name**, select the algorithm from the list.

h. Select **Requests must use one of the following providers** and in **Providers**, select **nCipher Security World Key Storage Provider only**.

If CA is on **Windows Server Core** and you are managing it remotely using `certtmpl.msc` on a different PC, you need to install the nShield Key Storage Provider on the PC that is running `certtmpl.msc`. Otherwise, the nShield provider will not appear.

i. In **Request Hash**, select a hash type.

j. Select **Subject Name** tab and deselect **Include e-mail name** in subject name and deselect **E-mail name**.

k. Select **Apply** and **OK** to save the template settings and close the **Certificate Template** console.

2. Make sure the `RpcLocator` service is running, then run `certsrv.msc`.

   Windows Server Core:

   - If a CA is configured on Windows Server Core and is managed via the Microsoft Management Console (MMC) from a different machine, you might get an error which states: **Cannot manage Active Directory Certificate Services**. To fix this, select **OK**, then in the `certsrv.msc` console that appears, select **Action → Retarget Certification Authority**. In the window that appears, select **Another Computer**, then select **Browse** to find the CA you want to manage.
   - Sometimes an error appears indicating that the RPC server is unavailable. To fix this, sign in to the Windows Server Core machine and minimize the command prompt. A window prompts you to load a key. Complete the steps in the window and attempt to select the CA again from `certsrv.msc`.

3. In the left-hand pane, double-click the CA name.

4. Right-click the **Certificate Template** node, then select **New > Certificate Template to Issue**.
5. Select the template you just created, then select **OK**.
6. Request a certificate based on the template:
    a. Run `certmgr.msc`.
    b. In the left-hand pane, right-click the **Personal** node, then select **All Tasks > Request New Certificate**.
    c. Select **Next** in the first two windows.
    d. Select the template that you created, then select **Enroll**.

If a CA installed on Windows Server Core is managed remotely, steps e-h may not take place. A new key is still created to be associated with the certificate. If the STATUS: Succeeded message appears, the procedure is complete.

    e. The **Key Storage Provider** window appears. Select **Next**.
    f. Insert the Administrator card(s), and enter the passphrase or pin when prompted.
    g. Proceed to create the new key to be associated with the certificate.
    h. Select the type of protection you want to use. Select **Next**.
    i. Depending on key protection method, enter the required credentials. The **Certificate Installation Results** window should show **STATUS: Succeeded**. Select **Finish**.

If passphrase authentication is enabled, a prompt for passphrase appears.

7. Verify that the certificate is enrolled successfully. If the certificate fails to enroll because the CA is not started or the RPC ports are blocked, the following error appears:

```
Error: the RPC server is unavailable. 0x800706ba (win32: 1722 RPC_S_SERVER_UNAVAILABLE
```

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

3.6. Set up key use counter

3.6.1. Key use counter overview

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

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

The key use counter audits usage of the CA signing key. It maintains a count of how many times the key has been used. The key use counter should only be used 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.

Note the following information about the key use counter:

- The counter is in the NVRAM of the HSM. To access the key count value in NVRAM, users must present the ACS to 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 select which HSM stores the counter.
- If the module firmware is upgraded, the counter value is lost.
- The key counter can only be set at HSM initialization. It cannot be activated after deployment.

3.6.2. Install Certificate Services with key use counter

To install Certificate Services with key use counter:

1. If it is not already on your system installation, create the `%SystemRoot%\capolicy.inf` file, 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.

2. Install the CA using the HSM KSP.
3. Enable auditing for the CA service by running the command:

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

4. Stop the `certsvc` service. Run:

```
> net stop certsvc
```

5. Select **Start > Administrative Tools > Certification Authority**, right-click the CA, then select **Properties**.
6. Select the **Auditing** tab and check the box for **Start and Stop Active Directory Certificate Services**.
7. Select **Start > Administrative Tools > Local Security Policy**.

   Windows Server Core:

   - You need to follow steps 7-10 on the machine that is remotely managing the Windows Server Core, export the local security policy, then import it to the Windows Server Core machine.
8. Select **Local Policy**, expand it, then select **Audit Policy**.
9. In the right pane, double-click **Audit Object Access**, then select **Success and Failure**.
10. Select **Apply**, select **OK**, then close the window.

    Windows Server Core:

    - After step 10, run `secpol.msc`. Select **Security Settings > Export Policy**. Give the `.inf` file a name, then select **Save**. Transfer the file from this machine to Windows Server Core, then run the following command:

      ```
      secedit.exe /configure /db Windows\security\local.sdb /cfg C:\securitypolicy.inf
      ```

      When this command completed successfully, continue with step 11.
11. Update the local security policies by opening a command prompt and running the command:

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

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

```
> net start certsvc
```

You will be prompted to enter the CA certificate credentials upon CA restart.

13. Run `Eventvwr.exe`.

    Windows Server Core:

    Launch the **Microsoft Management Console**. Select **File → Add/Remove Snap-in → Event Viewer → Add**. In the window that appears, select **Another computer**, then select **Browse**. Enter the name of the machine, then select **OK** several more times. Event Viewer should now be managing the Windows Server Core machine remotely.

14. Select **Windows Logs > Security**.
15. Filter for event ID 4881 (CA startup event) or event ID 4880.
16. Verify the CA startup event shows the **PrivateKeyUsageCount** property with a corresponding value.

Chapter 4. CRL-Based Revocation Validation

4.1. CRL-Based testing

This section documents the testing performed for validation of certificate revocations using Certificate Revocation Lists (CRLs), without requiring an Online Certificate Status Protocol (OCSP) Online Responder.

This test does not require a configured OCSP Online Responder. It is intended for environments where OCSP support is not available or the Online Responder is not installed.

4.1.1. Prerequisites

The testing in this section was conducted in an AD CS environment configured as follows:

- AD CS is installed, and a Certification Authority (CA) has been set up and initialized.
- CA services are running, and not stopped.
- An nShield HSM is set up and connected to Security World software.

4.1.2. Procedures

4.1.2.1. Certificate Enrollment

You can skip this step if your environment contains a valid test certificate signed by your Certification Authority.

1. Launch `certmgr.msc`.
2. Right-click the folder labeled **Personal** and select **All Tasks** > **Request New Certificate**.
3. Complete the Wizard:
   a. Select **Next** in the first two windows.
   b. Select the template that you created, then select **Enroll**.
   The **Key Storage Provider** window appears.

If a CA installed on Windows Server Core is managed remotely, the next steps may not appear. A new key is still created to be associated with the certificate. If the STATUS: Succeeded message appears, the procedure is complete.

c. Select **Next**.
d. Insert the administrator cards and enter the passphrase or PIN when prompted.
e. Create the new key to be associated with the certificate.
f. Select the type of protection you want to use, then select **Next**.
g. Depending on the key protection method, enter the required credentials.
The **Certificate Installation Results** window should show **STATUS: Succeeded**.
h. Select **Finish**.

If passphrase authentication is enabled, a prompt for passphrase appears.

4. Verify that the certificate is enrolled.

4.1.2.2. Certificate Verification

1. Launch the Certification Authority application, `certsrv.msc`, and find your Certificate within the `Issued Certificates` folder`.
2. Double-click your certificate to open its information, then select the **Details** tab.
3. Ensure the following fields are correct and match your configuration specifications:
   - **Issuer**: Ensure your CA's name is listed.
   - **Signature Algorithm**: Ensure this certificate is using the correct signing algorithm.
   - **Serial Number**: Ensure this field exists; note the serial number for future reference.

4.1.2.3. Export the Certificate

1. On the certificate **Details** tab, select **Copy to File**.
2. Complete the Certificate Export Wizard:
   - On the Welcome page, select **Next**.
   - On the Export File Format page, select `Base-64 encoded X.509 (.cer)`, then select **Next**.
   - Input a name for the file, then select **Next**.
   - On the last page, note the location of the exported file and select **Finish**. Select **OK** in the pop-up and confirm that the export was successful.

4.1.2.4. Revoke the Certificate

When revoking certificates, it is recommended that you use a test certificate first, for trial purposes. Complete the above steps to

> generate a trial certificate for revocation.

1. Launch the Certification Authority application, `certsrv.msc`, and find your certificate in the `Issued Certificates` folder`.
2. Right-click your certificate and select **All Tasks > Revoke Certificate**.
3. The Certificate Revocation window appears, prompting you for a valid **Reason Code**. Select a reason, or **Unspecified**, and then select **Yes** to revoke the certificate.
4. Close and reopen the Certification Authority application. You should now see your certificate under the `Revoked Certificates` folder`.

4.1.2.5. Publish the new CRL

Using the Certification Authority GUI:

1. Launch `certsrv.msc`, if it is not already open.
2. Right-click the `Revoked Certificates` folder and select **All Tasks > Publish** to publish a new CRL.
3. When the Publish CRL window appears, select **New CRL** and then **OK** to finish.

Using the CLI:

1. Publish a new CRL:

```
> certutil -crl
```

2. (Optional) Force the new CRL to be used:

```
> certutil -setreg chain\ChainCacheResyncFiletime @now
```

4.1.2.6. CRL Verification

1. Using the CLI, navigate to the location of your exported certificate. Run the following command and replace `testcert.cer` with your exported certificate's full file name:

```
> certutil -verify -urlfetch .\testcert.cer
```

2. The expected result is below. The last few lines show that the certificate was properly revoked and the CertUtil command completed without issue.

```
> certutil -verify -urlfetch .\testcert.cer
Issuer:
CN=interop-ADCSOCSPWINS25-CA
```

```
DC=interop
DC=local
Name Hash(sha1): ...
Name Hash(md5): ...
Subject:
.
.
.
The certificate is revoked. 0x80092010 (-2146885616 CRYPT_E_REVOKED)
------------------------------------
Certificate is REVOKED
Leaf certificate is REVOKED (Reason=0)
CertUtil: -verify command completed successfully.
```

Chapter 5. OCSP Procedures

5.1. Install the OCSP Responder role

The Online Responder is a Microsoft Windows service that implements the OCSP services by decoding revocation status requests for specific certificates. This is an optional role you may install within AD CS. The service provides up-to-date validation of certificates based on the contents of the latest Certificate Revocation List (CRL) issued by the CA, 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. OCSP uses the Entrust nShield HSM to protect their private keys, and also uses the HSM for important operations such as key generation, certificate signing, and CRL signing.

These steps will configure the OCSP Responder to use an HSM for generation and storage of the private key for the OCSP Responder. The OCSP Responder will provide digitally signed responses to certificate status requests from Relying Parties. An OCSP Responder provides responses for the Issuing CA or CAs that it is configured to provide responses for.

The OCSP Responder is installed on top of Microsoft Internet Information Services (IIS). The OCSP service can be installed and configured on an existing IIS system that is providing other services. This includes IIS systems configured to be PKI Repositories or CRL Distribution Points.

5.1.1. Prerequisites

- Install the Security World software both on the OCSP server and on the CA server. Share the Security World by copying the `%NFAST_KMDATA%\local` directory from the CA server to the OCSP server.
- Ensure that the HSM(s) has enough client licenses to support the OCSP Responder node.
- Configure firewall rules appropriately so that the OCSP Responder can communicate both ways, with both the HSM and the RFS on TCP 9004.
- Create a new OCSP Signing Template, based on the original version, that uses the nShield KSP for key pair generation.
- Configure the OCSP Responder as a client of the HSM and the HSM as a client of the OCSP Responder.
- Ensure that the machine where the CA is installed and which will be configured to issue the OCSP Response Signing certificate.

- Ensure that the OCSP Responder that will need access to the OCSP Response Signing private key has been set up with the following:
  - Security World software has been installed.
  - The correct CSP/CNG/KSP configured.
  - Access to the HSM or HSMs where the private key will be stored.

5.1.2. Configure the OCSP Response Signing Template for use with an HSM

The Online Responder must be set up as co-operating client/gang-client in relation to the RFS. This will ensure that it can both push and pull Security World data from the RFS.

It is recommended to use module key protection only when configuring the security for the OCSP Response signing private key(s). This will allow all generation and interaction with the private keys to be handled by the OCSP Responder without any need for administrator interaction.

1. Sign in to the machine where the CA is installed, with an account that has Domain Admin level privileges.
2. Run `certtmpl.msc` from a command prompt, or via the **Run** command.
3. Right-click the **OCSP Response Signing Template** and select **Duplicate Template**.

   The new template opens, with the Compatibility tab open.
4. Change the **Compatibility Settings** to the following:
   - Certification Authority: **Windows Server 2016**
   - Certificate Recipient: **Windows 10 / Windows Server 2016**
5. Select **OK**.

    Do not select Apply.
6. Select **General > Template Display Name** and enter a name for the new OCSP Response Signing template.
7. Select **Request handling > Authorize additional service accounts to access the private key**.
8. Select **Key Permissions**.
9. In the **Permissions** window, select **Add**, then select **Object Types**.
10. Select the **Service Accounts** option, then select **OK**.
11. In **Enter the object names to select**, enter **Network Service**, select **Check Names**, then select **OK**.

Ensure that **Network Service** has **Read** permissions.

12. The default validity period and renewal period for an OCSP Signing certificate are 2 weeks and 2 days respectively. If the private key(s) of the OCSP Signing key pair(s) are to be protected by an HSM, then the validity period of the certificate can be extended because of the improved security protection afforded by the private key(s).

    If required, change the validity period or the renewal period.

13. Select **Cryptography > Provider Category**, then select the provider from the list.
14. Select a cryptographic algorithm name from the list, then specify the minimum key size.
15. Select **Requests must use one of the following providers**. This will enable the selection of the cryptographic providers populated in the list. Select the nShield CSP or KSP as available.
16. Modify the request hash to your required hash algorithm.
17. If the environment in which the certificate will be used contains either Windows XP or Windows Server 2003 machines, do not select **Use alternate signature format**.

    The contents of the tab may take a while to appear due to the number of cryptographic providers on the server.

    If no nShield CSPs or KSPs are visible in the list of providers, ensure that both the Security World software has been installed and the relevant Configuration Wizard (CSP or CNG or both) has been run on the server.

18. Select **Security > Add**, then select **Object Types**.

    Object Types appears.

19. Select **Computers**, then select **OK**.
20. In **Select Users**, enter the name of a server that will act as an OCSP Responder, then select **Check Names**. If the name of the server is found, it will appear underlined in the box. Then select **OK**.
21. Select the server name and in **Permissions**, ensure that **Read & Enroll** permissions are selected.
22. Configure permissions for all servers that will use this template.

    If the Online Responder is installed on Windows Server Core, you also need to add the machine that is used to manage Windows Server Core remotely. Both the Windows Server Core machine and the remote machine have to be added and assigned **Read & Enroll** permissions in this step.

23. To add all servers at once, separate the names with a semi-colon (;), then select **Check Names**. If the entries are correct, all server names will be underlined. Then the permissions for each server can be set to have **Read & Enroll**.
24. Select **OK**. This will create the new OCSP Signing Template ready for use.
25. On the CA that will be making use of the OCSP Responder, enable the new template for issuance.

    a. In the Certification Authority MMC, right-click **Certificate Templates**, select **New > Certificate Template to Issue**.

    b. In Enable Certificate Templates, select the new OCSP Signing Template, then select OK.

    If the CA is installed on Windows Server Core, you need to retarget the CA to the Windows Server Core machine:

    a. Right-click **Certification Authority (Local)**, then select **Retarget Certification Authority**.

    b. Select **Another computer > Browse**, then select your CA.

5.1.3. Install Security World software on the OCSP Responder

Skip this section if the CA and OCSP Responder are on the same server because the Security World software should already be present on the server.

1. Ensure that the installer is 12.40.02 or later.
2. Do not permit the AutoRun to start the installation process. If it does, cancel or quit the installation immediately.
3. Open a File Explorer window and browse to the CD root directory.
4. Right-click `Setup.exe` and select **Run as Administrator**.
5. Depending on the configuration, your local administrator credentials may be requested to execute this step.
6. From the list of components to install, select:
    - nShield Hardware Support
    - nShield Core Tools
    - nShield CSPs (CNG, CAPI)
7. Then select **Next** on each of the dialogs which appear. The software is installed, then confirmation dialogs appear. Accept all the default parameters for these. The installer will then quit.

8. Add the `%nfast_home%\bin` directory to the system PATH environment variable. This should be done via the **Advanced System Settings** and **Environment Variables** options from the **System** link on the **Start** menu.
9. This allows the Security World binaries to be accessible system wide without having to specify the `%nfast_home%\bin` directory every time.

5.1.4. Configure Windows Firewall

To allow the Connect HSM to communicate with the hardserver on the host with CA, the hardserver must be able to communicate through the Windows Firewall. If Windows Firewall is turned off, no further action is required.

Turning off Windows Firewall is not recommended but is dependent on local operating and security policies.

If Windows Firewall is turned on, follow these steps:

1. Determine which location the network connection has been configured with. Public is the default unless specified otherwise.
2. Right-click the Windows icon on the task bar and select **Control Panel**.
3. Select **System and Security** and then **Allow an app through Windows Firewall**.
4. Select **Change Settings** and then **Allow another app**.
5. Select **Browse**, navigate to **hardserver.exe**, select **Open**, then select **Add**. Location:
    - Before 12.60: `C:\Program Files (x86)\nCipher\nfast\bin\hardserver.exe`
    - From 12.60 onwards: `C:\Program Files\nCipher\nfast\bin\hardserver.exe`
    - Ensure that **nfserv** (**nShield hardserver** in Security World versions 12.60 onwards) is set for the following properties:
        - **Private**
        - **Public**
        - **Domain** (if required)

    Select **OK**.

5.1.5. Enroll the Online Responder as a client of the HSM

There is only one Remote File System (RFS) per Security World. One of the CAs can be used as the RFS or alternatively, a single system acts as the RFS but is not a client of the HSM.

1. On the OCSP Server, enroll the client with the HSM:

```
> nethsmenroll --force --verify-nethsm-details <IP_address_of_HSM>
```

You can check that the client is correctly configured to make use of the HSM by running the enquiry command and checking the output shows that the HSM is available.

2. Manually copy the World file and the module file from `C:\ProgramData\nCipher\Key Management Data\local` on the RFS to the same location on the OCSP Responder node.

   These files have to be copied so that the OCSP Responder node can make use the of the HSMs and Security World.

5.1.6. Install the Key Service Provider on the OCSP Responder

1. Sign in to the OCSP Responder as the local administrator or using a Domain account with local administrator privileges.
2. Security World software and wizards must be run using the true local administrator account in order for all file permissions to be written correctly.
3. Select the Windows icon on the taskbar, select the down arrow, then select **nCipher > CNG Configuration Wizard**.
4. If a **User Account Control (UAC)** dialog appears, select **Yes**.
5. In the wizard, select **Next**. Ensure **Use the existing security world** is selected, then select **Next**.
6. In **Set Module States**, ensure that **Mode** is set to **operational** and that **State** is **usable**. Select **Next**.
7. If the mode is not operational, that is, it states pre-initialization, ensure that the Security World is loaded into the module.
8. In **Key Protection Setup**, ensure that Operator Card Set protection is selected if you are using OCS protection. Do not select **Always use the wizard when creating or importing keys**. Do not create a new Operator Card Set. Select **Next**.
9. If you are not using an OCS, select **Module Protection**. Module protection should be used for the OCSP Responder to ensure that certificate auto-enrolment completes without needing administrator interaction.
10. To install the Key Service Provider (KSP), in **Software Installation**, select **Next**, then select **Finish**.
11. To check whether the nShield KSP is properly installed, run the following command at a command prompt:

```
> certutil -csplist
```

In the output, look for an entry which states:

```
Provider Name: nCipher Security World Key Storage Provider
```

If this entry is not available, investigate the KSP configuration before proceeding.

5.1.7. Install and configure the OCSP Responder service

1. On the OCSP Responder server, in **Server Manager**, select **Add Roles and Features**.
2. On the **Before You Begin** screen, select **Next**.
3. On the **Select Installation Type** screen, select **Next**.
4. On the **Select Destination Server** screen, select **Next**.
5. On the **Select Server Roles** screen, select **Active Directory Certificate Services**.
6. In the **Add Roles and Features Wizard** dialog that appears, select **Add Features**.
7. On the **Server Roles** screen, select **Next**.
8. On the **Select Features** page, select **Next**.
9. On the **Active Directory Certificate Services** screen, select **Next**.
10. Clear **Certification Authority**, select **Online Responder** instead, then select **Next**.

    Only one option should be selected.

    If the CA and OCSP responder are on the same server, you cannot clear the **Certification Authority** option.

11. If the **Add Roles and Features** wizard appears, select **Add Features**.
12. On the **Role Services** screen, select **Next**.
13. Confirm the chosen installation options by selecting **Install**.
14. On the **Installation Results** screen, select **Close**.
15. Ensure that all the chosen configuration options successfully installed. Investigate any errors before proceeding.
16. From the notifications section in **Server Manager Dashboard**, select **Post-Deployment Configuration**.
17. In the resulting window, select **Next** and then select **Configure**.

The account being used to do the configuration must be a member of the Local Administrators group on the server.

18. Check that the output shows that the Online Responder role has been successfully configured.
19. From the **Administrative Tools** folder, open **Online Responder Management**.
20. On the left hand side, select **Revocation Configuration**.
21. In the **Actions** pane, select **Add Revocation Configuration**.
22. On the **Getting started** screen, select **Next**.
23. On the **Name the Revocation Configuration** page, type a friendly name for the configuration and then select **Next**.
24. The selected name should represent the CA that the Responder configuration is being created for. This name is only used to identify the configuration to administrators.
25. Select **Select CA Certificate Location > Select a certificate for an existing Enterprise CA**, then select **Next**.
26. Select **Choose CA Certificate screen > Browse CA certificates published in Active Directory**, then select **Browse**.
27. In **Select Certification Authority**, select the CA that the Responder configuration is created for, select **OK**, then select **Next**.
28. In **Select Signing Certificate**, ensure that **Automatically select a signing certificate** and **Auto-enrol for an OCSP Signing certificate** are selected. Also ensure that the OCSPResponseSigning template is selected, then select **Next**.

    

    If you want the OCSP Responder to protect its OCSP Signing certificate private key using an HSM, you should select the certificate template you created instead of the default template shown in these instructions.

29. On the **Revocation Provider** screen, select **Provider**.
30. In the **Base CRLs** section of the resulting dialog box, select the URL, then select **OK**.
31. The OCSP Responder uses the CRL generated by the selected CA it is being configured for to obtain its information about the status of certificates issued by the CA.

    If you are using Delta CRLs, select **Delta CRLs > Add** in the dialog box. In the window that appears, paste the URL to the Delta CRL issued by the Issuing CA whose configuration is being created on the OCSP Responder. Select **OK**.

32. Ensure the URL includes the correct encoding, with **%20** for space characters.
33. Clear **Refresh CRLs based on their validity periods** box. Enter the required value for Update CRLs at this refresh interval (min).

    CRLs are issued from the Issuing CA every 12 hours. Unless this setting is configured,

the OCSP Responder will not retrieve manually issued CRLs that were issued between the automated issuance periods because of CRL caching and because the OCSP Responder uses CRLs to determine a certificate's status. This forces the OCSP Responder to check for a new CRL every 5 minutes. In turn, this setting also invalidates the IIS and OCSP Responder caches meaning new responses will be sent to queries based on the 5-minute setting as opposed to the validity period specified in the CRL, for example 24 hours.

34. Back on the **Revocation Provider** screen, select **Finish**.
35. Ensure that the configuration of the OCSP Responder completes successfully. Investigate any issues before proceeding.
36. Right click the newly created **Revocation Configuration** and select **Edit Properties**.
37. Select the **Signing** tab.
38. Change the **Hash algorithm** to at least **SHA256**. This is mandatory if using FIPS 140-2 Level 3 because the default **SHA1** option is not supported.
39. Select **OK**.
40. Right-click the server FQDN under the **Array Configuration** option, then select **Set as Array Controller**.

    This server will act as the Array Controller for the OCSP Responder Service.

41. After the OCSP Responder has been configured and the key pair generated successfully on the HSM, the following command should be run to commit local Security World data, such as application key tokens, to the RFS:

    ```
    > rfs-sync --commit
    ```

    This is important because the RFS holds copies of all key tokens and the World file. Assuming that all key tokens used by clients are synchronized, a backup of the RFS Security World files.

42. In the **Certification Authority** MMC, right-click the CA and select **Properties**.
43. Select **Extensions > Select Extension > Authority Information Access (AIA)**, then select **Add**, and enter the name of the OCSP URL:

    ```
    http://<FQDN-of-OCSP-server>/ocsp.
    ```

44. Select **OK**.
45. Select **Include in the online certificate status protocol (OCSP) extension**, then select **OK**.

46. A window prompts you to restart the CA. Select **Yes** and wait for the CA to restart.

5.2. Verify that OCSP works correctly

If OCSP is on Windows Server Core, execute these steps on the Windows Server Core machine.

5.2.1. Generate a certificate request

The WebServer certificate template must be available. If required, install the WebServer certificate template in `certsrv.msc`. Right-click Certificate Templates, select **New > Certificate Templates to issue**, then select the WebServer template.

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 = "C=GB,CN=rsa.inf"
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 `rsa.inf` file, replace the subject with your CA common name.

2. From the command prompt navigate to your local C drive and run the following command:

```
> certreq -new rsa.inf rsa.req
```

   Select the CA certificate from the window that appears and save it as `rsa.cer` in your local directory.

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

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

5. Select the CA certificate from the Certification Authority list window that appears and save it as `rsa.cer` in your local directory.
6. Navigate to the directory where you saved the certificate and look for `rsa.cer`.
7. Run the following command:

```
> certutil -verify -urlfetch rsa.cer
```

Make sure the command completes successfully and the output contains the following lines:

```
Leaf certificate revocation check passed
CertUtil: -verify command completed successfully.
```

5.2.2. Remove information about the certificate's CRL

1. Select **Start > Run**, enter `certsrv.msc`, then select **OK**.
2. Windows Server Enterprise:

   Select **Certificate Authority**.

   A list of folders appears below the CA.

3. Windows Server Core:

   If CA is on Server Core, on the machine used to manage the CA remotely, right-click **Certification Authority (Local)**, then select **Retarget Certification Authority**. Select **Another computer**, select **Browse**, and select your CA.

4. Right-click the **Revoked Certificates** folder, then select **All Tasks**, **Publish**.

   A **Publish CRL** dialog appears.

5. Select **OK** to select a New CRL.
6. Right-click the CA, then select **Properties**.
7. Select the **Extensions** tab.
8. Check that the **Select extension** drop-down list box shows **CRL Distribution Point (CDP)**.
9. Select any of the listed CRL distribution points, then select **Remove**, then **Yes**.
10. Select **Apply**.

    A dialog appears saying you need to restart the service.

11. Select **Yes** to restart the service, then select **OK** to close the dialog.

5.2.3. 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.

2. Select **Certs (from AIA)**, then select **Retrieve**.

   The list contains the verified Certificate and its URL.

3. Select **CRLs (from CDP)**, then select **Retrieve**.
4. Compare the results to what you had earlier when you removed a CRL distributed point. CRLs show they have been verified.
5. Select **OCSP (from AIA)**, then select **Retrieve**.

   The list contains the Verified OCSP URL.

6. Select **Exit**.

5.2.4. 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 where the certificate is stored, then type:

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

2. 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.

5.3. Back up, migrate, and restore CA

The most common procedure related to backup, migrate and restore for the CA and HSM is to use the options:

- Select a certificate and use its associated private key.
- Select an existing private key.

This procedure describes backing up the CA / HSM data on an existing server, then restoring the CA / HSM data onto a new server. Entrust has successfully tested this procedure in the following configurations:

- Windows Server 2012 (CNG) to Windows Server 2012 R2 (CNG)
- Windows Server 2016 (CNG) to Windows Server 2019 (CNG)
- Windows Server 2019 (CNG) to Windows Server 2022 (CNG)

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`.

5.3.1. Migrate the CA using an existing certificate and associated private key using Module Protection

For this procedure your CA must be protected with module-only protection or 1/N OCS without passphrase as key protection method.

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

On machine #1:

1. Using PowerShell, back up the CA database by running the command:

   ```
   > Backup-CARoleService - Path <path_to_backup_file> - DatabaseOnly
   ```

   Alternatively, if you are using CMD (where **CA_config_string = Computername\CA-Name**), run:

   ```
   > certutil - config WINserver1\CA-example -backupdb C:\Users\Administrator\Documents\dbexample backup
   ```

   Default location of the CA .edb file: `C:\Windows\System32\CertLog`.

2. Export the certificate on machine #1:

   For Windows Server Core, execute the following steps from the remote machine that is

managing the Windows Server Core.

a. Run **mmc**.
b. In the console, select **File > Add/Remove Snap-in**.
c. Select the **Certificates** tab, then select **Add**.
d. The certificate snap-in window opens. Select **Computer Account**. Select **Next**.
e. Keep the default selection, select **Finish**, then select **OK**.
f. Select **Trusted Root Certification Authorities > Certificates**.
g. Right-click the CA certificate, then select **All Tasks > Export**. Select **Next**.
h. Select **Base-64 encoded X.509 (.CER)**. Select **Next**.
i. Specify the path and file name to save the certificate. Select **Next**.
j. Select **Finish**.
k. Select **OK** to close the export success message.

3. Back up the contents of the Security World data from the following location: `C:\ProgramData\nCipher\KeyManagement Data\local`.
4. Uninstall the CA from machine #1.

On machine #2:

1. Copy the backup of the Security World data to the following folder on machine #2: `C:\ProgramData\nCipher\KeyManagement Data\local`.
2. Load the Security World onto the HSM on machine #2 by running the command:

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

For more information about loading a Security World, refer to the *User Guide* for the HSM.

3. Run the **CNG Configuration Wizard**.

Windows Server Core:

```
> capingwizard
```

If you are selecting Operator Card Set protection, clear **Always use the wizard when creating or importing keys**.

4. Copy and install the X.509 certificate into the local user Trusted Root CA Store on machine #2:
   a. Right-click the certificate, then select **Install**. Select **Next**.

b. Select **Local Machine**.
c. Select **Place all certificates in the following store**, then select **Browse**.
d. Select **Trusted Root Certification Authorities**, then select **OK**. Select **Next**, then select **Finish**.
e. Select **OK** to close the import success message.

5. Install the certificate to the `Cert:\LocalMachine\My\` store. Using PowerShell, navigate to the LocalMachine:

```
> Set-Location -Path Cert:\LocalMachine\My\
```

Run the following command:

```
> Import-Certificate -FilePath <path to certificate>\Certificate_Name.cer
```

6. Repair the certificate store by running the following command from the console:

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

You should receive confirmation similar to:

```
my "Personal"
================ Certificate 0 ================
Serial Number: 13fa1422bfba4f9a4303e2aa162c25b2
Issuer: CN=ADCS-IO-CA, DC=ADCSDC, DC=internal
NotBefore: 11/10/2019 09:44
NotAfter: 11/10/2024 09:51
Subject: CN=ADCS-IO-CA, DC=ADCSDC, DC=internal
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): 486232dc0583012d47c75c74eb0d1b65da9f9484
Key Container = ADCS-IO-CA
Provider = nCipher Security World Key Storage Provider
Private key is NOT exportable
Signature test passed
CertUtil: -repairstore command completed successfully.
```

7. Select **Start > Server Manager** to open Server Manager.
8. Install and configure the CA as described in Install AD CS with Enterprise.
9. Install and configure AD CS with the following settings:
    a. In the **Set Up Private Key** window, select **Use existing certificate and private key**.
    b. In the existing **Certificate** window, the imported certificate is shown. Select the certificate, then select **Allow administrator interaction when the private key is accessed by the CA.** Select **Next**.

c. In the **Certificate Database** window, select **Next**.

d. In the **Confirmation** window, select **Configure**.

10. When the CA installation is complete, select **Close** in the **Results** window.
11. Stop the CA service.
12. Copy the backup of the CA database data to machine #2.
13. Run the command:

```
> certutil -shutdown
```

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

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

15. Restart the CA by running the command:

```
> net start certsvc
```

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

```
> sc query certsvc
```

5.3.2. Migrate the CA using an existing certificate and associated private key using OCS and Softcard protection

For this procedure your CA is assumed to be protected with OCS or Softcards as a key protection method.

On machine #1:

1. Using PowerShell, back up the CA database by running the command:

```
> Backup-CARoleService - Path <path_to_backup_file> - DatabaseOnly
```

Alternatively, if you are using CMD (where **CA_config_string = Computername\CA-Name**), run:

```
> certutil - config WINserver1\CA-example -backupdb C:\Users\Administrator\Documents\dbexample backup
```

Default location of the CA .edb file: `C:\Windows\System32\CertLog`.

2. Export the certificate on machine #1:

   

   For Windows Server Core, execute the following steps from the remote machine that is managing the Windows Server Core.

   a. Run **mmc**.
   b. In the console, select **File > Add/Remove Snap-in**.
   c. Select the **Certificates** tab, then select **Add**.
   d. The certificate snap-in window opens. Select **Computer Account**. Select **Next**.
   e. Keep the default selection, select **Finish**, then select **OK**.
   f. Select **Trusted Root Certification Authorities > Certificates**.
   g. Right-click the CA certificate, then select **All Tasks > Export**. Select **Next**.
   h. Select **Base-64 encoded X.509 (.CER)**. Select **Next**.
   i. Specify the path and file name to save the certificate. Select **Next**.
   j. Select **Finish**.
   k. Select **OK** to close the export success message.

3. Back up the contents of the Security World data from the following location: `C:\ProgramData\nCipher\KeyManagement Data\local`.
4. Uninstall the CA from machine #1.

On machine #2:

1. Copy the backed-up Security World data on the following path on machine #2: `C:\ProgramData\nCipher\KeyManagement Data\local`.
2. Load the Security World onto the HSM on machine #2, by running the command:

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

   For more information about loading a Security World, refer to the *User Guide* for the HSM.

3. Run the **CNG Configuration Wizard**.

   Windows Server Core:

   ```
   > capingwizard
   ```

   If you are selecting operator card set protection, do not select **Always use the wizard when creating or importing keys**.

4. Create the temporary folder `C:\temp`.
5. Add the system environment variable `NFAST_NFKM_TOKENSFILE`:
    a. Go to **Control Panel > System and Security > System > Advanced System Settings**.
    b. Select **Environment Variables**.
    c. Select **New** at the bottom under **System Variables**.
    d. Add `NFAST_NFKM_TOKENSFILE=c:\temp\nfast_nfkm_tokensfile`.
6. Copy and install the X.509 certificate into the local user Trusted Root CA Store on machine #2:
    a. Right-click the certificate, then select **Install**. Select **Next**.
    b. Select **Local Machine**.
    c. Select **Place all certificates in the following store**, then select **Browse**.
    d. Select **Trusted Root Certification Authorities**, then select **OK**. Select **Next**, then select **Finish**.
    e. Select **OK** to close the import success message.
7. Install the certificate into `Cert:\LocalMachine\My\` store. Using PowerShell, navigate to the LocalMachine:

    ```
    > Set-Location -Path Cert:\LocalMachine\My\
    ```

    Run the following command:

    ```
    > Import-Certificate -FilePath <path to certificate>\Certificate_Name.cer
    ```

8. At an elevated command prompt, use preload to relink the CA certificate and private key.

    For OCS protection:

    ```
    > preload --module=1 -f c:\temp\nfast_nfkm_tokensfile --cardset-name="<CARDSET_NAME>" certutil -repairstore
    -csp "ncipher security world key storage provider" my "<SHA-1_THUMBPRINT_OF_CA_CERT>"
    ```

    For Softcard protection:

    ```
    > preload --module=1 -f c:\temp\nfast_nfkm_tokensfile --softcard-name="<CARDSET_NAME>" certutil
    -repairstore -csp "ncipher security world key storage provider" my "<SHA-1_THUMBPRINT_OF_CA_CERT>"
    ```

    You should receive confirmation similar to:

    ```
    my "Personal"
    ```

```
================ Certificate 0 ================
Serial Number: 13fa1422bfba4f9a4303e2aa162c25b2
Issuer: CN=ADCS-IO-CA, DC=ADCSDC, DC=internal
NotBefore: 11/10/2019 09:44
NotAfter: 11/10/2024 09:51
Subject: CN=ADCS-IO-CA, DC=ADCSDC, DC=internal
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): 486232dc0583012d47c75c74eb0d1b65da9f9484
Key Container = ADCS-IO-CA
Provider = nCipher Security World Key Storage Provider
Private key is NOT exportable
Signature test passed
CertUtil: -repairstore command completed successfully.
```

9. Ensure that the nShield Service Agent is running. This can be viewed in the task tray.
10. At an elevated command prompt, use `preload` before you install the CA.

    For OCS protection:

    ```
    > preload --module=1 -f c:\temp\nfast_nfkm_tokensfile --cardset-name="<CARDSET_NAME>" pause
    ```

    For Softcard protection:

    ```
    > preload --module=1 -f c:\temp\nfast_nfkm_tokensfile --softcard-name="<CARDSET_NAME>" pause
    ```

11. Select **Start > Server Manager** to open Server Manager.
12. Install and configure the CA as described in Install AD CS with Enterprise.
13. Install and configure AD CS with the following settings:
    a. In the **Set Up Private Key** window, select **Use existing certificate and private key**.
    b. In the existing **Certificate** window, the imported certificate is shown. Select the certificate, then select **Allow administrator interaction when the private key is accessed by the CA.** Select **Next**.
    c. In the **Certificate Database** window, select **Next**.
    d. In the **Confirmation** window, select **Configure**.
14. When the CA installation is complete, select **Close** in the **Results** window.
15. Remove the previously added system environment variable `NFAST_NFKM_TOKENSFILE`.
16. Stop the CA service, then copy the backed-up CA database data onto machine #2.
17. Run the command:

    ```
    >certutil -shutdown
    ```

18. 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
```

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

```
>sc query certsvc
```

5.3.3. Migrate the CA using an existing private key

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

On machine #1:

1. Back up the CA database by running the command:

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

2. Back up the Security World data and the private key, which are found in `C:\ProgramData\nCipher\Key Management Data\local`. For more information about backing up a Security World, refer to the *User Guide* for the HSM.
3. Uninstall the CA from machine #1.

On machine #2:

1. Copy the backed-up Security World data and the private key to `C:\ProgramData\nCipher\Key Management Data\local` on machine #2.
2. Load the Security World onto the HSM on machine #2, by running the command:

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

   For more information about loading a Security World, refer to the *User Guide* for the HSM.

3. Run the CNG Configuration Wizard, then select **Use existing Security World**.
4. Install Microsoft Active Directory Certificate Services with the following settings:

a. In the **Private Key** window, select **Use existing private key** and use existing private key on this computer. Select **Next**.
b. In the **Select Existing Key** window, select **Change**. The **Change Cryptographic Provider** window opens.
c. Select the CSP that contains the created key. Delete the contents of the **CA common name** field, then select **Search**. The search results should find the existing private key.
d. Select the key that you generated on machine #1.

   If the private key is protected by Softcard or OCS, select **Allow administrator interaction when the private key is accessed by the CA**. Select **Next**.

e. In the **Cryptography for CA** window, select **Next**.
f. In the **CA name** window, select **Next**.
g. In the **Validity Period** window, specify the validity period. Select **Next**.
h. In the **Certificate Database** window, specify the certificate database location. Select **Next**.
i. In the **Confirmation** window, select **Configure**.
j. In the **Installation Results** window, select **Close**.

5. Copy the backed-up CA database data onto machine #2.
6. Run the command:

```
> certutil -shutdown
```

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

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

8. Restart the CA by running the command:

```
> net start certsvc
```

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

```
> sc query certsvc
```

5.4. Uninstall AD CS and OCSP

To uninstall AD CS and OCSP:

1. Open **Server Manager**, then select **Start > Server Manager**.
2. Select **Manage**, then select **Remove Roles & Features**.

   The **Before you begin** window opens. Select **Next**.
3. On **Server selection**, select a server from the server pool. Select **Next**.
4. Clear **Active Directory Certificate Services and Online Responder**. Select **Next**.
5. When the removal process is complete, select **Close** and restart the machine.

Chapter 6. Post-Quantum Cryptography Testing

This section outlines the product configurations and specific testing steps needed to configure AD CS for post-quantum key creation and certificate signing.

6.1. Product Configurations

Entrust has successfully tested integrating nShield HSM integration with Microsoft Windows Server 2025 to create a post-quantum Certification Authority, capable of signing certificates with a ML-DSA signing key.

Microsoft Windows Server	nShield HSM	nShield Security World Software	nShield Security World Firmware
2025	Connect XC	13.9.5	13.8.3
2025	nShield 5c	13.9.5	13.8.4

6.2. Supported nShield functionality

Feature	Support
Module-only key	Yes
Softcards	Yes
K-of-N card set	Yes
Key management	Yes
Mixed Estate	Yes

6.3. Testing Procedures

This section of the guide assumes the environment is set up using the procedures outlined earlier in this document within the Environment setup procedures and AD CS Procedures sections. The steps below only highlight the variations required for post-quantum testing; all other aspects follow the standard process.

The post-quantum environment setup process follows the standard procedure with the following differences:

- During AD CS configuration (after AD CS installation), in the **Cryptography for CA** screen, select post-quantum cryptographic providers such as **ML-DSA:87#nCipher Security World Key Storage Provider**.
  - The key length should default to **4096**, however this value may vary depending on your selected provider.
  - The hash algorithm for signing certificates issued by this CA should be set to **NoHash** by default.
  - Ensure the **Allow administrator interaction when the private key is accessed by CA** option is enabled.

    

    You will be able to verify your choices on the **Confirmation** screen of the AD CS Configuration window.

- Certificate template creation for post-quantum environments largely follows the standard procedure, except for the following changes:
  - To access your template's properties, run `certtmpl.msc` and then select your template. The Administrator template was used during testing.
  - You must ensure **Key Storage Provider** is selected in the Provider Category field.
  - In the **Algorithm Name** field, you need to select a post-quantum algorithm. For example, **ML-DSA:87**.
  - You must ensure that **Requests must use one of the following providers** is selected, and, in **Providers**, only **nCipher Security World Key Storage Provider** is selected.
- After AD CS is configured and the post-quantum certificate is requested and enrolled, you can view the signed certificate and verify use of the post-quantum signing key as follows.
  a. Open `certsrv.msc` or the Certification Authority application.
  b. Navigate to **Issued Certificates**.
  c. Select the required certificate to display its information.
  d. Select **Details** and view the **Signature algorithm** field. It should display your PQC signing algorithm.

Chapter 7. Troubleshooting

Use the following table to troubleshoot the error messages shown.

Problem	Cause	Resolution
Online Responder reports **Bad Signing Certificate on Array Controller**.	This error shows that the OCSP Signing key or certificate cannot be used by the Responder.	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 shows that there is a problem with the certificate location.	Check the suggested location to ensure that the CA certificate is both published and named correctly as per the URI specified in the **AIA** field.
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 2012.	Contact Microsoft.
When presenting a Java card OCS (V12 onwards only), the **AD CS Configuration Wizard** does not detect the OCS. `cardpp --examine` shows **TokenSecureChannelError**.	**TokenSecureChannelError** can occasionally be seen when presenting a Java card OCS.	Remove and re-insert the OCS until it is picked up by `cardpp` and the **AD CS Configuration Wizard**.

Chapter 8. Additional resources and related products

8.1. nShield HSMs

8.2. nShield as a Service

8.3. Entrust products

8.4. nShield product documentation