

# Microsoft AD CS and NDES

nShield<sup>®</sup> HSM Integration Guide for Microsoft Windows Server

2024-10-21

Member of Microsoft Intelligent Security Association

© 2025 Entrust Corporation. All rights reserved.

Microsoft Security

## Table of Contents

1. Introduction	1
1.1. Product configurations	1
1.2. Supported nShield hardware and software versions	1
1.3. Supported nShield HSM functionality	. 2
1.4. Requirements	. 2
2. Procedures	. 4
2.1. Select the protection method	. 4
2.2. Install the Security World software and create a Security World	. 4
2.3. Generate the OCS or softcard in the CA server.	. 5
2.4. Configure the CNG provider in the CA server	. 7
2.5. Configure the CNG provider on the NDES server	. 8
2.6. Install and configure AD CS on the CA server	. 8
2.7. Add certificates templates to the CA server	. 12
2.8. Install Web Server (IIS) on the CA server	. 13
2.9. Create a virtual directory to serve as the public key infrastructure (PKI)	
repository	14
2.10. Create domain user accounts to act as the NDES service account	. 16
2.11. Add the SCEPAdmin account and SCEPSvc service account to the local	
IIS_IUSRS group	. 17
2.12. Configure the SCEPAdmin account and SCEPSvc service account with	
request permission on the CA	. 17
2.13. Configure the SCEPDeviceAdmin account with enroll permission to the IPSEC	
(offline request) certificate template	18
2.14. Install and configure NDES	. 19
2.15. Test access to the NDES web site (unsecured).	. 21
2.16. Configure the NDES admin page to use an SSL certificate.	22
3. Use a HSM for RA certificate private keys	30
3.1. Procedures changes.	30
4. Troubleshooting.	32
4.1. Using the certreq -new <.req file here> command returns an Invalid	
Provider Specified error.	32
4.2. If using remote admin, the AD CS Configuration Wizard does not detect the	
OCS.	32
4.3. Failed to add Certificate Templates at the End of the NDES installation	32
5. Additional resources and related products.	35
5.1. nShield Connect	35
5.2. nShield as a Service.	35

5.3. nShield Edge	35
5.4. Entrust products	35
5.5. nShield product documentation	35

## Chapter 1. Introduction

This guide describes how MS NDES can utilize a Microsoft Certificate Authority enrolled with an Entrust nShield Hardware Security Module (HSM) as a Root of Trust for storage encryption, to protect the private keys and meet FIPS 140 Level 2 or Level 3.

The Entrust nShield is also used to protect the NDES Admin web page using TLS, where the private key for the certificate is nShield managed. NDES implements the Simple Certificate Enrollment Protocol (SCEP), which defines the communication between network devices and a Registration Authority (RA) for certificate enrollment.

SCEP supports the secure issuance of certificates to network devices which do not run with domain credentials to enroll for x509 version 3 certificates from a Certification Authority (CA).

Ultimately, the network device will have a private key and associated certificate issued by a CA protected by the Entrust nShield HSM. Applications on the device may use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

### 1.1. Product configurations

Entrust tested the integration with the following versions:

Product	Version
Base OS	Windows Server 2022 Server
Entrust Security World	13.6.3

### 1.2. Supported nShield hardware and software versions

Entrust tested the integration with the following nShield HSM hardware and software versions:

Product	Security World	Firmware	Netimage
Connect XC	13.6.2	12.72.1 (FIPS 140-2 certified)	13.4.5

Product	Security World	Firmware	Netimage
nShield 5c	13.6.3	13.2.4 (FIPS 140-3 certified)	13.6.1

### 1.3. Supported nShield HSM functionality

Feature	Support
Module-only key	Yes
OCS cards	Yes
Softcards	Yes
nSaaS	Yes
FIPS 140 Level 3	Yes

The following table states the different scenarios for secure/unsecure connections during the integration and what features worked:

Secure/Unsecure	Module	Softcards	OCS Cards	Notes
Unsecure	Yes	Yes	Yes	
Secure	Yes	No	Yes	OCS Card with no passphrase

- unsecure = http connection
- secure = https connection

#### 1.4. Requirements

Familiarize yourself with:

- Active Directory Certificate Services (AD CS): Network Device Enrollment Service (NDES) documentation (https://docs.microsoft.com).
- The Installation Guide and User Guide for the HSM.
- Your organizational Certificate Policy and Certificate Practice Statement and a Security Policy or Procedure in place covering administration of the PKI and HSM:

- The number and quorum of Administrator cards in the Administrator Card Set (ACS) and the policy for managing these cards.
- The number and quorum of operator cards in the Operator Card Set (OCS) and the policy for managing these cards.
- ° The keys protection method: Module, Softcard, or OCS.
- $^\circ\,$  The level of compliance for the Security World, FIPS 140 Level 3.
  - Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.
- ° Key attributes such as key size, time-out, or need for auditing key usage.

### Chapter 2. Procedures

Prerequisites:

- A Windows domain controller.
- Domain administrator privileges to add accounts and join clients.
- A Windows server in the domain with Internet Information Services (IIS) installed. Active Directory Certificate Service (AD CS) will be installed in this server per the instructions below.
- A second Windows server in the domain with IIS installed. NDES will be installed in this server per the instructions below.
- A Windows client in the domain to request CA hash and challenge password pairs.

#### 2.1. Select the protection method

OCS, softcard, or Module protection can be used to authorize access to the keys protected by the HSM. Follow your organization's security policy to select which one. The following protection methods were used in this integration:

- HSM OCS with passphrase protection was used to protect the CA. This is the highest level of protection.
- HSM Module protection was used to generate the certificate request for IIS binding for secure access to the NDES server. IIS binding is only possible with:
  - ° OCS without a passphrase
  - Module protection
- Microsoft cryptography provider was used to protect the RA keys. For RA keys, only Cryptographic Application Programming Interface (CryptoAPI) Service Providers are supported.

For secure HTTPS connections, you can only use OCS with no passphrase or module protection. This is required when setting up the binding on the IIS server for the https protocol. At that stage the IIS server does not provide any mechanism to enter passphrases for OCS or softcard protection, therefore any protection method that uses a passphrase will fail.

## 2.2. Install the Security World software and create a Security World

- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- 2. Install the Security World software by double-clicking on the SecWorld\_Windowsxx.xx.iso file. For detailed instructions, see the *Installation Guide* for the HSM on https://nshielddocs.entrust.com/.
- 3. Add the Security World utilities path C:\Program Files\nCipher\nfast\bin to the Windows system path.
- 4. Open the firewall port 9004 outbound for the HSM connections.
- 5. Install the nShield Connect HSM locally, remotely, or remotely via the serial console.
- 6. Open a command window and run the following to confirm that the HSM is **operational**:

```
C:\Users\dbuser>enquiry
Server:
enquiry reply flags none
enquiry reply level Six
serial number ...
mode operational
...
Module #1:
enquiry reply flags none
enquiry reply level Six
serial number ...
mode operational.
...
```

- 7. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy for this. ACS cards cannot be duplicated after the Security World is created. Create a quorum K/N appropriate for your implementation and to protect against card failure or loss.
- 8. Confirm the Security World is usable:

```
C:\Users\dbuser>nfkminfo
World
generation 2
state 0x37270008 Initialised Usable ...
...
Module #1
generation 2
state 0x2 Usable
...
```

9. Sign in to the NDES server using the domain name, <domain\_name>\Administrator and repeat the above steps, but copying the Security World from the CA server.

#### 2.3. Generate the OCS or softcard in the CA server

To create the OCS:

- If you are using remote administration, ensure that the C:\ProgramData\nCipher\Key Management Data\config\cardList file contains the serial number of the card(s) to be presented.
- 2. Open a command window as a user with administrator privileges.
- 3. Execute the following command.

Follow your organization's security policy for the values K/N. In this example, K=1 and N=1.

The OCS cards cannot be duplicated after it was created. Enter a passphrase at the prompt. Notice **slot** 2, remote via a Trusted Verification Device, is used to present the card.

The authentication provided by the OCS as shown in the command is non-persistent and is only available for K=1 and while the OCS card is present in the HSM front panel slot, or TVD. If you are using OCS card protection and non-persistent card configuration, OCS cards need to be inserted in the front panel or always present in the TVD. Add the -p (persistent) option in the command to retain authentication after the OCS card has been removed from the HSM front panel slot or from the TVD.

```
>createocs -m1 -s2 -N testOCS -Q 1/1
FIPS 140-2 level 3 auth obtained.
Creating Cardset:
Module 1: 0 cards of 1 written
Module 1 slot 0: Admin Card #1
Module 1 slot 2: empty
Module 1 slot 3: empty
Module 1 slot 2: blank card
Module 1 slot 2:- passphrase specified - writing card
Card writing complete.
cardset created; hkltu = ...
```

4. Verify that the OCS has been created:

nfkminfo -c Cardset list - 1 cardsets: (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only Operator logical token hash k/n timeout name 8b652e480d6307c32a1b1395a7a12c8ef07fbd24 1/1 none-NL testOCS

The **rocs** utility also shows the OCS that was created:

```
>rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardset
No. Name Keys (recov) Sharing
1 testOCS 0 (0) 1 of 1
```

rocs> quit

If you are using softcard protection, create the softcard now.

1. Ensure the C:\Program Files\nCipher\nfast\cknfastrc file exists with the following content. Otherwise create it.

> type "C:\Program Files\nCipher\nfast\cknfastrc"
CKNFAST\_LOADSHARING=1

2. Execute the following command and enter a passphrase at the prompt:

```
>ppmk -n testSC
Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU f2f7d34e4ddc950038db430ddbe06488f4c21ee7
```

3. Verify the softcard was created:

```
>nfkminfo -s
SoftCard summary - 1 softcards:
Operator logical token hash name
f2f7d34e4ddc950038db430ddbe06488f4c21ee7 testSC
```

The rocs utility also shows the OCS and softcard created.

```
>rocs
'rocs' key recovery tool
Useful commands: 'help', 'help intro', 'quit'.
rocs> list cardset
No. Name Keys (recov) Sharing
1 testOCS 0 (0) 1 of 1
2 testSC 0 (0) (softcard)
rocs>quit
```

#### 2.4. Configure the CNG provider in the CA server

- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- 2. Select Start > nCipher > CNG configuration wizard.
- 3. Select Next on the Welcome window.
- Select Next on the Enable HSM Pool Mode window, leaving Enable HSM Mode for CNG Providers un-checked.
- 5. Select Use existing security world on the Initial setup window. Then select Next.
- 6. Select the HSM (Module) if more than one is available on the **Set Module States** window. Then select **Next**.

nShie	ld CNG Provid	lers Configuration Wiza	rd	×
Se	Set Module States Ensure modules are in the correct state before you proceed.			
	The following (	modules are available in ye	our system:	
	Module ID	Mode	State	
	1	operational	usable	
	2	operational	foreign	
	3	operational	foreign	
	Or reset modul world to uniniti Refer to the us state. If you ne	odule is usable in the curre les 2, and 3 to the initializa alized nShield modules. ser guide for details of how sed to power down your co ard on boot up to continue	ition state to enable you to v to put your nShield modu omputer, select the tickbo	o restore your security ule in the initialization
	🗌 The machi	ne must be switched off to	) change the hardware sta	ate.
			< Back	Next > Cancel

 In Key Protection Setup, select Operator Card Set protection > Next, then select the relevant option: Module protection, Softcard protection, or Operator Card Set protection.

For Module Protection, the Software Installation window will come up. For Softcard Protection and OCS Protection, choose from Current Operator Card Sets or Current Softcards. Notice these were created above.

- 8. Select Next > Finish.
- 9. Verify the provider:

>certutil -csplist | findstr nCipher
Provider Name: nCipher Security World Key Storage Provider

#### 2.5. Configure the CNG provider on the NDES server

- 1. Sign in to the NDES server using the domain name, <domain\_name>\Administrator.
- Select Start > nCipher > CNG configuration wizard, then follow the steps to configure the CNG as described in Configure the CNG provider in the CA server.

#### 2.6. Install and configure AD CS on the CA server

- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- 2. Select **Start > Server Manager** to open the Server Manager.

- 3. Select Manage, then select Add Roles & Features. The Before you begin window appears. Select Next.
- 4. Select **Role-based or feature-based installation** on the **Select installation type** window. Select **Next**.
- Select the local server from the pool on the Select destination server window. Select Next.
- Select Active Directory Certificate Services role on the Select server roles window. The Add Roles and Features Wizard will appear. Select Add Features and then select Next.
- 7. In Select features, select Next.
- 8. Select Next on the Active Directory Certificate Services window.
- 9. Select Certification Authority on the Select role services windows.
- 10. Select Next.
- 11. Verify the information, then select **Install** on the **Confirm installation selections** window.

📥 Add Roles and Features Wizard		_		×
Confirm installatio	Confirm installation selections		ATION SERV A.interop.co	
Before You Begin	To install the following roles, role services, or features on selected server, click In	istall.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this page			
Server Roles	been selected automatically. If you do not want to install these optional features their check boxes.	s, click Previ	ious to cle	ar
Features				
AD CS	Active Directory Certificate Services			
Role Services	Certification Authority			
Confirmation	Remote Server Administration Tools Role Administration Tools			
Results	Active Directory Certificate Services Tools			
	Certification Authority Management Tools			
	Export configuration settings Specify an alternate source path			
	< Previous Next >	nstall	Cancel	

 Do not select Close the Installation progress windows once the installation is complete. Instead, select the Configure Active Directory Certificate Services on the destination server link.

📥 Server Manager		- <b>C</b> × <b>C</b> ×
۰۰ ۲	Dashboard 🔹 🕄 🖌	anage Tools View Help ATION SERVER
Dasbboard	A Post-deployment Configura TASKS 👻 🛛 🗙	<u>^</u>
Dashboard     Loca     Add Roles an     All S     Add Roles an     All S	Certificate Services at MS-NDES-CA <u>Configure Active Directory Certificate Services on th</u>	DESTINATION SERVER MS-NDES-CAInterop.com
File Before You Installation Server Sele Server Role	Configuration required, installation succeeded on Type MS-NDES-CA.interop.com. Add Roles and Features	ed on MS-NDES-CA.interop.com.
Features AD CS Role Se Confirmati Results	ervices Server Configure Active Directory Certificate Services	bols
	You can close this wizard without interruptin page again by clicking Notifications in the c	ng running tasks. View task progress or open this command bar, and then Task Details.

- Verify the Administrator credentials, <domain\_name>\Administrator on the Credentials text box on the Credentials windows. If needed select Change and specify the appropriate credentials. Select Next.
- 14. Select Certification Authority on the Role Services window. This is the only available selection when the certification authority role is installed on the server. If using OCS key protection, present the OCS card in the HSM or TVD. When the communication with the HSM has been established the button becomes active. Select Next.
- 15. Select Enterprise CA on the Setup Type window. Select Next.
- 16. Select Root CA on the CA Type window. Select Next.
- 17. Select Create a new private key on the Private Key window. Select Next.
- 18. In Cryptography for CA > nCipher Security World Key Storage Provider, select a provider with key length 2048 or longer. Also check Allow administrator interaction when the private key is accessed by the CA. Then select Next.
- Take the default CA name given, or modify if required on the CA Name window. Select Next.
- 20. Enter the number of years for the certificate to be valid on the **Validity Period** window. Select **Next**.
- 21. Take the default locations for the database and database log files, or modify if required on the **CA Database** window. Select **Next**.
- 22. Select Configure on the Confirmation window.
- 23. A **Create new key** wizard window appears on the task bar. It may be hidden behind the other windows. Open it and select **Next**.
- 24. Select the protection method for the new key. Select Next.

You will be prompted to enter the softcard passphrase or present the OCS (token) if either protection method was chosen when the CNG provider was installed. There will be no prompt if Module protection was chosen.

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

- 25. Present the softcard passphrase or OCS and select the module if more than one nShield Connect is available. Select **Finish** to close the wizard.
- 26. Select Next on the Load key window.
- 27. Select the module on the **Choose modules you wish to load the key onto** window. Select **Next**.
- 28. Enter the passphrase. Select **Next**. You may be prompted more than once for the same information.
- 29. Select Finish. Successful configuration is shown as follows. Select Close.

📥 AD CS Configuration			-		×
Results			DESTINAT MS-NDES-CA		
	The following roles, role services, or f	eatures were configured:			
	Active Directory Certificate Ser	rvices			
	Certification Authority	Configuration s	ucceeded		
СА Туре	More about CA Configuration	Configurations	ucceeueu		
	-				
Results					
	<	Previous Next >	Close	Cance	I

30. The key generated can be verified using a CLI command:

>nfkminfo -l
Keys protected by cardsets: key_caping_machine75393afa6878b98e3d91b5ff360284f706a97572 `interop-MS-NDES-CA-CA`

#### The **rocs** utility shows the names and protection methods of the keys.

```
>rocs
`rocs' key recovery tool
Useful commands: `help', `help_intro', `quit'.
```

rocs>	list keys		
No.	Name	Арр	Protected by
1	interop-MS-NDES-CA-CA	caping	MSaDCSnDESocs
rocs>	quit		

31. 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

Example output:

Dependency change succeeded.

32. Verify that the CA service has started successfully.

Run the command:

>sc query certsvc

Example output:

```
SERVICE_NAME: certsvc

TYPE : 110 WIN32_OWN_PROCESS (interactive)

STATE : 4 RUNNING

(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0
```

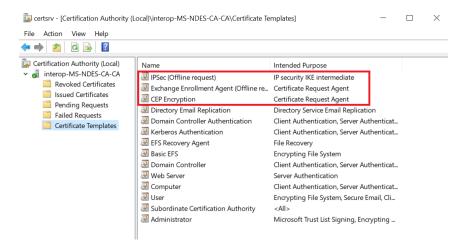
33. In Installation progress, select Close.

#### 2.7. Add certificates templates to the CA server

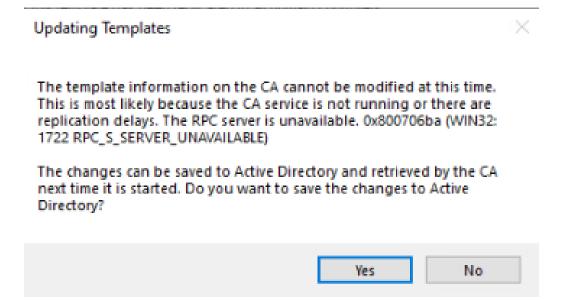
- 1. Sign in to the CA server using <domain\_name>\Administrator.
- 2. Select Server Manager > Tools > Certification Authority.
- 3. Expand the issuing CA node in the left-hand pane.
- 4. Right-click Certificate Templates, then select New > Certificate Template to Issue.
- 5. Select the following templates, then select OK:

Exchange Enrollment Agent (Offline Request)

- CEP Encryption
- IPSEC (Offline request)
- 6. Check that the templates have been added.



If you get a message indicating the CA service is not running, stop and then restart the Certificate Authority Service or reboot the CA server and try to add the certificate template again. A message like this gets displayed when this occurs:



#### 2.8. Install Web Server (IIS) on the CA server

- 1. Sign in to the CA server using <domain\_name>\Administrator.
- 2. Select Start > Server Manager to open the Server Manager.
- 3. Select Manage, then select Add Roles & Features. The Before you begin window appears. Select Next.
- 4. Select Role-based or feature-based installation on the Select installation type

window. Select Next.

- Select the local server from the pool on the Select destination server window. Select Next.
- Select Web Server (IIS) on the Select server roles window. The Add Roles and Features Wizard will appear. Select Add Features and then select Next.
- 7. In Select features, select Next.
- 8. Select Next on the Web Server Role (IIS) window.
- 9. Select Next on the Select role services window.
- 10. Verify the information, then select **Install** on the **Confirm installation selections** window.
- 11. Select Close, once installation completes.

## 2.9. Create a virtual directory to serve as the public key infrastructure (PKI) repository

- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- Create a local directory for PKI repository, for example C:\PKIRepository. See the following Microsoft link for instructions, https://docs.microsoft.com/en-us/ troubleshoot/windows-server/networking/create-virtual-directory-folder-remotecomputer.
- 3. Create a virtual directory. Notice the alias, physical path, and path credentials.
  - a. Create a local directory for PKI repository, for example C:\PKIRepository.

% mkdir c:\PKIRepository

- b. Select Start, point to Programs > Administrative Tools, and then select Internet Information Services (IIS) Manager.
- c. In the **Internet Information Services** window, expand **server name** (where server name is the name of the server).
- d. Right-click the Web site that you want (for example, **Default Web Site**), and select **Add Virtual Directory**.
- e. On the Add Virtual Directory window, type the Alias that you want (for example, **PKIRepository**), select the **Physical Path**, and then select **OK**.

Add Virtual Direct	tory		ī	?	×
Site name: E Path: /	Default Web Site				
Alias: PKIRepository					
Example: image Physical path: C:\PKIRepositor					
Pass-through an Connect as	uthentication Test Settings				
		ОК	Ca	ncel	

- f. Right-click the new created Virtual Directory and select Manage Virtual Directory
   > Advanced Settings.
- g. In the Advanced Settings window, select Physical Path Credentials.

Connect As	?	$\times$
Path credentials:		
Specific user:		
	Set	
○ Application user (pass-through authentication)		
ОК	Cancel	

- h. In the Connect As window, select Specific User > Set.
- i. In the **Set Credentials** windows, enter the domain name user id for **User Name**, and the password information for the user. Select **OK**.

Set Credentials	?	$\times$
User name:		
INTEROP\Administrator		
Password:		
Confirm password:		
•••••		
ОК	Cancel	
U.N.	concer	

- 4. Test the virtual directory per the same link above.
  - a. Start Microsoft Edge.
  - b. In the Address box, type the URL to your Web server (for example, http://CA-SERVER-IP-ADDRESS), and then select **Go**.
  - c. Verify that you can view the default Web site.

- d. Append the alias of the virtual directory to the address that you typed (for example, http://CA-SERVER-IP-ADDRESS/PKIRepository), and then select **Go**.
- e. The virtual directory Web content is displayed in the browser window. You may get a forbidden error. If that's the case, create a index.htm file in C:\PKIRepository with some HTML content on it and reload the page, which should display properly.

## 2.10. Create domain user accounts to act as the NDES service account

- 1. Sign in to the Domain Controller as Domain Administrator.
- 2. Select Active Directory Users and Computers from the Start menu.

Add users SCEPAdmin, SCEPSvc, and SCEPDeviceAdmin.

- 1. Expand <domain\_name>.com, right-click **Users** and select **New** > **User**.
- 2. Enter the name **SCEPAdmin** and select **Next**. Follow your organization's security policies to set the password. Never expires was selected for the purpose of this integration.

ew Object - User		×
Create in:	interop.com/Users	
First name:	SCEP Initials:	
Last name:	Admin	
Full name:	SCEP Admin	
User logon name:		
SCEPAdmin	@interop.com ~	
User logon name (pre-	Windows 2000):	
INTEROP\	SCEPAdmin	
	< Back Next > Cancel	

 Create new users for SCEPSvc and SCEPDeviceAdmin by repeating the previous steps.

Add user SCEPAdmin to the Enterprise Admins and Domain Admins groups.

- 1. Right-click Enterprise Admins on the right pane and select Properties.
- 2. Select the Members tab and then select Add.
- 3. Enter the SCEPAdmin account, select Check Names, and if found then select OK.
- 4. Select Apply and OK.
- 5. Repeat the above steps for the **Domain Admins** group.

## 2.11. Add the SCEPAdmin account and SCEPSvc service account to the local IIS\_IUSRS group

- 1. Sign in to the NDES server using the domain name, <domain\_name>\Administrator.
- 2. Open Computer Management (compmgmt.msc).
- 3. Expand Local User and Groups on the Computer Management console tree, under System Tools. Select Groups.
- 4. Double-click IIS\_IUSRS on the details pane.
- 5. Select Add on the IIS\_IUSRS Properties window.
- 6. Enter the SCEPAdmin account, select Check Names, and if found then select OK.
- 7. Select Apply and OK.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Service Accounts, or Groups	Object Types
From this location:	
interop.com	Locations
Enter the object names to select ( <u>examples</u> ):	
SCEP Admin (SCEPAdmin@interop.com)	Check Names
Advanced	OK Cancel

8. Repeat the above steps for the SCEPSvc service account.

# 2.12. Configure the SCEPAdmin account and SCEPSvc service account with request permission on the CA

- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- 2. Select Certification Authority from the Tools menu on the Server Manager window.
- 3. Right-click the certification authority (this CA server) and then select **Properties**.

4. Select the **Security** tab.

Notice the accounts that have **Request Certificates** permissions. By default the group **Authenticated Users** has this permission. The **SCEPAdmin** account will be a member of **Authenticated Users** when it is in use, which has **Request Certificates** permission. However, if that is not the case, do as follows:

- 5. Select Add.
- 6. On the **Select Users, Computers, Service Accounts, or Groups** text box, type the name of the **SCEPSvc** account, select **Check Names**, and if found select **OK**.
- Select the SCEPSvc account and select the Allow check box that corresponds to Request Certificates.
- 8. Select Apply and then select OK.

erop-MS-NDES-CA-0					
Extensions	Storage		Certificate	e Managers	
General	Policy Mod	lule	E	Exit Module	
Enrollment Agents	Auditing	Recover	y Agents	Securi	
Group or user names:					
Authenticated Use	ers				
SCEP Svc (SCEPSvc@interop.com)					
Sealar Admins (II					
Enterprise Admins	•		·		
Administrators (MS	S-NDES-CA\Adn	ninistrators)			
		Ad	d	Remove	
Permissions for SCEP S	Svc	Ad	d Allow	Remove Deny	
Permissions for SCEP S	Svc	Ad			
		Ad	Allow		
Read		Ad	Allow		
Read Issue and Manage C	Certificates	Ad	Allow		
Read Issue and Manage C Manage CA	Certificates	Ad	Allow		
Read Issue and Manage C Manage CA	Certificates	Ad	Allow		
Read Issue and Manage C Manage CA	Certificates	Ad	Allow		
Read Issue and Manage C Manage CA	Certificates	Ad	Allow		
Read Issue and Manage C Manage CA	Certificates	Ad	Allow		
Read Issue and Manage C Manage CA	Certificates	Ad	Allow		
Read Issue and Manage C Manage CA	Certificates		Allow		

9. Repeat the steps for the SCEPAdmin account.

# 2.13. Configure the SCEPDeviceAdmin account with enroll permission to the IPSEC (offline request) certificate template

- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- 2. Select Certification Authority from the Tools menu on the Server Manager window.

- 3. Expand the server on the left pane, then right-click **Certificate Templates** and select **Manage**.
- 4. Right-click IPSEC on the Template Display Name pane and select Properties.
- 5. Select the **Security** tab. Then select **Add**.
- On the Select Users, Computers, Service Accounts, or Groups text box, type the name of the SCEPDeviceAdmin account, select Check Names, and if found then select OK.
- 7. Select the **SCEPDeviceAdmin** account and verify the **Allow** check box that corresponds to **Enroll** is selected. Select **Apply** and then select **OK**.

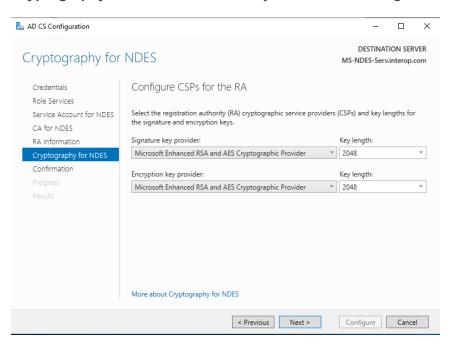
#### 2.14. Install and configure NDES

- 1. Sign in to the NDES server using the domain name, <domain\_name>\Administrator.
- 2. Select **Start > Server Manager** to open the Server Manager.
- 3. Select Manage, then select Add Roles & Features. The Before you begin window appears. Select Next.
- 4. Select **Role-based or feature-based installation** on the **Select installation type** window. Select **Next**.
- Select the local server from the pool on the Select destination server window. Select Next.
- Select Active Directory Certificate Services role on the Select server roles window. The Add Roles and Features Wizard appears. Select Add Features and then select Next.
- 7. Select Next on the Select features window.
- 8. Select Next on the Active Directory Certificate Services window.
- 9. Uncheck Certification Authority and check Network Device Enrollment Service on the Select role services window. The Add Roles and Features Wizard will appear.
- 10. Select Add Features and then select Next on the Select role services window.
- 11. Verify the information, then select **Install** on the **Confirm installation selections** window.
- Do not select Close on the Installation progress windows once the installation is complete. Select the Configure Active Directory Certificate Services on the destination server link instead.
- 13. Change the **Credentials** to <domain\_name>\SCEPAdmin on the **Credentials** windows. Select **Change**, enter new credential, then select **Next**.
- 14. From Select Role Services to configure, select Network Device Enrollment Service, then select Next.

- 15. Select the **Specify service account** on the **Service Account** window, then select **Select**.
- 16. Enter the credential for the SCEPSvc service account and then select OK and Next.
- 17. Select CA name on the CA for NDES windows, then select Select.
- Choose the CA server on the Select Certificate Authority window, then select OK and Next.
- Note the specified Registration Authority (RA Name) on the RA Information window. Complete any of the optional information as required. Then select Next.

AD CS Configuration		-		×
RA Information		DESTIN MS-NDES-Se	ATION SER	
Credentials Role Services Service Account for NDES CA for NDES		d information to enroll for an RA certifi		iES)
RA Information	Required information			
Cryptography for NDES	RA Name:	MS-NDES-SERV-MSCEP-RA		
Confirmation	Country/Region:	US (United States)		*
	Optional information E-mail: Company: Department: City: State/Province:	Entrust Interop Sunrise FL		
	More about RA Informatio		Cance	

20. Choose the **Signature key provider** and **Encryption key provider** on the **Cryptography for NDES** window. A key size of 2048 or larger is recommended.



- 21. Select **Next** and review the chosen options at the **Confirmation** window. Then select **Configure**.
- 22. Sign in to the CA server and present the OCS or enter the passphrase if either OCS or softcard protection was selected. Look for an icon on the **Taskbar** if the **Load key** window is not present. You may be prompted to present the OCS or enter the passphrase more than once.
- 23. Go back to the NDES server. Check for the **Configuration succeeded** message on the **Results** window, then select **Close**.

If you get a message that it failed to add certificate templates at the end of the NDES installation see Failed to add Certificate Templates at the End of the NDES installation.

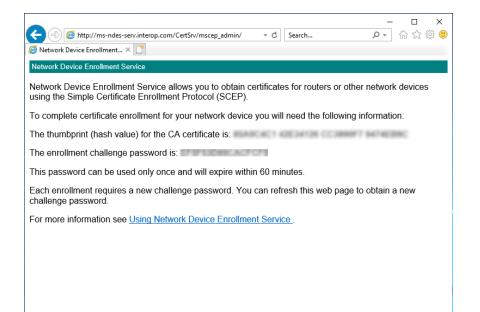
### 2.15. Test access to the NDES web site (unsecured).

In this example, the **SCEPSvc** account was used for testing access to the NDES web site. Consult your security team and reference Microsoft best practices for deploying in a production environment.

- 1. Sign in to the Windows client.
- 2. Launch the browser and go to the following address: <a href="http://<NDES-server-address/">http://<NDES-server-address/</a> CertSrv/mscep\_admin. Sign in as <domain-name>\SCEPSvc.

					×
( ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	es-serv.interop.com/CertSrv/mscep_admin	/ - X Search		<b>♀</b> ☆☆ ☆	
<ul> <li>Waiting for ms-ndes-serv.i.</li> </ul>	× 📑				
	Internet Explorer Enhanced Security Con number of security settings that define h configuration also reduces the exposure a complete list of the security settings in Security Configuration. Windows Security	figuration is currently enabled ow users browse Internet and of your server to Web sites th	l on your se l intranet W at might po s of Interne X	erver. This configures a /eb sites. The ose a security risk. For	^
	iexplore Connecting to ms-ndes-serv.inter INTEROP\SCEPSvc	rop.com.		For more information,	
	Domain: INTEROP     Remember my credentials	¢			
	ОК	Cancel			~

3. Notice the hash value of the CA certificate and the challenge password. Refreshing the browser generates a new challenge password.



An unsecure HTTP address to access NDES server is only done above to demonstrate NDES is running. You may want to configure your HTTP address to be redirected to HTTPS for the devices requesting to be enrolled. Refer to Microsoft documentation to perform this configuration.

## 2.16. Configure the NDES admin page to use an SSL certificate

## 2.16.1. Create a template for the NDES Admin web service certificate request.

This will ensure that the nCipher KSP is used to generate the key pair.

- 1. Sign in to the NDES server using the domain name, <domain\_name>\Administrator.
- Create a request.inf file using a text editor as follows. Change Subject to the Fully Qualified Domain Name (FQDN) of the NDES Server, for example: ms-ndesserv.interop.com.

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "CN=<FQDN-of-NDES-Server>"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "nCipher Security World Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
```

[EnhancedKeyUsageExtension] OID=1.3.6.1.5.5.7.3.1

For example:

[Version] Signature= "\$Windows NT\$" [NewRequest] Subject = "CN=ms-ndes-serv.interop.com" HashAlgorithm = SHA256 KeyAlgorithm = RSA KeyLength = 2048 ProviderName = "nCipher Security World Key Storage Provider" KeyUsage = 0xf0 MachineKeySet = True [EnhancedKeyUsageExtension] OID=1.3.6.1.5.5.7.3.1

3. Create a Certificate request file by running the following command. Select **Module protection** when prompted.

		<
~	nCipher Key Storage Provider - Create key	
	Select a method to protect new key.	
	<ul> <li>Module protection (requires no extra cards but is less secure)</li> <li>Softcard protection (unavailable in HSM Pool mode)</li> <li>Operator Card Set protection (unavailable in HSM Pool mode)</li> </ul>	
	<u>Einish</u> Cancel	

certreq.exe -new <Path-to-Request.inf> <Name-of-Request>.req

#### Example output:

>certreq -new NDES-SSL-Cert.inf NDES-SSL-Cert.req CertReq: Request Created

- 4. For OCS and softcard protection the system will ask for the card password.
- 5. Copy the above certificate request file to the CA server.

## 2.16.2. Have the CA issue a certificate based on the Web service certificate template and the certificate request above.

In this example, **Authenticated Users** is used for provisioning certificates. Consult your security team and reference Microsoft best practices for deploying in a production environment.

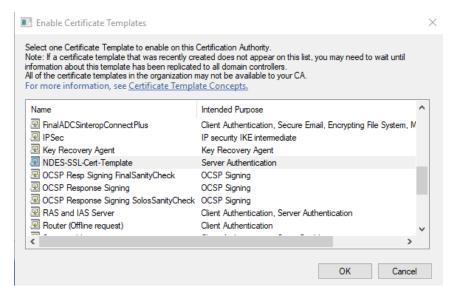
- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- 2. Enable the **Web Server** certificate template option. Open the **Certification Authority** tool and expand the issuing CA node on the left hand pane.
- 3. Right-click Certificate Templates and select Manage.
- 4. Right-click **Web Server** and select **Duplicate Template** on the **Certificate Template Console** window.
- 5. Select the **General** tab in the **Properties of New Template** dialog. Type the name you want to use on the **Template Display Name**. Then select **Apply** and **OK**.

Properties of	New Temp	olate			×
Subject N	lame	Ser	ver	Issuance	Requirements
Supersec	ded Templa	ites	Exte	ensions	Security
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation
Template dis	play name				
NDES-SSL-					
Template na NDES-SSL-		ate			
Validity perio	d:		Renewa	I period:	
2 yea	rs ~		6	weeks	
				cate certificate	exists in Active

- 6. Select the **Security** tab.
- 7. Select Authenticated Users in Groups and user names. Then check Enroll in Permissions for Authenticated Users. Then select Apply and OK.

NDES-SS	L-Cert-Templa	te Properties	5		?	×
	Subject Name		k	ssuance Requir	ements	
General	Compatibility	Request Ha	ndling	Cryptography	Key Attest	ation
Super	seded Templates	s Exte	nsions	Security	Sen	/er
Group	or user names:					
Ad State	uthenticated Use ESTPC\$ Iministrator omain Admins (IN nterprise Admins	ITEROP\Don				
				Add	Remove	
Permiss	ions for Authenti	cated Users		Allow	Deny	
Full C	Control					
Read	ł			$\checkmark$		
Write	•					
Enrol	I					
Auto	enroll					
For spe Advanc	cial permissions ( ced.	or advanced	settings	, click	Advanced	
	OK	Can	cel	Apply	Hel	p

- Return to the Certification Authority window, right-click Certificate Templates, and select New > Certificate Template to Issue.
- 9. Select the certificate template that you created earlier, then select OK.



10. Run the following command to generated the certificate:

certreq -submit -attrib "CertificateTemplate:<New-Template-Name>" <Path-to-request.req>

Partial output before executing the following steps:

```
>certreq -submit -attrib "CertificateTemplate:NDES-SSL-Cert-Template" NDES-SSL-Cert.req NDES-SSL-Cert.cer
Active Directory Enrollment Policy
{96E14557-DDD4-48BD-BE1A-AA453F20D859}
ldap:
```

11. Select the CA server from the **Certification Authority List** dialog, then select **OK**. Look for a cog icon which may be flashing on the Taskbar. Present the OCS and enter the passphrase, or enter the softcard passphrase.

Certification Authority List		?	$\times$
Select Certification Authority			
CA	Computer		^
ADFSsoftcardCA (Kerberos)	WIN-RGLUBQVT	QBD.inter	or
ADFSsoftcardENVca (Kerberos)	WIN-RGLUBQVT	QBD.inter	ot
AlexCASolosSanityCheck (Kerberos)	TestPC1.interop	.com	
Fips-128-Module-CA-1 (Kerberos)	WIN-UFBT3PKT	JA0.intero	p.
interop-MS-NDES-CA-CA (Kerberos)	MS-NDES-CA.int	erop.com	
🙀 InteropADFSmodule (Kerberos)	WIN-RGLUBQVT	QBD.inter	ot 🗸
<		:	>
	OK	Cano	el
	UN	Canc	

12. Enter the name for the certificate generated on the **Save Certificate** dialog.

Save Certificate					×
$\leftarrow$ $\rightarrow$ $\checkmark$ $\bigstar$ This PC $\Rightarrow$ Documents			∨ Ö S	earch Documents	Q
Organize 🔻 New folder					::: <b>-</b> ?
E Pictures 🖈 ^ Name	Date modified	Туре	Size		
💻 This PC	No items matc	h your search.			
3D Objects					
E Desktop					
Documents					
🖶 Downloads					
Music					
Pictures					
Videos					
🏪 Local Disk (C:)					
File name: NDES-SSL-Cert					~
Save as type: X.509 Certificate (*.cer; *.crt; *.der)					~
∧ Hide Folders			[	Save	Cancel

The final output is shown below:

```
>certreq -submit -attrib "CertificateTemplate:NDES-SSL-Cert-Template" NDES-SSL-Cert.req NDES-SSL-Cert.cer
Active Directory Enrollment Policy
{96E14557-DDD4-48BD-BE1A-AA453F20D859}
ldap:
RequestId: 11
RequestId: "11"
```

13. Copy the above certificate to the NDES server.

## 2.16.3. Install the certificate on the NDES server, matching it with the private key previously created using the nCipher CSP.

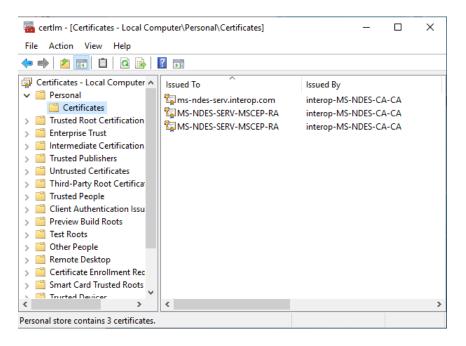
- 1. Sign in to the NDES server using the domain name, <domain\_name>\Administrator.
- 2. Run the following command. If you are using OCS or softcard protection, present the card or enter the softcard passphrase when prompted.

>certreq.exe -accept <Name-of-Certificate>.cer

Example output:

```
>certreq -accept NDES-SSL-Cert.cer
Installed Certificate:
Serial Number: 7c000000bf544d43dadb23a2f0000000000b
Subject: CN=ms-ndes-serv.interop.com
NotBefore: 10/7/2021 12:00 AM
NotAfter: 10/7/2023 12:10 AM
Thumbprint: a07344a115b23f7cd903851af3b66884e55aa3ea
```

- 3. Open certlm.msc by right-clicking on the Windows Start menu, then select Run, type certlm.msc, and select OK.
- 4. Expand the Personal store on the left pane and then select Certificates.
- 5. Check the certificate installed above is available.



6. Open the IIS manager, expand the server and **Sites** on the **Connections** pane and select **Default Web Site**.

- 7. Select Bindings on the Actions pane.
- 8. Select Add on the Site Bindings dialog.
- 9. Select https in Type: on the Add Site Binding dialog. Choose the certificate previously created in SSL certificate. Then select OK and Close.

Add Site Binding     ?       Type:     IP address:     Port:       https     All Unassigned     443       Host name:     443       I     Postassigned     443       I     Disable HTTP/2     Disable OCSP Stapling       SSL certificate:     Select     View							
https       All Unassigned       443         Host name:	×	?				iding	Add Site Bind
Host name:  Host name:  Require Server Name Indication  Disable HTTP/2  Disable OCSP Stapling  SSL certificate:		1				~	
Disable HTTP/2 Disable OCSP Stapling SSL certificate:						e:	
Disable HTTP/2 Disable OCSP Stapling SSL certificate:			]				
Disable OCSP Stapling SSL certificate:			1		ne Indication	e Server Nam	Require
SSL certificate:						HTTP/2	Disable I
					ing	OCSP Stapli	Disable (
ms-ndes-serv.interop.com View View						cate:	SSL certifica
		View.	Select	~	com	serv.interop.	ms-ndes-se
				_			
OK Cancel	cel	Canc	OK	L			

# 2.16.4. Increase the maximum number of allowed unique passwords generated by the NDES service to 30 before the service needs to be restarted.

- 1. Sign in to the NDES server using the domain name, <domain\_name>\Administrator.
- 2. Open **regedit** by right-clicking on the Windows **Start** menu, then select **Run**, type certlm.msc, and select **OK**.
- 3. Navigate to

#### Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.

- Right-click the right pane and select New > Key > DWORD (32-bit). Name the key PasswordMax.
- Right-click the key and select Modify. Set Value data to 30 on the Edit DWORD (32bit) Value dialog. Then select OK.
- 6. Restart the IIS server. Open the IIS manager, select the server on the **Connections** pane and select **Restart** on the **Actions** pane.

#### 2.16.5. Test access to the NDES web site (secured).

- 1. Sign in to the Windows client.
- Launch the browser and go to the following address: https://<NDES-server-address>/ CertSrv/mscep\_admin. Sign in as <domain-name>\SCEPSvc.

🕞 🔿 🥖 💋 https://ms-	-ndes-serv.interop.co	m/CertSrv/mscep_admin/ - X	Search		× 89 🙂
<ul> <li>Waiting for ms-ndes-ser</li> </ul>	v.i × 📑				
	Internet Explorer number of security configuration also a complete list of <u>Security Configura</u> This enhanced lev	Interest Enhanced Security Configuration is curry settings that define how users brows reduces the exposure of your server to the security settings in this configuration is the security settings in this configuration.         I of security can prevent Web sites fine twork resources, such as files on Unit work resources, such as files on Unit windows Security         I of security can prevent Web sites fine twork resources, such as files on Unit windows Security         I of security can prevent Web sites fine twork resources, such as files on Unit windows Security         I of connecting to ms-ndes-servinted         INTEROP\SCEPSvc         IDomain: INTEROP         Remember my credentials         OK	rently enabled on your servi- e Internet and intranet Web o Web sites that might pose on, see <u>Effects of Internet E</u> om displaying correctly in In iversal Naming Convention (	er. This configur sites. The a security risk. I <u>xplorer Enhance</u> ternet Explorer a UNC) shares. If	For d

3. Notice the hash value of the CA certificate and the challenge password. Refreshing the browser generates a new challenge password.

- □ × → ② ● https://ms-ndes-serv.interop.com/CertSrv/mscep_admin/ マ 會 C Search
Network Device Enrollment Service
Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).
To complete certificate enrollment for your network device you will need the following information:
The thumbprint (hash value) for the CA certificate is: 85A9C4C1 42E34126 CC3890F7 9474EB9C
The enrollment challenge password is: 5DB902533D5C0C47
This password can be used only once and will expire within 60 minutes.
Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.
For more information see Using Network Device Enrollment Service.

# Chapter 3. Use a HSM for RA certificate private keys

The instructions on this guide recommends that software based keys are used for the NDES Registration Authority (RA) certificates. Microsoft have recently posted a blog article about securing NDES. One of their recommendations is that a HSM should be used for the RA certificate private keys. See: https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ndes-security-best-practices/ba-p/2832619 for more information - pub: 11th October, 2021.)

On this basis, this section describes what needs to be done to cover this off.

nCipher CAPI can be used with the NDES RA private keys though there are limitations:

- 1. You cannot use a FIPS 140 Level 3 Security World in the NDES server, as CAPI does not meet the requirements for its use.
- 2. The nCipher CAPI provider MUST be set up as the 'default' CAPI Provider on the NDES server via the CAPI Configuration wizards. If this is not done, using the CAPI provider is not provided as an option when installing/configuring NDES.
- 3. Only module key protection and a 1/N OCS with NO passphrase will work. Essentially, the nCipher CAPI provider has no way of prompting for PINs etc. due to not being supported by the nShield Service Agent and Interactive Services Detection being removed from later versions of Windows.

#### 3.1. Procedures changes.

- 1. When asked to configure the CNG provider for the NDES server, you should use the **CSP Install Wizard** instead.
  - a. Log into the NDES server using the domain name, INTEROP\Administrator.
  - b. Select Start > Entrust nShield Security World > CSP Install wizard.
  - c. Proceed with the configuration but make sure you select **Module Protection** or **OCS Protection**. Make sure the OCS has been created with no passphrase.
- During the NDES Installation and configuration, in the Configure CSPs for the RA, choose the Signature key provider and Encryption key provider on the Cryptography for NDES window. A key size of 2048 or larger is recommended. Select one of the nCipher providers, like:
  - a. nCipher Enhanced Cryptographic Provider
  - b. nCipher Enhanced RSA and AES Cryptographic Provider

📥 AD CS Configuration		_		×
Cryptography for	NDES M	DESTINAT S-2022-NDES-Serv.		
Credentials Role Services Service Account for NDES CA for NDES	Configure CSPs for the RA Select the registration authority (RA) cryptographic service provide the signature and encryption keys.	rs (CSPs) and key le	ngths for	
RA Information	Signature key provider:	Key length:		
Cryptography for NDES	nCipher Enhanced Cryptographic Provider	× 2048		~
Confirmation Progress Results	Encryption key provider: nCipher Enhanced Cryptographic Provider	Key length: 2048		*
	More about Cryptography for NDES			
	< Previous Next >	Configure	Cance	ł

3. Once NDES is configured and installed successfully, before configuring the NDES admin page to use an SSL certificate, run the CNG provider configuration utility in the NDES server. It can coexist with the CSP setup done earlier. This is needed so the certificate request for the SSL certificate can be created.

### Chapter 4. Troubleshooting

## 4.1. Using the certreq -new <.req file here> command returns an Invalid Provider Specified error.

This error occurs when the CSPs are not installed or not set up correctly.

#### 4.1.1. Resolution

Ensure that the 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.

## 4.2. If using remote admin, the **AD CS Configuration Wizard** does not detect the OCS.

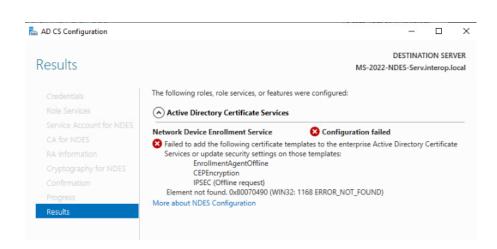
cardpp --examine shows TokenSecureChannelError. TokenSecureChannelError can occasionally be seen when presenting the OCS.

#### 4.2.1. Resolution

Remove and re-insert the cards until it is picked up by cardpp and the **AD CS Configuration Wizard**.

## 4.3. Failed to add Certificate Templates at the End of the NDES installation

You see an error similar to this:



#### 4.3.1. Resolution

To get around this issue you will need to add the CA certificate under trusted root certification authorities on the NDES server.

- 1. Sign in to the CA server using the domain name, <domain\_name>\Administrator.
- 2. Bring up the certmgr.msc utility.
- 3. Expand the **Trusted Root Certification Authorities** under **Certificates Current User** in the Left Pane and select **Certificates**.
- 4. Look for the CA Certificate that you are using and double-click it.
- Select the Certificates tab, and select Copy to File. This will bring up the Certificate Export Wizard. Select Next.
- Select DER encoded binary X.509(.CER) format for the format you want to use. Select Next.
- 7. In the **File to Export** windows, select **Browse** and pick a location and specify the file name. Select **Save**.
- 8. Select Next and then Finish to finish the export of the CA certificate.
- Now you need to import the certificate in the NDES server. Copy the file to the NDES server.
- 10. Sign in to the NDES server using the domain name, <domain\_name>\Administrator.
- 11. Double-click the CA certificated file you just exported.
- 12. Select Install Certificate.
- 13. In the Certificate Import Wizard, select Local Machine then select Next.
- 14. For the Certificate Store, select **Place all certificates in the following store**, then select **Browse**.
- 15. Select Trust Root Certification Authorities then select OK.
- 16. Select Next.

- 17. Select Finish, then OK in the Import was successful dialog.
- 18. Select **OK** to close the **Certificate** window.
- 19. Now Uninstall NDES and install it again.

# Chapter 5. Additional resources and related products

- 5.1. nShield Connect
- 5.2. nShield as a Service
- 5.3. nShield Edge
- 5.4. Entrust products
- 5.5. nShield product documentation