

Member of Microsoft Intelligent Security Association

Microsoft Security

# Microsoft Internet Information Services

## nShield<sup>®</sup> HSM Integration Guide

2023-12-05

© 2023 Entrust Corporation. All rights reserved.

# Table of Contents

1. Introduction
1.1. Product configuration
1.2. Supported nShield hardware and software versions
1.3. Requirements
2. Procedures
2.1. Select the protection method
2.2. Install the nShield HSM
2.3. Install the Security World software and create a Security World
2.4. Create the OCS
2.5. Install and register the CNG provider
2.6. Install IIS
2.7. Create a certificate request
2.8. Get the signed certificate
2.9. Install the certificate
2.10. Integrate an nShield HSM with an existing IIS deployment
3. Appendix
3.1. Import a Microsoft CAPI key into the nCipher Security World key
storage provider

# Chapter 1. Introduction

Microsoft Internet Information Services (IIS) for Windows Server is a Web server application. nShield Hardware Security Modules (HSMs) integrate with IIS 10.0 to provide key protection with FIPS-certified hardware. Integration of the nShield HSM with IIS 10.0 provides the following benefits:

- Uses hardware validated to the FIPS 140 standards.
- Enables secure storage of the IIS keys.

## 1.1. Product configuration

Entrust has successfully tested the nShield HSM integration with IIS in the following configuration:

Product	Version
Operating System	Windows 2022 Server
IIS version	10.0

# 1.2. Supported nShield hardware and software versions

Entrust successfully tested with the following nShield hardware and software versions:

#### 1.2.1. nShield

Product	Security World Software	Firmware	Netimage	OCS	Softcard	Module
nSaaS	13.3.2	12.72.1 (FIPS Certified)	12.80.5	$\checkmark$		$\checkmark$
Connect XC	13.3.2	12.72.1 (FIPS Certified)	12.80.5	$\checkmark$		$\checkmark$

Product	Security World Software	Firmware	Netimage	ocs	Softcard	Module
nShield 5c	13.3.2	13.3.2 (FIPS Pending)	13.3.2	$\checkmark$		$\checkmark$

### 1.3. Requirements

Before installing the software, Entrust recommends that you familiarize yourself with the IIS documentation and set-up process, and that you have the nShield documentation available. Entrust also recommends that there is an agreed organizational Certificate Practices Statement and a Security Policy/Procedure in place covering administration of the HSM. In particular, these documents should specify the following aspects of HSM administration:

- The number and quorum of Administrator Cards in the Administrator Card Set (ACS) and the policy for managing these cards.
- Whether the application keys are protected by the HSM module key or an Operator Card Set (OCS) protection.
- Whether the Security World should be compliant with FIPS 140 Level 3.
- Key attributes such as the key algorithm, key length and key usage.



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

For more information, see the User Guide for the HSM.

# Chapter 2. Procedures

Integration procedures include:

- Select the protection method
- Install the nShield HSM
- Install the Security World software and create a Security World
- Create the OCS
- Install and register the CNG provider
- Install IIS
- Create a certificate request
- Get the signed certificate
- Install the certificate
- Integrate an nShield HSM with an existing IIS deployment

## 2.1. Select the protection method

For this integration, IIS binding is only possible with:

- OCS without a passphrase.
- Module protection.

Follow your organization's security policy to select which one.

## 2.2. Install the nShield HSM

Install the HSM and Security World software using the instructions in the *Installation Guide* for the HSM. Entrust recommends that you do this before installing and configuring IIS.

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

- 1. Install the Security World software. For instructions, see the *Installation Guide* and the *User Guide* for the HSM.
- Add the Security World utilities path C:\Program Files\nCipher\nfast\bin to the Windows system path.

- 3. Open the firewall port 9004 for the HSM connections.
- 4. Install the nShield Connect HSM locally, remotely, or remotely via the serial console. See the following nShield Support articles and the *Installation Guide* for the HSM:
  - How to locally set up a new or replacement nShield Connect
  - How to remotely set up a new or replacement nShield Connect
  - How to remotely set up a new or replacement nShield Connect XC Serial Console model



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

5. Open a command window and confirm that the HSM is operational:

```
C:\Users\Administrator.INTEROP>enquiry
Server:
enquiry reply flags none
enquiry reply level Six
serial number 5F08-02E0-D947 6A74-1261-7843
mode
                    operational
version
                   12.80.4
. . .
Module #1:
enquiry reply flags none
enquiry reply level Six
serial number
                    5F08-02E0-D947
                    operational
mode
                    12.72.1
version
 . . .
```

- 6. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy for this.
- 7. Confirm that the Security World is **usable**:

```
C:\Users\Administrator.INTEROP>nfkminfo
World
generation 2
state 0x3737000c Initialised Usable ...
...
Module #1
generation 2
state 0x2 Usable
...
```

#### 2.4. Create the OCS

If using OCS protection, create the OCS now. Follow your organization's security

policy for the value N of K/N. As required, create extra OCS cards, one for each person with access privilege, plus spares.



Administrator Card Set (ACS) authorization is required to create an OCS in FIPS 140 level 3.



After an OCS card set has been created, the cards cannot be duplicated.

- If using remote administration, ensure 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 administrator.
- Execute the following command. Follow your organization's security policy for the values K/N. The OCS cards cannot be duplicated after they are created. Do **not** enter a passphrase or password at the prompt, just press **Return**. Notice slot 4, remote via a Trusted Verification Device (TVD), is used to present the card. In this example, K=1 and N=1.

```
>createocs -m1 -s4 -N testOCS -Q 1/1
FIPS 140 level 3 auth obtained.
Creating Cardset:
Module 1: 0 cards of 1 written
Module 1 slot 0: Admin Card #1
Module 1 slot 4: blank card
Module 1 slot 3: unknown card
Module 1 slot 2: empty
Module 1 slot 5: empty
Module 1 slot 4:- no passphrase specified - writing card
Card writing complete.
cardset created: hkltu = 991b6cb36db1adbe317964086273eee97e466123
```

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

4. Verify the OCS created:

991b6cb36db1adbe317964086273eee97e466123 1/1 none-NL testOCS

The **rocs** utility also shows the OCS 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> guit

#### 2.5. Install and register the CNG provider

- 1. Select Start > Entrust > CNG configuration wizard.
- 2. Select Next on the Welcome window.

nShield CNG Providers Confi	guration Wizard	$\times$
	Welcome to the nShield support software This wizard guides you through the installation of nShield's Cryptographic Service Providers.	
	nShield CNG Providers enable the use of nShield modules with the wide range of security-enabled applications provided with Windows.	
	If you have not already created an nShield security world or a suitable card set, the wizard guides you through their creation before registering the CNG Providers.	
	To continue, click Next.	
ENTRUST		
	< Back Next > Cance	ł

 Select Next on the Enable HSM Pool Mode window, leaving Enable HSM Mode for CNG Providers un-checked.



If you intend to use multiple HSMs in a failover and loadsharing capacity, select **Enable HSM Pool Mode for CNG Providers**. If you do, you can only use module protected keys. Module protection does not provide conventional 1 or 2 factor authentication. Instead, the keys are encrypted and stored as an application key token, also referred to as a Binary Large Object (blob), in the kmdata/local directory.

 Select Use existing security world on the Initial setup window. Then select Next. 5. Select the HSM (Module) if more than one is available on the **Set Module States** window. Then select **Next**.

Ensure module	tes es are in the correct s	state before you proceed.	EM
The following	modules are available	e in your system:	
Module ID	Mode	State	
1	operational	usable	
2	operational	foreign	
Or reset modu uninitialized n	le 2 to the initializatio Shield modules. ser guide for details o eed to power down y	e current world. Click Next to con n state to enable you to restore y of how to put your nShield module our computer, select the tickbox i ntinue the installation.	our security world to in the initialization
state. If you n			

6. In Key Protection Setup, select Operator Card Set protection. Then select Next.

nShield CNG Providers Configuration Wizard	×
Key Protection Setup Set up the private key-protection method.	ENTRUST
Select the default method that will be used to protect private keys generated by the CNG Key Storage Provider.	
If softcard or DCS protection is selected, the choice will be offered on the next page whether to use an existing token or create a new one.	
O Module protection (requires no extra cards but is less secure).	
O Softcard protection (unavailable in HSM Pool Mode).	
Operator Card Set protection (unavailable in HSM Pool Mode).	
Allow any protection method to be selected in the GUI when generating.	
< Back Next > C	ancel

7. Choose from the **Current Operator Card Sets** or **Current Softcards** list. Notice these were created above. Then select **Next** and **Finish**.

Shield CNG Providers Configuration Token for Key Protection Select the token that will be used t			reate a new token.	X
Current Operator Card Sets: testOCS	Nam Tok Sha Time	ator Card Set Tok ne: en hash: ring parameters: sout: ently protecting:	testOCS 0xa165a26f	
Create a new Operator Card Set r	name			
Number of cards required (K):		Tota	al number of cards (N):	
Card set has a time- Persistent		Card set time- e remotely	out: sec	conds
		< Back	Next > (	Cancel

8. Verify the provider with the following commands:



9. Check the registry in CNGRegistry:

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Cryptography\Providers\nCipherSecurityWorldKeyStorageProvid er



### 2.6. Install IIS

To install Microsoft Internet Information Services:

- 1. Open Server Manager by selecting **Start > Server Manager**.
- 2. Select Manage and then select Add Roles and Features.

Server Manager	anager • Dashl	ooard	• @   🏲 м	- 🗗 nage Tools View F Add Roles and Features
Dashboard	WELCOME TO SERVI	ER MANAGER		Remove Roles and Features
Local Server				Add Servers Create Server Group
All Servers		1 Configure this local s	server	Server Manager Properties
File and Storage Services	QUICK START			
		2 Add roles and features	;	
		3 Add other servers to m	nanage	
	WHAT'S NEW	4 Create a server group		
		5 Connect this server to	cloud services	
	LEARN MORE			Hide

3. On the **Before you begin** screen, select **Next**.

🚔 Add Roles and Features Wizard		2		×
Before you begin			TION SERV HARDSERV	
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine which ro features to install based on the computing needs of your organization, such as shar hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, clo complete the steps, and then run the wizard again. To continue, click Next.	ing docu	uments, o	
	Skip this page by default			
	< Previous Next > Insta		Cancel	

 On the Select installation type screen, ensure the default selection of Role or Feature Based Installation is selected and select Next.

elect installation	on type	 HARDSER
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select the installation type. You can install roles and features on a running machine, or on an offline virtual hard disk (VHD).	

5. On the **Server Selection** screen, select a server from the server pool and select **Next**.

	on server			DESTINATION SER WIN-HARDSER
Before You Begin	Select a server or a virtu	al hard disk on which	to install roles and features.	
nstallation Type	<ul> <li>Select a server from</li> </ul>	the server pool		
Server Selection	O Select a virtual hard	disk		
Server Roles	Server Pool			
eatures				
	Filter:			
	Name	IP Address	Operating System	
	WIN-HARDSERVER	10.194.146.166	Microsoft Windows Server	2019 Datacenter
	1 Computer(s) found			
	This page shows server		ndows Server 2012 or a newer	
	This page shows servers and that have been add	ed by using the Add	ndows Server 2012 or a newer Servers command in Server Ma on is still incomplete are not s	anager. Offline servers a

6. On the **Select server roles** screen, select the **Web Server (IIS) Role** and select **Next** 

ᡖ Add Roles and Features Wizard		– 🗆 X
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select one or more roles to install on the selected server. Roles Active Directory Domain Services Active Directory Federation Services Active Directory Rights Management Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server Fax Server Fax Server Fax Server Fax Server Fax Server	DESCRIPTION SERVER WIN-HARDSERVER Description Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
	Host Guardian Service     Hyper-V     Network Controller     Network Policy and Access Services     Print and Document Services     Remote Access     Remote Desktop Services     Volume Activation Services     Windows Deployment Services     Windows Server Update Services	ext > Install Cancel

7. When prompted to install Remote Server Administration Tools, select **Add Features** and select **Next**.

C. Harrison to a la serie	re required for Web Server (IIS)?
e tollowing tools are re ve to be installed on th	equired to manage this feature, but do not le same server.
Web Server (IIS)	
<ul> <li>Management Too [Tools] IIS Ma</li> </ul>	ols nagement Console
	2

8. On the **Select features** screen, keep the default selection and select **Next**.

📩 Add Roles and Features Wizard				21		×
Select features				0001110	ATION SERV HARDSERV	
Before You Begin	Select one or more features to install on the selected se	erver.				
Installation Type	Features		Description			
Server Selection	INET Framework 3.5 Features	~	.NET Framew	ork 3.5 com	bines the	e
Server Roles	<ul> <li>NET Framework 3.7 Features (2 of 7 installed)</li> </ul>		power of the			
Features	Background Intelligent Transfer Service (BITS)     BitLocker Drive Encryption		APIs with nev building appl			
Web Server Role (IIS)	BitLocker Network Unlock		appealing us			
Role Services	BranchCache Client for NES		your custome information,			
Confirmation	Containers		secure comm			de
	Data Center Bridging Direct Play		the ability to business pro		nge of	
	Enhanced Storage					
	Group Policy Management					
	Host Guardian Hyper-V Support I/O Quality of Service					
	IIS Hostable Web Core					
	Internet Printing Client IP Address Management (IPAM) Server					
	SNS Server service	$\sim$				
	<	>				
	< Previous	Next :	>	nstall	Cance	el 👘
		1000				

9. On the Web Server Role (IIS) screen, select Next.

📥 Add Roles and Features Wizard		-		×
Web Server Role	(IIS)		TION SERV HARDSERV	
Before You Begin Installation Type Server Selection Server Roles	Web servers are computers that let you share information over the Internet, or thro extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.1 Communication Foundation.	enhance	ed securit	y,
Features Web Server Role (IIS) Role Services Confirmation Results	<ul> <li>The default installation for the Web Server (IIS) role includes the installation of ro enable you to serve static content, make minor customizations (such as default d errors), monitor and log server activity, and configure static content compression</li> </ul>	ocument		ΠP
	More information about Web Server IIS			
	< Previous Next > Insta		Cance	

10. On the **Select Role Service** screen, select **Next**.

📥 Add Roles and Features Wizard		- 🗆 ×
Select role service	S	DESTINATION SERVER WIN-HARDSERVER
Before You Begin Installation Type	Select the role services to install for Web Server (IIS) Role services	Description
Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results		Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
	Request Monitor     Tracing     Verformance     Static Content Compression     Dynamic Content Compression     VSecurity	> Install Cancel

11. On the confirmation screen, select **Install**.

📥 Add Roles and Features Wizar	d	28		×
Confirm installat	ion selections		ATION SER HARDSER	
Before You Begin	To install the following roles, role services, or features on selected server, click Inst	all.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this page I			
Server Roles	been selected automatically. If you do not want to install these optional features, their check boxes.	click Previ	ious to c	ear
Features				
Web Server Role (IIS)	Web Server (IIS)			^
Role Services	Management Tools			
Confirmation	IIS Management Console			
Results	Web Server Common HTTP Features Default Document Directory Browsing HTTP Errors Static Content Health and Diagnostics			~
	Export configuration settings Specify an alternate source path			
	< Previous Next > Ins	tall	Cance	al

12. Once the installation completes, Select **Close**.

📥 Add Roles and Features Wizard		_		×
Installation progre	255		ATION SERV HARDSERV	
	View installation progress			
	() Feature installation			
	Installation succeeded on WIN-HARDSERVER.			
	Web Server (IIS)			$\sim$
	Management Tools			
Role Services	IIS Management Console			
	Web Server Common HTTP Features			
Results	Default Document			
	Directory Browsing			
	HTTP Errors			
	Static Content			
	Health and Diagnostics HTTP Logging			~
	You can close this wizard without interrupting running tasks. View task pro page again by clicking Notifications in the command bar, and then Task D Export configuration settings		open this	;
	< Previous Next > Cla	ose	Cance	2

### 2.7. Create a certificate request

IIS Manager does not support the creation of certificates protected by CNG Keys and these must be created using the Microsoft command line utilities. Commands executed in this section are run on a PowerShell in Windows.



Due to limitations of IIS itself, no GUI prompts (even via nShield Service Agent) can be displayed, so any OCS protection must be passphrase-less 1/n quorum. For this reason, use only OCS or module protection.

Complete the following steps to create a certificate request:

1. Make sure the nCipher Primitive Provider and nCipher Security World Key Storage Providers are listed:

```
% cnglist.exe --list-providers
```

```
Microsoft Key Protection Provider
Microsoft Passport Key Storage Provider
Microsoft Platform Crypto Provider
Microsoft Primitive Provider
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Microsoft SSL Protocol Provider
Windows Client Key Protection Provider
nCipher Primitive Provider
nCipher Security World Key Storage Provider
```



If the nCipher Primitive Provider and nCipher Security World Key Storage Provider are not listed, follow the steps in Install

#### and register the CNG provider.

- 2. Set up a template file:
  - a. Generate a request for an SSL certificate linked to a 2K RSA key by creating a file called request.inf with the following information:

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
Subject = "CN=interop.com,C=US,ST=Florida,L=Sunrise,O=InteropCom,OU=WebServer"
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
```

Your **request.inf** file can vary from the code given above. This is an example, not a definitive model.

- b. Specify the subject details of the Domain Controller which is issuing the certificate.
- c. Specify the key algorithm and key length as required, for example RSA 2048.
- d. Specify the Provider name as **nCipher Security World Key Storage Provider**.
- e. After you set up the template successfully, save it as request.inf on the C:\ drive.

This PC > Local Disk (C:)		✓ U Searc	h Local Disk (C:)
Name	Date modified	Туре	Size
📜 inetpub	1/26/2023 3:32 PM	File folder	
📜 PerfLogs	6/7/2021 4:55 PM	File folder	
📜 Program Files	1/25/2023 2:54 PM	File folder	
📜 Program Files (x86)	1/23/2023 11:35	File folder	
📒 ProgramData	1/25/2023 2:54 PM	File folder	
📜 Users	6/7/2021 9:36 PM	File folder	
📜 Windows	1/26/2023 3:39 PM	File folder	
🔊 request	1/26/2023 3:35 PM	Setup Information	1 KB

- 3. Open a command prompt and go to the local drive, in this case C:\.
- 4. To create the certificate request for the Certification Authority, execute the command:

```
% certreq.exe -new request.inf IISCertRequest.csr
CertReq: Request Created
```

A certificate request called **IISCertRequest.csr** is generated and placed on the **C**:\ drive. This file is used to be sent to a Certificate Authority.

#### 2.8. Get the signed certificate

- 1. Submit the CSR file to a CA such as VeriSign, Entrust, and so on.
- 2. The CA authenticates the request and returns a signed certificate or a certificate chain.
- 3. Save the reply from the CA in the current working directory.

In this guide the signed certificate file is **IISCertRequest.cer**.

### 2.9. Install the certificate

Make the certificate available to be used in IIS and bind the certificate with the https settings in IIS.

Commands used in this section are run from a Windows PowerShell.

#### 2.9.1. Make the certificate available for use in IIS

To make the certificate available for use in IIS, run the following command:

```
% certreq -accept IISCertRequest.cer
```

Where **IISCertRequest.cer** is the binary certificate exported from the CA. Running this command makes the CA certificate trusted on the Web Server.

```
Installed Certificate:
Serial Number: 1c0000002685e0d9d057707290000000002
Subject: CN=interop.com, OU=WebServer, O=InteropCom, L=Sunrise, S=Florida, C=US
NotBefore: 1/25/2023 2:18 PM
NotAfter: 1/25/2024 2:28 PM
Thumbprint: 7a814f14f77db1eae717a4c753fd7b184d6a6037
```

#### 2.9.2. Bind the certificate with a secure IIS web server

- 1. Go to Start > Internet Information Service Manager.
- 2. Select the hostname, then double-click **Server Certificates** and verify the certificate you accepted in the previous step is listed.

3. Under **Sites** on the left-hand side of the IIS Manager screen, select **Default website**.

Internet Information Services (IIS)	Manager	- 🗆 ×
← → ♥ WIN-HARDSERV	/ER → Sites → Default Web Site →	🖬 🖂 🏠 🔞 ·
<u>F</u> ile ⊻iew <u>H</u> elp		
pie gew gep Connections	Default Web Site Home         Filter:          •          •          •	Actions       Open Feature       Edit Peninsions       Edit Stee       Bendrom       Bendrom       Bendrom       Beschort       Wew Applications       Wew Vindual Directories       Manage Website       © Restart       > Start       Browne Website       @ Browne Website       @ Browne Website       @ Browne Website       @ Browne Medited       @ Help
< >> Ready	Eestures View 🕅 Content View Administrator: Windows PowerShell	•
Neauy		1

- 4. Select **Bindings** link on the right-hand side of the IIS Manager.
- 5. Access the **Site Bindings** screen.
- If the https protocol is not listed, you must add it now. To do this, select Add, set the protocol as https and select the required certificate from the list.

Site Bindir	ngs				? ×
Type http https	Host Name	Port 80 443	IP Address * *	Binding Informa	Add Edit Remove Browse
					Close

7. Select the **https** protocol, select **Edit**, and then select the certificate from the list:

Edit Site Binding			? ×
<b>Type:</b> https ∨	IP address: All Unassigned	Port:	
Host name:		]	
Require Server Na	me Indication		
Disable HTTP/2			
Disable OCSP Stap	ling		
SSL certificate:		1	
interop.com	~	Select	View
		OK	Cancel

- 8. Select **OK** to complete the certificate binding for SSL connection.
- 9. Select Close on the Site Bindings screen.
- 10. Restart the IIS server.

# 2.10. Integrate an nShield HSM with an existing IIS deployment

This section describes how to upgrade an existing IIS server installation to use an nShield HSM to protect the private key. It is assumed that the existing certificate must continue to be used by the server afterwards.

The Prerequisites to integrate are:

- An IIS set-up with software-protected certificate and private key.
- nShield Software installed and a Security World created using The CNG Configuration Wizard, or the front panel of an nShield Connect.

#### 2.10.1. Export the software-protected certificate

Complete the following procedure to export the software-protected certificate:

1. Type MMC at the command prompt and select **OK**.

The Microsoft Management Console starts.

- 2. On the initial screen, select **File > Add/Remove Snap-in** and select **Add**.
- 3. Select Certificates from Available Standalone Snap-ins and select Add.

		^	Selected snap-ins:	Edit Extensions
nap-in	Vendor		Console Root	Edit Extensions
ActiveX Control	Microsoft Corp			Remove
Authorization Manager	Microsoft Corp			Remove
Certificate Templates	Microsoft Corp			
Certificates	Microsoft Corp			Move Up
Certification Authority	Microsoft Corp			
Component Services	Microsoft Corp			Move Down
Computer Managem	Microsoft Corp		Add >	
Device Manager	Microsoft Corp			
P Disk Management	Microsoft and			
Enterprise PKI	Microsoft Corp			
Event Viewer	Microsoft Corp			
🖥 Folder	Microsoft Corp			
Group Policy Object	Microsoft Corp			
Internet Information	Microsoft Corp			Advanced
TD Security Monitor	Microcoft Corn	~		Auvancea

- 4. On the **Certificates snap-in** screen, select **Computer account** and select **Next**.
- 5. On the Select Computer screen, select Local computer, select Finish then OK.
- 6. Navigate to **Certificates (Local Computer) > Personal > Certificates**.

🔿 🙍 🛅 📋 💁 🕼							-
	ssued To	Issued By	Expiration Date	Intended Purposes	Friend	Actions	
	interop.com	interop-WIN-MSIIS-CA-15	1/26/2024	Server Authentication	<non< td=""><td>Certificates</td><td></td></non<>	Certificates	
<ul> <li>Personal</li> <li>Certificates</li> </ul>	interop-WIN-MSIIS-CA-15	interop-WIN-MSIIS-CA-15	1/26/2028	<all></all>	<non< td=""><td>More Actions</td><td></td></non<>	More Actions	
Trusted Root Certificatio							
> interprise Trust							
Intermediate Certificatio							
> 📔 Trusted Publishers							
Untrusted Certificates							
> 📔 Third-Party Root Certific							
Trusted People							
> 📋 Client Authentication Iss							
Preview Build Roots							
> 🧮 Test Roots							
> 🧮 Remote Desktop							
> Certificate Enrollment Re							
> Construction Similar Simi							
> intrusted Devices							
Web Hosting     Windows Live ID Token I							
Windows Live ID Token I:     WindowsServerUpdateSi							

- 7. Right-select the certificate file and select **All Tasks** > **Export**.
- 8. The Welcome to the Certificate Export Wizard screen appears. Select Next.
- 9. On the **Export Private Key** screen, select **No, do not export the private key** and select **Next**.

	×
Certificate Export Wizard	
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
○ Yes, export the private key	
• No, do not export the private key	
	Export Private Key You can choose to export the private key with the certificate. Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page. Do you want to export the private key with the certificate? O Yes, export the private key

10. On the Export File Format screen, select Base-64 encoded X.509 (.Cer) and select Next.

Se	lect the format you want to use:
	○ <u>D</u> ER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	$\bigcirc$ Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export <u>all</u> extended properties
	Enable certificate privacy
	Microsoft Serialized Certificate Store (.SST)

11. On the **File to Export** screen, select an absolute path and filename to save the exported Certificate.

Select Next.

← 😺 Certificate Export Wizard

12. The Completing the Certificate Export Wizard screen appears.

#### Select Finish.

13. After exporting the certificate, delete the certificate from the certificate store.

#### 2.10.2. Import a certificate into the certificate store

- Go to the command prompt and type MMC, then select OK to open the Microsoft Management Console.
- 2. On the initial screen, select **File** > **Add/Remove Snap-in** and select **Add**.
- 3. From Available Standalone Snap-ins, select Certificates and select Add.

		_	Selected snap-ins:	
nap-in	Vendor	^	Console Root	Edit Extensions
ActiveX Control	Microsoft Corp			Remove
Authorization Manager	Microsoft Corp			Remove
Certificate Templates	Microsoft Corp			
Certificates	Microsoft Corp			Move Up
Certification Authority	Microsoft Corp			
Component Services	Microsoft Corp			Move Down
Computer Managem	Microsoft Corp		Add >	
Device Manager	Microsoft Corp			
Disk Management	Microsoft and			
Enterprise PKI	Microsoft Corp			
Event Viewer	Microsoft Corp			
Folder	Microsoft Corp			
Group Policy Object	Microsoft Corp			
Internet Information	. Microsoft Corp			Advanced
TD Security Monitor	Microsoft Corn	~		Advancea

- 4. On the Certificates snap-in screen, select Computer account and select Next.
- 5. On the **Select Computer** screen, select **Local computer**, select **Finish** and select **OK**.
- 6. Navigate to Certificates (Local Computer) > Personal > Certificates.
- 7. Right-click the certificate folder and select **All Tasks** > **Import**.
- 8. The Welcome to the Certificate Import Wizard screen appears. Select Next.
- Navigate to the location of the certificate from the Origin Server and select Next.
- 10. On the **Certificate Store** screen, select **Place all certificates in the following store**.

Certifi	cate Import Wizard		
	<b>te Store</b> tificate stores are system areas where certificates are kep	t.	
Win	dows can automatically select a certificate store, or you ca certificate.	an specify a location for	
(	$\supset$ Automatically select the certificate store based on the ty	pe of certificate	
(	Place all certificates in the following store		1
	Certificate store:		
	Personal	Browse	
		Next Car	ncel

- 11. Make sure that the default selection in **Certificate Store** is **Personal**, then select **Next**.
- 12. The **Completing the Certificate Import Wizard** screen appears.

Select Next, then select OK.

 Locate the serial number for the certificate. To do this on the Microsoft Management Console, access **Certificates**, select the certificate, and select the **Details** tab to see the **Serial Number**.

🐖 Certifica	te		$\times$
General D	etails Certification Path		
Show: <,	All>	~	
Field		Value	^
🛅 Versio	n	V3	
🛅 Serial	number	72d80d6e3c2ea29641f3589de	
🛅 Signat	ure algorithm	sha256RSA	
🛅 Signat	ure hash algorithm	sha256	
🛅 Issue		interop-WIN-MSIIS-CA-13, inte	
🛅 Valid f	rom	Wednesday, January 25, 2023	
🛅 Valid t	0	Tuesday, January 25, 2028 2:1	
Subje		interop-WIN-MSIIS-CA-13, inte	~

14. Run the following command from the Windows terminal:

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

- Open the IIS Manager from Start > Internet Information Services (IIS) Manager.
- 16. Under **Sites** on the left-hand side of the **IIS Manager** screen, select the required web site.
- 17. On the right-hand side of the **IIS Manager** screen, select **Bindings**.
- 18. On the **Site Bindings** screen, select **Add**.
- 19. Select the protocol **HTTPS**.
- 20. Select the certificate from the drop-down list.
- 21. To complete the certificate binding for SSL connection, select  $\mathbf{OK}$ .

# Chapter 3. Appendix

### 3.1. Import a Microsoft CAPI key into the nCipher Security World key storage provider

To import a Microsoft CAPI key into the nCipher Security World key storage provider:

 Navigate to the C:\Program Files\nCipher\nfast\bin folder and run cngimport.exe in the command prompt:

cngimport -m -M -k "MS CAPI key" "imp\_key\_name"

The Microsoft CNG key is in the C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys folder. For example:

cngimport -m -M -k,"48753e97af4e829f\_b2885b-321a-42b9-9122-81d377654436" "Importedkeyname"

2. To check the success of the import, list the keys in the Security World in the command prompt:

cnglist --list-key