DigiCert[®] PKI Platform

HSM Installation and Configuration for nShield

August 20, 2020



Legal Notice

Copyright © 2020 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Other names may be trademarks of their respective owners.

The product described in this document is provided by DigiCert, Inc. and distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of DigiCert, Inc. and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DIGICERT, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the licensed software and documentation by the U.S. Government shall be solely in accordance with the terms of this documentation.

DigiCert, Inc. 2801 North Thanksgiving Way, Suite 500 Lehi, UT 84043 https://www.digicert.com/

Table of Contents

INTRODUCTION	4
REVISION HISTORY	4
SUPPORTED HSMS	4
NSHIELD CONNECT HSM	5
INSTALL SECURITY WORLD SOFTWARE	5
CONFIGURE SECURITY WORLD SOFTWARE	9
CONFIGURE HA (HIGH AVAILABILITY)	14
CONFIGURE CSP (MODULE PROTECTION)	15
CONFIGURE CNG/KSP (MODULE PROTECTION)	21
GENERATE CSR (MODULE PROTECTION)	26
GET RA CERTIFICATE IN PKI-MANAGER	27
INSTALL RA CERTIFICATE	29
SHARING THE EXISTING CERTIFICATE BETWEEN 2 MACHINES ON NCIPHER HSM (OPTIONAL)	30

Introduction

This document describes the installation and configuration steps for the nShield Connect HSM, to be used by the DigiCert PKI Enterprise Gateway and Autoenrollment server.

Revision History

No.	Date	Summary
1.	2020/07/02	Create a new entry
2.	2020/07/28	Incorporated feedback from PSO and added HA configuration section
3	2020/08/20	Incorporated feedback from PSO

Supported HSMs

HSM Type	Client Version	Software Version	Firmware Version
nShield Connect XC Base HSM	12.60.3 (hotfix-	12.60.3 (hotfix- 111745-TAC-	12.50.11
• Strict FIPS 140-2 Level 3 disabled	111745- TAC-656)	656)	vo security world
Module protection for CSP and CNG			

nShield Connect HSM

nShield Connect is network HSM, which allows to create a module (Operator Card Sets) to store a key. Security World Software will be able to access the partition of the HSM through secure channel.



Install Security World Software

1. Install hotfix version v12.60.3 (hotfix-111745-TAC-656). Extract (or Mount) iso image.

N 🛃 📕 =	Manage	DVD Drive (F:) nCipher Security World	-	- 🗆 ×
File Home Share Vie	Application Tools			~ 🥐
$\leftarrow \rightarrow \checkmark \uparrow$ (N) > This PC > DVD Drive (F:) nCipher Security World \checkmark (C) Search DVD Drive (F:)			/e (F:) nCipher 🔎	
Quick access	Name	^ Date modified	Туре	Size
	documentation	9/24/2019 9:44 PM	File folder	
🧢 This PC	license	9/24/2019 9:45 PM	File folder	
🧊 3D Objects	release	9/24/2019 9:44 PM	File folder	
E. Desktop	🔬 autorun.inf	9/24/2019 9:44 PM	Setup Information	1 KB
Documents	Dipher-EULA.pd	f 9/24/2019 9:44 PM	PDF File	216 KB
Downloads	N nCipher-N.ico	9/24/2019 9:44 PM	lcon	104 KB
Music	👘 setup.msi	9/24/2019 9:44 PM	Windows Installer	576,232 KB
Pictures	version.txt	9/24/2019 9:44 PM	Text Document	1 KB
8 items 1 item selected 562 M	В			

NOTE: If you try to upgrade the client software, the old version must be uninstalled. After uninstallation, the system requires to reboot the computer.

Even if you uninstall the old version, you do not have to configure the client software again because the HSM has already configured the client.



2. Run "setup.msi" as administrator and click Next.

3. Accept the Software License Agreement and click Next.



4. Click Next to Install the nShield to default folder or click Change to choose another

🖟 nShield Software Setup		_		×
Destination Folder Click Next to install to the default folder or	click Change to o	choose another.	6	N
Install nShield Software to:				
C:\Program Files\nCipher\nfast\ Change				
	<u>B</u> ack	Next	Can	cel

5. Select the product features and click **Install**.

nShield Software Setup -	
Product Features	
Select the way you want features to be installed.	
nShield Software	
□ - nShield Hardware Support	
Shield Core Tools	
□ Inshield cer's (a'u', erd)	
nShield Debug	
nShield Device Drivers	
nShield Java	
Shield Java Developer	
	*
All binaries and nShield libraries.	
This feature requires 184KB on your hard drive. It has 13 of 13 subfeatures selected. subfeatures require 2153MB on your hard drive.	The
<u>B</u> ack <u>I</u> nstall	Cancel

6. Wait for the completion.

ß	nShield Software Setup — 🗆 🗙
	Installing nShield Software
	Please wait while the Setup Wizard installs nShield Software.
	Status: Validating install
	<u>B</u> ack <u>N</u> ext Cancel

7. Installation process is now complete. Click Finish.



NOTE: After uninstallation, several files of the old software remains at the Program folders under "**Programs and Features**". You need to manually remove the files for the installation to proceed.

Configure Security World Software

1. Setting the PATH for nShield utilities.

It is recommended that the PATH environment variable be changed to include %NFAST_HOME%\bin (usually C:\Program Files\nCipher\nfast\bin).

dit environment variable	>
C:\Program Files (x86)\Common Files\Oracle\Java\javapath	New
%SystemRoot%\system32	
%SystemRoot%	<u>E</u> dit
%SystemRoot%\System32\Wbem	
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\	<u>B</u> rowse
C:\Program Files\Java\jre1.8.0_251	
C:\Program Files\nCipher\nfast\bin	<u>D</u> elete
	_
	Move <u>U</u> p
	Move Down
	E alta a sua
	Edit <u>t</u> ext
OK	Cancel
UK UK	Cancel

2. Configuring client computers to use the nShield Connect.

Each client computer must be configured to use the internal security module of your nShield Connect. There are two methods for achieving this:

- Enrolling the client with the configuration file.
- Enrolling the client with command-line utilities.
- 3. Check if the tool works.

The **nethsmenroll** command-line utility edits the client hardserver's configuration file to add the specified nShield Connect. For more information about the options available to use with **nethsmenroll**, read the following section Client configuration utilities, or run the command:

nethsmenroll -help

4. Obtain HSM information (ESN and HKNETI).

Obtain the following information about the HSM before you set up an RFS for the first time:

- The IP Address
- The electronic serial number (ESN)
- The hash of the KNETI key (HKNETI)

The KNETI key authenticates the HSM to clients. It is generated when the HSM is first initialized from factory state.

To retrieve the nShield Connect's ESN and HKNETI, run the command:

anonkneti <Unit IP>

The output example of the command is as follows.

```
>anonkneti.exe 10.100.132.220
2C17-03E0-D947 918953c37e0d4dc5d723a359295ff93cfe6eb4a6
```

5. Register the HSM in client configuration.

The nethsmenroll command-line utility edits the client hardserver's configuration file to add the specified nShield Connect.

If you are enrolling the client without an nToken, run the command:

```
> nethsmenroll [Options] --privileged < Unit IP> < Unit ESN> < Unit KNETI
HASH>
```

The example of outputs is as follows.

```
> nethsmenroll -p <SERVER-IP> <ESN> <KNETIHASH>
OK configuring hardserver's nethsm imports
```

NOTE: The following is an output of the command if the entry that you want to add already exist.

> nethsmenroll -p nethsmenroll 10.100.132.220 2C17-03E0-D947 918953c37e0d4dc5d723a359295ff93cfe6eb4a6

nethsmenroll: an entry with ESN 2C17-03E0-D947 already exists; use `--force' to overwrite it

6. Testing the installation.

To test the installation and configuration, follow these steps:

- Log in on the client computer as a regular user and open a command window.
- Run the command:
 - > enquiry

A successful enquiry command returns an output of the following form:

```
Server:
enquiry reply flags none
enquiry reply level Six
mode operational
version #-#-#
speed index #######
rec. queue ####..####
- - -
version serial #
remote server port ####
Module ##:
enquiry reply flags none
enquiry reply level Six
mode operational
version #-#-#
speed index #####
rec. queue ##..###
- - -
rec. LongJobs queue ##
SEE machine type PowerPCELF
supported KML types DSAp1024s160 DSAp3072s256
hardware status O
```

NOTE: If the enquiry command says that the unit is not found:

Restart the client computer

Re-run the enquiry command

7. Configure RFS synchronization.

The remote file system (RFS) contains the master copy of the HSM Security World data for backup purposes. The RFS can be located on either a client or another network-accessible computer where the Security World Software is installed. If the RFS is on a client, the same file structure also contains the configuration files for that client.

NOTE: Refer **rfs-sync** section from **"User Guide nShield Connect for Windows"** for more details

```
C:\Users\Administrator> rfs-sync.exe --setup --no-authenticate <RFS-IP>
No current RFS synchronization configuration.
Configuration successfully written; new config details:
Using RFS at <RFS-IP>:9004: not authenticating.
C:\Users\Administrator> rfs-sync.exe --update
Starting synchronisation, task ID 5ca6fa8a.32f596d69d1bb3ca
Updated (new) card b5310850ab6c82e1605382c7b68b183cda60d13a 1
Updated (new) card b5310850ab6c82e1605382c7b68b183cda60d13a 2
Updated (new) card_b5310850ab6c82e1605382c7b68b183cda60d13a_3
. . .
Updated (new) module_2C17-03E0-D947
Updated (new) module_2C17-03E0-D947
Updated (new) world
Finished synchronisation: 53 files updated, 0 committed.
C:\Users\Administrator> rfs-sync --commit
Starting synchronisation, task ID 5ca48468.764b879a080c7eca
This client does not have commit permission to the RFS; you must run 'rfs-
setup --gang-client' on the RFS first.
```

NOTE: The port of RFS synchronization is 9004.

8. Check status through KeySafe and run the following command.

```
C:\Program Files\nCipher\nfast\bin\ksafe-app.jar
```

OR

Go to **Start->nCipher->KeySafe**. Review the configuration and confirm if the operational state is usable.



NOTE: Please find the details of KeySafe in "User Guide nShield Connect for Windows"

Configure HA (High Availability)

To configure HA for a multi- hardserver setup, add all the hardservers as follows:

1. Obtain the HSM ESN and HKNETI information.

To retrieve the nShield Connect's ESN and HKNETI, run the command:

anonkneti <Unit IP>

The example of output of the command is as follows:

>anonkneti.exe <Server-A IP> 0401-03E0-D947 18fd6da2186bd778259d31bd63cee09a01b68794 >anonkneti.exe <Server-B IP> 4711-02E0-D947 c4405efd401b3719c109cde104832e3eec18376c

2. Add all the hardservers.

The nethsmenroll command-line utility edits the client hardserver's configuration file to add the specified nShield Connect.

If you are enrolling the client without an nToken, run the command:

```
> nethsmenroll [Options] --privileged < Unit IP> < Unit ESN> < Unit KNETI
HASH>
```

The example of outputs is as follows.

> nethsmenroll -p <Server-A IP> 0401-03E0-D947
18fd6da2186bd778259d31bd63cee09a01b68794
OK configuring hardserver's nethsm imports
> nethsmenroll -p <Server-B IP> 4711-02E0-D947
c4405efd401b3719c109cde104832e3eec18376c
OK configuring hardserver's nethsm imports

Configure CSP (Module protection)

NOTE: Please note that for the deployment of the Autoenrollment Server, you need to Configure CSP.

1. Go to Start-> nCipher and run CSP Install wizard (64bit).



2. Click Next.



3. On Enable HSM Pool Mode, click Next.

nCipher CAPI Providers Configuration Wizard	\times
Enable HSM Pool Mode Set options for Pool Mode CAPI provider.	N
Would you like to enable HSM Pool Mode for CAPI? HSM Pool Mode means that the nCipher CAPI providers will see a single logical view with all the available HSMs seer one resource and no distinction between modules.	e i as
Note: Operator Card Set protection for private keys generated by the CAPI Providers unavailable in HSM Pool mode.	is
Enable HSM Pool Mode for CAPI Providers.	
	. 1
< <u>B</u> ack <u>N</u> ext > C	ancel

NOTE: Do not select the "Enable HSM Pool Mode for CAPI Providers" checkbox.

4. On Initial setup dialog box, click Next.

nCipher CSP Install Wizard	×
Initial setup Perform initial setup steps required for correct operation of nCipher Windows Support Software.	
You already have a security world set up on this server. You can use this security w or create a new security world. Use the existing security world Select this option to keep all your existing settings and keys, allowing you to interaction and when the security world.	orld
C Create a new security world Select this option to create a totally new security world; all your existing card sets private keys, and certificates created with the nCipher modules will stop working.	s,
Any existing security world is backed up. Unly select this option if you do not hav an existing security world or are sure you need a new security world environment C Install cruptographic acceleration only	/e
Select this option if you have an nFast or do not want to use the nCipher CSPs.	
< <u>B</u> ack <u>N</u> ext >	Cancel

NOTE: The first one (**Use the existing security world**) must be selectable. If not, please check the configuration of module. (eg rfs-sync).

5. On Set Module States dialog box, click Next.

nCiphe	er CSP Install V	Wizard			×
Set	Set Module States Ensure modules are in the correct state before you proceed.				
	The following n	nodules are available in yo	our system:		
	Module ID	Mode	State		
	1 2	operational operational	usable usable		
	, All modules are key-protection	now in the correct state I method and install the CS	to proceed. Click Next to Ps.	choose a	
			< <u>B</u> ack	Next > Cance	

6. On the Key Protection Setup dialog box, select 'Module protection' and click Next.

nCipher CSP Install Wizard	×
Key Protection Setup Set up the private key-protection method and ensure a suitable Operator Card Set exists if necessary.	
Select a method to protect private keys generated by the CSPs.	
 Module protection (requires no extra cards but is less secure) 	
 Operator Card Set protection (unavailable in Pool Mode) 	
Always use the wizard when creating or importing keys	
Create a new Operator Card Set	
Card set name: mscapi	
Number of cards required (K): 2 Total number of cards (N): 3	_
Card set has a time-out Card set time-out: seconds	
🗖 Persistent 🔲 Usable remotely 🔽 Recoverable PP	
< <u>B</u> ack <u>N</u> ext > C	ancel

7. On the Software Installation dialog box, click Next.

nCipher CSP Install Wizard	×
Software Installation Ready to install nCipher support software.	N
You now have a valid security world. The wizard will now install the CSP. Select the option below to set the nCipher CSP as the default SChannel CSP, enabling it for the IIS certificate enrollment wizard. Leaving it unselected sets the Microsoft CSP as the default, but the nCipher CSP is still available to applications.	
Select to set the nCipher CSP as the default SChannel CSP.	
< <u>B</u> ack <u>N</u> ext > Can	cel

8. Click Finish.



9. Confirm the CSP Providers for nCipher.

C:\Users\Administrator>certutil -csplist Provider Name: DigiCert PKI Client CSP Provider Type: 1 - PROV RSA FULL Provider Name: Luna Cryptographic Services for Microsoft Windows Provider Type: 1 - PROV RSA FULL Provider Name: Luna enhanced RSA and AES provider for Microsoft Windows Provider Type: 24 - PROV_RSA_AES Provider Name: Luna SChannel Cryptographic Services for Microsoft Windows Provider Type: 12 - PROV RSA SCHANNEL Provider Name: Microsoft Base Cryptographic Provider v1.0 Provider Type: 1 - PROV RSA FULL Provider Name: Microsoft Base DSS and Diffie-Hellman Cryptographic Provider Provider Type: 13 - PROV DSS DH Provider Name: Microsoft Base DSS Cryptographic Provider Provider Type: 3 - PROV DSS Provider Name: Microsoft Base Smart Card Crypto Provider Provider Type: 1 - PROV_RSA_FULL Provider Name: Microsoft DH SChannel Cryptographic Provider Provider Type: 18 - PROV_DH_SCHANNEL Provider Name: Microsoft Enhanced Cryptographic Provider v1.0 Provider Type: 1 - PROV_RSA_FULL Provider Name: Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider Provider Type: 13 - PROV_DSS_DH Provider Name: Microsoft Enhanced RSA and AES Cryptographic Provider Provider Type: 24 - PROV_RSA_AES Provider Name: Microsoft RSA SChannel Cryptographic Provider Provider Type: 12 - PROV_RSA_SCHANNEL Provider Name: Microsoft Strong Cryptographic Provider Provider Type: 1 - PROV_RSA_FULL Provider Name: nCipher DSS Signature Cryptographic Provider Provider Type: 3 - PROV DSS Provider Name: nCipher Enhanced Cryptographic Provider Provider Type: 1 - PROV_RSA_FULL Provider Name: nCipher Enhanced DSS and Diffie-Hellman Cryptographic Provider Provider Type: 13 - PROV DSS DH Provider Name: nCipher Enhanced DSS and Diffie-Hellman SChannel Cryptographic Provider Provider Type: 18 - PROV_DH_SCHANNEL

Provider Name: nCipher Enhanced RSA and AES Cryptographic Provider Provider Type: 24 - PROV RSA AES Provider Name: nCipher Enhanced SChannel Cryptographic Provider Provider Type: 12 - PROV RSA SCHANNEL Provider Name: nCipher Signature Cryptographic Provider Provider Type: 2 - PROV_RSA_SIG Provider Name: Microsoft Software Key Storage Provider Provider Name: nCipher Security World Key Storage Provider Provider Name: DigiCert PKI Client KSP Provider Name: Microsoft Passport Key Storage Provider Provider Name: Microsoft Platform Crypto Provider Microsoft Platform Crypto Provider: The device that is required by this cryptographic provider is not ready for use. Provider Name: Microsoft Smart Card Key Storage Provider Provider Name: SafeNet Key Storage Provider C:\Users\Administrator>

NOTE: You can find the following providers:

nCipher DSS Signature Cryptographic Provider nCipher Enhanced Cryptographic Provider nCipher Enhanced DSS and Diffie-Hellman Cryptographic Provider nCipher Enhanced DSS and Diffie-Hellman SChannel Cryptographic Provider nCipher Enhanced RSA and AES Cryptographic Provider nCipher Enhanced SChannel Cryptographic Provider

Configure CNG/KSP (Module protection)

NOTE: Please note that for the deployment of the Enterprise Gateway Server, you need to Configure CNG/KSP.

1. Go to Start-> nCipher and run CNG Configuration wizard.



2. Click Next.

nShield CNG Providers Config	uration Wizard	\times
	Welcome to the nShield support software configuration wizard	
	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.	
	< Back Next > Cancel	

3. On Enable HSM Pool Mode, click Next.

nShield CNG Providers Configuration Wizard	×
Enable HSM Pool Mode Set options for Pool Mode CNG provider.	N
Would you like to enable HSM Pool Mode for CNG? HSM Pool Mode means that the nShield CNG providers will see a single logical view with all the available HSMs seen a one resource and no distinction between modules.	35
Note: Operator Card Set and Softcard protection for private keys generated by the CN Providers is unavailable in HSM Pool mode.	G
Enable HSM Pool Mode for CNG Providers.	
< <u>B</u> ack <u>N</u> ext > Car	ncel

NOTE: Do not check the "Enable HSM Pool Mode for CNG Providers" checkbox.

4. On Initial setup dialog box, click Next.

nShield CNG Providers Configuration Wizard	×
Initial setup Perform initial setup steps required by nShield Windows Support Software.	
You already have a security world set up on this server. You can use this security wo or create a new security world.	rld
Use the existing security world	
Select this option to keep all your existing settings and keys, allowing you to integrate new nShield modules into an existing security world.	
Create a new security world	
Select this option to create a totally new security world; all your existing card sets, private keys, and certificates created with the nShield modules will stop working. A existing security world is backed up. Only select this option if you do not have an existing security world or are sure you need a new security world environment.	λny
< <u>B</u> ack <u>N</u> ext > Ca	ancel

NOTE: The first one (**Use the existing security world**) must be selectable. If not, please check the configuration of the module. (e.g. rfs-sync).

5. On Module States dialog box, click Next.

	odules are available	e in your system:		
Module ID	Mode	State		
1	operational	usable		
2	operational	usable		
All modules are i world to uninitial	now in the correct : ized nShield modul	state to proceed. Click 1 es.	Next to restore you	r security

6. On the Key Protection Setup dialog box, select 'Module protection' and click Next.

nShield CNG Providers Configuration Wizard	×
Key Protection Setup Set up the private key-protection method.	
Select the default method that will be used to protect private keys generated by the CNG Key Storage Provider.	
If softcard or OCS protection is selected, the choice will be offered on the next page whether to use an existing token or create a new one.	
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.	
< <u>B</u> ack <u>N</u> ext > C	ancel

7. On Software Installation dialog box, click Next.

nShield CNG Providers Configuration Wizard	×
Software Installation Ready to install nShield support software.	
You now have a valid security world and key protection mechanism. The Wizar now register the nShield CNG Providers. The nShield providers will not be defau providers, and you must select them explicitly by name through your application. press Next to continue.	d will Ilt Please
< <u>B</u> ack <u>N</u> ext >	Cancel

8. Click Finish.



9. Confirm the providers for nCipher.

C:\Users\Administrator>cnglist --list-providers DigiCert PKI Client KSP 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 SafeNet Key Storage Provider Windows Client Key Protection Provider nCipher Primitive Provider nCipher Security World Key Storage Provider

C:\Users\Administrator>

NOTE: You can find the following providers:

nCipher Primitive Provider nCipher Security World Key Storage Provide

Generate CSR (Module protection)

- 1. Create the information file for CSR.
 - a) To generate CSR through certreq.exe through CSP, the ProviderName must be "nCipher Enhanced Cryptographic Provider". The sample of inf file is as follows.

```
[Version]
Signature = "$Windows NT$"
[NewRequest]
RequestType = PKCS10
ProviderName = "nCipher Enhanced Cryptographic Provider"
Subject = "CN=Registration Authority"
KeyContainer = "CSPRA20200525"
MachineKeySet = TRUE
KeyAlgorithm = RSA
KeyLength = 2048
KeyUsage = 0xf0
```

NOTE: At present, Only SHA1 HashAlgorithm is supported by "**nCipher Enhanced Cryptographic Provider**". However, RA certificate issued by DigiCert is signed with sha256RSA algorithm.

b) To generate CSR through certreq.exe through KSP, the ProviderName must be "nCipher Security World Key Storage Provider". The sample of inf file is as follows.

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "nCipher Security World Key Storage Provider"
ProviderType = 0
Subject = "CN=Registration Authority"
KeyContainer = "KSPRA20200525"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

2. Generate CSR through HSM

NOTE: <inf-file> is the file created at Step 1, <csr-file> is an output file.

a) Open command prompt and run the following command:

```
> certreq -new <inf-file> <csr-file>
```

b) The CSR file will be generated as follows.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
....
C610uaqncn6FvLu5pygZYFEVtOanCXNQRRUWiDGWKjHF+10GMh+V5YUur55T4W80
0uwK
```

```
-----END NEW CERTIFICATE REQUEST-----
```

Get RA Certificate in PKI-Manager

The generated CSR(PKCS#10) can be copied and pasted onto the "**Get an RA certificate**" page on PKI Manager (by an authorized PKI Administrator) and save the resulting RA (PKCS#7) certificate onto a local folder.

1. Go to PKI Manager and sign in by using your certificate.

DigiCert PKI Platform	digicerť	Logged in as:	
Account activity	Alerts	Account status	
Last updated: Jul 19, 2019 12:58 AM	The DigiCert PKI Platform 8.19 release includes:	Status: OK	
	Rebranding from Symantec to DigiCert	Next service rener	wal: May 2, 2020
Recent activity	Email domain validation for S/MIME certificates via DCV (Domain Control Validation) process Support for Microsoft Intune to issue Client Authentication certificates via SCEP enrollment flow		
Action Date	 Enterprise Gateway and Autoenrolment Server support for SafeNet Luna Network HSM 7 (FIPS and non-FIPS Mode, Cloning and Export Mode) and pShield Connect HSM 		
Certificate profile created Jul 18, 2019	Windows Server 2016 support for Enterprise Gateway, Autoenrollment Server and Local Key Management Service (LKMS)		
Certificate profile deleted Jul 18, 2019	PKI Client support for the provisioning of Client Authentication certificates to Android devices Removal of Adobe Individual, Adobe Organization and Adobe CDS certificate templates		
Certificate options custo Jul 18, 2019	Bug fixes		
Certificate profile created Jul 18, 2019			
Certificate for user revo Jul 18, 2019	Certificate history Seat activity		
Certificate for user revo Jul 18, 2019	All certificate profiles v		
Certificate profile deleted Jul 18, 2019	2.5		
	2		
		Seat usage	
		Refresh	
	v 1.5	Seat pool U	Ised Purchased
	Lice at a second s	2	
	e ti	User	46 1000
		• III	
		Device	
	0.5	8	
		Server	8 10
		` #	
	0 12 jul 13 jul 14 jul 15 jul 16 jul 17 jul 18 jul	Organization	
	- Certificates issued - Certificates revoked	Buy more seats	
	1 week 1 month 3 months 6 months 1 year All		
M			

2. Click Menu and select "Get an RA Certificate".

DigiCert PKI Platform	digicert	X III	Logged in as
Account activity	Alerts		Account status
Last updated: Jul 19, 2019 12:58 AM	The DigiCert PKI Platform 8.19 release includes:		Status: OK
Refresh	Rebranding from Symantec to DigiCert		
All	 Email domain validation for S/MIME certificates via DCV (Domain Control Validation) 	process	Next service renewal: May 2, 2020
Recent activity	 Support for Microsoft intune to issue client Authentication certificates via SCEP en Enterprise Gateway and Autoenrollment Server support for SafeNet Luna Networ 	k HSM 7 (FIPS and non-FIPS Mode, Cloning and Export Mode) and	
Cartificate profile greated	nShield Connect HSM Windows Server 2016 support for Enterprise Gateway, Autoenrolment Server an	d I ocal Kay Management Service (I KMS)	
Castificate and to delated	 PKI Client support for the provisioning of Client Authentication certificates to Andro 	id devices	
Certificate profile deleted Jul 18, 2019	 Removal of Adobe Individual, Adobe Organization and Adobe CDS certificate temp Bug fixes 	iates	
Certificate options ousto Jul 18, 2019			
Certificate profile created Jul 18, 2019	Contribution Minimum		
Certificate for user revo Jul 18, 2019	Certificate instory Seat activity	All cartificatio profiles	
Certificate for user revo Jul 18, 2019	All certificate profiles	All certificate promes	
Certificate profile deleted Jul 18, 2019	2.5		
	2	line of the former of the form	
		Manage users	Seat usage
		Manage certificates	Refresh
	1.5	Manage certificate profiles	Seat pool Used Purchased
	cate	Manage Domains	÷
	Centif	Manage self service portal	User 48 1000
	- 1	Reporting	* #
		View recent reports	Device
	0.5	View audit trais	
		Your account	Server 8 10
		Manage account and sub- accounts	·
	0	Manage administrators	Companization
	Certificates issued — Certificates revoked	Manage CAs 18 Jul	Buy more seats
		Manage PKI Enterprise Gateways	
	1 week 1 month 3 months 6 months 1 year All	Get an roy certificate	
n 💿	S 🚚 🐸 🗽	MM 😵 ^	

3. Paste your CSR and enter a certificate friendly name and then click "Continue".

Get an RA certificate		
If you are setting up PKI Enterprise Gateway or PKI Web Servic communications between your client and the Web Service.	ces, you must install an RA certificate to s	ecure
If you are not setting up these services, or have already gotten process.	your RA certificate, you do not need to co	mplete this
Enter Certificate Signing Request (CSR)		
according to the instructions in the installation guide for your sa	ennicate, your administrator must genera ervice,	te the CSR
You can access the resources page by clicking on the 🛞 ico	on on the dashboard.	
Paste your CSR:		
Important Service Requirements. If you discover or have reason to be you must immediately revoke the certificate or notify the issuing certie or your organization name has changed, please notify the issuing cert your certificate at any time without notice (if) you fail to perform your (ii) in the issuing center's sole discretion, you have engaged in activitie systems.	leve that there has been a compromise of you to do so. Similarly, if the information within yo ter. Note that the issuing center retains the right obligations under the terms of your service a so which the issuing center determines are har	r private key, ur certificate at to revoke greement; or rmful to its
Important Service Requirements: If you discover or have reason to be you must immediately revoke the certificate or notify the issuing cente or your organization name has changed, please notify the issuing cent gour certificate and ym tew without notice if (i) you fails perform your (ii) in the issuing center's sole discretion, you have engaged in activite systems. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate renewal info he menu and select Manage account and sub-account(s). Se	ieve that there has been a compromise of you to do so. Similarly, if the information within yo ter. Note that the issuing center retains the right obligations under the terms of your service a so which the issuing center determines are har instruction. If you would like to change this o lect Edit renewal email notification to upd	r private key, ur certificate to revoke greement; or rmful to its ontact, go to late.
Important Service Requirements. If you discover or have reason to be you must immediately revoke the certificate or notify the issuing certer or your organization name has changed, plases notify the issuing come (i) in the issuing center's sole discretion, you have engaged in activitie systems. Inter a certificate friendly name: Renewal email notification The following email: contact will receive certificate renewal info he menu and select Manage account and sub-account(s). Se Email address: Ashish_RanjanPartner@yopmail.com	ieve that there has been a compromise of you to do so. Similarly, if the information within yo ter. Note that the issuing center retains the right obligations under the terms of your service a ter which the issuing center determines are had swhich the issuing center determines are had rmation. If you would like to change this c lect Edit renewal email notification to upd	r private key, ur certificate it to revoke greement, or rmful to its ontact, go to late.
Important Service Requirements. If you discover or have reason to be you must immediately revoke the certificate or notify the issuing cent or your organization name has changed, please notify the issuing cent your certificate at any time without notice if (i) you fail to perform your (i) in the issuing center's sole discretion, you have engaged in activitie systeme. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate renewal info the menu and select Manage account and sub-account(s). Se Email address: Ashish_RanjanPartner@yopmail.com * Required information	ieve that there has been a compromise of you to do so. Similarly, if the information within yo ter. Note that the issuing center retains the right obligations under the terms of your service a swhich the issuing center determines are har here the issuing center determines are har provided to the issuing center determines are har remation. If you would like to change this c lect Edit renewal email notification to upd	r private key, ur certificate it to revoke greement, or rmful to its ontlact, go to ate.
Important Service Requirements. If you discover or have reason to be you must immediately revoke the certificate or notify the issuing center or your organization name has changed plases notify the issuing center (i) in the issuing center's sole discretion, you have emgaged in activitie systems. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate renewal info the menu and select Manage account and sub-account(s). Se Email address: Ashish_RanjanPartner@yopmail.com * Required information	leve that there has been a compromise of you to do so. Similarly, if the information within yo ter. Note that the issuing center retains the right obligation under the terms of your service a res which the issuing center determines are had remation. If you would like to change this co lect Edit renewal email notification to upd	r private key, ur certificate it to revoke greement, or rmful to its ontact, go to ate.

The CSR looks as follows; Please paste it.

```
-----BEGIN NEW CERTIFICATE REQUEST----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
...
zbnTmg1IIY4NSgFcRsbs5j5GQDN86gSKmQ8/EvOjbpC62X3ZDhVmYSMBJU01Jgv6
1tyz
-----END NEW CERTIFICATE REQUEST----
```

4. Click "Download" then the PKCS#7 file will be downloaded.

Your RA cert Your RA certifica Services is inst	ficate is ready e must be installed on the server where your PKI Enterprise Gateway or PKI Web Iled.	
Install your F	A certificate	
1. Download yo	r RA certificate.	
Issued to:		
Jul 18, 2020	e.	
Download		
2. Forward the F in the installatio	A certificate to your server administrator. Your administrator must follow the instructions guide for your service.You can download the appropriate installation guide from the	3
resources page	by clicking on the 💿 icon on the dashboard.	
		Done

5. Click "Done" to go back to the PKI Dashboard.

Install RA certificate

a) Before Installing the RA certificate, the trusted root certificate must be installed. if not, the following error will be displayed.

Certificate Request Processor: A certificate chain could not be built to a trusted root authority. 0x800b010a (-2146762486 CERT_E_CHAINING)

b) Open command prompt (on the folder where the PKCS#7 file exists) and run the following command.

```
> certreq -accept <issued-cert>
```

Note: Repeat the above commands to download and install RA certificate for both CSR's.

c) RFS Commit.

Run the below command to commit local key-management data changes to the remote file system.

```
C:\Users\Administrator> rfs-sync --commit
Starting synchronisation, task ID 5ca48468.764b879a080c7eca
```

Sharing the existing certificate between 2 machines on nCipher HSM (Optional)

Follow the below steps to share the RA certificate between 2 EG/AE machines.

1. On Machine A, commit all the updates into hardserver.

```
> rfs-sync -U
> rfs-sync -c
```

2. On Machine B, synchronize all the updates.

```
> rfs-sync -U
```

Note: It is assumed that the RA certificate key material is generated on machine A only.

- 3. Copy the issued RA Certificate (PKCS#7) from Machine A to Machine B.
- 4. On Machine B, import RA Certificate for AE through mmc (Local Computer).

After a successful import, note down the serial number of the certificate imported for the next step.

Note: You can also use certificate thumbprint in place of serial number to run the command in next step.

5. On Machine B, repair the RA Certificate through certutil.

Usage: certutil -f -repairstore -csp <CSP Provider> my <Serial Number of the RA Certificate>

After that, you can find the RA Certificate has private key through mmc.exe.

C:\Users\Administrator>certutil -f -repairstore -csp "nCipher Enhanced Cryptographic Provider" my "4973ee1fd23091cdc34be471ed97aa96"

my "Personal"

========= Certificate 23 ===========

Serial Number: 4973ee1fd23091cdc34be471ed97aa96

```
Issuer: CN=Symantec Private Class 3 Registration Authority TEST CA, OU=FOR
TEST PURPOSES ONLY, O=Symantec Corporation, C=US
NotBefore: 7/21/2020 5:00 PM
NotAfter: 7/22/2021 4:59 PM
Subject: O=LTE STD Full, OU=MULTI-ALLOWED, OU=RA, CN=Registration Authority
1595422928419
Non-root Certificate
Cert Hash(sha1): 999f781c659efca61f9f9814d8fbaaebd7f2d5b3
cbData: 15 ==> 40
 Key Container = CSPRA20200722
 Provider = nCipher Enhanced Cryptographic Provider
Private key is NOT exportable
nCipher Enhanced Cryptographic Provider: KeySpec=2
AES256+RSAES_OAEP(RSA:AT_SIGNATURE) test skipped
Signature test passed
Encryption test FAILED (CNG)
----- End force NCrypt ------
CertUtil: -repairstore command completed successfully.
C:\Users\Administrator>
```

Note: Make sure Signature test passed, -repairstore command completed successfully.

6. On machine B, import RA Certificate for EG through mmc (Local Computer)

After a successful import, note down the serial number of the certificate for the next step.

Note: You can also use certificate thumbprint in place of serial number to run the command in next step.

7. On Machine B, repair the RA Certificate through certutil.

Usage: certutil -f -repairstore -csp <CNG Provider> my <Serial Number of the RA Certificate>

After that, you can find the RA Certificate has private key through mmc.exe.

C:\Users\Administrator>certutil -f -repairstore -csp "nCipher Security World Key Storage Provider" my "653ff667735c50dbf7b68bf694908af6"

my "Personal"

=========== Certificate 13 ===============

Serial Number: 653ff667735c50dbf7b68bf694908af6

Issuer: CN=Symantec Private Class 3 Registration Authority TEST CA, OU=FOR TEST PURPOSES ONLY, O=Symantec Corporation, C=US

NotBefore: 7/21/2020 5:00 PM

NotAfter: 7/22/2021 4:59 PM

Subject: O=LTE STD Full, OU=MULTI-ALLOWED, OU=RA, CN=Registration Authority 1595422979423

Non-root Certificate

Cert Hash(sha1): c291f6f2bec306773cce3b896f3e0d62cfece170

Key Container = KSPRA20200722

Provider = nCipher Security World Key Storage Provider

Private key is NOT exportable

nCipher Security World Key Storage Provider: KeySpec=0

AES256+RSAES_OAEP(RSA:CNG) test FAILED: Cannot find the certificate and private key to use for decryption. 0x8009200c (-2146885620 CRYPT_E_NO_DECRYPT_CERT)

Encryption test passed

Signature test passed

CertUtil: -repairstore command completed successfully.

C:\Users\Administrator>

Note: Make sure Encryption and Signature test passed, -repairstore command completed successfully.