DigiCert® PKI Platform

HSM Installation and Configuration for nShield

August 20, 2020

digicert®

Legal Notice

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

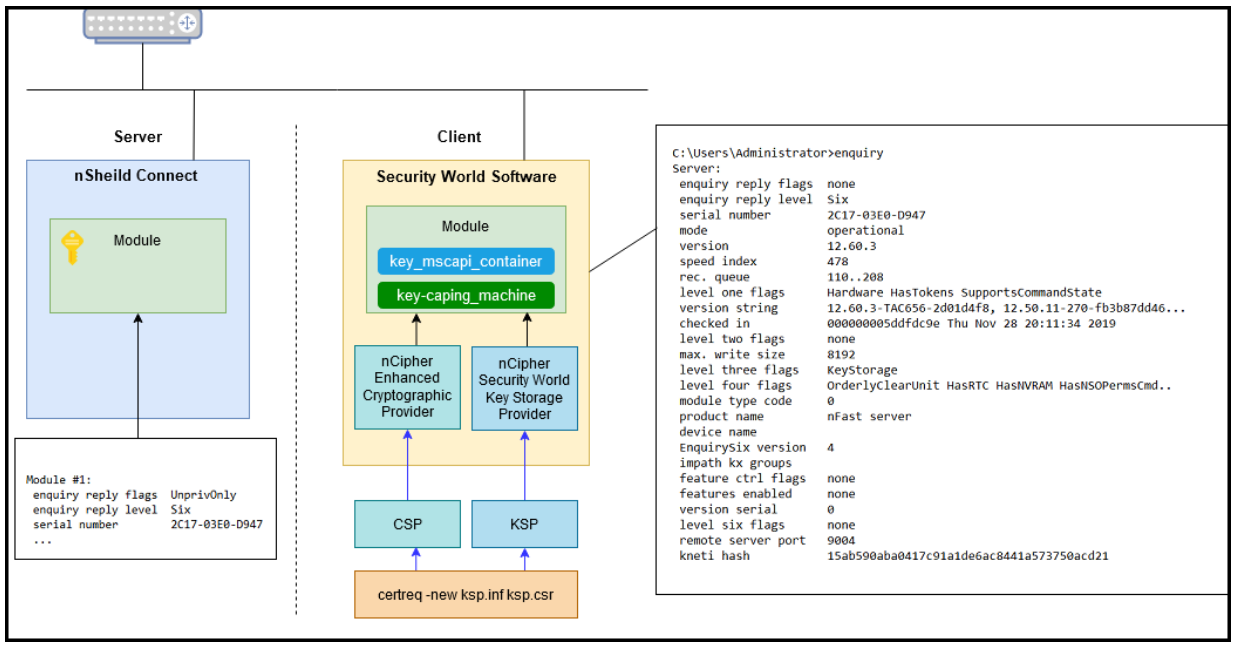
No.	Date	Summary
1.	2020/07/02	Create a new entry
2.	2020/07/28	Incorporated feedback from PSO and added HA configuration section
3	2020/08/20	Incorporated feedback from PSO

Supported HSMs

HSM Type	Client Version	Software Version	Firmware Version
nShield Connect XC Base HSM • Strict FIPS 140-2 Level 3 **disabled** • Module protection for CSP and CNG	12.60.3 (hotfix-111745-TAC-656)	12.60.3 (hotfix-111745-TAC-656)	12.50.11 v3 security world

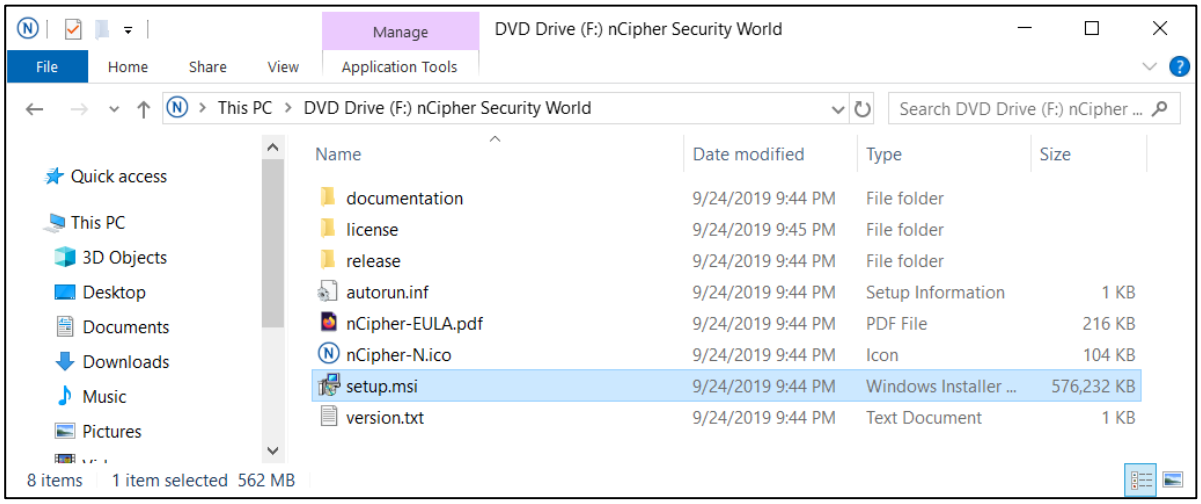
nShield Connect HSM

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.

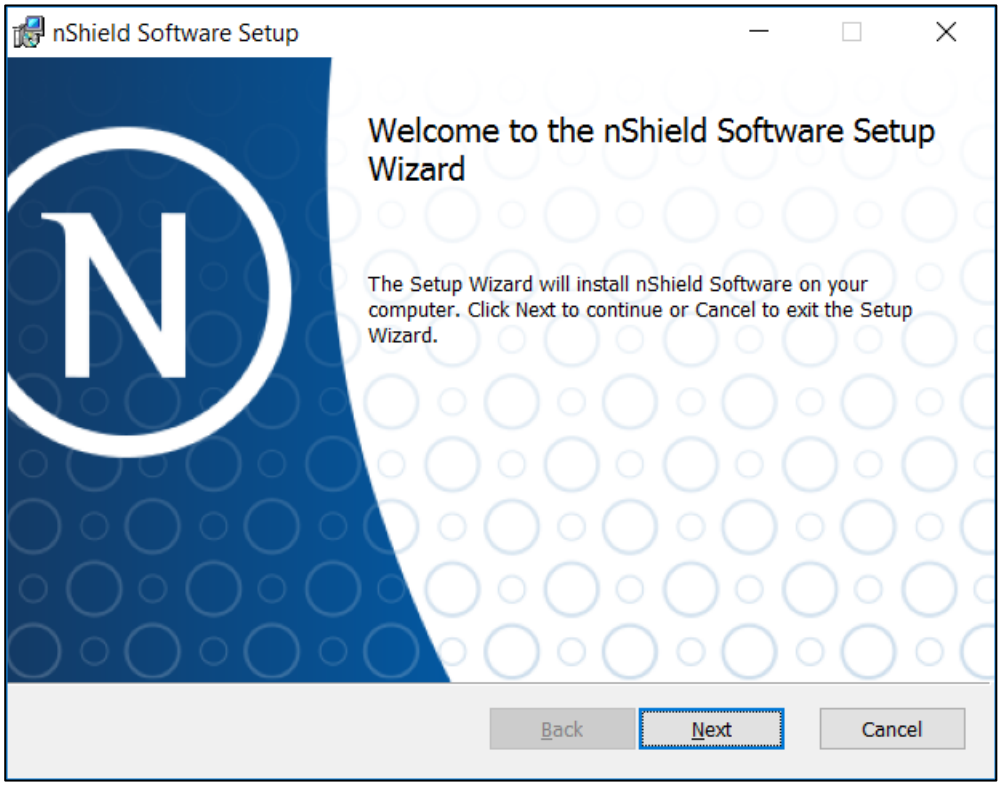


NOTE: If you try to upgrade the client software, the old version must be uninstalled. After uninstallation, the system requires to reboot the computer.

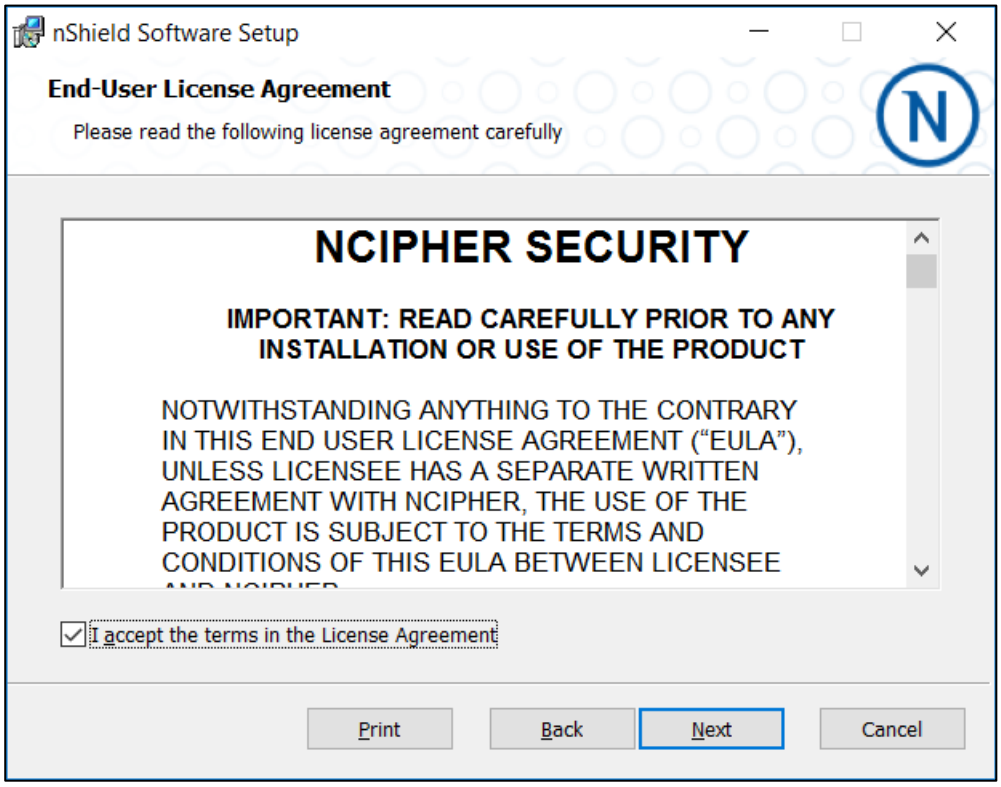
Even if you uninstall the old version, you do not have to configure the client software again because the HSM has already configured the client.

---

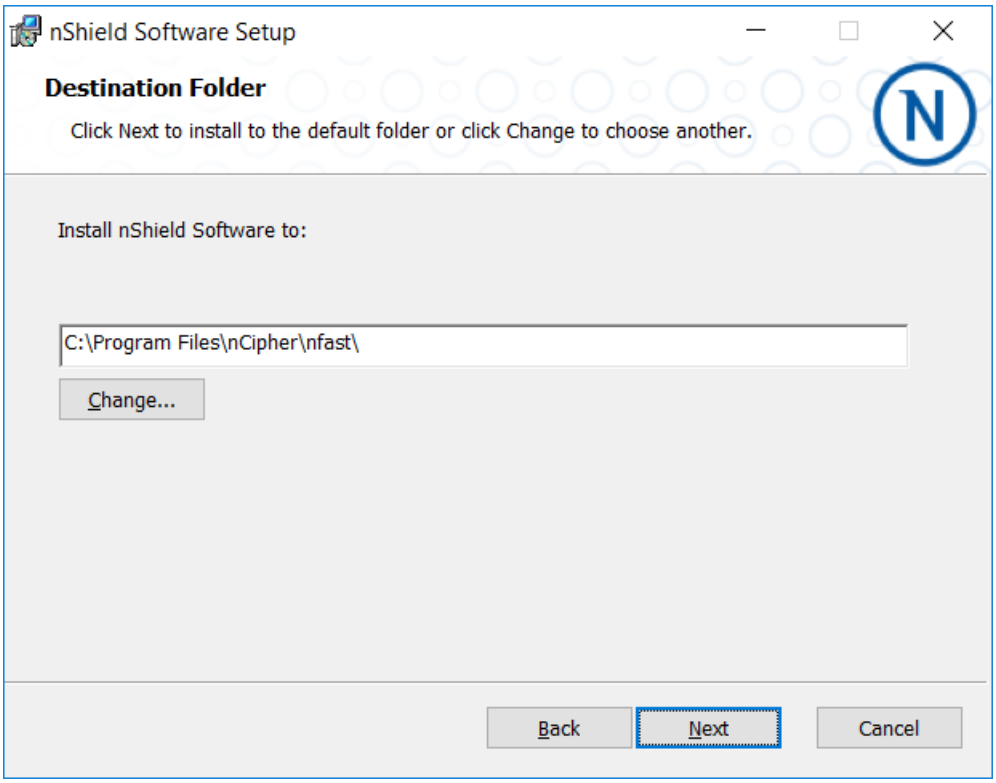
2. Run "setup.msi" as administrator and click Next.



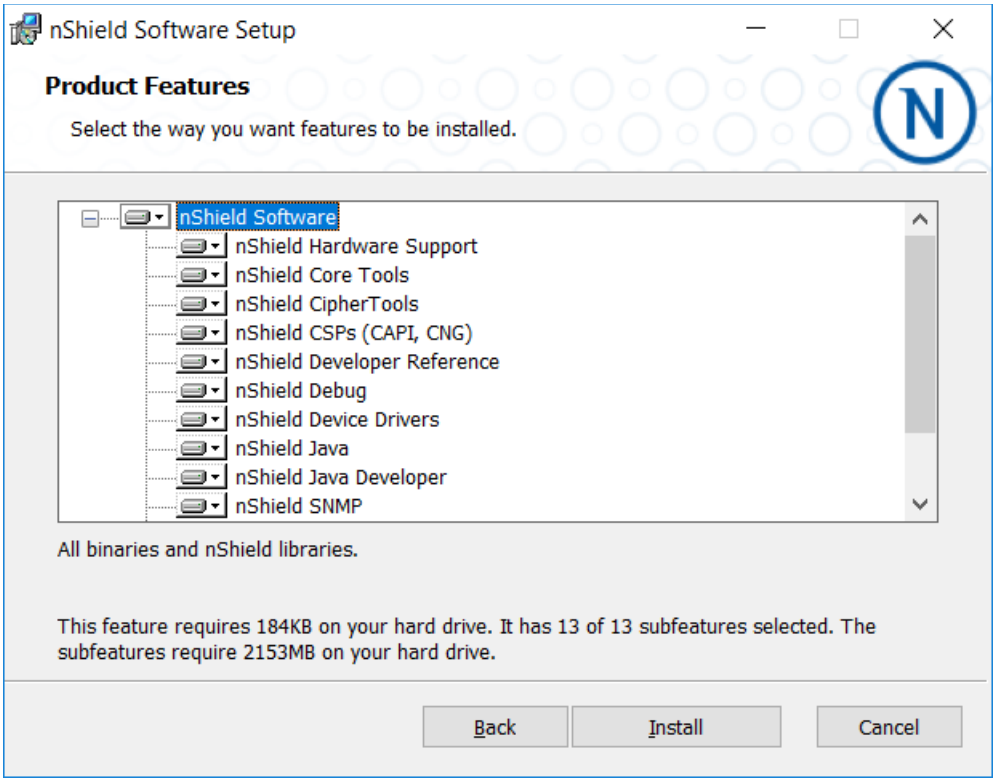
3. Accept the Software License Agreement and click Next.



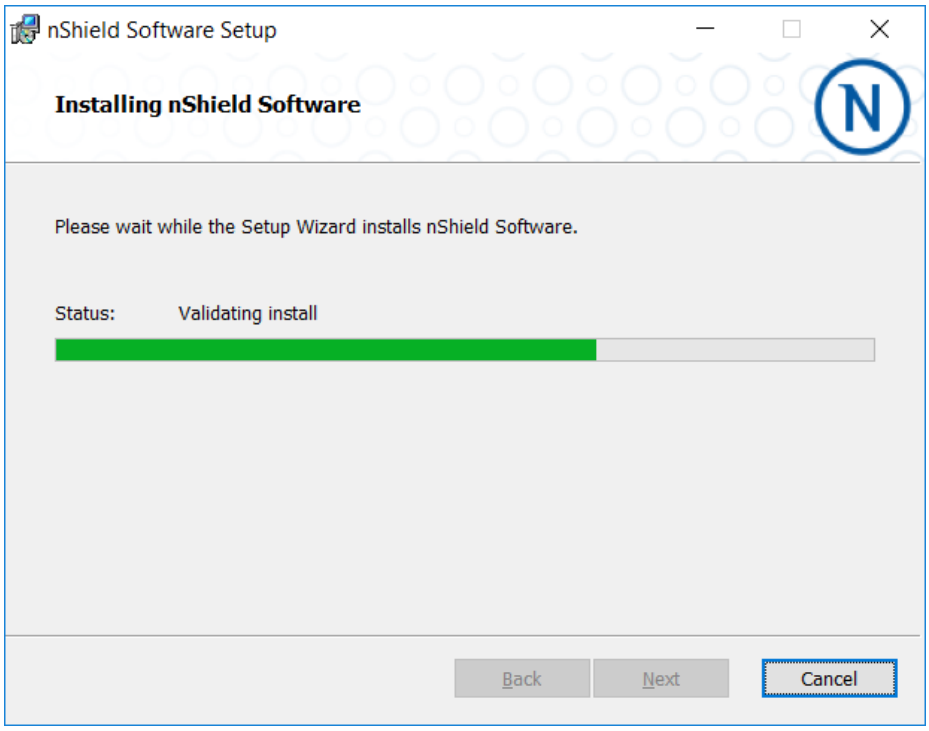
4. Click Next to Install the nShield to default folder or click Change to choose another



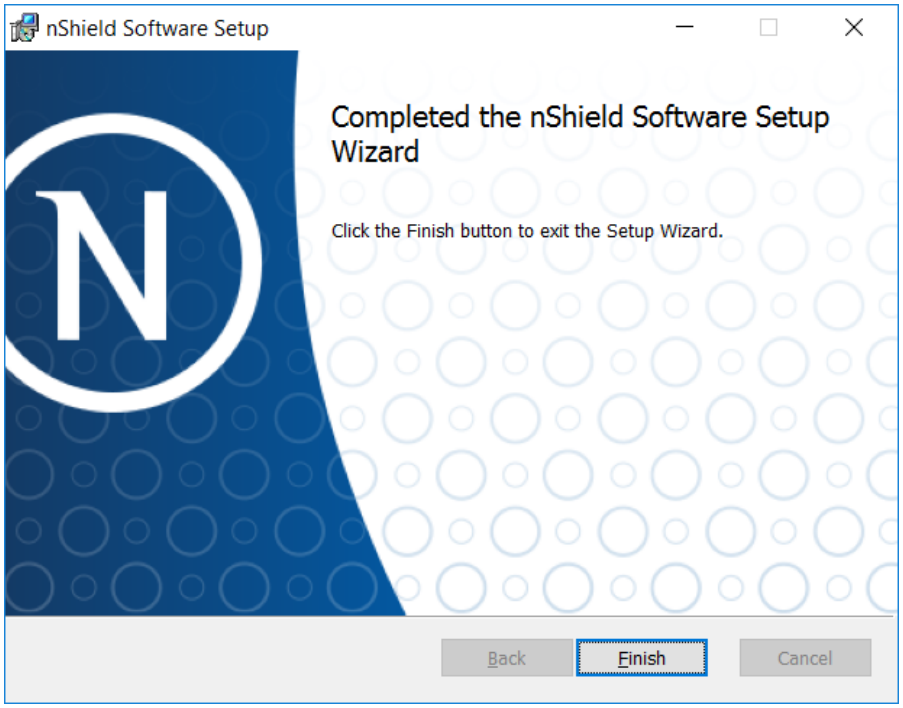
5. Select the product features and click **Install**.



6. Wait for the completion.



7. Installation process is now complete. Click **Finish**.

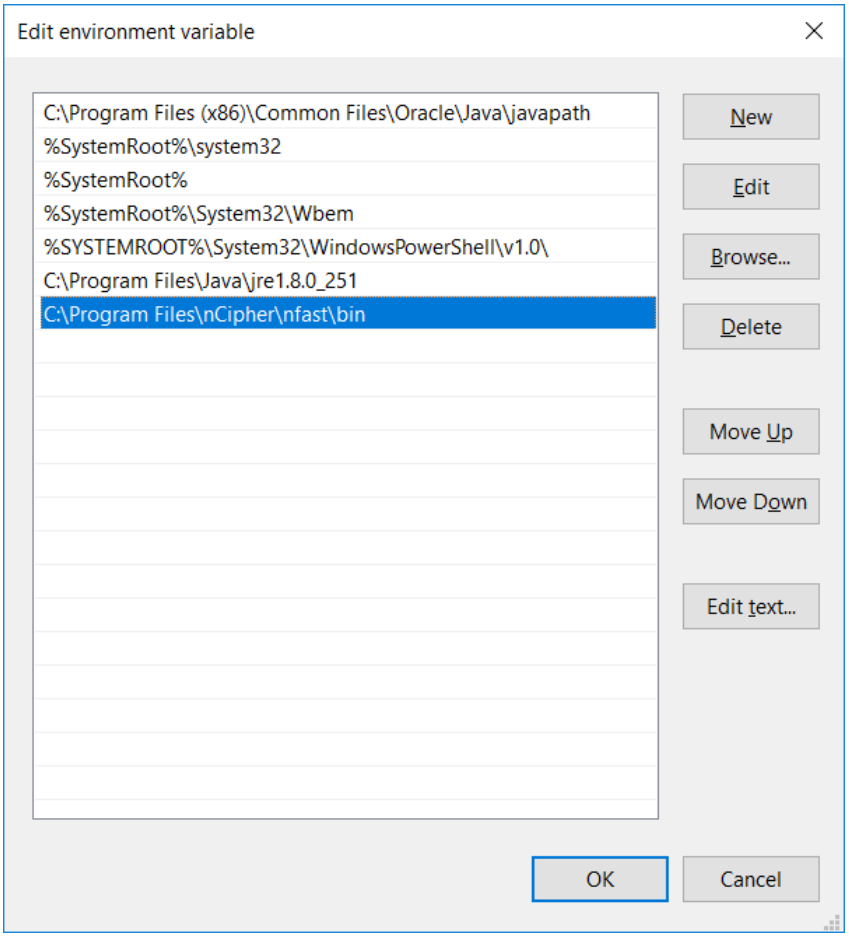


NOTE: After uninstallation, several files of the old software remains at the Program folders under "**Programs and Features**". You need to manually remove the files for the installation to proceed.

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).



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
   serial number ####-####-####
   mode operational
   version #-#-#
   speed index ######
   rec. queue ####..####
   ---
   version serial #
   remote server port ####
   Module ##:
   enquiry reply flags none
   enquiry reply level Six
   serial number ####-####-####
   mode operational
   version #-#-#
   speed index #####
   rec. queue ##..###
   ---
   rec. LongJobs queue ##
   SEE machine type PowerPCELF
   supported KML types DSAp1024s160 DSAp3072s256
   hardware status 0
   ```

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.
```

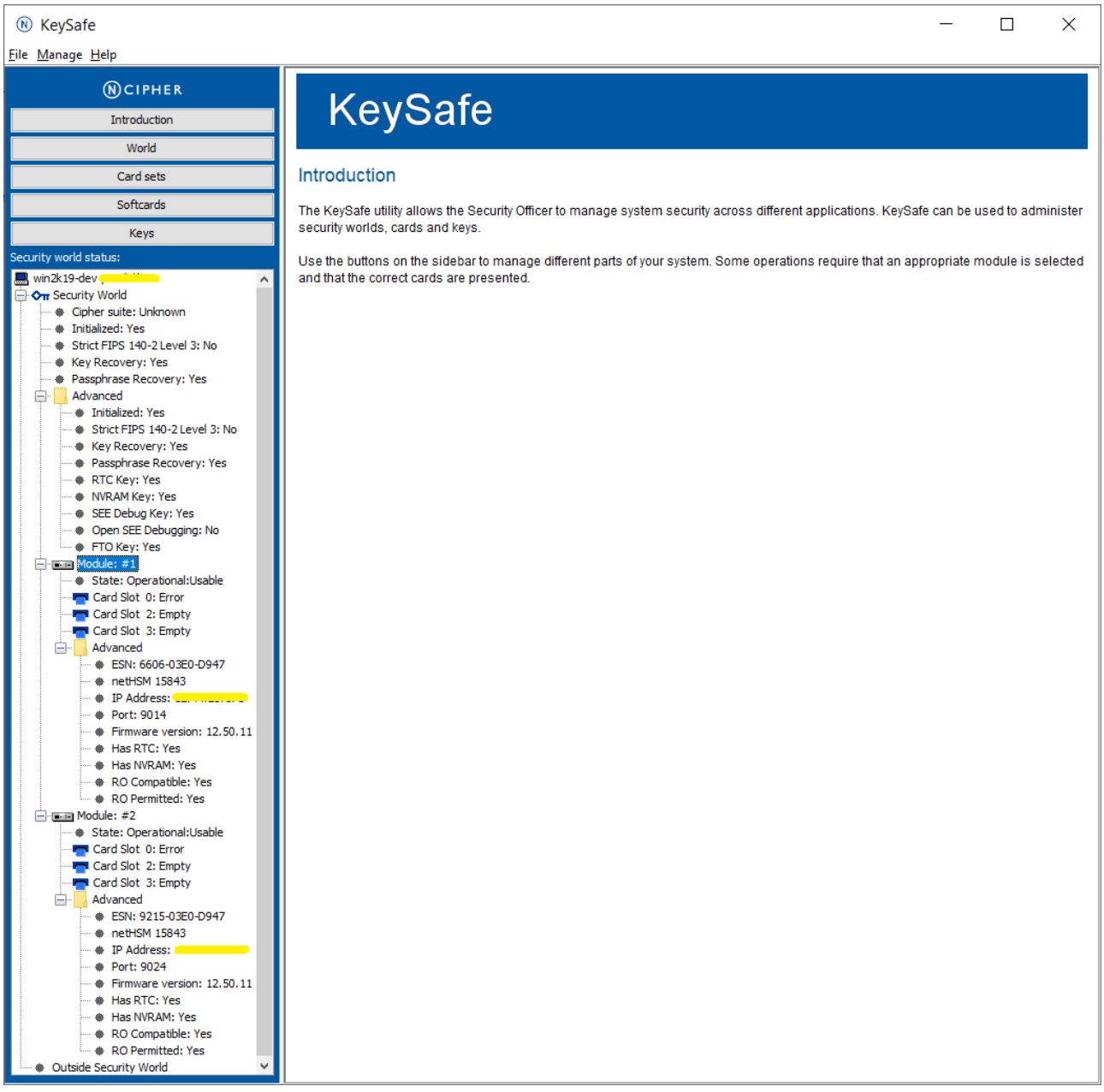
NOTE: The port of RFS synchronization is 9004.

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>
   ```

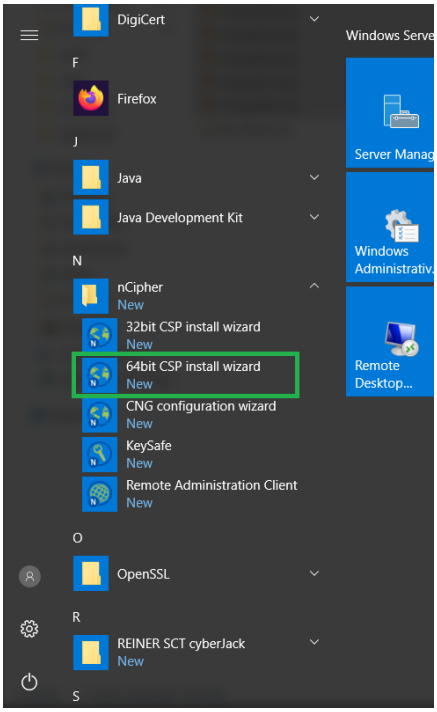
   The example of outputs is as follows.

   ```
   > 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)

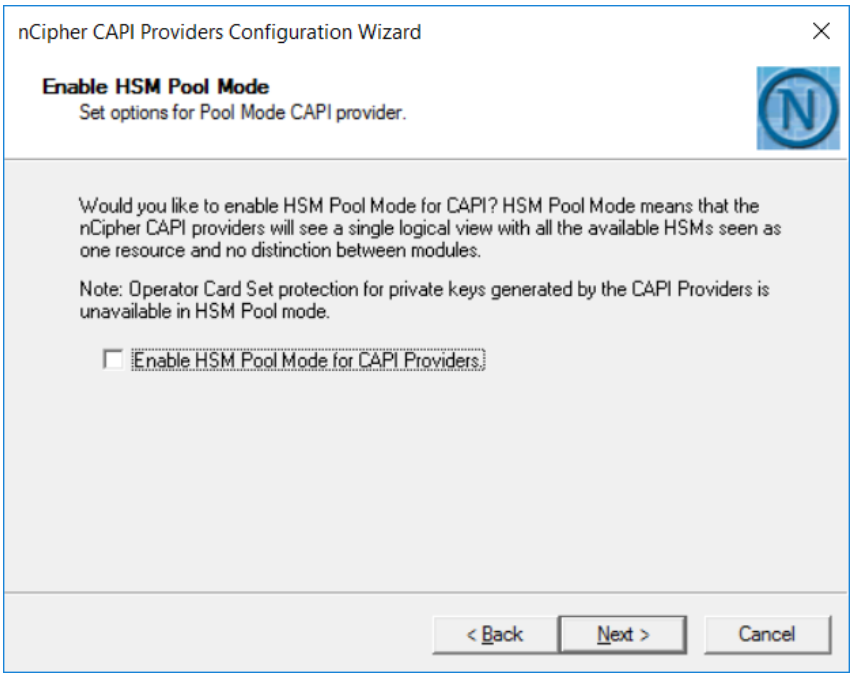
NOTE: Please note that for the deployment of the Autoenrollment Server, you need to Configure CSP.

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



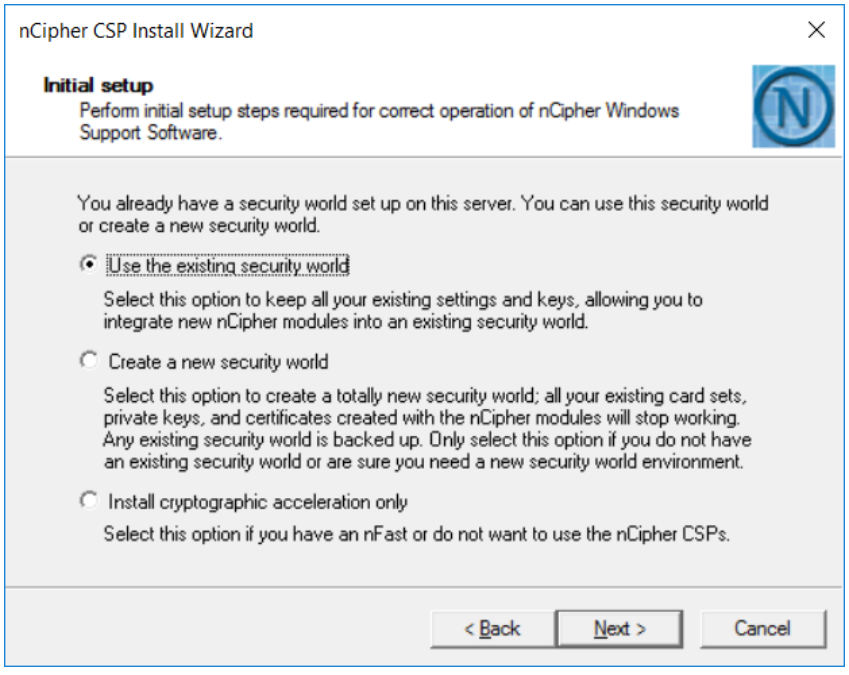
2. Click **Next**.

3. On Enable HSM Pool Mode, click **Next**.



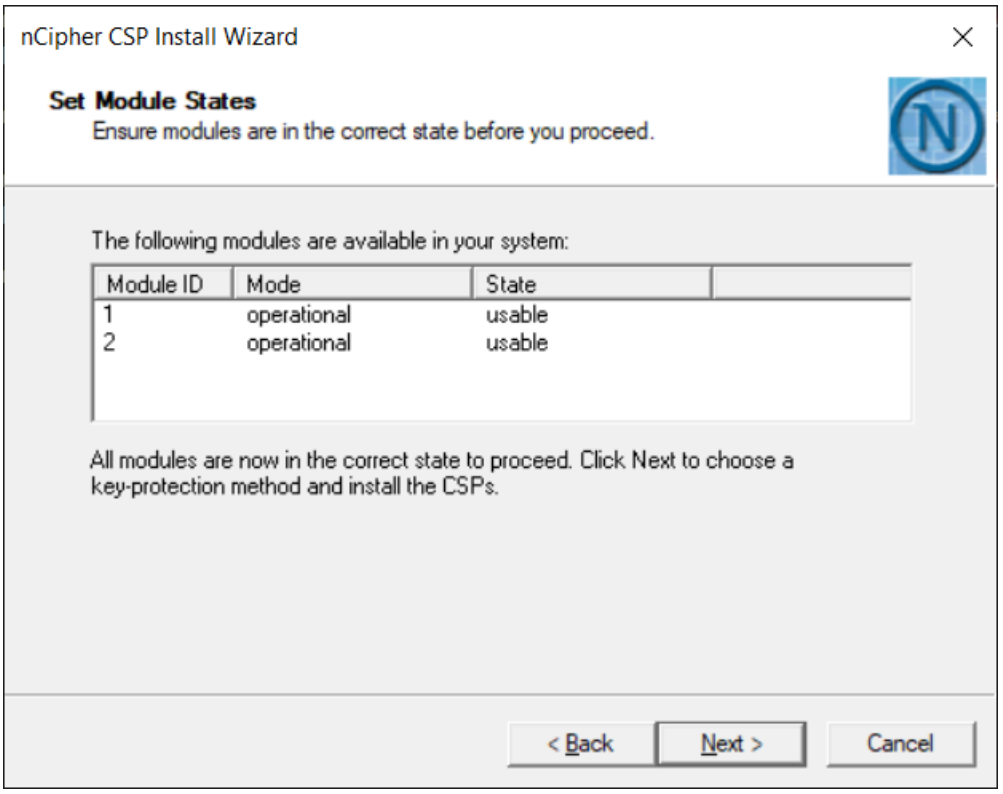
NOTE: Do not select the "Enable HSM Pool Mode for CAPI Providers" checkbox.

4. On Initial setup dialog box, click **Next**.

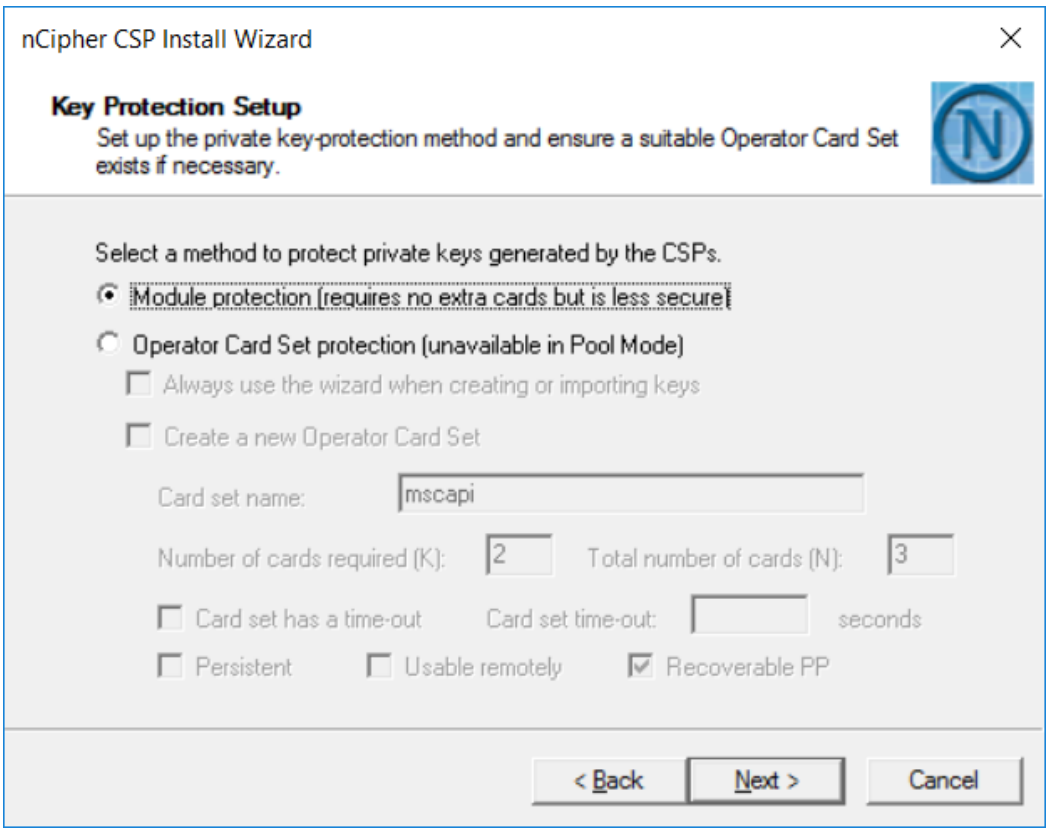


NOTE: The first one (**Use the existing security world**) must be selectable. If not, please check the configuration of module. (eg rfs-sync).

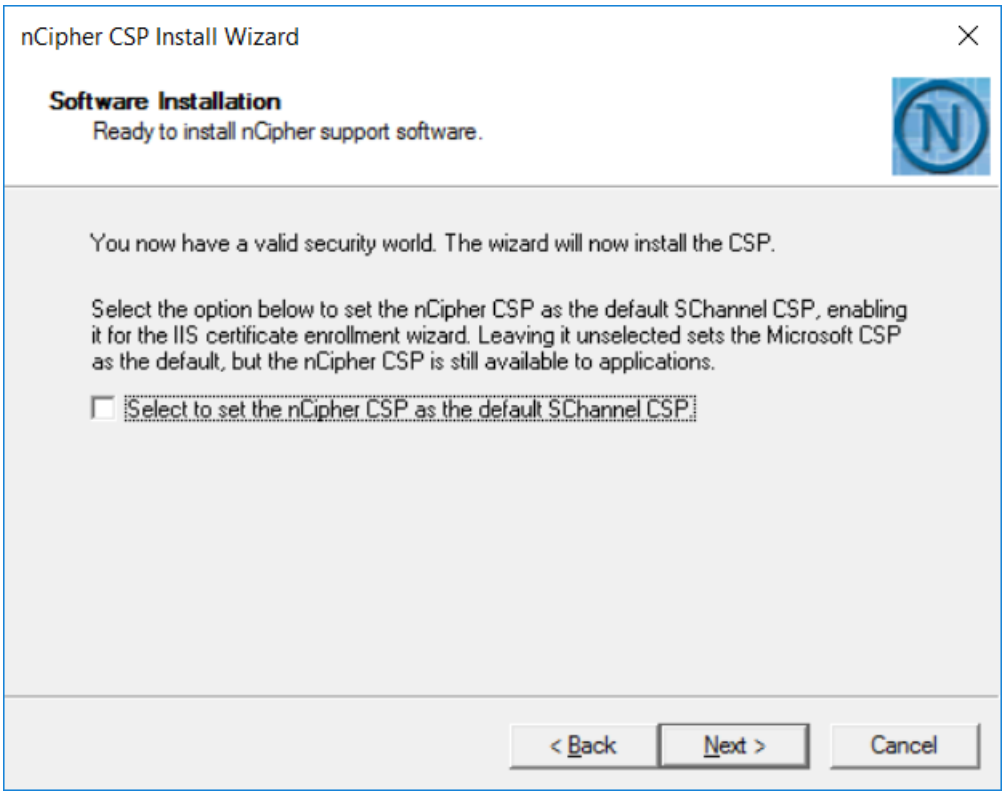
5. On Set Module States dialog box, click **Next**.



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



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



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>
```

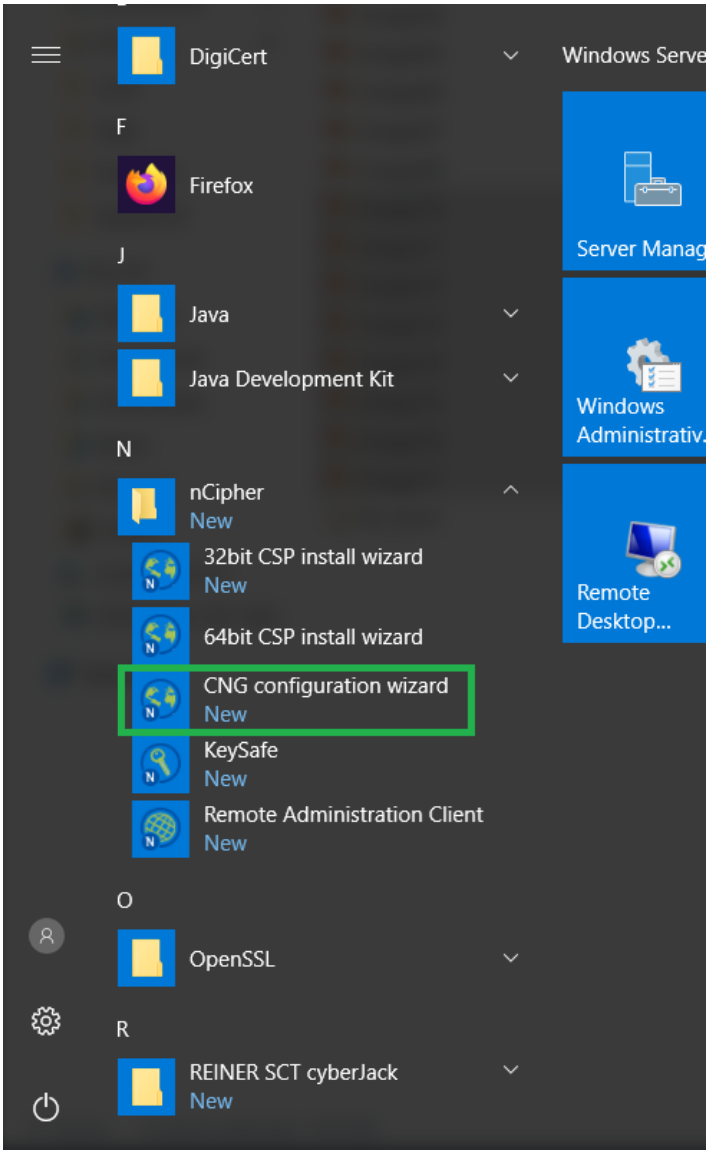
NOTE: You can find the following providers:

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

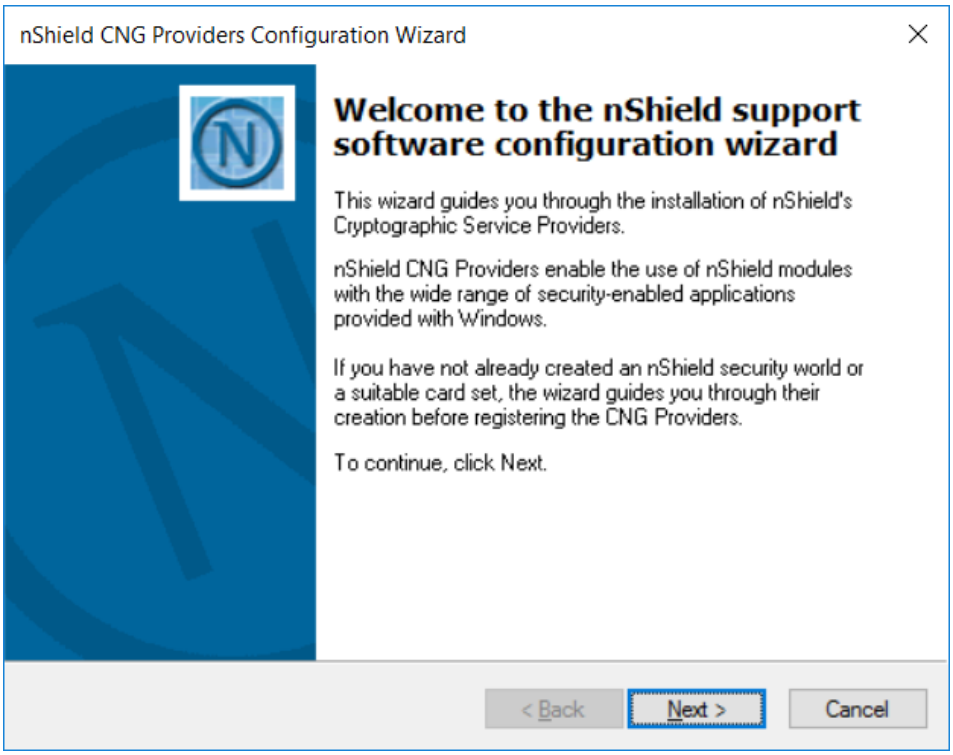
Configure CNG/KSP (Module protection)

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

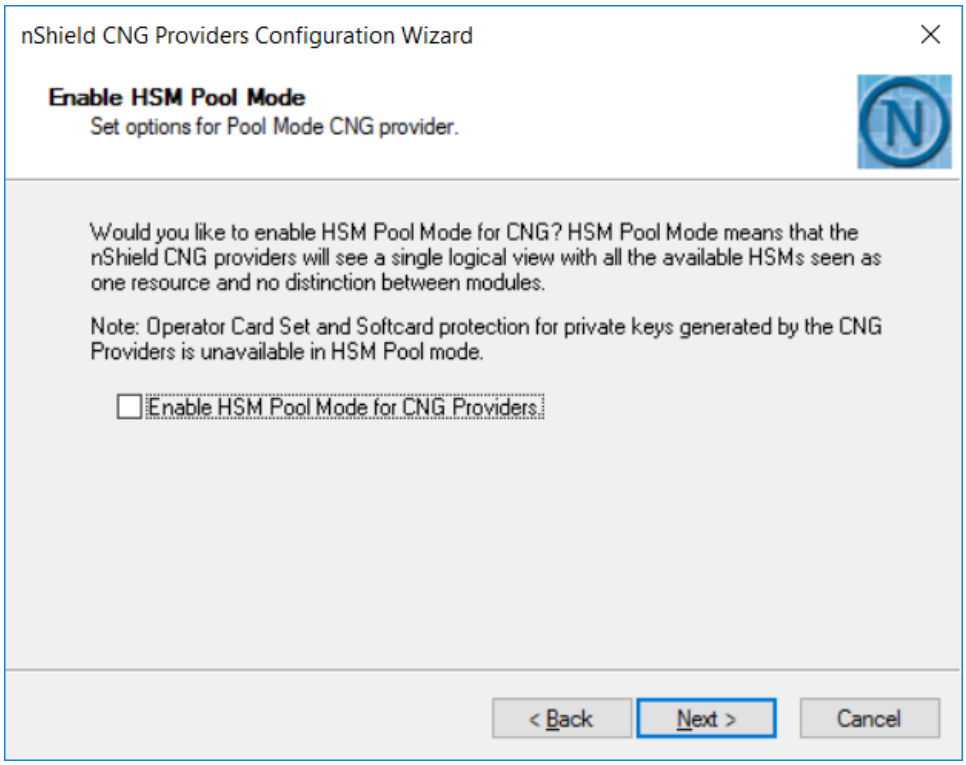
1. Go to Start-> nCipher and run CNG Configuration wizard.



2. Click **Next**.

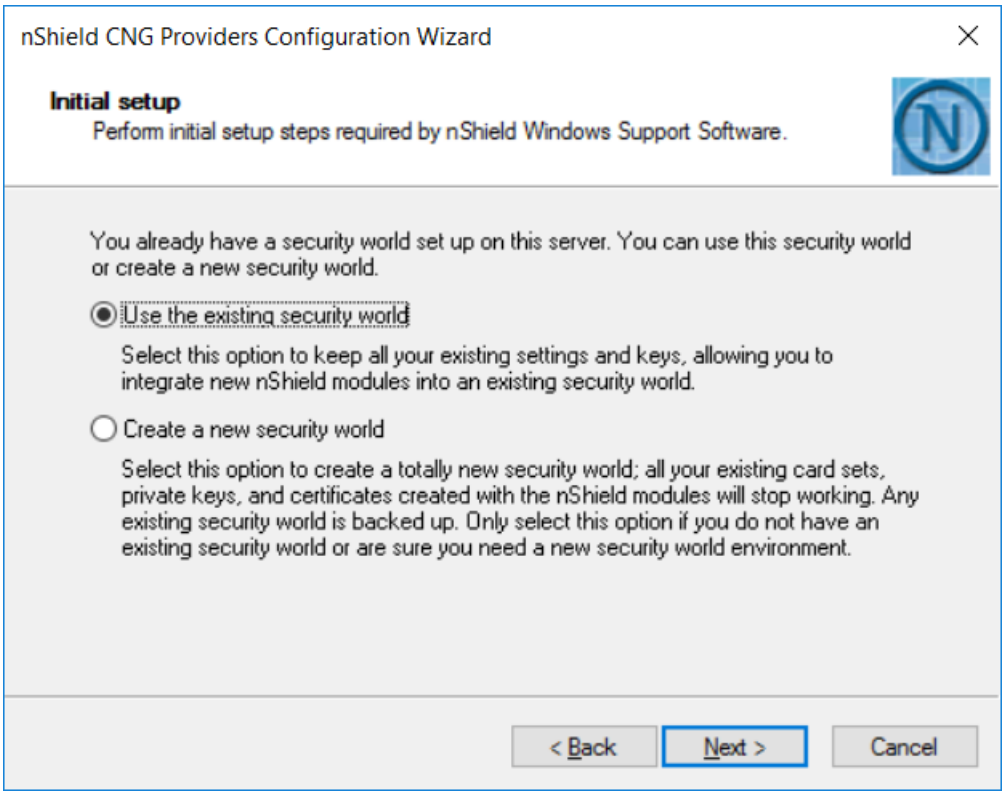


3. On Enable HSM Pool Mode, click **Next**.



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

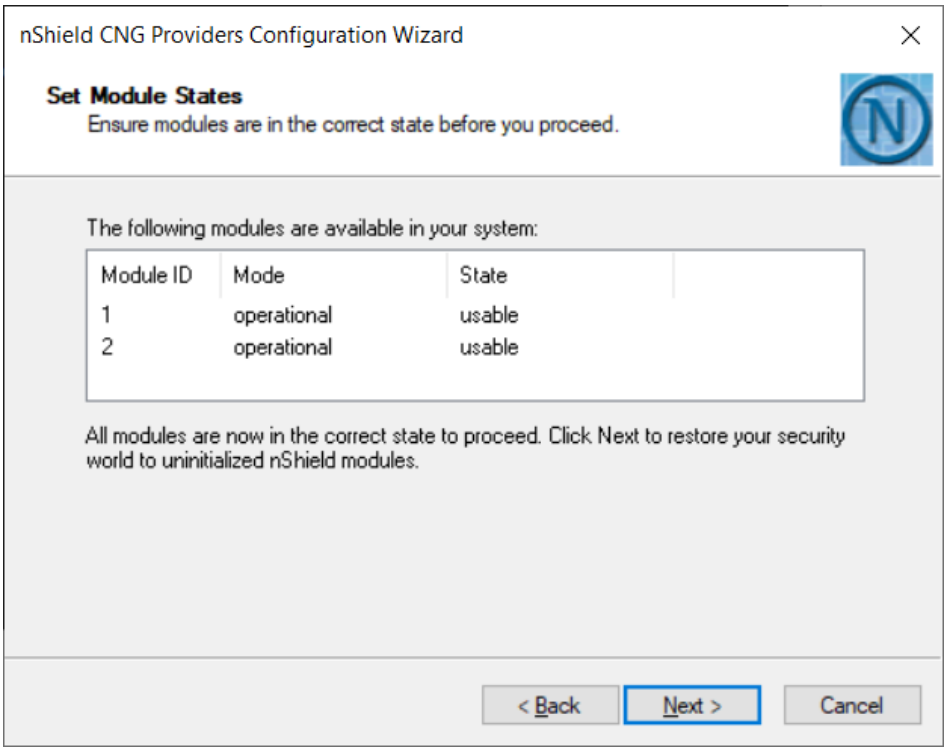
4. On Initial setup dialog box, click **Next**.



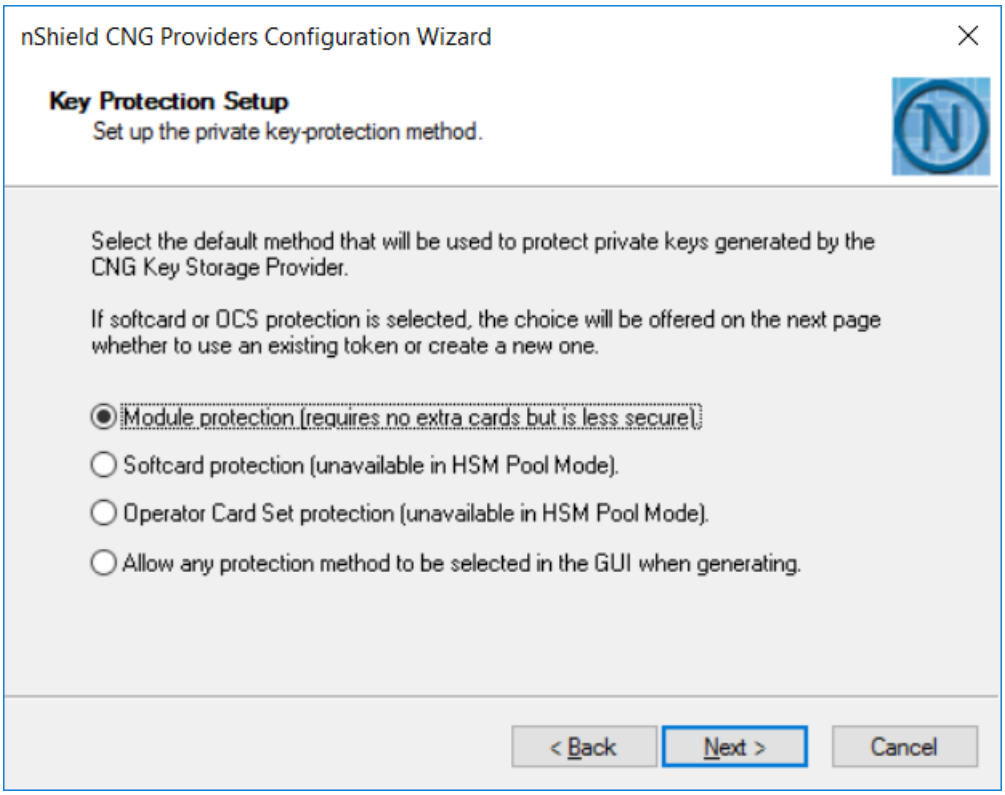
NOTE: The first one (**Use the existing security world**) must be selectable. If not, please check the configuration of the module. (e.g. rfs-sync).

---

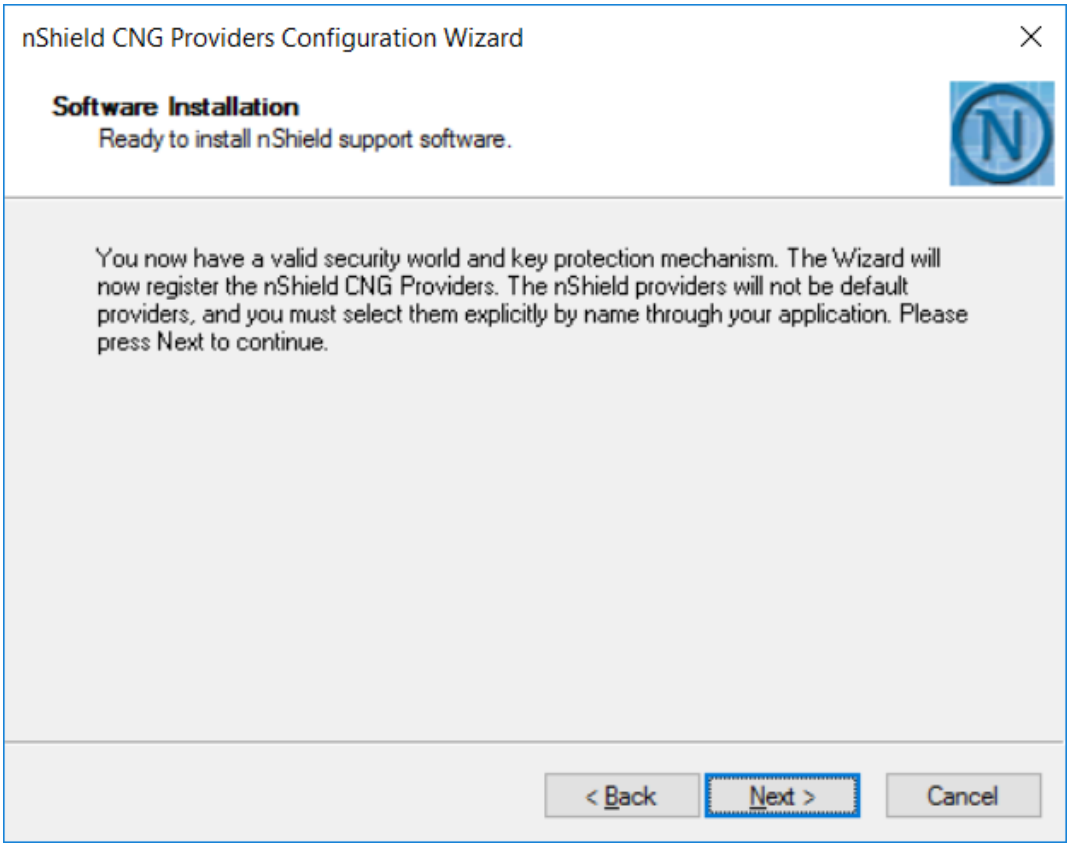
5. On Module States dialog box, click **Next**.



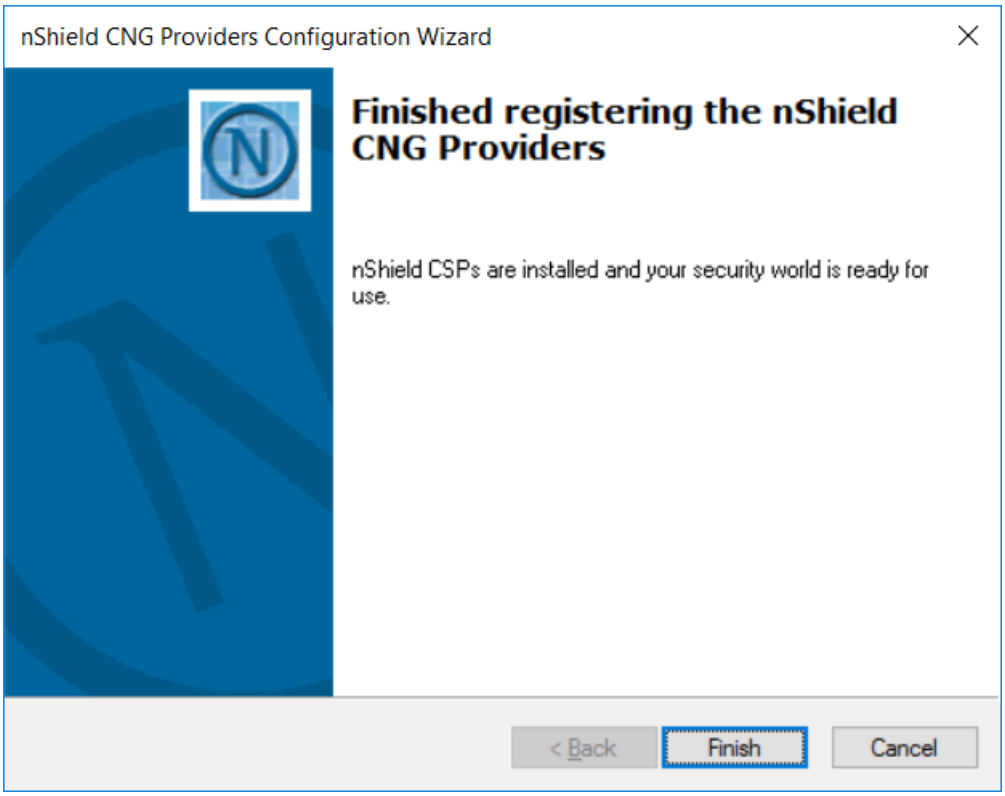
6. On the Key Protection Setup dialog box, select '**Module protection**' and click **Next**.



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



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.

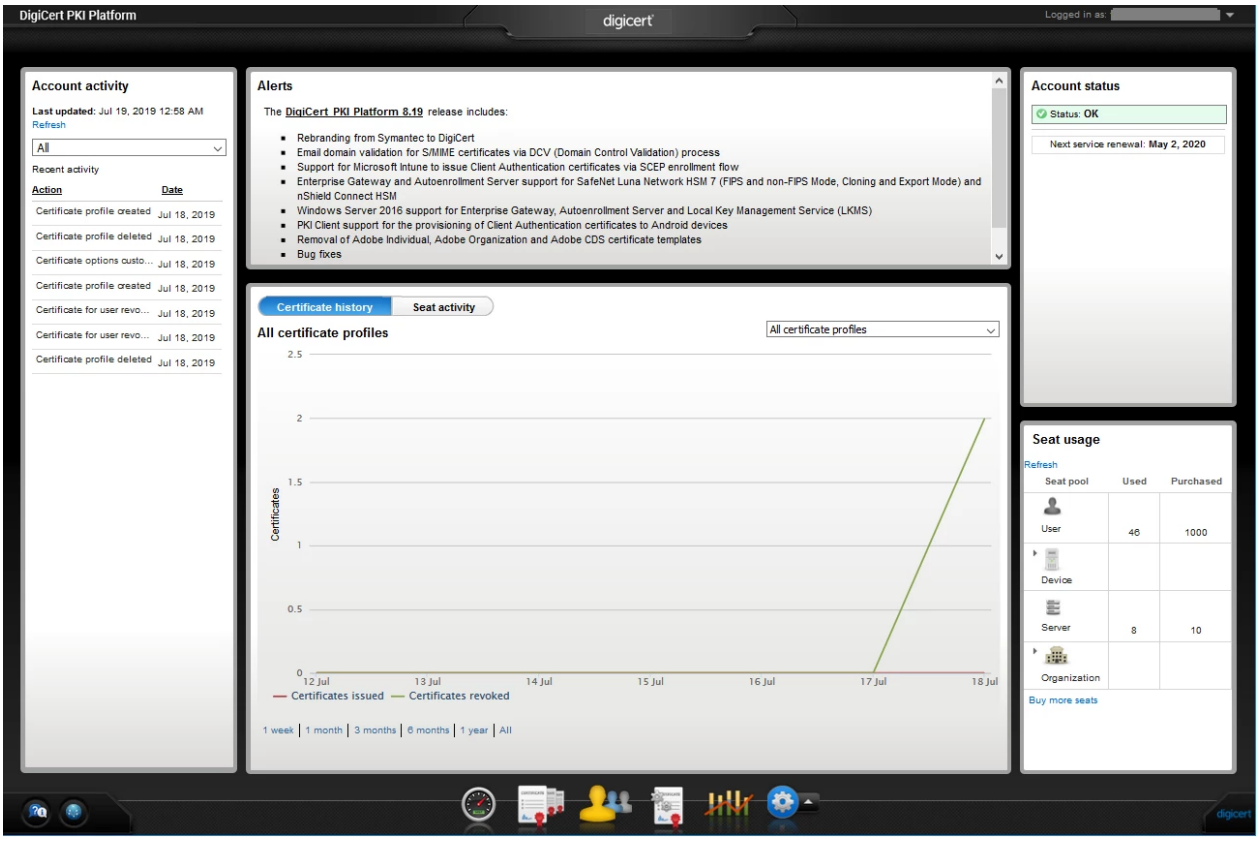
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
....
C610uaqncn6FvLu5pygZYFEVtOanCXNQRRUWiDGWKjHF+10GMh+V5YUur55T4W80
0uwK
```

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

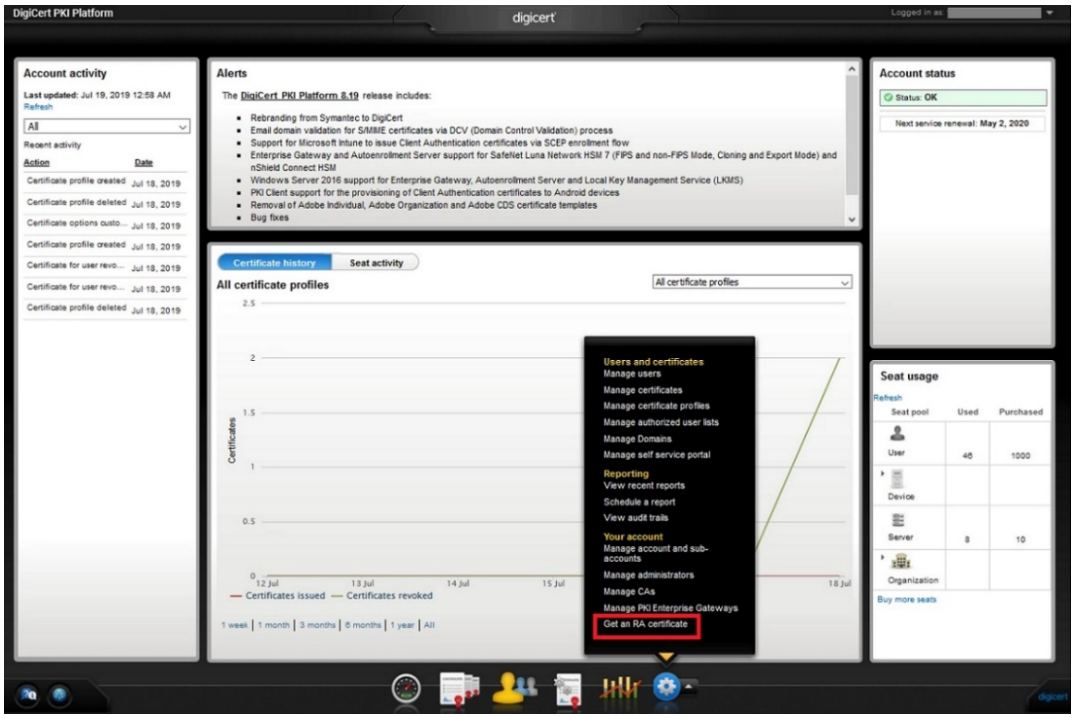
Get RA Certificate in PKI-Manager

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.

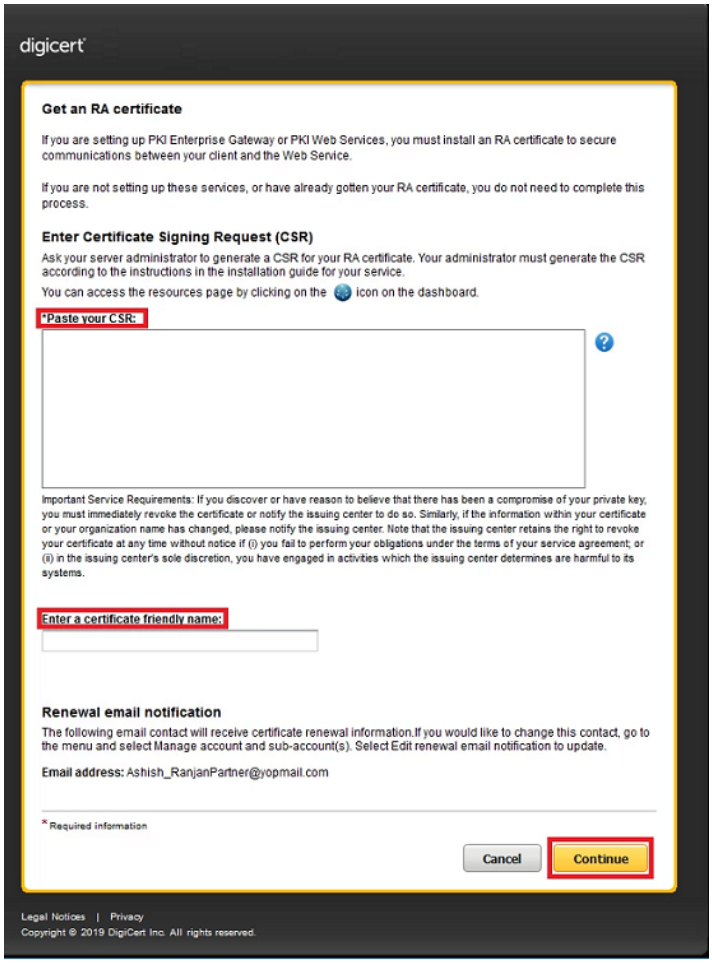
1. Go to PKI Manager and sign in by using your certificate.



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



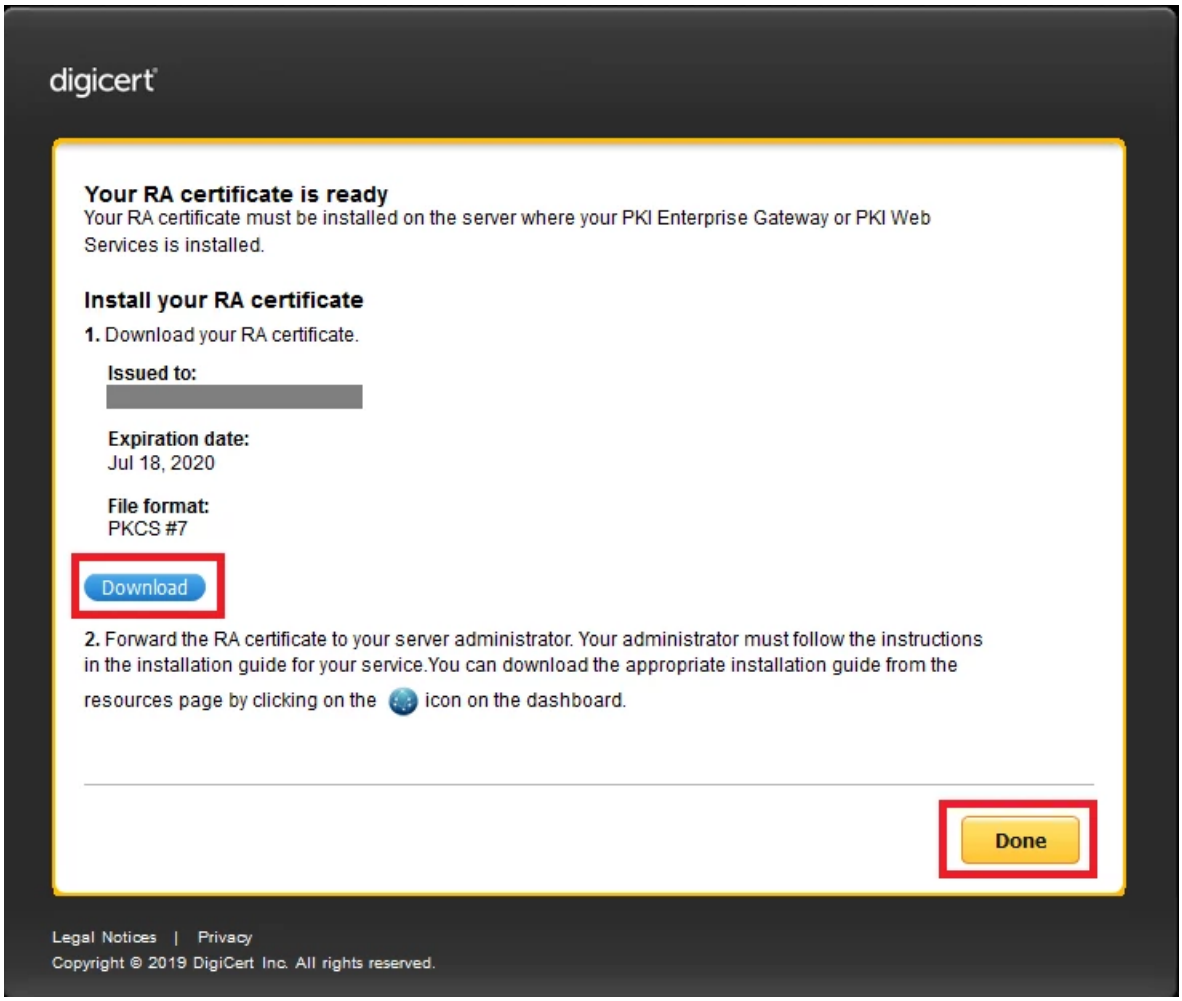
3. Paste your CSR and enter a certificate friendly name and then click "**Continue**".



The CSR looks as follows; Please paste it.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDjzCCAncCAQAwITEfMB0GA1UEAwwWUmVnaXN0cmF0aW9uIEF1dGhvcml0eTCC
...
zbnTmg1IIY4NSgFcRsbs5j5GQDN86gSKmQ8/EvOjbpC62X3ZDhVmYSMBJUO1Jgv6
1tyz
-----END NEW CERTIFICATE REQUEST-----
```

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



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

================ Begin force NCrypt ================

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.