DigiCert[®] PKI Platform

HSM Installation and Configuration for SafeNet

Version 8.19

February 12, 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	5
REVISION HISTORY	5
SUPPORTED HSMS	7
SAFENET NETWORK HSM	8
INSTALL LUNA HSM CLIENT	-
CONFIGURE LUNA HSM CLIENT	
CONFIGURE HA (HIGH AVAILABILITY)	
CONFIGURE CSP	
CONFIGURE KSP	
GENERATE CSR AND INSTALL CERTIFICATE	
INTEGRATION FOR JAVA ENVIRONMENT	21
Register Luna Provider	21
INSTALL RA CERTIFICATE	22
SAFENET DPOD CLOUD HSM	22
INSTALL LUNACLIENT	
Add a Subscriber Group as Tenant Administrator	
ADD AN APPLICATION OWNER AS TENANT ADMINISTRATOR	
ADD ADMINISTRATOR AS TENANT ADMINISTRATOR	
ENABLE HSM ON DEMAND SERVICES AS TENANT ADMINISTRATOR	
ADD NEW SERVICES AND SERVICE CLIENT AS APPLICATION OWNER	
CREATE SERVICE CREDENTIALS AS APPLICATION OWNER	
DOWNLOAD CLIENT AS APPLICATION OWNER	
INSTALL SERVICE CLIENT FOR WINDOWS	40
CONFIGURE LUNACLIENT	
INITIALIZE THE PARTITION AND USERS	
CONFIGURE HA (HIGH AVAILABILITY)	
CONFIGURE CSP	46
CONFIGURE KSP	47
GENERATE CSR AND INSTALL CERTIFICATE	50
INTEGRATION FOR JAVA ENVIRONMENT	51

Register Luna Provider	51
INSTALL RA CERTIFICATE	52

GET RA CERTIFICATE IN PKI-MANAGER	
-----------------------------------	--

Introduction

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

Revision History

No.	Date	Summary
1.	2019/05/10	Create a new entry
2.	2019/05/20	 Updated all the screenshots in "Install LunaClient" because the location path included '¥' instead of '\' (backslash).
		2. Added "Create CSR and Install Certificate" chapter for each HSMs
3.	2019/07/17	1. Added "SafeNet DPoD Cloud HSM"
		2. Added "Get RA Certificate in PKI-Manager" as an Appendix
4.	2019/08/16	1. Added "Create Service Credentials as Application Owner" section.
		2. Added "Download Client as Application Owner" section.
		3. Added Step 9 under the "Configure LunaClient".
5.	2019/08/30	1. The algorithm of signature for PKCS#10(CSR) has been changed from SHA1 to SHA256.
6.	2019/11/20	1. Removed the SafeNet Network HSM version
		 Provider Type changed to 0 as Provider Type is not defined for KSP
7.	2020/01/06	 Updated SafeNet Network HSM Luna Client version 7.3.0-165 with 7.4.1-2.
		2. Added SafeNet Network HSM Luna Client version 10.1.0.32.
		3. Updated all screenshots in Install LunaClient.
		4. Updated codes with client version 10.1.0.32 in Configure Luna HSM Client, Configure HA (High Availability), and Configure CSP .

8.	2020/01/17	5. Updated SafeNet DPoD Cloud HSM Client, Software, and Firmware versions.
		 Updated codes with Client, Software, and Firmware versions in Install Service Client for Windows, Configure LunaClient, and Configure CSP.
9.	2020/02/11	 Added "Integration for Java Environment" new topic on both SafeNet Network HSM and DPoD Cloud HSM
		 Updated SafeNet DPoD Cloud HSM Client version to v10.1.0- 32

HSM Туре	Client Version	Software Version	Firmware Version
SafeNet Network HSM (*a, *b)	6.1	6.1	6.10.9
SafeNet Network HSM (*a, *c, *d)	7.4.1-2	7.2.0-220	7.2.0 LunaPED FW Version: 2.8.0-1
SafeNet Network HSM (*a, *c, *d)	10.1.0.32	7.2.0-220	7.2.0
SafeNet DPoD Cloud HSM	10.1.0.32	7.3.0	The service client can be downloaded from your site. Firmware Version: 7.3.0 CV Firmware Version: 1.3.0

Supported HSMs

*a : Both Export and Signing variants were qualified with the supported HSM types.

*b : SafeNet Network HSM 7 Luna PCI, and Luna G5 are functionally identical and the above qualified versions of SafeNet Network HSM 7 should work with Luna PCI and Luna G5.

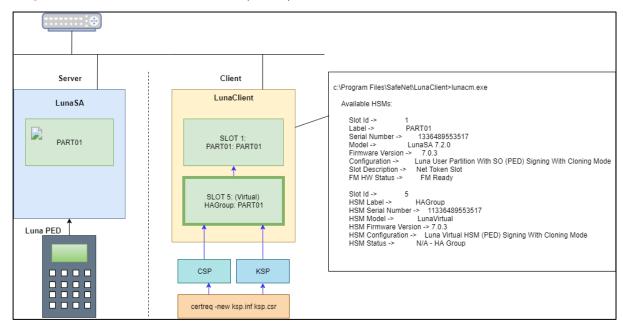
*c : If the listed Luna Client and Software versions are deployed, the Luna SA 6 HSM should also work, although not formally qualified by DigiCert.

*d : SafeNet Network HSM 7 supports FIPS and non-FIPS Mode, Cloning and Export Mode.

SafeNet Network HSM

The SafeNet Network HSM 7 (formerly known as Luna SA) is network HSM which allows to create a partition to store a key, such as the RA key required to strongly authenticate to the DigiCert PKI Platform. It includes many features that increase security, connectivity, and ease-of-administration in dedicated and shared security applications.

To access the partition of SafeNet Network HSM 7, we can use the Luna HSM Client through Network Trust Link Service (NTLS).



Install Luna HSM Client

In the Client location, follow the steps below to install the Luna HSM Client software:

1. Run LunaHSMClient.exe as Administrator.

Luna HS Version: 10.1.0.32	SM Client	gemalto security to be free	
This setup wizard install below. Install location:		Client setup wizard t on your computer. Please customize th Select folder	ne
Install options:	Luna Devices Select All Network PCle USB Backup Remote PED	Features Select All CSP (CAPI) / KSP (CNG) JCE / JCA Provider (JSP) PKCS #11 (JCProv) Software SDK SNMP Subagent FM Tools FM Tools FM SDK	
I agree to the	e terms of the <u>SafeNet Softw</u>	<u>are License Agreement</u> .	
		INSTALL	

2. Select Install options and features.

Check the following **Luna Devices** (some options and features are optional, depending on your environment):

- a) Network
- b) (Optional) Remote PED

Check the following Features. (Option: depends on your environment):

- c) CSP(CAPI) / KSP(CNG)
- d) (Optional) JCE / JCA Provider (JSP)
- e) (Optional) PKCS #11 (JCProv)

gemalto Luna HSM Client Version: 10.1.0.32 Welcome to the Luna HSM Client setup wizard This setup wizard will install Luna HSM Client on your computer. Please customize the install below. Install location: C:\Program Files\SafeNet\LunaClient Select folder Install options: Luna Devices Features Select All Select All CSP (CAPI) / KSP (CNG) ✓ Network JCE / JCA Provider (JSP) PCle ✓ PKCS #11 (JCProv) USB Backup Software SDK Remote PED SNMP Subagent FM Tools FM SDK ✓ I agree to the terms of the <u>SafeNet Software License Agreement</u>; INSTALL QUIT

Check Software License Agreement, and then Click INSTALL.

3. Wait for completion.

The progress bar will get displayed at the bottom of the dialog.

Luna HS	M Client	ge	security to be free
	to the Luna HSM Cl I will install Luna HSM Client o		
	\SafeNet\LunaClient		Select folder
Install options:	Luna Devices Select All Vetwork PCle USB Backup Remote PED	Features Select All ✓ CSP (CAPI) ✓ JCE / JCA F ✓ PKCS #11 (Software S SNMP Sub FM Tools FM SDK	Provider (JSP) JCProv) DK
✓ I agree to the	e terms of the <u>SafeNet Softwar</u>	re License Agreement	
File: ckdemo.exe, 1	Directory: C:\Program Files\Sat	e INSTALL QUIT	

4. Once the Installation is completed, the **UNINSTALL** and **MODIFY** button will get displayed. Click **QUIT**.

Luna HS	M Client	genalto security to be free
Welcome to the Luna HSM Client setup wizard This setup wizard will install Luna HSM Client on your computer. Please customize the install below. Install location: C:\Program Files\SafeNet\LunaClient\		
Install options:	Luna Devices Select All Vetwork PCle USB Backup Remote PED	Features Select All CSP (CAPI) / KSP (CNG) JCE / JCA Provider (JSP) PKCS #11 (JCProv) Software SDK SNMP Subagent FM Tools FM SDK
		UNINSTALL MODIFY QUIT

Configure Luna HSM Client

Before following the steps, a partition must be created, named as <PARTITION-NAME> throughout the rest of this document.

Follow the below steps to configure the Luna HSM Client:

1. Open a Command Prompt and run the following commands.

```
> cd C:\Program Files\SafeNet\LunaClient
> lunacm.exe
```

2. Create a Network Trust Link (NTL) - this is a one-step setup.

If you have already created an NTL, you can skip to Step 3.

```
lunacm:> clientconfig deploy -server <SERVER-HOSTNAME> -client <CLIENT-
HOSTNAME> -par <PARTITION-NAME>
Please wait while we set up the connection to the HSM. This may take several
minutes...
Please enter appliance admin role user's password:
Command Result : No Error
lunacm.exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights
reserved.
Slot Id -> 1
Label ->
```

```
Serial Number ->
                              1314971349473
       Model ->
                              LunaSA 7.2.0
       Firmware Version ->
                              7.2.0
                             Luna User Partition With SO (PED) Signing
       Configuration ->
With Cloning Mode
       Slot Description ->
                             Net Token Slot
       FM H Status ->
                             FM Ready
       Current Slot Id: 1
lunacm:> clientconfig v
The following Luna SA Slots/Partitions were found:
Slot
       Serial #
                              Label
====
                              =====
       _____
                              <PARTITION-NAME>
          1314971349473
   1
```

```
Command Result : No Error
```

If you do not want to follow the one step setup (Step 2), follow the below steps:

a) Obtain the Server Certificate.

The Server Certificate has been created on the HSM, so we need to copy it from the server.

> pscp -scp admin@<SERVER-HOSTNAME>:server.pem .

b) Add Server for the Client side.

```
> vtl addServer -n <SERVER-HOSTNAME> -c server.pem
New server <SERVER-HOSTNAME> successfully added to server list.
```

c) Create a Client certificate.

```
> vtl createCert -n <CLIENT-HOSTNAME>
Private Key created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\<CLIENT-HOSTNAME>Key.pem
Certificate created and written to: C:\Program
Files\SafeNet\LunaClient\cert\client\<CLIENT-HOSTNAME>.pem
```

d) Upload the Client certificate to the Server.

```
> pscp -scp cert\client\<CLIENT-HOSTNAME>.pem admin@<SERVER-HOSTNAME>:
admin@<SERVER-HOSTNAME>'s password:
<CLIENT-HOSTNAME>.pem | 1 kB | 1.1 kB/s | ETA: 00:00:00 | 100%
```

Now, at the Server,

e) Register the Client and connect to the HSM via SSH.

```
lunash:> client register -client <CLIENT-HOSTNAME> -hostname <CLIENT-
HOSTNAME>
```

```
'client register' successful.
Command Result : 0 (Success)
```

f) Assign a partition to a Client and connect to the HSM via SSH.

```
lunash:> client assignPartition -client <CLIENT-HOSTNAME> -partition
<PARTITION-NAME>
'client assignPartition' successful.
Command Result : 0 (Success)
```

Now, at the Client,

3. Confirm connection settings.

The working directory is "C:\Program Files\SafeNet\LunaClient"

4. Configure Logging (Optional)

The working directory is "C:\Program Files\SafeNet\LunaClient". The name of the log folder is "c:\temp" in the following example and it can be changed.

```
> vtl logging configure c:\temp
Success setting log path to c:\temp
> vtl logging show
Client logging written to: c:\temp\LunaCryptokiLog.htm
```

Configure HA (High Availability)

1. Create an HA Group.

Open Command Prompt and run the following client commands.

```
> cd C:\Program Files\SafeNet\LunaClient
> lunacm.exe
lunacm:> slot set -s <SLOT-NUMBER>
lunacm:> hagroup creategroup -se <SERIALNUMBER> -label <HA-LABEL>
Enter the password: **********
New group with label "HAGroup" created with group number <SERIALNUMBER>.
Group configuration is:
```

```
HA Group Label: <HA-LABEL>
HA Group Number: 11336489553517
HA Group Slot ID: Not Available
Synchronization: enabled
Group Members: 1336489553517
Needs sync: no
Standby Members: <none>
Slot # Member S/N Member Label Status
----- ------ ------- ------
1 1336489553517 <PARTITION-NAME>alive
Command Result : No Error
lunacm.exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights
reserved.
Available HSMs:
Slot Id -> 1
Label -> <PARTITION-NAME>
Serial Number -> 1336489553517
Model -> LunaSA 7.2.0
Firmware Version -> 7.0.3
Configuration -> Luna User Partition With SO (PED) Signing With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready
Slot Id -> 5
HSM Label -> <HA-LABEL>
HSM Serial Number -> 11336489553517
HSM Model -> LunaVirtual
HSM Firmware Version -> 7.0.3
HSM Configuration -> Luna Virtual HSM (PED) Signing With Cloning Mode
HSM Status -> N/A - HA Group
```

Current Slot Id: 1

NOTE: Both "Configure CSP" and "Configure KSP" must be configured again if you run the steps above.

2. Enable "HA Only"

Command Result : No Error

Configure CSP

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

For SafeNet CSP, the utility **register.exe** (64-bit version) takes care of the registry. To configure CSP, open a command prompt and run the following commands.

Register CSP Library

C:\Program Files\SafeNet\LunaClient\CSP>register.exe /library

Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna enhanced RSA and AES provider for Microsoft Windows. Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna Cryptographic Services for Microsoft Windows. Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna SChannel Cryptographic Services for Microsoft Windows.

Register the partition

```
C:\Program Files\SafeNet\LunaClient\CSP>register.exe
register.exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights
reserved.
```

* * * Safenet LunaCSP, Partition Registration * * * Protect the HSM's challenge for the selected partitions. NOTE: * This is a WEAK protection of the challenge. After you have configured all applications that will use * the LunaCSP and ran them once, you MUST run: * register /partition /strongprotect * to strongly protect the registered challenges.

This is a destructive procedure and will overwrite any previous registrations.

Do you wish to continue?: [y/n]y Do you want to register the partition named '<PARTITION-NAME>'?[y/n]: y Enter challenge for partition '<PARTITION-NAME>' : <Only hit "Enter" then the PED Authentication will be requested>

Success registering the ENCRYPTED challenge for partition '<PARTITION-NAME>:1'. Only the LunaCSP will be able to use this data. Registered 1 partition(s) for use by the LunaCSP.

Register the HA partition

Run the following commands if HA is configured.

```
c:\Program Files\SafeNet\LunaClient\CSP>register.exe /h
register.exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights
reserved.
 *
                                                                *
       Safenet LunaCSP, Partition Registration
 *
 *
       Protect the HSM's challenge for the selected partitions.
       NOTE:
            This is a WEAK protection of the challenge.
            After you have configured all applications that will use
            the LunaCSP and ran them once, you MUST run:
               register /partition /strongprotect
            to strongly protect the registered challenges.
 This is a destructive procedure and will overwrite any previous
registrations.
Do you wish to continue?: [y/n]y
Do you want to register the partition named '<HA-LABEL>'?[y/n]: y
Enter challenge for partition '<HA-LABEL>' :***********
Success registering the ENCRYPTED challenge for partition '<HA-LABEL>:1'.
Only the LunaCSP will be able to use this data.
```

Registered 1 partition(s) for use by the LunaCSP.

Configure KSP

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

To configure KSP (CNG), run KspConfig.exe (Default location is "C:\Program Files\SafeNet\LunaClient\KSP\").

Follow instructions for the use of the graphical **KspConfig.exe** as described in KSP for CNG in the SDK Reference Guide.

The following window will appear.

N - SafeNet Key Storage Provider Config Wizard	
Eile Help	
J	
SafeNet KSP Config	
- Register Or View Security Library	
Register HSM Slots	
Ready	

Double-click **Register Or View Security Library**, and then confirm the value "C:\Program Files\SafeNet\LunaClient\cryptoki.dll".

N - SafeNet Key Storage Provider Config Wizard		
<u>File</u> <u>H</u> elp		
SafeNet KSP Config Register Or View Security Library Register HSM Slots	LibraryPath CNProgram FilesNSafeNettLunaClienttcryptoki.dll Browse	
 Ready		

Double-click Register HSM Slots for Administrator/<Domain Name>

- Select Administrator
- Select <Domain Name>
- Select "HA Group" for Available Slots
- Enter Slot Password

Click Register Slot.

SafeNet Key Storage Provider Config W	izard		- 0	×
<u>File</u> <u>H</u> elp				
SafeNet KSP Config Register Or View Security Library Register HSM Slots	Administrator Available Slots 1 HAGroup	FKIDEV2016 Slot Password	Register By F Stot Label C Stot Number	
			Register Slot View Registered Slots	
	Registered Slots		Hew Registered blob	
	SlotLabel HAGroup			
Ready			Delete Registered Slot	

Double-click Register HSM Slots for SYSTEM/NT AUTHORITY.

- Select SYSTEM
- Select NT AUTHORITY
- Select "HA Group" for Available Slots
- Enter Slot Password

Click Register Slot.

- SafeNet Key Storage Provider Config Wiz Eile Help	ard				- 🗆 X
J = SafeNet KSP Config ⊢ Register Or View Security Library ⊢ Register HSM Slots	SYSTEM Available Slots 1 HAGroup	•	NT AUTHORITY Slot Password	•	Register By G Slot Label C Slot Number
	Registered Slots				Register Slot View Registered Slots
	SIGLADELHAGROUD				
				ļ	Delete Registered Slot
Ready					

NOTE: When you click "**Register Slot**", there is no change on "Registered Slot", but this step is necessary.

When registering the Luna KSP (with the Luna KSPConfig utility), use the following user and domain combinations:

- The user and domain performing these procedures.
- The user and domain running the web application and using the private key.
- The local user and NT Authority domain user.
- The LocalSystem and NTAuthority of the system.

NOTE: If you implement the Autoenrollment server, you must also install and register the Luna CSP. Refer to the SafeNet product documentation for details.

Generate CSR and Install Certificate

- 1. Create the information file for CSR.
 - a) To generate CSR using certreq.exe through CSP, the ProviderName must be "Luna Cryptographic Services for Microsoft Windows". The sample of inf file is as follows;

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "Luna Cryptographic Services for Microsoft Windows"
ProviderType = 1
Subject = "CN=Registration Authority"
KeyContainer = "CSPRA20190418"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

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

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "SafeNet Key Storage Provider"
ProviderType = 0
Subject = "CN=Registration Authority"
KeyContainer = KSPRAID20190418
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
KeyUsage = 0xf0
```

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-----

- 3. Install a certificate.
 - a) Open command prompt (on the folder where the PKCS#7 file exists) and run the following command.
 - > certreq -accept <issued-cert>
 - b) Before running the command, 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)

Integration for Java Environment

Register Luna Provider

You must update the **java.security** configuration file to use the SafeNet security providers and the HSM.

To configure the java.security file:

- 1. Open the Java security configuration file **java.security** in a text editor. The file is available at <JDK_installation_directory>\jre\lib\security.
- 2. Update the Luna Providers in the **java.security** file so they appear as follows:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
security.provider.7=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.8=sun.security.smartcardio.SunPCSC
security.provider.9=com.safenetinc.luna.provider.LunaProvider
```

3. Save the changes to the java.security file.

Enabling the HSM keystore

You must configure the Java Code Signing utility to use the keystore located on the HSM.

To enable the HSM keystore

- 1. Copy the LunaProvider.jar files from the <Luna_installation_directory>\JSP\lib to the Java extension folder located at <JDK_installation_directory>\jre\lib\ext.
- 2. Set the environment variables for JAVA_HOME and PATH.

NOTE: We recommend setting the PATH variable in Windows environments using the System Environments menu.

Install RA Certificate

Refer section "Using an RA Certificate on HSM" of DigiCert® PKI Enterprise Gateway Deployment Guide document.

SafeNet DPoD Cloud HSM

The SafeNet DPoD (**Data Protection on Demand**) service provides "HSM on Demand" which is one of HSM on Demand Services. This section introduces how to generate key on Cloud HSM and use it. Please see the SafeNet Official Guide if you need details or other information. Click "⁽²⁾" icon on your site on SafeNet DPoD Service, to avail the guide.

gemalto [*]	[20 Tenant Administrator	@digicert.com 🖕	0
Accounts		Reports			

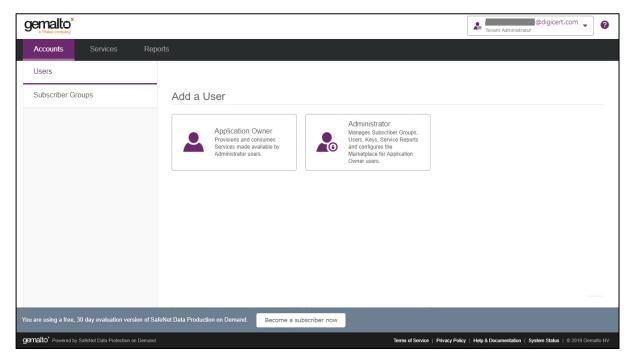
Before proceeding, we should understand the 3 types of users in the DPoD role hierarchy which are as follows:

No	Туре	Responsibility	Note
1	Service Provider Administrators	Managing and distributing additional DPoD tenants.	On this document, there is no description about this user. Please see the SafeNet Official Guide.
2	Tenant Administrators	Managing an enterprise tenant and distributing cryptographic resources in the form of services to application owners.	The user can create, subscribe group and Application Owner, and also configure services.
3	Application Owners	Managing cryptographic services, and consuming cryptographic resources in an enterprise tenant.	

Install LunaClient

Add a Subscriber Group as Tenant Administrator

1. Sign in to DPoD site using your Tenant Administrator credential.



2. Select "Subscriber Groups" followed by "Add a Subscriber Group".

	@digicert.com 🗸 📀
Accounts Services Rej	ports
Users	
Subscriber Groups	Add a Subscriber Group Group Users according to your openrated key material: generated key material:
You are using a free, 30 day evaluation version of S	afeNet Data Production on Demand. Become a subscriber now
gemallo" Powered by SafeNet Data Protection on Demand	Terms of Service Privacy Policy Help & Documentation System Status © 2019 Gemailto NV

3. Enter "Group Name" and "Description" and then click "Add".

In this document, "Group Name" is "DPPC-QA" but you can use any other value.

gemalto*		@digicert.com 🗸 🕜
Accounts Services Reports	Add Subscriber Group	
Sul Grou	Group Name	ers 🔶 No. Services 🔶 No. Clients 🔶 Actions
You are using a free, 30 day evaluation version of SafeNet Data Production on I	Demand. Become a subscriber now	
gemalto* Powered by SafeNet Data Protection on Demand		Ferms of Service Privacy Policy Help & Documentation System Status © 2019 Gematic NV

4. The designated group has been created.

		@digicert.com	0
Accounts Services Repo	rts		
Users	Mu Cubacibar Oroung		
Subscriber Groups	My Subscriber Groups		
	Search P Name Description	No. Users	
	Name Description DPPC-QA No description provided	No. Users No. Services No. Clients Actions 1 1 1	
	Add a Subscriber Group		
	Subscriber Group		
	Group Users according to your		
You are using a free, 30 day evaluation version of Saf	eNet Data Production on Demand. Become a subscriber now		
gemalto [*] Powered by SafeNet Data Protection on Demand		Terms of Service Privacy Policy Help & Documentation System Status © 2019 Gem	alto NV

5. Click on the link of group which has been created to view the Group details.

		digicert.com 🔪 💡
Accounts Services Re	ports	
Users	Subscriber Groups > DPPC-QA	Delete Subscriber Group
Subscriber Groups	Name DPPC-QA Description	er ا
	Users and Services Users Services	
	Email Address	Role Actions T
You are using a free, 30 day evaluation version of :	SafeNet Data Production on Demand. Become a subscriber now	
gemalto* Powered by SafeNet Data Protection on Deman	nd	Terms of Service Privacy Policy Help & Documentation System Status © 2019 Gemailo NV

Add an Application Owner as Tenant Administrator

1. Sign in to DPoD site using your Tenant Administrator credential. Select "Accounts" tab and click on "Users".

	Tenant Administrator
Accounts Services Rep	orts
Users	
Subscriber Groups	Add a User
	Application Owner Frovisions and consumes administrator users. Administrator users. Administrator users. Administrator users. Administrator users. Administrator of Application Owner users.
You are using a free, 30 day evaluation version of Sa	feNet Data Production on Demand.
gemalto Powered by SafeNet Data Protection on Demand	Terms of Service Privacy Policy Help & Documentation System Status © 2019 Gemaito NV

2. Select "Application Owner", under Add a User.

		@digicert.com 🖕
Accounts Services	Reports	
Users		
Subscriber Groups	Add a User	
	Application Owner Provisions and consumes Administrator users.	
u are using a free, 30 day evaluation version	of SafeNet Data Production on Demand. Become a subscriber now	
emalto [*] Powered by SafeNet Data Protection on D	nandTerms of Service Privacy Pol	licy Help & Documentation System Status © 2019 Gemaito №

3. Fill out the form with the User details and then click "Add User".

gemalto [×]	Add Application Owner	@digicert.com 🔪 🕖
Accounts Services Reports	Add Application Owner	
Email Address @df	Subscriber Group DPPC-QA First Name Last Name Email Address Create Password O Add User Cancel	• Last Name Created By Actions @digicert.com * a@digicert.com *
Prov Serv	Alication Owner sions and consumes ces made available by nistrator users.	orts
gemalio" Powered by SateNet Data Protection on Demand	Tem	is of Service Privacy Policy Help & Documentation System Status © 2019 Gemails NV

		@digicert.com 🗸 🕜
Accounts Services Repo	ts	
Users	My Users	
Subscriber Groups	Search P	
	Email Address Role Subscriber Group First Name First Name Composition DPPC-0A Composition Composition <th< th=""><th>Last Name Created By Actions Image: Comparison of the state of the s</th></th<>	Last Name Created By Actions Image: Comparison of the state of the s
	Odigicent.com Administrator None	€ Gigicert.com (♥)
	Add a User	
You are using a free, 30 day evaluation version of Safe	Net Data Production on Demand. Become a subscriber now	
gemalto [*] Powered by SafeNet Data Protection on Demand	Terms of Servic	ce Privacy Policy Help & Documentation System Status © 2019 Gemaito NV

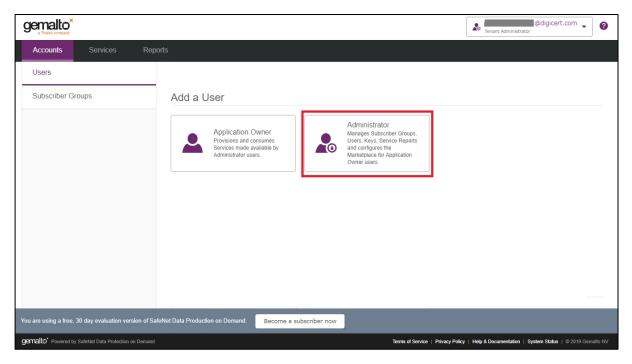
4. The user has been created.

5. Click on the user link created to see the User's profile.

				@digicert.	^{com} • 0
Accounts Services Rep	orts				
Users	Users >	@digicert.com	Reset MFA Token	Reset User Password Delet	e User
Subscriber Groups	03613 2	@digicert.com		,	
	Email Address @digicert.com				ď
	First Name	Last Name	Role Application Owner	Subscriber Group(s) DPPC-QA	
	Created By @digicert.co	Date Created om 10-Jul-2019 13:33			
You are using a free, 30 day evaluation version of Sa	feNet Data Production on Demand.	Become a subscriber now			
gemalto' Powered by SafeNet Data Protection on Demand			Terms of Service Privacy Policy	Help & Documentation System Status	© 2019 Gemalto NV

Add Administrator as Tenant Administrator

- 1. Sign in DPoD site and select "Accounts" tab followed by "Users".
- 2. Select "Administrator".



3. Fill out the form with the Administrator details then click "Add User".

gemalto*		@digicert.com 🔪 🕐
Accounts Services Reports	Add Administrator	
Email Address	First Name Last Name tot Name Canfirm Password Confirm Password Original Create Password Canfirm Password Original Cancel	Created By
Add a User Application Ov Provision and con Services made ava Administrator users You are using a free, 30 day evaluation version of Safe/Net Data Production on Demand	sumes Users, Keys, Service Reports lable by and configures the	
gemalto* Powered by SafeNet Data Protection on Demand	Terms of St	ervice Privacy Policy Help & Documentation System Status © 2019 Gemailto NV
Survey of the state of the state of the state of the state	Terris of 3	The Printed Policy Print & Documentation System Status @ 2018 Genation (V

						Tenant Administ	@digicert.co	om 🗸	8
Accounts Services Repor	ts								
Users	Mulleore								
Subscriber Groups	My Users Search	م							
	Email Address	Role Application Owner	Subscriber Group 🜲	First Name ಿ	Last Name	Created By	€ @digicert.com	Actions	1
	@digicert.com	Administrator	None				@digicert.com	▼	
	Add a User								
You are using a free, 30 day evaluation version of Safe	Net Data Production on Demand.	Become a subsc	riber now						
gemalto' Powered by SafeNet Data Protection on Demand				Terms of Service	Privacy Policy	Help & Documentation	System Status ©	2019 Gemalto	NV

4. The Administrator has been created.

Enable HSM On Demand Services as Tenant Administrator

1. Select "Services" tab then click on "Configure Services".

	©digicert.com ↓ 🚱
Accounts Services Reports	
Services Configure Services	
You are using a free, 30 day evaluation version of SafeNet Data Production on Demand.	Become a subscriber now
gemaito' Powered by SafeNet Data Protection on Demand	Terms of Service Privacy Policy Help & Documentation System Status © 2019 Gernatio NV

- 2. HSM on Demand: Set up and access an HSM on Demand service for your organization's cryptographic operations.
- 3. Under the "HSM on Demand" service tile, click the toggle to enable service.

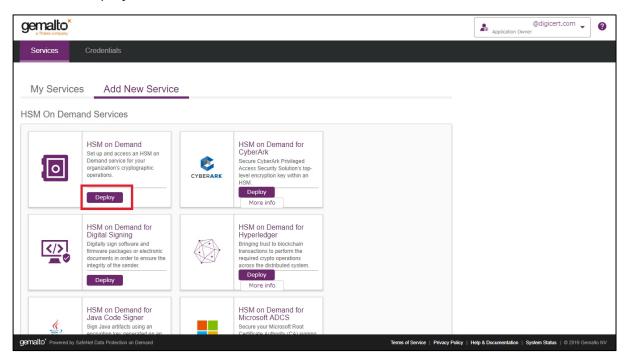
gemalto			@digicert.com 🗸 🕐
Accounts	Services Reports		
Services	Configure Services		
0	ices for your users ble or disable a service tile; your users will not be able to deploy disabled	services.	
HSM On Dem	and Services		
•	Set up and access an HSM on Demand service for your organization's cryptographic	Demand for k verArk Privileged urity Solutions top- tion key within an	
	Service is enabled	ice is enabled	
✓	Digital Signing Digital sign software and firmware packages or electronic documents in order to ensure the	Demand for Iger st to blockchain s to perform the prop operations distributed system.	
You are using a free, 3	0 day evaluation version of SafeNet Data Production on Demand.	ecome a subscriber now	
gemalto [*] Powered by	afeNet Data Protection on Demand	Terms of Service Privacy Policy	y Help & Documentation System Status © 2019 Gematto NV

Add New Services and Service Client as Application Owner

1. Sign in as an Application Owner and then select "Add New Service".

gemalto [×]		@digicert.com	• 0
Services Credentials			
My Services Add New Service			
gemailto' Powered by SafeNet Data Protection on Demand Terms of Service 1	Privacy Policy He	elp & Documentation System Status © 201	9 Gemalto NV

2. Click on "Deploy" under the "HSM on Demand" service tile.



• Step 1: Review Terms of Service

Check "I have read and accept the Terms of Service above." and then click "Next".

gemalto [*]		• @digicert.com • @
Services Credentials	Add HSM on Demand Service	Application Owner
	1 Terms of Service 2 Configure Service 3 Summary	
My Services Add Nev	Step 1 : Review Terms of Service	
HSM On Demand Services	TERMS OF SERVICES DPOD ("TOS")	
HSM on Demand	THESE TERMS OF SERVICE ARE THE TERMS AND CONDITIONS ON WHICH YOU MAKE USE OF THE SERVICE, AS DEFINED BELOW.	
Set up and access an Demand service for yo organization's cryptog operations.	YOU MUST READ THESE TERMS OF SERVICE CAREFULLY BEFORE YOU ACCESS THE SERVICE. BY ACCESSING THE SERVICE, YOU AGREE TO THESE TERMS OF SERVICE AND YOU REPRESENT AND WARRANT YOUR FULL AUTHORITY TO ENTER INTO THESE TERMS OF SERVICE ON BEHALF OF THE END CUSTOMER. IF YOU DO NOT AGREE WITH THESE TERMS OF SERVICE YOU MUST NOT USE THE	
Deploy	SERVICE. 1. DEFINED TERMS	
HSM on Deman Digital Signing Digitaly sign software firmware packages of occurrents in order to integrity of the sender	"Account" means an account with SafeNet to access and use the Service; "Affiliates" means any legally independent corporation or non-corporate entity which controls, is controlled by, or is under common control with a party hereto subject to a common management or in the party of Service above.	
Deploy	Cancel	
HSM on Demand Java Code Signe Sign Java antifacts usin encountion kay capacit	r Microsoft ADCS	
gemalto* Powered by SafeNet Data Protection on De	Terms of Service Privacy Policy H	elp & Documentation System Status @ 2019 Gemailo NV

• Step 2: Give your Service a name.

Enter "Service Name" and check if you allow non-FIPS approved algorithms, and then click "Next".

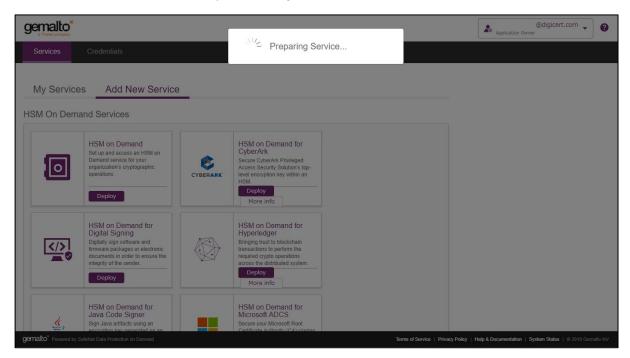
gemalto [*]		@digicert.com 🗸 🕜
Services Credentials	Add HSM on Demand Service	Application Owner
Services Credenialis	Terms of Service 2 Configure Service 3 Summary	
My Services Add Nev	Step 2 : Give your Service a name	
HSM On Demand Services	Service Name	
HSM on Deman Set up and access an Demand service for y organizations' cryptog operations.	Allow non-FIPS approved algorithms	
Deploy		-
HSM on Deman Digital Signing Digitaly sign software firmware packages or occurrents in order to integrity of the sender		
Deploy	Cancel Go Back N	ext
HSM on Demand Java Code Signe Sign Java artifacts usi according for a starting to the second	or Microsoft ADCS	
gemalto* Powered by SafeNet Data Protection on De	mand Terms of Service Privacy Polic	y Help & Documentation System Status © 2019 Gemaito NV

• Step 3: Review your configuration

Confirm your Service Name and click "Finish".

gemalto		Application Owner
Services Credentials	Add HSM on Demand Service	Apprication Owner
Services Credentials	Terms of Service Configure Service	- 3 Summary
My Services Add Nev	Step 3 : Review your configuration	
HSM On Demand Services	Service Name	HSMTEST
HSM on Deman Set up and access an Demand service for y organization's cryptog operations:		
HSM on Deman Digital Signing Ugitally sign software firmware packages or urtegrity of the sender		
Deploy	Cancel	Go Back Finish
HSM on Deman- Java Code Sign Sign Java artifacts us encrution kay agent	er Microsoft ADCS ng an Secure your Microsoft Root	
gemalto* Powered by SafeNet Data Protection on D	emand	Terms of Service Privacy Policy Help & Documentation System Status © 2019 Gematic NV

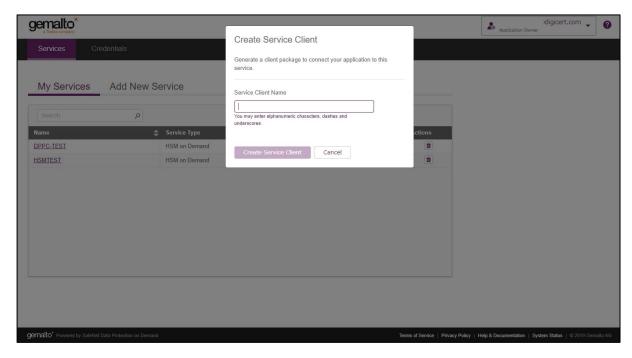
3. It takes several seconds for processing.



4. Click "Create Service Client".

gemalto*)@digicert.com 🗸 🕜
Services Credentials		ate Service Client?		Application Owner
My Services Add Net	Do you	u wish to create a Service Client to connect to this service? elect "Not Now", you can create one later from the service	If	
Search D	Cr	eate Service Client Not Now		
Name	Service Type	🗢 Created	Actions	
DPPC-TEST	HSM on Demand	11-Jul-2019 17:52	1	
HSMTEST	HSM on Demand	12-Jul-2019 20:48	Û	
gemalio" Powered by SafeNet Data Protection on D	lemand		Terms of Service Privacy Policy	Help & Documentation System Status © 2019 Gemalto NV

5. Enter "Service Client Name" and then click "Create Service Client".



6. It takes several seconds to process.

				@digicert.com
Services Credenti	als	Preparing Service Client		
My Services Ad	dd New Service			
	٩			
Name	Service Type	Created	Actions	
DPPC-TEST	HSM on Demand	11-Jul-2019 17:52	۲	
HSMTEST	HSM on Demand	12-Jul-2019 20:48		
	fection on Demand			

7. Click "Download Client" to download the service client software onto your workstation.

The name of the archive file will be **setup-<Service Client Name>**.zip. All the tools are included into the file.

Services Credentia	ls	ur client is ready. the button below to download your client.		digicert.com
My Services Ad	d New Service	Download Client Cancel		
	٩			
Name	Service Type	Created	Actions	
DPPC-TEST	HSM on Demand	11-Jul-2019 17:52	0	
HSMTEST	HSM on Demand	12-Jul-2019 20:48	0	

8. Confirm that the service has been created.

				,@digicert.com _
Services Credentia	ls			
My Services Ad	ld New Service			
Ny Services Au	d New Service			
Search	Q			
Name	Service Type	Created	Actions	
DPPC-TEST	HSM on Demand	11-Jul-2019 17:52		
HSMTEST	HSM on Demand	12-Jul-2019 20:48	û	

Create Service Credentials as Application Owner

1. Select/Click on the Name under "My Services" (For example: DPPC-QA1).

Services Credentials				
Ma Organization Antich Ma				
Max O a mala a a A al al Mar				
My Services Add Ne	ew Service			
Search P	þ			•
Name	Service Type	Created	Actions	
DPPC-QA-PA-CloudHSM	HSM on Demand	1-Aug-2019 12:52	۵	
DPPC-QA1	HSM on Demand	13-Aug-2019 9:41		
DPPC-QA2	HSM on Demand	13-Aug-2019 15:53	û	

2. Click on "Credentials" and then click on "Create Service Credentials".

gemalto [×]							Application Owner	edigicert.com	- 0
Services	Credentials								
My Services >	DPPC-QA1				Delete Service		٥		
Configuration									
Service Name DPPC-QA1	Service Type HSM on Demand	Created 13-Aug-2019 9:41	Partition Serial Number 1285325034348	Non-FIPS Algorithms Yes					
Service Clier	nts Credential	S							
Search	٩				New Service Client				
Name	Created I	-	▲ Cr		🗢 Actions				
DPPC-QA1		@digicert.co	m 13	-Aug-2019 9:41	V				
gemalto" Powered by Safe						Terms of Service Privacy Poli	cy Help & Documentation	I System Status © 2019	

3. Click on "Next".

gemalto*		Application Owner
Services Credentials	Generate Service Credentials	
	Review Permissions 2	
My Services > DPPC-QA1	Step 1 : Review permissions and optionally enter a name.	
Configuration	These credentials will allow a client to perform the following operations on the service "DPPC-QA1":	
Service Name Service Type C		
DPPC-QA1 HSM on Demand 1	Create, regenerate & delete service clients Create, regenerate & delete service credentials	
Service Clients Credentials		
Search P	Credentials Name HSMonDemand_Creds_01	
Name 🔶 Client ID		
	Cancel	
gemalto* Powered by SafeNet Data Protection on Demand	Terms of Service Priva	cy Policy Help & Documentation System Status © 2019 Gemalto NV

4. Click "Close".

gemalto*		Application Owner
Services Credentials	Generate Service Credentials	
My Services > DPPC-QA1	Review Permissions 2 Summary Step 2 : Here are your service credentials. The Client ID will be stored here and in the Credentials section.	
Service Name Service Type (Service Name DPPC-QA1	
DPPC-QA1 HSM on Demand 1	Credentials Name HSMonDemand_Creds_01	
Service Clients Credentials Search Aame Client D HSMonDemand_Creds_01 Ba8cdade-5bcc-48id-a72 HSMonDemand_Creds_01 Ba8cdade-5bcc-48id-a72	Please copy and save your Client Secret in a secure location; il will not be stored. Client D Client Secret Ba8cdade-5bcc-48fd-a729-e6a49a5163dd Client Client Secret Se	Phago Policy Help & Decomentation System Status 0.2019 Comulae MV

5. Ensure that the Credentials are created.

gemalto*	Application Owner
Services Credentials	
My Services > DPPC-QA1 Delete Service	
Configuration	
Service Name Service Type Created Partition Serial Non-FIPS Algorithms Number	
DPPC-QA1 HSM on Demand 13-Aug-2019 9:41 1285325034348 Yes	
Service Clients Credentials	
Search O Create Service Credentials	
Name Client ID Created Created By Actions	
HSMonDemand Creds_01 8e8cdade-5bcc-48fd-a729 (5) 16-Aug-2019 09:40 @digicert.com	
gemallo' Powered by SafeNet Data Protection on Demand	vacy Policy Help & Documentation System Status © 2019 Gemalto NV

Download Client as Application Owner

1. Select/Click on the Name under "My Services" (For example: DPPC-QA1).

gemalto [×]				Application Owner	@digicert.com 🗸 💡
Services Credentials					
My Services Add N	lew Service				
Search	٩				
Name	Service Type	Created	Actions		
DPPC-QA-PA-CloudHSM	HSM on Demand	1-Aug-2019 12:52	۵		
DPPC-QA1	HSM on Demand	13-Aug-2019 9:41			
DPPC-QA2	HSM on Demand	13-Aug-2019 15:53	ů		
gemalto" Powered by SafeNet Data Protection				Terms of Service Privacy Policy Help & Documentation	

2. Under "Actions" column, select "Download" to download the client.

gemalto [×]							Application Owner
Services	Credentials						
My Services	s > DPPC-QA1				Delete Service		
Configuration							
Service Name DPPC-QA1	Service Type HSM on Demand	Created 13-Aug-2019 9:41	Partition Serial Number 1285325034348	Non-FIPS Algorithms Yes			
Service Cl	ents Credentia	s					
Search	٩				New Service Client		
Name	Created	Ву	•	Created	Actions		
DPPC-QA1	-	@digicert.co	om	13-Aug-2019 9:41	Download Delete Client		
cemalto' Powered by	SafeNet Data Protection on Demand					Terms of Service Privac	y Policy Help & Documentation System Status © 2019 Gemaito N

3. This will take several seconds to prepare the client for download.

gemalto [*]		Application Owner
Services Credentials	Preparing Service Client	
My Services > DPPC-QA1	Delete Service	
Configuration		
Service Name Service Type Created Partitio Numbe DPPC-QA1 HSM on Demand 13-Aug-2019 9:41 128532		
DPPC-UAT Hom on Demand 13-Aug-2019 3:41 126632	5034345 165	
Service Clients Credentials		
Search D	New Service Client	
Name 🚖 Created By	Created	
DPPC-QA1 @digicert.com	13-Aug-2019 9:41	
gemalto* Powered by SafeNet Data Protection on Demand		Terms of Service Privacy Policy Help & Documentation System Status © 2019 Gemaito NV

4. Click on "Download Client" and then save it.

gemallo [*] Services C My Services >	redentials DPPC-QA1		Use the bu	ient is ready. uton below to download your client. bad Client Cancel			Application Owner	.@digicert.com 🖌 🦉
Configuration Service Name DPPC-QA1	Service Type	Created 13-Aug-2019 9:41	Partition Serial Number 1285325034348	Non-FIPS Algorithms Yes				
Service Client	s Credentials	3			New Service Client			
Name DPPC-QA1	Created B	У @digicert.co		Created 13-Aug-2019 9:41	Actions			
gemalto" Powered by SafeNe	et Data Protection on Demand					Terms of Service P	rivacy Policy Help & Documentation	System Status © 2019 Gemaito N

NOTE: Ensure that you Install/Configure the client that is downloaded in previous step i.e. (Step 4) and ignore the client that was downloaded earlier.

Install Service Client for Windows

The Windows service client installation uses a .zip file to deliver the HSM on Demand (HSMoD) service client materials required for configuring your system's connection to the HSMoD service. The service client .zip includes a pre-configured crystoki-template.ini file along with a client archive file containing a set of library and binary files. Complete the following procedures to access your HSMoD service from a Windows operating system.

1. Extract the downloaded archive file.

Using the Windows GUI or an unzip tool, unzip the file. The extracted files are as follows:

01/31/2020 01/31/2020		-	Chrystoki.conf crystoki-template.ini
01/31/2020	05:56 AM		cvclient-min.tar
01/31/2020	05:56 AM	7,577,395	cvclient-min.zip
01/31/2020	05:56 AM	176,008	EULA.zip
01/31/2020	05:56 AM	7,709	partition-ca-certificate.pem
01/31/2020	05:56 AM	1,387	partition-certificate.pem
01/31/2020	05:56 AM	6,690	<pre>server-certificate.pem</pre>

2. Extract the cvclient-min-zip file.

Using the Windows GUI or an unzip tool, unzip the file at the same folder. The extracted files are as follows:

02/12/2020	04:51 PM	<dir></dir>	cert
02/12/2020	04:51 PM	<dir></dir>	csp

02/12/2020	04:51	PM	<dir></dir>	ksp
02/12/2020	04:51	PM	<dir></dir>	plugins
01/31/2020	05:56	AM	1,147	Chrystoki.conf
10/04/2019	02:09	PM	377,704	ckdemo.exe
10/04/2019	02:09	PM	1,736,040	cmu.exe
10/04/2019	02:09	PM	3,958,120	cryptoki.dll
01/31/2020	05:56	AM	906	crystoki-template.ini
01/31/2020	05:56	AM	26,593,280	cvclient-min.tar
01/31/2020	05:56	AM	7,577,395	cvclient-min.zip
01/31/2020	05:56	AM	176,008	EULA.zip
10/04/2019	02:09	PM	170,856	LunaAPI.dll
10/04/2019	02:09	PM	3,482,472	lunacm.exe
10/04/2019	02:09	PM	613,205	LunaProvider.jar
10/04/2019	02:09	PM	463,720	multitoken.exe
10/04/2019	02:09	PM	7,145	openssl.cnf
01/31/2020	05:56	AM	7,709	partition-ca-certificate.pem
01/31/2020	05:56	AM	1,387	partition-certificate.pem
10/04/2019	02:09	PM	162,152	SafeNetKSP.dll
01/31/2020	05:56	AM	6,690	server-certificate.pem
10/04/2019	02:09	PM	189	setenv.cmd
10/04/2019	02:09	PM	26,087	setenv.ps1
10/04/2019	02:09	PM	2,148,712	vtl.exe

NOTE: Extract the cvclient-min.zip within the directory you created in the previous step. Do not extract to a new cvclient-min.zip directory. This location is required for the setenv command in the next step.

Please remove "crystoki.ini" if it exists before moving to next.

3. Set the environment variable.

Open "**Command Prompt**" as Administrator, then move to the directory where the cvclient-min file has been extracted and run the following command:

```
> setenv.cmd
Generated C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\crystoki.ini
```

The crystoki.ini is as follows:

```
[Chrystoki2]
LibNT="C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\cryptoki.dll"
LibNT32="C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\cryptoki.dll"
```

```
[CardReader]
RemoteCommand=1
```

[Luna] DefaultTimeOut=5000 PEDTimeout1=100000 PEDTimeout2=200000 PEDTimeout3=20000 KeypairGenTimeOut=2700000 CloningCommandTimeOut=300000

```
CommandTimeoutPedSet=720000
[Presentation]
ShowEmptySlots=no
[Misc]
PE1746Enabled=1
ToolsDir="C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\"
[XTC]
PartitionCAPath="C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\partition-ca-
certificate.pem"
PartitionCertPath00="C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\partition-
certificate.pem"
Enabled=1
TimeoutSec=10
[LunaSA Client]
SSLConfigFile="C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\openssl.cnf"
ReceiveTimeout=20
TCPKeepAlive=1
NetClient=1
ServerCAFile="C:\Users\test\CloudHSM\setup-DPPC-
CloudHSM\cert\server\CAFile.pem"
ClientCertFile="C:\Users\test\CloudHSM\setup-DPPC-
CloudHSM\cert\client\ClientNameCert.pem"
ClientPrivKeyFile="C:\Users\test\CloudHSM\setup-DPPC-
CloudHSM\cert\client\ClientNameKey.pem"
[REST]
RestClient=1
ClientTimeoutSec=120
ClientPoolSize=32
ClientEofRetryCount=15
ClientConnectRetryCount=900
ClientConnectIntervalMs=1000
PartitionData00=1285325032737, na.hsm.dpondemand.io, 443
SSLClientSideVerifyFile="C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\server-
certificate.pem"
```

NOTE: At that time, "ChrystokiConfigurationPath" will set on this directory.

The "crystoki.ini" file will be generated.

4. Start LunaCM.

Start LunaCM. From the directory where you unzipped the cvclient-min.zip file, execute **lunacm.exe**. If the command executes with no errors, your connection is working correctly.

```
>lunacm.exe
lunacm.exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights
reserved.
      Available HSMs:
      Slot Id ->
                              3
      Label ->
      Serial Number ->
                              1285325034359
      Model ->
                              Cryptovisor7
                              7.3.0
      Firmware Version ->
      CV Firmware Version -> 1.3.0
      Configuration ->
                              Luna User Partition With SO (PW) Signing With
Cloning Mode
      Slot Description ->
                              Net Token Slot
                              FM Not Supported
      FM HW Status ->
      Current Slot Id: 3
```

NOTE: If you use proxy server, you need to set environment variable of https_proxy as follows;

> set https_proxy=http://<proxy-server>/<port>

Configure LunaClient

Initialize the partition and users

1. Set the active slot.

Select the uninitialized application partition.

lunacm:> slot set -slot 3
Current Slot Id: 3 (Luna User Slot 7.3.0 (PW) Signing With Cloning Mode)
Command Result : No Error

NOTE: You can verify the slot number by executing "slot list" in lunacm.

2. Initialize the application partition.

Create a partition for the Security Officer (SO), set the initial password, domain name for cloning purposes, and respond to the prompts:

```
lunacm:> partition init -label DPPC-QA
Enter password for Partition SO: *******
Re-enter password for Partition SO: *******
You are about to initialize the partition.
All contents of the partition will be destroyed.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
Neither option -domain nor -defaultdomain nor -importpeddomain was
specified.
One is required.
Enter the domain name: *****
Re-enter the domain name: *****
Command Result : No Error
```

NOTE: Label: DPPC-QA and Domain: DEVJP

3. Log in as Partition SO.

Run the following command to login into the partition as the Security Officer (SO) - you can use the shortcut "po".

lunacm:> role login -name po enter password: ******* Command Result : No Error

4. Initialize the Crypto Officer role and set the initial password.

Run the following command to initialize the Crypto Office (CO) role - you can use the shortcut "co":

lunacm:> role init -name co enter new password: ******* re-enter new password: ******* Command Result : No Error

5. Log out.

The Partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. You must log out to allow the Crypto Officer to login with the newly-set password.

lunacm:> role logout
Command Result : No Error

NOTE: Once the Crypto Officer logs in and changes the initial credential set by the Partition SO, applications using the CO's challenge secret/password can perform cryptographic operations in the partition. The Crypto Officer can create, modify and delete crypto objects within the partition, and use existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer but cannot modify them. The separation of roles is important in some security regimes and operational situations, and where you might be required to satisfy audit criteria for industry or government oversight.

6. Log in as the Crypto Officer.

lunacm:> role login -name co enter password: ******* Command Result : No Error

NOTE: The password for the Crypto Officer role is valid for the initial login only. You must change the initial password using the command role changepw during the initial login session, or a subsequent login. Failing to change the password will result in a CKR_PIN_EXPIRED error when you perform role-dependent actions.

7. If you have not already done so, change the initial password set by the Partition SO.

```
lunacm:> role changepw -name co
enter existing password: *******
enter new password: *******
re-enter new password: *******
Command Result : No Error
```

8. Create the Crypto User.

lunacm:> role init -name cu
 enter new password: *******
 re-enter new password: ********
Command Result : No Error

The Crypto User can now log in with the credentials provided by the Crypto Officer and change the initial password. The Crypto User can now use applications to perform cryptographic operations using keys and objects created in the partition by the Crypto Officer.

NOTE: The password for the Crypto User role is valid for the initial login only. The CU must change the initial password using the command role changepw during the initial login session, or a subsequent login. Failing to change the password will result in a CKR_PIN_EXPIRED error when they perform role-dependent actions.

9. Login as Crypt User.

```
lunacm:> role logout
Command Result : No Error
lunacm:> role login -name cu
enter password: ********
Command Result : No Error
```

10. Change the password for Crypto User.

```
lunacm:> role changepw -name cu
enter existing password: *******
enter new password: *******
re-enter new password: *******
Command Result : No Error
```

NOTE: The initial PIN should be changed.

Configure HA (High Availability)

NOTE: The feature does not support on DPoP Service but there are redundant systems with several LunaPCI on Gemalto backend. Therefore, it is not required to configure any HA group.

Configure CSP

For SafeNet CSP, the utility **register.exe** takes care of the registry. To configure CSP, open command prompt as Administrator and run the following commands.

Register CSP Library

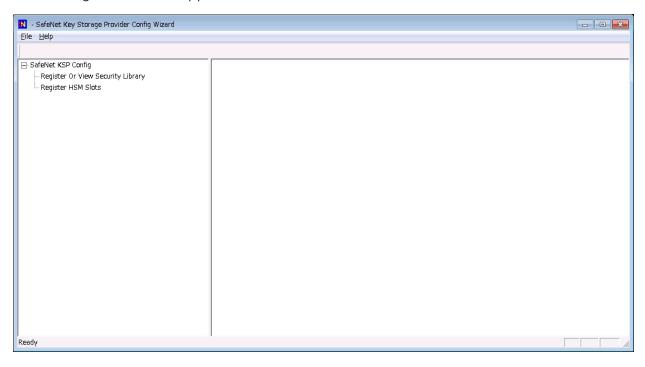
```
C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\csp>register.exe /library
register .exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights
reserved.
Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna
enhanced RSA and AES provider for Microsoft Windows !
Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna
Cryptographic Services for Microsoft Windows !
Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna
Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna
Schannel Cryptographic Services for Microsoft Windows !
```

Register the partition

```
C:\Users\test\CloudHSM\setup-DPPC-CloudHSM\csp>register.exe
register .exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights
reserved.
 *
 *
              Safenet LunaCSP, Partition Registration
 *
       Protect the HSM's challenge for the selected partitions.
       NOTE:
 *
            This is a WEAK protection of the challenge!!
 *
            After you have configured all applications that will use
            the LunaCSP, and ran them once, you MUST run:
               register /partition /strongprotect
            to strongly protect the registered challenges!!
 This procedure is a destructive procedure and will completely replace any
previous settings!!
Do you wish to continue?: [y/n]y
Do you want to register the partition named 'DPPC-QA'?[y/n]: y
Enter challenge for partition 'DPPC-QA' :*******
Success registering the ENCRYPTED challenge for partition 'DPPC-QA:3'.
Only the LunaCSP will be able to use this data!
Registered 1 partition(s) for use by the LunaCSP!
```

Configure KSP

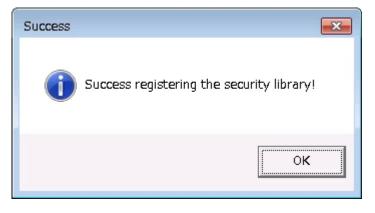
1. To configure KSP(CNG), run **KspConfig.exe**. Follow instructions for the use of the graphical KspConfig.exe as described in KSP for CNG in the SDK Reference Guide. The following window will appear:



2. Double-click **Register Or View Security Library**, then you can select the value is "<extracted-directory>\cryptoki.dll".

- SafeNet-Inc Key Storage Provider, Config Wiza	1	
ile <u>H</u> elp		
- SafeNet KSP Config - Register Or View Security Library		
Register HSM Slots	LibraryPath C:/Users\root(CloudHSM(SafeNet)\setup-DPPC-CloudHSM(cvclient-min)cryptoki.dll	
Register HSM Slots	Browse	Registe
	DIUMSE	Registe

3. Click on "Register" button, then you can see the message.



- 4. Double-click Register HSM Slots for Administrator/<Domain Name>
 - Select Administrator
 - Select <Domain Name>
 - Select the Group Name (DPPC-QA) for Available Slots
 - Enter Slot Password

5. Click Register Slot.

N	- SafeNet-Inc Key Storage Provider, Config Wizard	
<u>F</u> ile <u>H</u> elp		
□- SafeNet KSP Config □- Register Or View Security Library □ Register HSM Slots	Administrator Image: Constraint of the second descent	Register By
Ready		NUM

NOTE: When you click "Register Slot", there is no change, but this step is necessary.

- 6. When registering the Luna KSP (with the Luna KSPConfig utility), use the following user and domain combinations:
 - The user and domain performing these procedures.
 - The user and domain running the web application and using the private key.
 - The local user and NT Authority domain user.
 - The LocalSystem and NTAuthority of the system.

NOTE: If you implement the Autoenrollment server, you must also install and register the Luna CSP. Refer to the Luna product documentation for details.

Generate CSR and Install Certificate

1. Create the information file for CSR.

To generate CSR through certreq.exe via **CSP**, the ProviderName must be "**Luna Cryptographic Services for Microsoft Windows**". A sample inf file is shown below:

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "Luna Cryptographic Services for Microsoft Windows"
ProviderType = 1
Subject = "CN=Registration Authority"
KeyContainer = "CSPRA20190717"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

To generate CSR through certreq.exe via **KSP**, the ProviderName must be "**SafeNet Key Storage Provider**". A sample inf file is shown below:

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "SafeNet Key Storage Provider"
ProviderType = 0
Subject = "CN=Registration Authority"
KeyContainer = "KSPRA20190717"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
KeyUsage = 0xf0
```

2. Generate CSR through HSM.

Open command prompt as Administrator and run the following command. <inf-file> is the file created at **Step 1**, <csr-file> is an output file.

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

Then the CSR file will be generated as follows:

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

NOTE: When the following error message is displayed, SafeNetKSP.dll must be copied to c:\Windows\System32.

Certificate Request Processor: The system cannot find the file specified. 0x80070002 (WIN32: 2 ERROR_FILE_NOT_FOUND)

3. Get RA Certificate

See "Get RA Certificate in PKI-Manager".

4. Install a certificate.

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

> certreq -accept <issued-cert>

Before running the command, 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)
```

Integration for Java Environment

Register Luna Provider

You must update the **java.security** configuration file to use the SafeNet security providers and the HSM on Demand Service.

To configure the java.security file:

- 1. Open the Java security configuration file **java.security** in a text editor. The file is available at <JDK_installation_directory>\jre\lib\security.
- 2. Update the Luna Providers in the **java.security** file so they appear as follows:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
security.provider.7=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.8=sun.security.smartcardio.SunPCSC
security.provider.9=com.safenetinc.luna.provider.LunaProvider
```

3. Save the changes to the java.security file.

Enabling the HSM on Demand Service keystore

You must configure the Java Code Signing utility to use the keystore located on the HSM on Demand Service.

To enable the HSM on Demand Service keystore

- Copy the LunaAPI.dll and the LunaProvider.jar files from the <Luna_installation_directory> to the Java extension folder located at <JDK_installation_directory>\jre\lib\ext.
- 2. Set the environment variables for JAVA_HOME and PATH.

NOTE: We recommend setting the PATH variable in Windows environments using the System Environments menu.

Install RA Certificate

Refer section "Using an RA Certificate on HSM" of DigiCert® PKI Enterprise Gateway Deployment Guide document

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 statu	JS	
Last updated: Jul 19, 2019 12:58 AM Refresh	The DigiCert PKI Platform 8.19 release includes:	Status: OK		
All	Rebranding from Symantec to DigiCert Email domain validation for SMME certificates via DCV (Domain Control Validation) process	Next service r	enewal: Ma	y 2, 2020
Recent activity Action Date	 Support for Microsoft Intune to issue Client Authentication certificates via SCEP enrollment flow Enterprise Gateway and Autoenrolment Server support for SafeNet Luna Network HSM 7 (FIPS and non-FIPS Mode, Cloning and Export Mode) and 			
Certificate profile created Jul 18, 2019	nShield Connect HSM Windows Server 2016 support for Enterprise Gateway, Autoenrollment Server and Local Key Management Service (LKMS)			
Certificate profile deleted Jul 18, 2019	PRICtient 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	Reiroval of Adobe Individual, Adobe Organization and Adobe CDS Certificate templates Bug fixes			
Certificate profile created Jul 18, 2019		1		_
Certificate for user revo Jul 18, 2019	Certificate history Seat activity			
Certificate for user revo Jul 18, 2019	All certificate profiles All certificate profiles V			
Certificate profile deleted Jul 18, 2019	2.5			
	2			
		Seat usage		
	1.5	Refresh Seat pool	Used	Purchased
	ates 1.5	2	0.500	Turonasca
	Certificates	User	46	1000
		• .		
		Device		
	0.5	10		
		Server	8	10
		' #		
	0 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18 Jul — Certificates issued — Certificates revoked	Organization Buy more seats		
		buy more seats		
	1 week 1 month 3 months 6 months 1 year All			
	🕘 📑 🔐 🛜 JHF 🕸 -			

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



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 Wet communications between your client and the Web Serv		ust install an RA certi	ficate to secure
If you are not setting up these services, or have already process.	gotten your RA ce	rtificate, you do not n	eed to complete this
Enter Certificate Signing Request (CSR)			
Ask your server administrator to generate a CSR for you according to the instructions in the installation guide for		our administrator mu	st generate the CSR
You can access the resources page by clicking on the	icon on the d	ashboard.	
*Paste your CSR:			
Important Service Requirements: If you discover or have reast you must immediately revoke the certificate or notify the issuin or your organization name has changed, please notify the issu gour certificate at any time without note of (i) you fait be perfo (ii) in the issuing center's sole discretion, you have engaged in systems. Enter a certificate friendly name:	g center to do so. S ing center. Note tha rm your obligations	imilarly, if the information t the issuing center reta under the terms of your	n within your certificate ins the right to revoke service agreement; or
you must immediately revoke the certificate or notify the issue or your organization name has changed, plasse notify the issue your certificate at any time without notice if (i) you tails operfor (ii) in the issuing center's sole discretion, you have engaged in systems. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate renew	g center to do so. S ing center: Note that my our obligations activities which the val information. If 1	imilarly, if the informatio the issuing center reta under the terms of your issuing center determine issuing center determine you would like to char	n wehn your certificate ins the right to revoke service agreement, or nes are harmful to its
you must immediately revoke the certificate or notify the issuin or your organization name has changed, please notify the issu- your certificate at any time without notice if (i) you fail to perfo (ii) in the issuing center's sole discretion, you have engaged in systems.	g center to do so. S ing center: Note that my our obligations activities which the val information. If 1	imilarly, if the informatio the issuing center reta under the terms of your issuing center determine issuing center determine you would like to char	n wehn your certificate ins the right to revoke service agreement, or nes are harmful to its
you must immediately revoke the certificate or notify the issue or your organization name has changed, plasse notify the issue your certificate at any time without notice if (i) you tails operfor (ii) in the issuing center's sole discretion, you have engaged in systems. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate renew	g center to do so. S ing center: Note that my our obligations activities which the val information. If 1	imilarly, if the informatio the issuing center reta under the terms of your issuing center determine issuing center determine you would like to char	n wehn your certificate ins the right to revoke service agreement, or nes are harmful to its
you must immediately revoke the certificate or notify the issue or your organization name has changed, please notify the issue your certificate at any time without notice if (i) you fail to perfor (ii) in the issuing center's sole discretion, you have engaged in systems. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate renew the menu and select Manage account and sub-account	g center to do so. S ing center: Note that my our obligations activities which the val information. If 1	imilarly, if the informatio the issuing center reta under the terms of your issuing center determine issuing center determine you would like to char	n wehn your certificate ins the right to revoke service agreement, or nes are harmful to its

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.

d	ligicert
	Your RA certificate is ready Your RA certificate must be installed on the server where your PKI Enterprise Gateway or PKI Web Services is installed.
	Install your RA certificate
	1. Download your RA certificate.
	Issued to:
	Expiration date: Jul 18, 2020
	File format: PKCS #7
	Download
	2. Forward the RA certificate to your server administrator. Your administrator must follow the instructions in the installation guide for your service. You can download the appropriate installation guide from the
	resources page by clicking on the 🌍 icon on the dashboard.
	Done
	egal Notices Privacy opyright © 2019 DigiCert Inc. All rights reserved.

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