DigiCert[®] Trust Lifecycle Manager

HSM installation and configuration for SafeNet

Version 1.2 December 14, 2022



Legal Notice

Copyright © 2022 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Other names may be trademarks of their respective owners.

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

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

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

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

Table of Contents

INTRODUCTION	4
REVISION HISTORY	4
SUPPORTED HSMS	4
SAFENET NETWORK HSM	5
INSTALL LUNA HSM CLIENT	6
CONFIGURE LUNA HSM CLIENT	8
CONFIGURE HA (HIGH AVAILABILITY)	10
CONFIGURE CSP	12
CONFIGURE KSP	13
GENERATE CSR	17
SAFENET DPOD CLOUD HSM	
INSTALL LUNACLIENT	18
Add a Subscriber Group as Tenant Administrator	18
ADD AN APPLICATION OWNER AS TENANT ADMINISTRATOR	21
ADD ADMINISTRATOR AS TENANT ADMINISTRATOR	22
ENABLE LUNA CLOUD HSM SERVICES AS TENANT ADMINISTRATOR	23
ADD NEW SERVICES AND SERVICE CLIENT AS APPLICATION OWNER	23
CREATE SERVICE CREDENTIALS AS APPLICATION OWNER	27
INSTALL SERVICE CLIENT FOR WINDOWS	29
CONFIGURE LUNACLIENT	
INITIALIZE THE PARTITION AND USERS	32
CONFIGURE HA (HIGH AVAILABILITY)	35

CONFIGURE CSP	35
CONFIGURE KSP	36
GENERATE CSR AND INSTALL CERTIFICATE	

ADD USER/DEVICE SEAT
UPLOAD CLIENT AUTHENTICATION CERTIFICATE
INSTALL RA CERTIFICATE

Introduction

This document describes the installation and configuration steps for SafeNet Network HSMs to be used by the DigiCert Autoenrollment Server.

Revision History

No.	Date	Summary
1.	3 August, 2022	Version 1 published.
2.	12 October, 2022	Added support for SafeNet Data Protection On Demand (DPoD) Cloud HSM
3.	14 December, 2022	Added support for "Luna HSM Client 10.5.0"

Supported HSMs

HSM Type	Client Version	Software Version	Firmware Version
SafeNet Network HSM	10.5.0-470	7.2.0	7.0.3
SafeNet DPoD Cloud HSM	10.5.0-470	7.3.0	Firmware Version -> 7.3.0 CV Firmware Version -> 1.5.0 Plugin Version -> Cloud 2.2.0- 740

SafeNet Network HSM

The SafeNet Network HSM 7 (formerly known as Luna SA) is a network HSM which allows users to create a partition to store a key, such as the RA key required to strongly authenticate to the DigiCert[®] Trust Lifecycle Manager. 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, use the Luna HSM Client through Network Trust Link Service (NTLS).



Install Luna HSM Client

Follow the steps below to install the Luna HSM Client software on the client machine:

1. Run LunaHSMClient.exe as Administrator.

Luna HS Version: 10.5.0.470	SM Client	gemalto security to be free
Welcome to This setup wizard install below. Install location: C:\Program Files	to the Luna HSM (d will install Luna HSM Client s\SafeNet\LunaClient	Client setup wizard t on your computer. Please customize the Select folder
Install options:	Luna Devices Select All Network PCIe 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 re License Agreement:
		INSTALL QUIT

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 (optional features depend on your environment):

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

Luna HS Version: 10.5.0.470	M Client	ge	security to be free
Welcome t This setup wizard install below. Install location: C:\Program Files	o the Luna HSM (will install Luna HSM Clien	Client setup wiz	zard ase customize the Select folder
Install options:	Luna Devices Select All Image: PCle USB Backup Remote PED	Features Select All ✓ CSP (CAPI) ✓ JCE / JCA PI ✓ PKCS #11 (J Software SE SNMP Suba FM Tools FM SDK	/ KSP (CNG) rovider (JSP) ICProv) DK agent
✓ I agree to the	terms of the <u>Thales Softwa</u>	INSTALL QUIT	

Check the Software License Agreement, and then select **INSTALL**.

3. Wait for completion. The progress bar is displayed at the bottom of the window.

Luna HS Version: 10.5.0.470	M Client	ge	security to be free
Welcome t This setup wizarc install below. Install location:	to the Luna HSM (I will install Luna HSM Clien	Client setup wiz t on your computer. Ple	zard ase customize the
C:\Program Files	\SafeNet\LunaClient		Select folder
Install options:	Luna Devices Select All Vetwork PCle USB Backup Remote PED	Features Select All JCE / JCA PI PKCS #11 (. Software SI SNMP Suba FM Tools FM SDK	/ KSP (CNG) rovider (JSP) JCProv) DK agent
✓ I agree to the	e terms of the <u>Thales Softwa</u>	are License Agreement.	
1: 2 2: 1		INSTALL	

4. Once the installation is complete, select **OK**. The **UNINSTALL** and **MODIFY** button is displayed. Select **QUIT**.

Luna HS Version: 10.5.0.470	M Client	gemalto security to be free
Welcome t This setup wizard install below. Install location: C:\Program Files	o the Luna HSM (will install Luna HSM Clien \SafeNet\LunaClient\	Client setup wizard t on your computer. Please customize the
Install options:	Luna Devices Select All Vetwork PCIe 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 listed below, a partition must be created. This is referred to as **<PARTITION-NAME>** throughout this document.

Follow these steps to configure the Luna HSM Client:

1. Open a Command Prompt window 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, proceed to step 4.

```
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) v10.5.0-470. Copyright (c) 2022 SafeNet. All rights reserved. Slot Id -> 1 Label -> <PARTITION-NAME> Serial Number -> 1314971349473 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 H Status -> FM Ready Current Slot Id: 1 lunacm:> clientconfig v

The following Luna SA Slots/Partitions were found:

Slot	Serial #	Label
====	=================	=====
1	1314971349473	<partition-name></partition-name>

Command Result : No Error

- 3. If you do not want to follow the one step setup (Step 2 above), follow these steps:
 - a) Obtain the Server certificate.

The Server certificate has been created on the HSM, so it needs to be copied from the server.

- > pscp -scp admin@<SERVER-HOSTNAME>:server.pem
- b) Add a 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%
```

Next, 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:

4. Confirm connection settings.

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

 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 a Command Prompt window 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) v10.5.0-470. Copyright (c) 2022 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"

lunacm:> slot set -s <HA-SLOT-NO> Current Slot Id: <HA-SLOT-NO> (Virtual HSM 7.0.3 (PED) Signing With Cloning Mode) Command Result : No Error lunacm:> hagroup ho -e "HA Only" has been enabled. Command Result : No Error lunacm:> hagroup ho -s
 This system is configured to show only HA slots. (HA Only is
enabled)
Command Result : No Error

Configure CSP

Note: 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 window and run the following commands:

Register CSP Library

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

register.exe (64-bit) v10.5.0-470. Copyright (c) 2022 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 SChannel Cryptographic Services for Microsoft Windows.

Register the partition

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

register.exe (64-bit) v10.5.0-470. Copyright (c) 2022 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

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) v10.5.0-470. Copyright (c) 2022 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

To configure KSP (CNG), run KspConfig.exe (the 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	
E-SafeNet KSP Config	
- Register Or View Security Library	
Register HSM Slots	
Ready	

Double-click **Register Or View Security Library**, 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 C\Program FilestSafeNettLunaClienttcryptokl.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

Select Register Slot.

- SafeNet Key Storage Provider Config W	lizard		- 🗆 X
<u>File</u> Help			
SafeNet KSP Config Register Or View Security Library Register HSM Slots	Administrator Available Stots 1 HAGroup	Image: PKIDEV2016 Slot Password	Register By Stot Label Stot Number
			Register Slot
	Registered Slots		View Registered Slots
	SlotLabel:HAGroup		
			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

Select Register Slot.

IN - SafeNet Key Storage Provider Config W <u>File</u> <u>H</u> elp	fizard		X
SafeNet KSP Config Register Or View Security Library	SYSTEM		Register By
Register HSM Slots	Available Slots	Slot Password	Glot Laber
	1 HAGroup		C Slot Number
			Register Slot
	Registered Slots		View Registered Slots
	SlotLabel:HAGroup		
			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

 Create the information file for the CSR. To generate the CSR using certreq.exe through CSP, the ProviderName must be "Luna Cryptographic Services for Microsoft Windows". The .inf file looks as follows:

```
[NewRequest]
KeyUsageProperty = "NCRYPT_ALLOW_ALL_USAGES"
RequestType = PKCS10
ProviderName = "Luna Cryptographic Services for Microsoft Windows"
ProviderType = 1
Subject = "CN=Registration Authority"
KeyContainer = "CSPRA20220725"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

2. Generate the CSR through HSM.

Note: <inf-file> is the file created in 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. Get a client authentication certificate

Refer section Get a client authentication certificate

4. Install RA certificate

Refer section Install RA certificate

Refer to the "Configure the Autoenrollment Server" section of the DigiCert® Autoenrollment Server Deployment Guide in this KB article for more information.

SafeNet DPoD Cloud HSM

The SafeNet DPoD (**Data Protection on Demand**) service provides "HSM on Demand" which is one of HSM's 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 "¹ icon on your site on SafeNet DPoD Service, to avail the guide.

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 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.

THALES Developer Account Accounts Service	s Reports Credentials	Town A clinical and the second
Users Subscriber Groups		
Add a User		
Application Owner Providers and consumes Service on and washable by Administrator users.	Administrator Manages Subacober Graups, User, Reys Service Reports and configures the Morkeplace for Application Owner suers.	Ø
You are using a free, 30 day evaluation version of Thales Data Protection on Demand.	Become a subscriber now	

2. Select Subscriber Groups followed by Subscriber Group tile.

THALES Developer Account	Services Reports Credentials	remet Administrative remet Administrative
Users Subscriber C	iroups	
Add a Subscriber Group		
Subscriber Group Group Users according to yo organizational needs, and control access to user- generated key material.	ur	0
You are using a free, 30 day evaluation version of Thales Data Protection or	Demand. Become a subscriber now	
THALES Powered by Thales Data Protection on Demand		Terms of Service Privacy Policy Help & Documentation System Status @ 2022 Thales Group

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.

THALES Developer Accounts Services	Reports Credentials	Provent Administration Terrort Administrator Provent Administrator
Users Subscriber Groups	Add Subscriber Group Group Name Description (optional)	ents Actions
Add a Subscriber Group Subscriber Group Group Users according to your organizational needs, and generated key material.	Add Cancel	
You are using a free, 30 day evaluation version of Thales Data Protection on Demand.	Become a subscriber now	
THALES Powered by Thales Data Protection on Demand		Terms of Service Privacy Policy Help & Documentation System Status © 2022 Thales Group

4. The designated group has been created.

	THALES Developer Accounts Services Reports Credentials	Transe Administrative Tomer Administrator
	Users Subscriber Groups	•
	DPPC-QA- P Name Description	No. Users No. Services No. Clients Actions
	DPPC-QA-PA DigiCert PKI Platform Client, QA Group on persistent account	
	Add a Subscriber Group	
	Group Users according to your organizational needs, and control access to user- generated key material.	
You are using a free, 30 day ev	aluation version of Thales Data Protection on Demand. Become a subscriber now	
THALES Powered by Thales	Data Protection on Demand	Terms of Service Privacy Policy Help & Documentation System Status @ 2022 Thales Group

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

	THALES Developer Account	Accounts	Services	Reports	Credentials		Tenant Administrator	Ədigicert.com	Ť	
	Subscriber Gro	oups > DPP	C-QA-PA					Delete Subscriber	Group	
	Name DPPC-QA-PA								ď	
	Description DigiCert PKI Platform	n Client, QA Group or	n persistent acco	unt						0
	Users S	ervices								
	Search	ې	2							
	Email Address	@digicart or				First Name	Last Name	Activ	ons	
		energine (usilgice) Loc	<u>an</u>			, erageparan	1 – 1 of 1		>	
You are using a free, 30 day eva	uluation version of Thales	Data Protection on I	Demand.	Become a subsi	criber now					
THALES Powered by Thales	Data Protection on Demand						Terms of Service Privacy Po	olicy Help & Docum	entation S	System Status © 2022 Thales Group

Add an Application Owner as Tenant Administrator

1. Sign in to DPoD site using your Tenant Administrator credential. Select **Accounts** tab and Select **Users** and Select **Application Owner**, under **Add a User**.

THALES Developer Accounts Services	; Reports Credentials	mentelahlendigen@utiginementeen Torust Administrator attackationeteeneeneeneeneeneeneeneeneeneeneeneene
Users Subscriber Groups		
Add a User		
Application Owner Provisions and concurse Services mate whilehe by Administrator users.	Administrator Manages Subscriber Groups, Users, Koys, Sarvice Reports and configures the Marletplace for Application Owner users.	0
You are using a free, 30 day evaluation version of Thales Data Protection on Demand.	Become a subscriber now	
THALES Powered by Theles Data Protection on Demand		Terms of Service Privacy Policy Help & Documentation System Status © 2022 Thales Group

2. Fill out the form with the user details and then click Add User.

THALES Developer Account Accounts Services	Reports Credentials	ment Administration
Users Subscriber Groups	Add Application Owner Subscriber Group DPPC-QA-PA First Name Last Name Cmail Address Create Password Create Pa	Created By Actions
Application Owner Provision and consumes Service and available by administrator sizes.	Or Application Owner users.	
You are using a free, 30 day evaluation version of Thales Data Protection on Demand.	Become a subscriber now	

3. The user has been created.

Users	Subscriber Group	IS					
Email Addre	P	Role	Subscriber Group	First Name	Last Name	Created By	Actions
	@digicert.com	Application Owner	DPPC-QA-PA	Venegopoien	Dermoderen	pundalik.badiger@digicert.com	
						1-1of1 <	< > >1
Add a Us	er						
	Application Owner Provisions and consumes Services made available by Administrator users.	Adminis Manages Users, Key and config for Applic	strator Subscriber Groups, /e, Service Reports jures the Marketplace ation Owner users.				

Add Administrator as Tenant Administrator

1. Sign in DPoD site and Select Accounts tab and select Users and select Administrator, under Add a User.

Crevelager Accounts Service	s Reports Credentials	sendelikiesigen (Subjectiven)
Users Subscriber Groups		
Add a User		
Application Owner Provisions and consumes Services make available by Achtelameter users.	Administrator Manages Subscriber Groups, Users, Knyck, Sankor Reports and configures the Marketplace for Application Ower user.	٥
You are using a free, 30 day evaluation version of Thales Data Protection on Demand.	Become a subscriber now	
THALES Powered by Thales Data Protection on Demand		Terms of Service Privacy Policy Help & Documentation System Status © 2022 Thales Group

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

THALES Developer Account Accounts Services	Reports Credentials	pendelblakadiga @diglert.com Toract Administratic
Users Subscriber Groups	Add Administrator First Name	
u P Email Address Role School	Email Address Create Password Confirm Password	Created By Actives 0 of 0 { < > >
Add a User Application Owner Protocom make operative Service make operative Protocom make op	AddUber Cancel Addiministrator Monges Solonzier Group, Uner, Rays, Brance Reparts for Advanced Uner canon. for Advanced Uner canon.	
You are using a free, 30 day evaluation version of Thales Data Protection on Demand.	Become a subscriber now	

3. The Administrator has been created.

pun , D Email Address Role Subscriber Group	First Name Last Name Created By	Actions
Application Owner DPPC-QA-PA	Veryophere Considered participation @digicert.com	
and a contract of the contract	Fondulik Godiger Jameguldinsjima@digicert.com	
Hyteohofimme@digicertdemo.com Administrator Default	Hyles Hoffman pundailabadiger@digicert.com	
	1 – 3 of 3	>>1
Add a User		

Enable Luna Cloud HSM Services as Tenant Administrator

- 1. Select Services tab then click on Configure Services.
- 2. Under the Luna Cloud HSM service tile (Set up and access a Cloud HSM service for your organization's cryptographic operations), click the toggle to enable service.



Add New Services and Service Client as Application Owner

1. Sign in as an Application Owner and then select Add New Service and click on +TRY SERVICE under the Luna Cloud HSM service tile.



• Step 1: Service Information.

Click Next (By clicking 'Next' you agree to the *Trial Terms of Service*)

THALES	Services Credentials	Application Owner
	Add Luna Cloud HSM Service O Service Information O Configure Service	- 3 Summary
Set up and access a Clo		Code Signer
service for your organiza cryptographic operations More Info	By clicking 'Next' you agree to the Trial Terms of Service	ate and protect the private isociated with your Java Signer application in an
		into
+ TRY SERVICE		SERVICE
Microsoft		7
Luna Cloud HSM f		Cloud HSM for PKI
Microsoft ADCS		ite Key Protection
Secure the keys of your 1 Root Certificate Authorit an HSM.		e private keys belonging to cate Authorities notible for estabilishing PKI
More Info		lierarchy.
	Cancel	Next
+ TDV CEDVICE		SEDVICE

• Step 2: Configure Service.

Enter Service Name and check if you wish to opt for Remove FIPS restrictions, and then click Next.

THALES Beveloper Account	Services Credentials	
Luna Cloud HSM Bet up and access a Cit service for your organiz cryptographic operation More Info	Add Luna Cloud HSM Service	
+ TRY SERVICE	Remove FIPS restrictions	
Luna Cloud HSM 1 Microsoft ADCS	ft Cloud HSM for PKI the Key Protection	
Secure the keys of your Root Certificate Authort an HSM. More Info	e him e private keya belonging to cate Authorities naile for exabilising PKI elevant	
	Cancel Go Back Next	
+ TDV CEDVICE THALES Powered by Thales Data Protection on Demand	Terms of Service Privacy Policy Help & Documentation System Statu	is @ 2022 Thales Group

• Step 3: Summary

Confirm your Service Name and click Finish.

THALES Developer Account	Services Credentials	Application Owner	and and a construction and a con
Luna Cloud HSM	Add Luna Cloud HSM Service Service Information C C	onfigure Service 3 Summary	K wa i Cloud HSM for . Code Signer
service for your organiza cryptographic operation More info	Service Name	DPoD-QA	ate and protect the private esociated with your Java Signer application in an
* TRY SERVICE			into
Microsoft			7
Luna Cloud HSM f Microsoft ADCS			Cloud HSM for PKI Ite Key Protection
Secure the keys of your Root Certificate Authorit an HSM.			e private keys belonging to oate Authonities wable for establishing PKI incremby
More info	Cancel	Go Back Finish	Info

2. It takes several seconds for processing.

THALES	Services Credentials		Applean	on Owner	
My Service	es Add Service	Preparing Service			
Luna Cloud HSM 5	Services				
Luna Cloud HSN. Set op and access of across by your organization opposit Work into	A Cloud HSM Crown Cover Short Profilement Cover Short Profilement Short Profilement Short Profilement Short Profilement More into • Tary SERVICE	Europe Constraints of the constraint of the constraints of the constra	Euro Cloud HSM for Hyperfedger Brote biolochain tensactions before the regarded crystopractic generative acception to distributed system. Nors info + TRY SERVICE	java Luna Cloud HSM for Java Code Signer Grane and protect the pinet base Signer applications in an State. More liste	0
Minusi Luna Cloud HSN	A for Luna Cloud HSM for	SQL Server Luna Cloud HSM for	Luna Cloud HSM for	Luna Cloud HSM for PKI	

3. Click Create Service Client.

Service Name DPoD-QA	Service Type Luna Cloud HSM	Created 16-Aug-2022 13:50	Partition Serial Number 1334054172625	FIPS Restrictions Enabled	
Service Clients	Credentials				
	Create	Add a clien a new service client to get sta and initialize yo	It to your service red. Follow the process to insti- ur service. Need help?	all your client	



4. Enter Service Client Name and then click Create Service Client.

5. It takes several seconds to process.

	THALES Developer Account				Application O	and a second s	
	My Services > DPo	D-QA	Preparin	g Service Client		Delete Service	
	Service Name DPoD-QA	Service Type Luna Cloud HSM	Created 16-Aug-2022 13:50	Partition Serial Number 1334054172625	FIPS Restrictions Enabled		Ø
	Service Clients	Credentials					
		Create a	Add a clien new service client to get sta and initialize yo	It to your service rted. Follow the process to inst ur service. <u>Need help?</u>	all your client		
THALES Powered by Thales 1	Data Protection on Demand			<u>.</u>	Terms of Service P	Wary Policy Help & Documentation Syst	em Status = 2022 Thales Group

6. 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 Credentials			and the second s	nagogodan alamadaran Ədigicert.com 🚽	
	My Services > DI	PoD-QA	Your client is real	ady. wnload your client.		Delete Service	l.
	Service Name DPoD-QA	Service Type Luna Cloud HSM	Download Client	Cancel 1334054172625	JS Restrictions Enabled		0
	Service Clients	Credentials					
	Search Create a Service Client to	P securely connect to a service				New Service Client	
	Name			Created By		Created Actions	
	DPoD-QA-Luna-Cloud-H	ISM				19-Aug-2022 13:36	
						0 of 0 < < > >	
THALES Powe	red by Thales Data Protection on Demand				Terms of Se	rvice Privacy Policy Help & Documentation	System Status @ 2022 Thales Group

Create Service Credentials as Application Owner

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

	THALES Developer Account Services C	redentials		2	Application Owner et ces if	ert.com 🚽	
	My Services Add Serv	ice					
	Search P	Samias Tune	Created	Constal Br		Astion	
	DPoD-QA-EGW1	Luna Cloud HSM	23-Jul-2021 19:42	@digicert.com	n	(iii)	Ø
	DPoD-QA DPoD-QA-EGW-Non-FIPS	Luna Cloud HSM Luna Cloud HSM	16-Aug-2022 13:50 29-Jul-2021 16:20	venegopelandemodenen@digicert.cor	n	0	
					1 - 3 of 3 < <)	> >1	
THALES Powered by Thales D	ata Protection on Demand			Terms	of Service Privacy Policy Help & Docure	mentation System Status © 2022 Thales G	1010

- Application Ow THALES Credentials Services My Services > DPoD-QA Service Name DPoD-QA Service Type Luna Cloud HSM Partition Serial Number 1334054172625 FIPS Restrictions Enabled Created 16-Aug-2022 13:50 ? Service Clients Credentials Q Create Service Credentials to access and consume services using the DPoD API. Created By Client ID Created At Name Actions 0 of 0 |< < > >| THALES Powered by Thales Data Protection on Demand ms of Service | Privacy Policy | Help & Docu ation | System Status | © 2022 Thales
- 2. Click on Credentials and then click on Create Service Credentials.

3. Click on Next.

THALE	Services Credentials	Application Owner	adaman@digicert.com 🚽	
My Service	Generate Service Credentials s > [1 Review Permissions	2 Summary	Delete Service	
Service Name DPoD-QA	These credentials will allow a client to perform the following operations on the service "DPoD-QA":			
Service (Create, regenerate & delete service clients Create, regenerate & delete service credentials			0
Search Create Service Name	Credent Credentials Name LunaCloudHSM_Creds_01		Service Credentials	
			к « > > г	
	Cancel	Next		
THALES Powered by Thales Data Protection on Dem	nt	Terms of Service Privacy Po	licy Help & Documentation System Status @ 2023	2 Thales Group

4. Click Close.

THALES Developer Account	Services Credentials	annalaan (adigicert.com) 🚽
My Services >	Generate Service Credentials Review Permissions 2 Summary	Delete Service
Service Name DPoD-QA	The Client ID will be stored here and in the Credentials table.	
Service Clien	Service Name DPoD-QA Credentials Name LunaCloudHSM_Creds_01	
	Please copy and save your Client Secret in a secure location; it will not be stored.	Service Credentials
Create Service Creder Name	Client ID Client Secret f1b92f9a-a6ab-4e3d-819d-9b3c7def559d Client Secret	Actions
LunaCloudHSM_Cre	d	(D)
	Close	
THALES Powered by Thales Data Protection on Demand	Terms of Service Privac	y Policy Help & Documentation System Status @ 3022 Thales Unup

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:

26-09-2022	05:48	1,327	Chrystoki.conf
26-09-2022	05:48	1,129	crystoki-template.ini
26-09-2022	05:48	30,289,920	cvclient-min.tar
26-09-2022	05:48	8,483,712	cvclient-min.zip
26-09-2022	05:48	187,032	EULA.zip
26-09-2022	05:48	8,176	<pre>partition-ca-certificate.pem</pre>
26-09-2022	05:48	1,387	partition-certificate.pem
26-09-2022	05:48	5,660	server-certificate.pem

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:

21:13	<dir></dir>	cert
21:13	<dir></dir>	csp
21:13	<dir></dir>	ksp
21:13	<dir></dir>	plugins
	21:13 21:13 21:13 21:13 21:13	21:13 <dir> 21:13 <dir> 21:13 <dir> 21:13 <dir> 21:13 <dir></dir></dir></dir></dir></dir>

26-07-2022	21:13	<dir></dir>	WindowsEventProvider
26-09-2022	05:48	1,327	Chrystoki.conf
26-07-2022	21:13	510,184	ckdemo.exe
26-07-2022	21:13	1,844,968	cmu.exe
26-07-2022	21:13	4,267,752	cryptoki.dll
26-09-2022	05:48	1,129	crystoki-template.ini
26-09-2022	05:48	30,289,920	cvclient-min.tar
26-09-2022	05:48	8,483,712	cvclient-min.zip
26-09-2022	05:48	187,032	EULA.zip
26-07-2022	21:13	212,200	LunaAPI.dll
26-07-2022	21:13	3,701,992	lunacm.exe
26-07-2022	21:13	697,965	LunaProvider.jar
26-07-2022	21:13	568,040	multitoken.exe
26-07-2022	21:13	7,145	openssl.cnf
26-09-2022	05:48	8,176	partition-ca-certificate.pem
26-09-2022	05:48	1,387	partition-certificate.pem
26-07-2022	21:13	194,280	SafeNetKSP.dll
26-09-2022	05:48	5,660	server-certificate.pem
26-07-2022	21:13	490	setenv.cmd
26-07-2022	21:13	32,155	setenv.ps1
26-07-2022	21:13	2,166,504	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
LunaG5Slots=0
```

[Luna] DefaultTimeOut=500000 PEDTimeout1=100000 PEDTimeout2=200000 PEDTimeout3=20000 KeypairGenTimeOut=2700000 CloningCommandTimeOut=300000

```
CommandTimeoutPedSet=720000
[Presentation]
ShowEmptySlots=no
[Misc]
PE1746Enabled=1
ToolsDir=C:\Program Files\SafeNet\LunaClient\
PluginModuleDir=C:\Users\Test\CloudHSM\setup-DPPC-CloudHSM\plugins
WindowsEventProvider=C:\Users\Test\CloudHSM\setup-DPPC-
CloudHSM\WindowsEventProvider\LunaClientEventProvider.dll
[XTC]
Enabled=1
TimeoutSec=600
[LunaSA Client]
SSLConfigFile=C:\Users\Test\CloudHSM\setup-DPPC-CloudHSM\openssl.cnf
ReceiveTimeout=20000
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]
AuthTokenConfigURI=https://lab-digicert.uaa.system.snakefly.dpsas.io/.well-
known/openid-configuration
AuthTokenClientId=4dd589be-1d9d-43b1-9cf0-faee5f5006c5
RestClient=1
ClientTimeoutSec=120
ClientPoolSize=32
ClientEofRetryCount=15
ClientConnectRetryCount=900
ClientConnectIntervalMs=1000
ServerPort=443
ServerName=na.hsm.dpondemand.io
```

```
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) v10.5.0-470. Copyright (c) 2022 SafeNet. All rights
reserved.
```

Available HSMs:

	Slot Id ->	3
	Label ->	DPoD-QA-Luna-Cloud-HSM
	Serial Number ->	1334054172625
	Model ->	Cryptovisor7
	Firmware Version ->	7.3.0
	CV Firmware Version ->	1.5.0
	Plugin Version ->	Cloud 2.2.0-740
	Configuration ->	Luna User Partition With SO (PW) Signing
With	Cloning Mode	
	Slot Description ->	Net Token Slot
	FM HW Status ->	FM Not Supported

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 You are about to initialize the partition. Are you sure you wish to continue? Type 'proceed' to continue, or 'quit' to quit now -> proceed Enter password for Partition SO: ******* Re-enter password for Partition SO: ******* Option -domain was not specified. It 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 Thales 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) v10.5.0-470. Copyright (c) 2022 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 SChannel Cryptographic Services for Microsoft Windows.

Register the partition

```
C:\Users\Test\CloudHSM\setup-DPPC-CloudHSM\csp>register.exe
register.exe (64-bit) v10.5.0-470. Copyright (c) 2022 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
Success registering the encrypted challenge for partition "<partition
name>:3".
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:

🔣 - SafeNet Key Storage Provider Config Wizard	
Eile Help	
⊟- SafeNet KSP Config	
- Register Or View Security Library	
Register HSM Slots	
l Ready	

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 Wizard		
Eile Help		
⊟ SafeNet KSP Config		
Register Or View Security Library		
Register HSM Slots	LibraryPath C:UserstrootiC:loudHSM(SafeNet)setup-DPPC-CloudHSMcvclient-minicryptoki.dll	
	Browse	Register
	1	
	1	
	1	
	1	
	1	
Ready		/

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 Stora	ge Provider, Config Wizard	
<u>F</u> ile <u>H</u> elp			
E- SafeNet KSP Config Register Or View Security Library Register HSM Slots	Administrator Available Slots DPPC-QA Registered Slots SlotLabel:DPPC-QA	Slot Password	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 = "CSPRA20221001"
MachineKeySet = TRUE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
```

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 a client authentication certificate".

4. Install RA certificate

Refer section Install RA certificate

Get a client authentication certificate

This section describes steps to get a client authentication certificate using the **Generic User Certificate** template, **CSR** Enrollment Method, and **Enrollment Code** as Authentication Method. But you can get a client authentication certificate using any of the combinations below:

Template	Enrollment Method	Authentication Method
Generic User Certificate	CSR	Manual Approval
Generic User Certificate	REST API	Enrollment Code or 3 rd Party app
Generic Device Certificate	CSR	Manual Approval or Enrollment Code
Generic Device Certificate	REST API	Enrollment Code or 3 rd Party app

Create profile

- 1. Sign into DigiCert ONE and navigate to Trust Lifecycle Manager.
- 2. Select Manage Profiles from the left navigation menu, then Profiles.
- 3. Select Add profile.
- 4. Select the Generic User Certificate template.

Note: The appropriate license for the seat type of the template selected must be purchased and available in your account, otherwise that template's link will be disabled.

- 5. Under the **General information** section, enter the profile **Nickname** and choose the **Business Unit** and **Issuing CA**.
- 6. From the Enrollment method dropdown, select CSR.
- 7. From the Authentication method dropdown, select Enrollment Code.
- 8. Select Next.
- 9. Under **Certificate fields**, select the validity period unit (Years, Months, or Days) and enter the value in the textbox.

Note: You cannot issue an end entity certificate with a validity period longer than the remaining validity of the issuing CA. The issuing CA expiration date is shown as a reference in this section.

10. Select the **Algorithm** from the available algorithms in the dropdown list. Available algorithms are based on the issuing CA selected for the profile.

11. Select the Key type and attribute from the dropdown lists.



- 12. Select the checkbox to **Allow duplicate certificates** if multiple certificates are to be issued for the same seat ID.
- 13. Under Renewal options, select the **Renewal window** from the dropdown list. The default (recommended) value is 30 days.
- 14. Select **Subject DN** and **SAN** fields from the dropdown list. Select the **Common name** field, then select **Add fields**.

Click here to select additional fields	Add fields
General	
Certificate signing request (CSR)	Common name 🔟
Subject DN	Source for the field's value
	Entered by User

- 15. For each selected field, from the **Source for the field's value** dropdown, select **Entered by user**.
- 16. Select Next.
- 17. Specify the **Key usage (KU)** extension criticality and values. **Note:** the KU options shown differ depending on the certificate template being used.
- 18. Specify the **Extended key usage (EKU)** extension criticality and values. **Note: Client Authentication** is the minimum required EKU value.
- 19. Select Next.
- 20. Under Certificate delivery format, select PKCS#7 PEM and Include CA chain with Root CA as the certificate delivery format to use and chain certificates to include when certificates are issued.
- 21. Under **Email configuration & notifications**, specify the template to be used for certificate revocation notification emails.

- 22. Under Administrative contact, specify whether to include default or custom administrative contact details in certificate notification emails. Note: including internal support contact details for end users is optional, but recommended.
- 23. Under **Seat ID Mapping**, select the certificate field to be used as the seat ID. This uniquely identifies each enrollment entity, for licensing purposes.
- 24. Under **Service User binding**, select the Service user API token to be bound to the certificate profile. If no Service user is selected from the dropdown, then all API tokens in the account will be able to manage this profile.
- 25. Select **Create**. Your newly created certificate profile is now displayed in the certificate profiles list.

Add User/Device Seat

- 1. Select Manage Seats from the left navigation menu, then Add user seat.
- 2. Enter a Seat name.
- 3. Enter a Seat ID.
- 4. Enter an Email (optional).
- 5. Enter Phone details (optional).
- 6. Select a Business Unit.
- 7. Select Create user seat.
- 8. Select Enroll Now.
- 9. Select the profile created in the Create Profile section from the Choose A Profile dropdown.
- 10. Select Enroll.
- 11. Copy the **Enrollment Code** that is required to get the certificate.
- 12. Access the link provided in the email.
- 13. Enter the Enrollment Code copied in step 11.
- 14. Enter the **Certificate signing request (CSR)** that was generated in the Generate CSR section.
- 15. Enter the **Common name**.
- 16. Select Update.
- 17. Download the certificate.

Upload client authentication certificate

- 1. Navigate to Account Manager.
- 2. Select Access from the left navigation menu, then Service User.
- 3. Select the Service user for which you are uploading the client authentication certificate.
- 4. Select **Upload Client authentication certificate** under the **Authentication certificates** section.
- 5. Enter a Nickname.
- 6. Export the client authentication certificate downloaded under the Add User/Device Seat Section (step 17) in DER or PEM format. Select **Click or drag file to upload** and choose the certificate.
- 7. Select Upload client authentication certificate.

Install RA certificate

- 1. Open the command prompt (on the folder where the PKCS#7 file is stored) and run the following command:
 - > certreq -accept <issued-cert>
- 2. Before running the command above, the trusted root certificate must first 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)

Refer to the "Configure the Autoenrollment Server" section of the DigiCert® Autoenrollment Server Deployment Guide in this KB article for more information.