DigiCert[®] PKI Platform

HSM Installation and Configuration for SafeNetAT (Assured Technologies)

Version 8.21.3

June 10, 2021



Legal Notice

Copyright © 2021 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

INTRODUCTION4
REVISION HISTORY
SUPPORTED HSMS
SAFENETAT NETWORK HSM6
INSTALLING THE SAFENETAT LUNA CLIENT SOFTWARE
CONFIGURE LUNA HSM CLIENT
CONFIGURE HA (HIGH AVAILABILITY)
CONFIGURE CSP
CONFIGURE KSP
GENERATE CSR AND INSTALL CERTIFICATE21
INTEGRATION FOR JAVA ENVIRONMENT
REGISTER LUNA PROVIDER
INSTALL RA CERTIFICATE
GET RA CERTIFICATE IN PKI-MANAGER

Introduction

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

Revision History

No.	Date	Summary
1.	2020/11/04	Create a new entry
2.	2021/06/10	Added support for SafeNetAT Luna SA5

Supported HSMs

HSM Type	Client Version	Software Version	Firmware Version
SafeNetAT Network HSM (*a, *b)	7.10.1	7.10.1	7.10.1
SafeNetAT Network HSM (*a, *b)	5.4.9	5.4.7	6.11.2

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

*b : SafeNetAT Network HSM 5 and 7 supports FIPS and non-FIPS Mode, Cloning and Export Mode.

SafeNetAT Network HSM

The SafeNetAT Network HSM T-7 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 SafeNetAT Network HSM T-7, we can use the Luna HSM Client through Network Trust Link Service (NTLS).



Installing the SafeNetAT Luna Client Software

In the client location, follow the steps below to install the Luna Client software.

1. Run LunaClient.msi as Administrator and click Next.



2. Select "I accept the terms in the license agreement" and click Next.

🔀 SafeNetAT Luna Client 7.10.1 - InstallShield Wizard	×			
License Agreement Please read the following license agreement carefully.				
SafeNet Assured Technologies, LLC SOFTWARE LICENSE AGREEMENT for Luna HSM	^			
NOTICE TO USERS: THIS IS A LICENSE, NOT A SALE. THIS PRODUCT IS PROVIDED UNDER THE FOLLOWING TERMS AND CONDITIONS. CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT BEFORE YOU INSTALL OR USE THIS SOFTWARE. INSTALLING, COPYING, OR OTHERWISE USING THIS SOFTWARE INDICATES YOUR ACKNOWLEDGMENT THAT YOU HAVE READ THIS LICENSE AND ALL DOCUMENTS REFERRED TO THEREIN AND AGREE TO BE BOUND BY AND COMPLY WITH ALL OF THE TERMS.				
	Print			
\bigcirc I <u>do</u> not accept the terms in the license agreement	<u>r</u>			
InstallShield				
< <u>B</u> ack <u>N</u> ext >	Cancel			

3. Proceed and click Next.

🚮 SafeNetA	SafeNetAT Luna Client 7.10.1 - InstallShield Wizard X					
Destination Folder Click Next to install to this folder, or click Change to install to a different folder.				feNet AT		
	Install SafeNetAT Luna Client 7 C:\Program Files\SafeNet\Luna	.10.1 to: aClient\		<u>C</u> hange		
InstallShield –		< <u>B</u> ack	<u>N</u> ext >	Cancel		

4. Select the features to be Installed and click Next.

Here select Luna SA -> This feature, and all subfeatures, will be installed on local hard drive.

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

- a) Luna CSP (CAPI) / Luna KSP (CNG)
- b) Luna JSP (Java)
- c) Luna SDK
- d) Luna JCProv (Java)

<u>C</u>hange...

Cancel

🕼 SafeNetAT Luna Client 7.10.1 - InstallShield Wizard	×					
Custom Setup						
Select the product(s), peripherals, and options you want to in	Istall. SafeNet AT					
Click an icon below to select or de-select an item to be installed	I. Feature Description					
This feature will be installed on local hard on	drive.					
This feature, and all subfeatures, will be inst	talled on local hard drive. et					
This feature will not be available. Luna G5 Remote PED	I his reature requires 2008 on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 15MB on your hard drive.					
Install to:						
C:\Program Files\SafeNet\LunaClient\	<u>C</u> hange					
InstallShield	Next > Cancel					
SafeNetAT Luna Client 7.10.1 - InstallShield Wizard Custom Setup Select the product(s), peripherals, and options you want to in	nstall. SafeNet AT					
Click an icon below to select or de-select an item to be installed	ı.					
Luna SA Luna CSP (CAPI) / Luna KSP (CNG) Luna JSP (Java) Luna SDK Luna JCProv (Java) X V Luna PCI Remote PED	Feature Description Client library, client configuration, and administrative tools (HA, backup, etc.) for Luna SA, SafeNet Assured Technologies' network-attached hardware sec This feature requires 20MB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 15MB on your					

 Install to:
 subfeatures require 1

 C:\Program Files\SafeNet\LunaClient\

 InstallShield

 Help

 Space

 < Back</td>

 Next >

5. Click Install.



NOTE: If you see below error when installing Luna Client version 5.4.9 on Windows Server 2019, Ignore the error and proceed with installation and configuration.

Click **OK** and Click **Finish** and Close "Windows Features" window

SafeNet	Luna Client 5.4.9 - InstallShield Wizard	- D >	<
Installing	SafeNet Luna Client 5.4.9	SafeNet	
The pro	gram features you selected are being installed.	ASSURED TECHNOLOG	IES
1 1	Please wait while the InstallShield Wizard installs S This may take several minutes.	SafeNet Luna Client 5.4.9.	
	Status: SafeNet Luna Client 5.4.9 - InstallS	hield Wizard $ imes$	
	Failed to start HTL Client	service.	
Wi			ws
rea		ОК	
To for			dle
InstallShield			
	< Back	Next > Cancel	

6. Once the Installation is completed, click Finish.



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

Configure Luna HSM Client

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

In the client location, follow the below steps to configure the Luna HSM Client:

- 1. Open command prompt and run the following commands.
 - > cd C:\Program Files\SafeNet\LunaClient
 - > lunacm.exe
- 2. Obtain the server certificate.

The server certificate has been created on the HSM. Copy it from the server.

- > pscp -scp admin@<SERVER-HOSTNAME>:server.pem .
- 3. Add server for the client side.

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

4. Create 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

5. 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,

a) 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)
```

b) 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,

6. Confirm connection settings.

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

> vtl l Server:	istServers <server-host< th=""><th>NAME> HTL required: no</th></server-host<>	NAME> HTL required: no
> vtl v	verify	
The fol	lowing Luna S	A Slots/Partitions were found:
Slot	Serial #	Label
====	=======	=====
1	615340068	<partition-name></partition-name>

7. 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: 1615340039
HA Group Slot ID: Not Available
Group Members: 615340039
Needs sync: no
Standby Members: <none>
Slot # Member S/N Member Label Status
----- ------ ------- ------
1 615340039 <PARTITION-NAME> alive
It is recommended that you restart LunaCM to refresh the list of available
slots.
Command Result : No Error
lunacm v7.10.1 - Copyright (c) 2006-2020 SafeNet Assured Technologies, LLC.
Available HSMs:
Slot Id ->
                       1
HSM Label ->
                       '<PARTITION-NAME>'
HSM Serial Number ->
                       615340039
HSM Model ->
                       LunaSA-T7
HSM Firmware Version -> 7.10.1
HSM Configuration -> Luna Network HSM (PW) Signing With Cloning Mode
HSM Status ->
                       OK
Slot Id ->
                       3
                       <HA LABEL>
HSM Label ->
HSM Serial Number -> 1615340039
HSM Model ->
                       LunaVirtual
HSM Firmware Version -> 7.10.1
HSM Configuration -> Virtual HSM (PW) 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".

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
register v7.10.1
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 v7.10.1
SafeNet Assured Technologies, LLC. 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 '<PARTITION-NAME>'?[y/n]: y
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 v7.10.1
        *
                                                               *
*
                                                               *
    SafeNet Assured Technologies, LLC. 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 '(HA-LABEL)'?[y/n]: y
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.

SafeNet Assured Technologies, LLC. Key Storage Provider, Config Wizard Elle Help	7/	×
SafeNet KSP Config Register Or View Security Library Register HSM Slots		

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

SafeNet Assured Technologies, LLC. Key Sto File Help B- SafeNet KSP Config Register Or View Security Library Register HSM Slots	LibraryPath C:\Program Files\SafeNet\LunaClient\cryptoki.dll Browse Success X	Reg	ister
Ready	ОК		

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 Assured Technologies, LLC. Key S	torage Provider, Config Wizard			- 🗆 X
<u>F</u> ile <u>H</u> elp				
	Administrator	PUNWIN2K19FORES	-	Register By
Register HSM Slots	Available Slots	Slot Password		Slot Label
	1 cloningHA	▼		C Slot Number
				Register Slot
	Registered Slots			View Registered Slots
	SlotLabel:cloningHA			
				Delete Registered Slot
Ready				

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 Assured Technologies, LLC. Key Stora Eile Help	ge Provider, Config Wizard		_		×
□ - SafeNet KSP Config □ - SafeNet KSP Config □ - Register Or View Security Library □ - Register HSM Slots	Register For User SYSTEM Available Slots 1 cloningHA	Domain Image: With Authon Author Image: With Author Slot Password Image: With Author	Register By Slot Label Slot Number		
			View Registered	Slots	
	SlotLabel:cloningHA		Delete Registered	I Slot	
Ready	J				

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 SafeNetAT 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 = "CSPRA20201104"
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 = KSPRAID20201104
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. Get RA Certificate

See "Get RA Certificate in PKI-Manager"

- 4. 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)

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

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

- Copy the LunaAPI.dll and 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.

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.

Digiterrariation	digicert			
Account activity	Alerts	Account statu	IS	
Last updated: Jul 19, 2019 12:58 AM Refresh	The DigiCert PKI Platform 8.19 release includes:	Status: OK		
Al	Rebranding from Symantec to DigiCert Email domain validation for S/MIME certificates via DCV (Domain Control Validation) process	Next service r	enewal: Ma	y 2, 2020
Recent activity	 Support for Microsoft Intune to issue Client Authentication certificates via SCEP enrollment flow 			
Action Date	 Enterprise Gateway and Autoenrollment Server support for SateNet Luna Network HSM 7 (FIPS and non-FIPS Mode, Cloning and Export Mode) and nShield Connect HSM 			
Certificate profile created Jul 18, 2019	Windows Server 2016 support for Enterprise Gateway, Autoenrollment Server and Local Key Management Service (LKMS)			
Certificate profile deleted Jul 18, 2019	Removal of Adobe Individual, Adobe Organization and Adobe CDS certificates to Android devices			
Certificate options custo Jul 18, 2019	Bug fixes			
Certificate profile created Jul 18, 2019				
Certificate for user revo Jul 18, 2019	Certificate history Seat activity			
Certificate for user revo Jul 18, 2019	All certificate profiles All certificate profiles			
Certificate profile deleted Jul 18, 2019	2.5			
	2	Seat usage Refresh Seat pool User Device Server Server Organization Buy more seats	Used 46	Purchased 1000
1	🍥 📑 🚢 🔚 배 👰			

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 W communications between your client and the Web Set	eb Services, you mus	st install an RA certifica	ate to secure
If you are not setting up these services, or have alrea process.	dy gotten your RA cer	tificate, you do not nee	d to complete this
Enter Certificate Signing Request (CSR)			
Ask your server administrator to generate a CSR for y according to the instructions in the installation guide	our RA certificate. You for your service.	ur administrator must	generate the CSR
You can access the resources page by clicking on the	e 🛞 icon on the da	shboard.	
Paste your CSR:			
important Service Requirements: If you discover or have rea you must immediately revoke the certificate or notify the isu or your organization name has changed, please anotify the your certificate at any time without notice if (i) you fail to pe (i) in the issuing center's sole discretion, you have engaged systems. Enter a certificate friendly name:	ison to believe that ther uing center to do so. Sin suing center. Note that form your obligations u l in activities which the i	e has been a compromise mlarty, if the information w the issuing center retains nder the terms of your se issuing center determines	a of your private key, vžhin your certificate the right to revoke rvice agreement, or s are harmful to its
Important Service Requirements: If you discover or have re- you must immediately revole the certificate or notify the ias or your organization name has changed, please notify the is your certificate at any time without notice if (i) you fail to pe (i) in the issuing center's sole discretion, you have engaged systems. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate ren	eval information. If yo	e has been a compromis- miarty, if the information w the issuing center retains nder the terms of your as issuing center determines as a state of the state of the state state of the state	a of your private key, ithin your certificate the right to revoke ervice agreement, or s are harmful to its a this contact, go to to undete
mportant Service Requirements: If you discover or have re- you must immediately revoke the certificate or notify the isa or your organization name has changed, please notify the is your certificate at any time without notice if (i) you fail to pe (i) in the issuing center's sole discretion, you have engaged systems. Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate ren the menu and select Manage account and sub-accou Email address: Ashish_RanjanPartner@yopmail.cor	isson to believe that ther ing center to do so. Sin using center. Note that form your obligations u in activities which the i in activities which the i ewal information. If you inf(s). Select Edit ren n	e has been a compromise nilarly, if the information w the issuing center retains nder the terms of your se issuing center determines issuing center determines but would like to change ewal email notification	a of your private key, rithin your certificate the right to revoke rvice agreement; or a are harmful to its e this contact, go to to update.
mportant Service Requirements: If you discover or have rer you must immediately revoke the certificate or notify the iss or your organization name has changed, please notify the ip is) in the issuing center's sole discretion, you have engaged systems. Enter a certificate friendly name: Enter a certificate friendly name: Renewal email notification The following email contact will receive certificate ren the menu and select Manage account and sub-accou Email address: Ashish_RanjanPartner@yopmail.cor	ason to believe that ther uing center to do so. Sin issuing center. Note that form your obligations u in activities which the i in activities which the i in activities which the i serval information. If your unt(s). Select Edit ren m	e has been a compromise miarty, if the information w the issuing center retains dier the terms of your se issuing center determines sissuing center determines bu would like to change ewal email notification	a of your private key, xhin your certificate the right to revoke the right to revoke a are harmful to its a re harmful to its b this contact, go to to update.

The CSR looks as follows; Please paste it.

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

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

Your F Your F Servic Insta 1. Dov Iss	RA certificate is ready A certificate must be installed on the server where your PKI Enterprise Gateway or PKI Web es is installed. II your RA certificate vnload your RA certificate. ued to:
Insta 1. Dov Iss Exp	II your RA certificate vnload your RA certificate. ued to:
1. Dov Iss Exp	vnload your RA certificate. ued to:
lss Exp	ued to:
Exp	
Jui	5 January 19 January 1
File PK	format: CS #7
Dov	vnload
2. For in the	ward the RA certificate to your server administrator. Your administrator must follow the instructions installation guide for your service.You can download the appropriate installation guide from the
resou	rces page by clicking on the 🌍 icon on the dashboard.
	Done

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