THALES

Entrust: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

Document Information

Document Part Number	007-013456-001
Revision	R
Release Date	1 July 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

The Entrust Authority Security Manager (EASM) serves as the Certification Authority (CA) in the Entrust public key infrastructure. Although EASM can operate in "software" mode, it can optionally use hardware devices where cryptographic operations and key storage are performed. By managing the full lifecycles of certificate-based digital identities, EASM enables encryption, digital signature, and authentication capabilities to be consistently and transparently applied across a broad range of applications and platforms.

The benefits of securing the CA key with Luna HSM include:

- Secure generation, storage, and protection of the signing private key on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- Access to the HSM audit trail*.
- The advantage of cloud services with confidence.

*Luna Cloud HSM services do not have access to the secure audit trail.

Certified Platforms

Certified platforms for Luna HSM
Certified platforms for Luna Cloud HSM

Certified Platforms for Luna HSM

The following platforms are certified for integrating Entrust with Luna HSM:

HSM Type	EASM Version	Platforms Certified
Luna HSM	10.0	Windows Server 2019
Luna HSM	8.3	Windows Server 2019, Windows Server 2016, Windows Server 2012R2, RHEL7
Luna HSM	8.2	Windows Server 2012R2, RHEL7
Luna HSM	8.1 SP1 with Patch 192895	Windows Server 2012R2, RHEL7

NOTE: Entrust Integration is tested in HA as well as FIPS mode.

NOTE: Entrust Authority Security Manager 8.3 onwards works with 64-bit Luna HSM library/client. Entrust Authority Security Manager 8.2 or any other previous version is 32-bit application, so update chrystoki.ini file to point to the 32-bit Luna HSM library. For UNIX, install 32-bit Luna HSM client.

NOTE: For support with earlier versions of Luna HSM and Entrust Authority Security Manager, you require a previous version of the Luna HSM Integration Guide. Refer to Entrust_SafeNetLunaHSM_IntegrationGuide_RevL for legacy support.

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Certified Platforms for Luna Cloud HSM

The following platforms are certified for integrating Entrust with Luna Cloud HSM:

HSM Type	EASM Version	Platforms Certified
Luna Cloud HSM	8.3	Windows Server 2019, Windows Server 2016,Windows Server 2012R2, RHEL7
Luna Cloud HSM	8.2	Windows Server 2012R2, RHEL7

Luna Cloud HSM: Luna Cloud HSM provides on-demand HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.

Prerequisites

Before you proceed with the integration, complete the following tasks:

Configure Luna HSM

Configure Luna Cloud HSM Service

Install Entrust Authority Security Manager

Configure Luna HSM

To configure Luna HSM:

1. Ensure that the HSM is set up, initialized, provisioned, and ready for deployment. Refer to Luna HSM documentation for help.
2. Create a partition that will be later used by Entrust Authority Security Manager.
3. Create and exchange certificate between the Luna Network HSM and Client system. Register client and assign partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.

4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
# /usr/safenet/lunaclient/bin/lunacm

lunacm (64-bit) v10.3.0-275. Copyright (c) 2020 SafeNet. All rights
reserved.

Available HSMs:

Slot Id ->              0

Label ->                Entrust

Serial Number ->        1213475834492

Model ->                LunaSA 7.7.0

Firmware Version ->     7.7.0

Bootloader Version ->   1.1.2

Configuration ->        Luna User Partition With SO (PW) Signing With
Cloning Mode

Slot Description ->     Net Token Slot

FM HW Status ->         FM Ready
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** Refer to Luna HSM documentation for detailed steps about creating NTLS connection, initializing the partitions, and assigning various user roles.

> **NOTE**: For PED-based Luna HSM ,ensure that ProtectedAuthenticationPathFlagStatus is set to '1' in the Misc Section of Chrystoki.conf file.

Set up Luna HSM High-Availability

Refer to Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Set up Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna HSM in FIPS mode, you have to make the following change in the configuration file:

```
[Misc]
RSAKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

NOTE: The above setting is not required for Universal Client. This setting is applicable only for Luna Client 7.x.

Control User Access to the HSM

By default, only the root user has access to the HSM. You can specify a set of non-root users that are permitted to access the HSM by adding them to the hsmusers group. The client software installation automatically creates the hsmusers group. The hsmusers group is retained when you uninstall the client software. This allows you to upgrade your client software while retaining your hsmusers group configuration.

To add users to hsmusers group

To allow non-root users or applications access to the HSM, assign the users to the hsmusers group. The users you have assigned to the hsmusers group must exist on the client workstation. The HSM can be accessed only by the users whom you have added to the hsmusers group. To add a user to the hsmusers group:

a. Ensure that you have sudo privileges on the client workstation.

b. Add a user to the hsmusers group.

```
sudo gpasswd --add <username> hsmusers
```

where <username> is the name of the user you want to add to the hsmusers group.

To remove users from hsmusers group

To revoke a user's access to the HSM, you can remove them from the hsmusers group. To remove a user from the hsmusers group:

a. Ensure that you have sudo privileges on the client workstation.

b. Remove a user from the hsmusers group.

```
sudo gpasswd -d <username> hsmusers
```

where `<username>` is the name of the user you want to remove from the hsmusers group. To see the change, you need to log in again.

NOTE: The user you delete will continue to have access to the HSM until you reboot the client workstation.

Configure Luna Cloud HSM Service

You can configure Luna Cloud HSM Service in the following ways:

> Standalone Cloud HSM service using minimum client package

> Standalone Cloud HSM service using full Luna client package

> Luna HSM and Luna Cloud HSM service in hybrid mode

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   [Linux]
   cvclient-min.tar
   # tar -xvf cvclient-min.tar
   ```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Windows]
   Right-click setenv.cmd and select Run as Administrator.
   [Linux]
   Source the setenv script.
   # source ./setenv
   ```

5. Run the LunaCM utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   ```
   [Windows]
   cvclient-min.zip
   [Linux]
   cvclient-min.tar
   # tar -xvf cvclient-min.tar
   ```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

   ```
   [Windows]
   Right-click setenv.cmd and select Run as Administrator.
   ```

```
[Linux]
Source the setenv script.
# source ./setenv
```

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

   Cloud HSM Certificates:

   ```
   server-certificate.pem
   partition-ca-certificate.pem
   partition-certificate.pem
   ```

   LunaClient Certificate Directory:

   ```
   [Windows default location for Luna Client]
   C:\Program Files\Safenet\Lunaclient\cert\
   [Linux default location for Luna Client]
   /usr/safenet/lunaclient/cert/
   ```

   NOTE: Skip this step for Luna Client v10.2 or higher.

6. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

   ```
   [Windows]
   crystoki.ini
   [Linux]
   Chrystoki.conf
   ```

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.
8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

   [XTC]

   ```
   . . .
   PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
   PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
   . . .

   [REST]
   . . .
   SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
   . . .
   ```

   NOTE: Skip this step for Luna Client v10.2 or higher.

9. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```
Misc]
PluginModuleDir=<LunaClient_plugins_directory>
[Windows Default]
C:\Program Files\Safenet\Lunaclient\plugins\
[Linux Default]
/usr/safenet/lunaclient/plugins/
```

   Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

10. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

    Windows

    In the Control Panel, search for "environment" and select Edit the system environment variables. Click Environment Variables. In both list boxes for the current user and system variables, edit ChrystokiConfigurationPath and point to the crystoki.ini file in the Luna client install directory.

    Linux

    Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

```
# export ChrystokiConfigurationPath=/etc/
```

11. Run the LunaCM utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

> **NOTE:** Follow the Luna Cloud HSM documentation for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the Standalone Cloud HSM service using full Luna client package section above.

> **NOTE:** Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

To use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Install Entrust Authority Security Manager

Before proceeding further, ensure the following third party applications are installed on the machine:

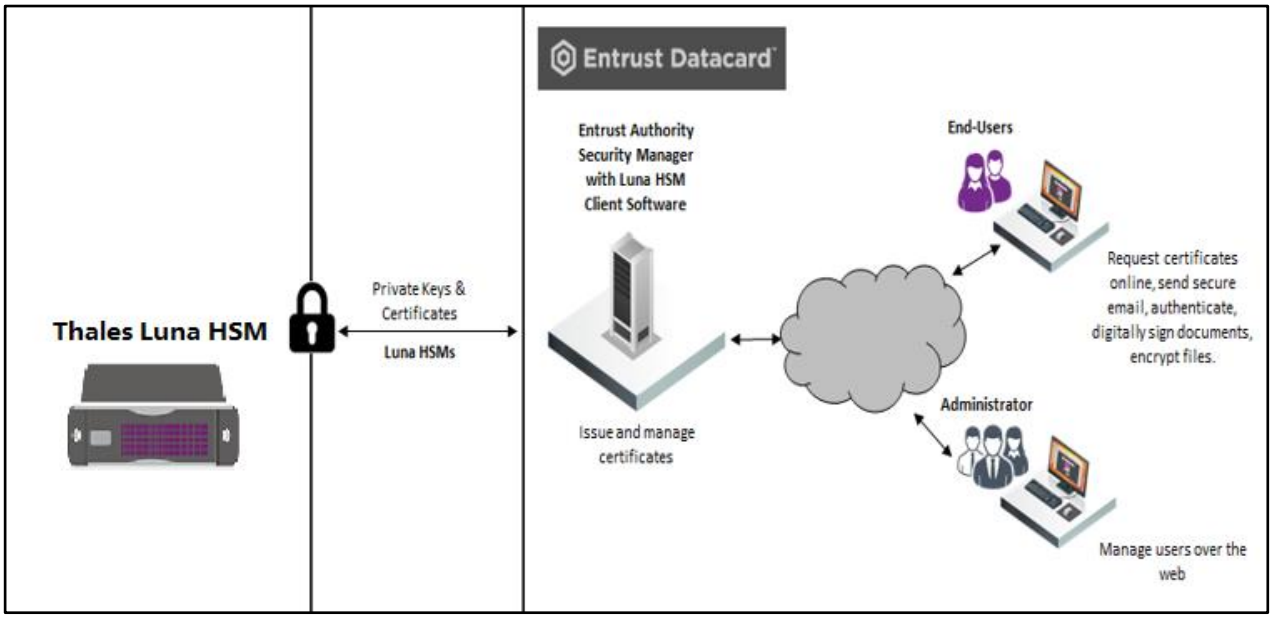
> Entrust Authority Security Manager PostgreSQL

> Directory Server

> Entrust Authority Security Manager

Integrating Entrust Authority Security Manager with Luna HSM

This section describes how to integrate new installations of Entrust Authority Security Manager with Luna HSMs. Note that in the procedure that follows, we will initialize the Entrust Authority Security Manager Server and configure it to use Luna HSM for generating the CA signing keys.



> Configure EASM on Windows

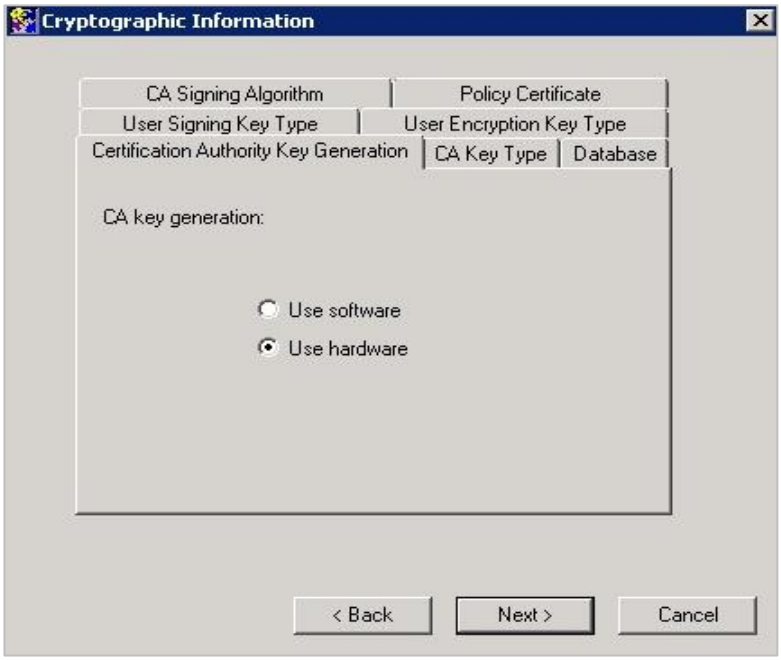
> Configure EASM on RHEL

Configure EASM on Windows

To configure EASM on Windows:

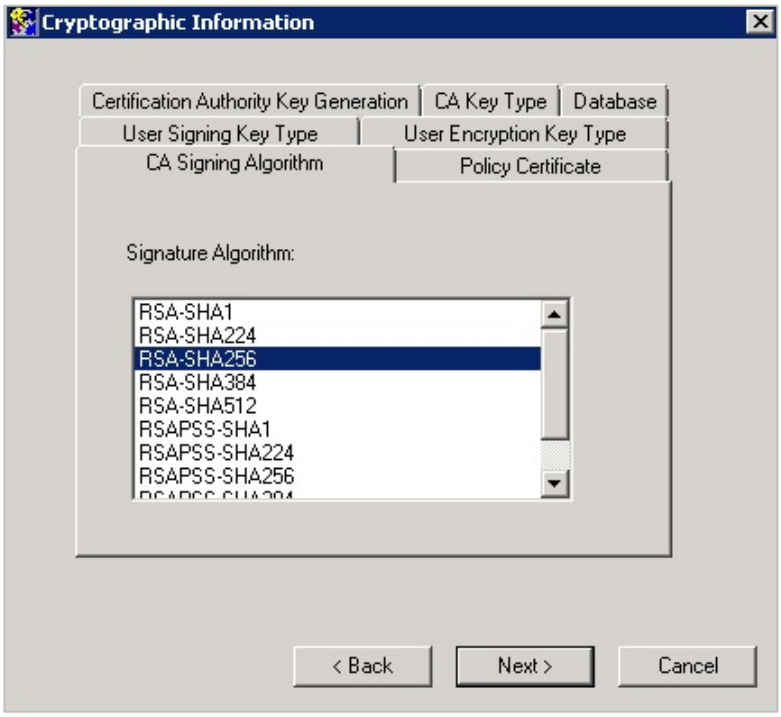
1. Run the Entrust Authority Security Manager Configuration utility. At the point where you choose whether to store keys in hardware or software, select hardware. Point to the Cryptoki library path.

2. On the **Certification Authority Key Generation** tab, select the Use hardware radio button and click **Next**.



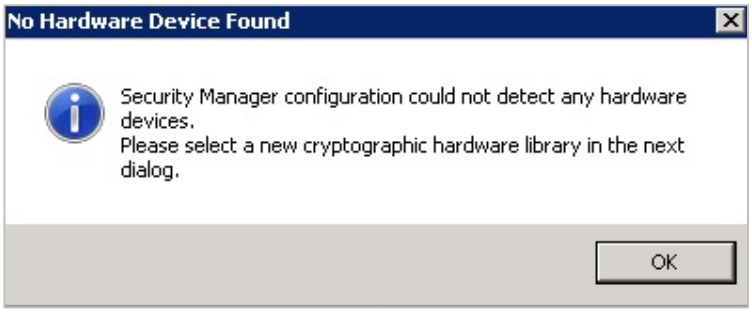
3. On the **CA Key Type tab** select the **RSA** radio button and select **2048** from the parameters drop-down menu. Click **Next**.

4. On the **CA Signing Algorithm** tab select "`RSA-SHA256`". Click **Next**.

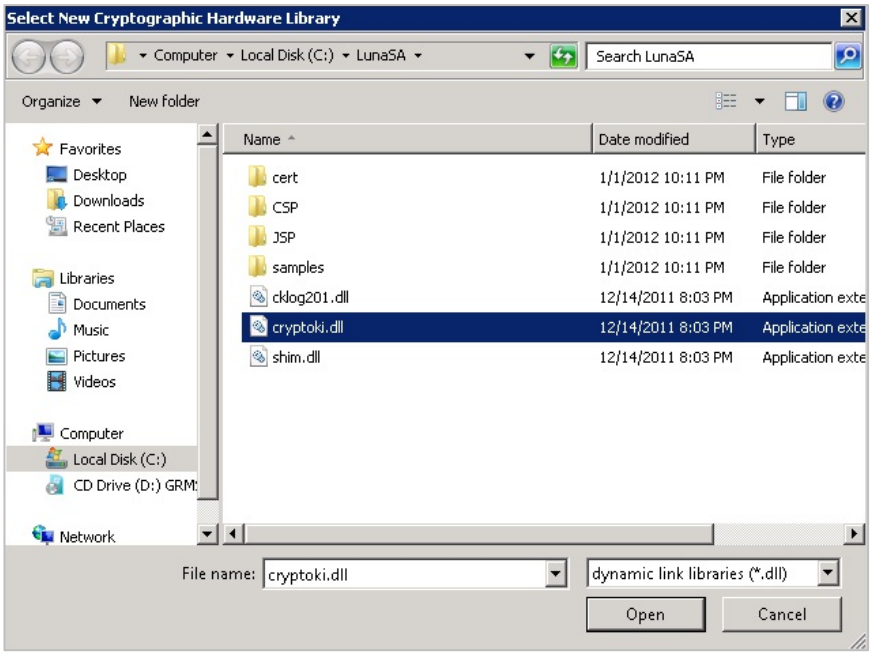


5. On the **Policy Certificate** tab, keep the default value in the **Policy Certificate Lifetime** field. Click **Next**.

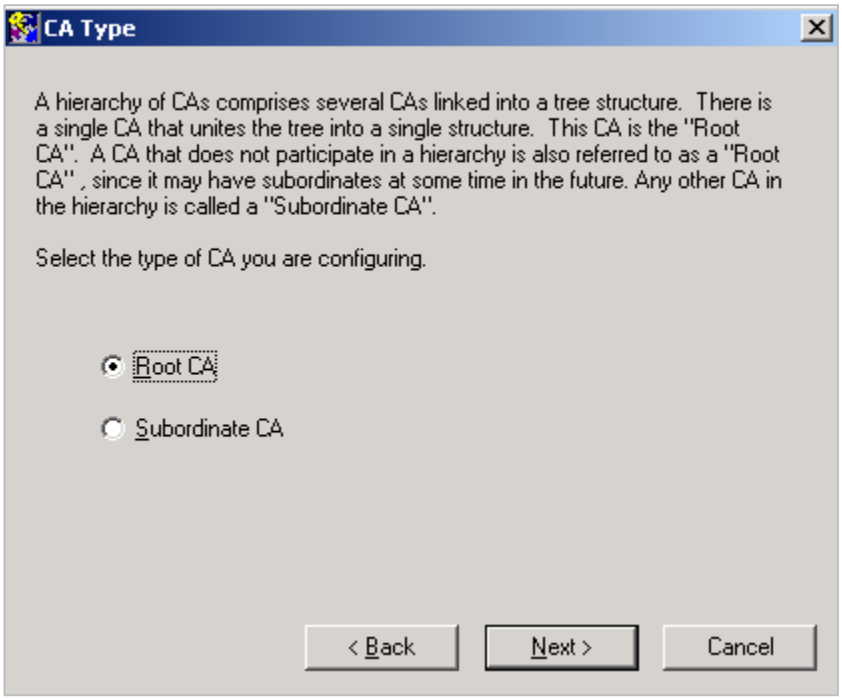
6. The "**No Hardware Device Found**" dialog displays. Click **OK**.



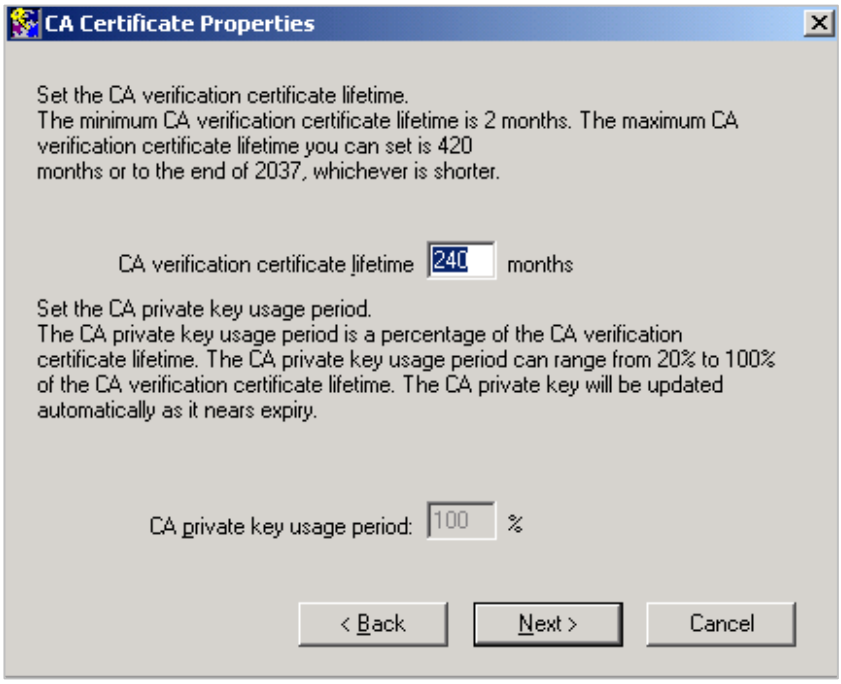
7. Select the `cryptoki.dll` in the file menu. Click **Open**.



8. Select the **Root CA** radio button and click **Next**.

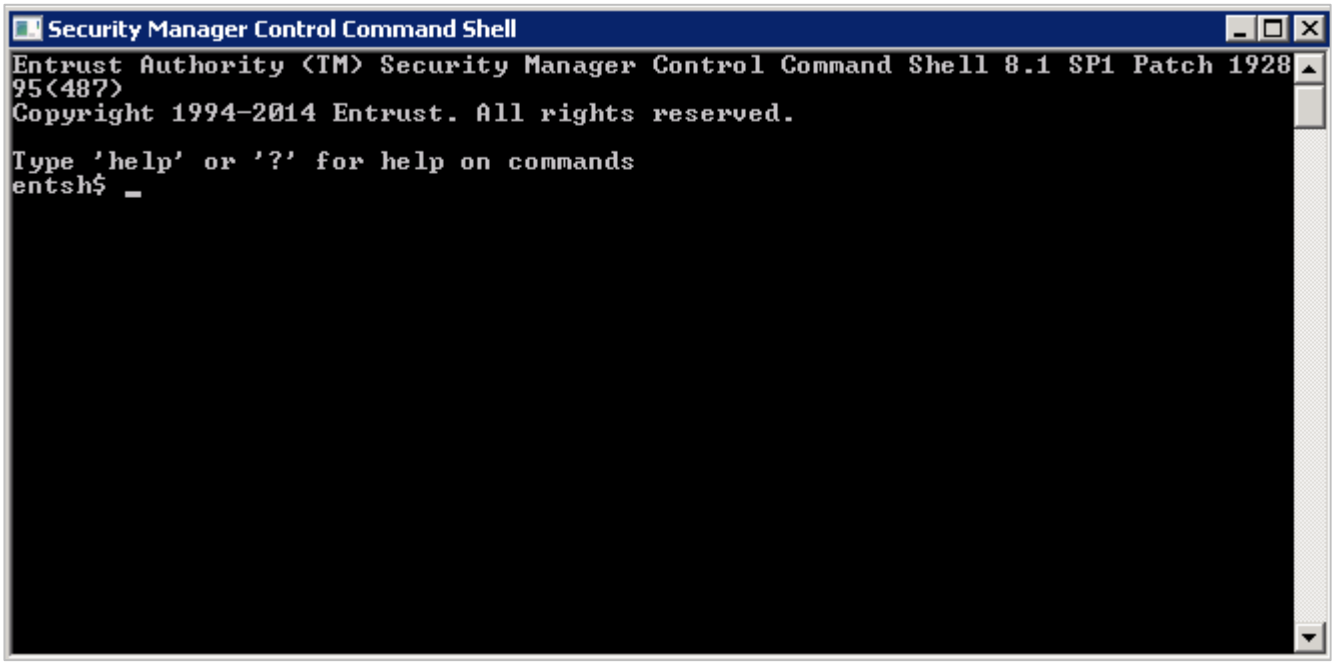


9. Accept the default CA Certificate Properties and click **Next**.



10. The configuration complete message appears on the screen. Click **OK** to complete the configuration process.

11. Click **Start** -> **Programs** -> **Entrust** -> **Security Manager Control Command Shell**.



12. Initialize Entrust Authority Security Manager through the “Entrust Authority Security Manager Control Command Shell”. For details, refer to *Entrust Authority Security Manager* documentation.

13. Entrust Authority Security Manager detects the HSM slot or service and requests its password. Enter the Luna HSM or HSM on Demand service partition password.

    Entrust Authority Security Manager generates the CA key on the Luna HSM.

Configure EASM on RHEL

To configure EASM on RHEL:

1. Create the “Entrust Authority Security Manager” user that will own the Entrust Authority Security Manager installation.
2. Run the Entrust Authority Security Manager Configuration utility. When you receive a prompt from the system to check whether you want to use a hardware device for the CA keys, type Yes.
3. Point to the Cryptoki library path from `<SafeNet HSM installation directory>/lib/libCryptoki2_64.so`
4. The EASM Configuration utility presents the option to use a Luna HSM with a given serial number. Select the correct Luna HSM slot
5. Complete the EASM configuration by following the instructions provided by configuration utility..
6. Initialize EASM for the first time using the Entrust Authority Security Manager Master Control Command Shell. Add passwords for the Master1, Master2, Master3, and First Officer user.
7. Entrust Authority Security Manager detects slot and requests for the partition password. Enter the HSM partition password. If you are using a Luna Network HSM with Secure Authentication & Access Control, ensure that the black PED Key is inserted in the PED.
8. Entrust Authority Security Manager generates the root CA key on the Luna HSM in the partition.
9. Entrust Authority Security Manager performs a database backup and restart the Entrust Authority Security Manager Service. Ensure that service is started successfully.

The Integration of Luna HSM is successful with Entrust Authority Security Manager.

Use the `ca key show-cache` command on the Entrust Authority Security Manager command line. This command displays all the keys created during the integration.

You can use `partition showcontents` command on the HSM to view the content of the partition used for Entrust Authority Security Manager.

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.