ENTRUST

SafeNet HSM Integration Guide

gemalto

security to be free

Document Part Number: PN 007-013456-001, Rev. C

Release Date: May 2016

Contents

Preface

This document covers the necessary information to install, configure, and integrate Entrust Authority Security Manager with SafeNet Luna Hardware Security Module.

Scope

This technical integration guide provides an overview of how to integrate Entrust Authority Security Manager with SafeNet HSM.

When using it in “hardware” mode, you can use the Luna HSMs for cryptographic operations and key storage. Among the operations performed on hardware devices are:

- Secure generation, storage and protection of the CA signing private key
- Signing of certificates and CRL’s using the CA signing private key

Entrust Authority Security Manager utilizes the following APIs: PKCS #11.

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna Client	SafeNet HSM Client

NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

> **NOTE:** Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

> **CAUTION:** Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

> **WARNING:** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name:** Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • User input (In the **Date** box, type **April 1**.)

Convention	Description
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

The Entrust Authority Security Manager serves as the Certification Authority in an Entrust infrastructure. Although it 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, Entrust Authority Security Manager enables encryption, digital signature and authentication capabilities to be consistently, transparently applied across a broad range of applications and platforms.

3rd party Application Details

- Entrust Authority Security Manager
- Entrust Authority Security Manager PostgreSQL
- Directory Server (Critical Path Directory server/Open LDAP/OpenDJ/Atos DirX/Microsoft Active Directory LDS).

Supported Platforms

Entrust Authority Security Manager 8.1 SP1 with Patch 192895

FIPS Validated

Platforms Tested	SafeNet Luna HSM Appliance Software version	SafeNet Network HSM Client Software version	Firmware Version
Windows 2008 R2 Windows 2012 R2 RHEL 6.5 HP-UX 11	Luna SA 6.1	Luna SA CS 6.1 with 630-010467-001_SW_Patch_SA6_SA5_Compatibility_Shim_CLNT_Luna_6.0_Alpha3	6.10.9
Windows 2008 R2 Windows 2012 R2	Luna G5	Luna SA CS 6.1 with 630-010467-001_SW_Patch_SA6_SA5_Compatibility_Shim_CLNT_Luna_6.0_Alpha3	6.10.9

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- SafeNet Network HSM appliance and a secure admin password
- SafeNet Network HSM, and a hostname, suitable for your network
- SafeNet Network HSM network parameters are set to work with your network
- Initialized the HSM on the SafeNet Network HSM appliance.
- Created and exchanged certificates between the SafeNet Network HSM and your Client system.
- Created a partition on the HSM, remember the partition password that will be later used by Entrust Authority Security Manager. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Network HSM.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).
- Entrust Authority Security Manager is 32 bit application so update chrystoki.ini/chrystoki.conf file to point to 32 bit Luna HSM library. “chrystoki.ini” on Windows is located at “C:\Program Files\SafeNet\LunaClient” and on Unix under /etc. For example on Windows: Chrystoki.ini file will look like:

  [Chrystoki2]

  LibNT= C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll

Installation Overview

This section describes how to integrate new installations of Entrust Authority Security Manager with SafeNet Luna HSMs. Note that in the following discussion, there will be Entrust Authority Security Manager Server, and SafeNet Luna HSM configured with Entrust Authority Security Manager Server machine. For the purpose of this discussion, the Entrust Authority Security Manager system assumes the role of Client to the Luna HSM.

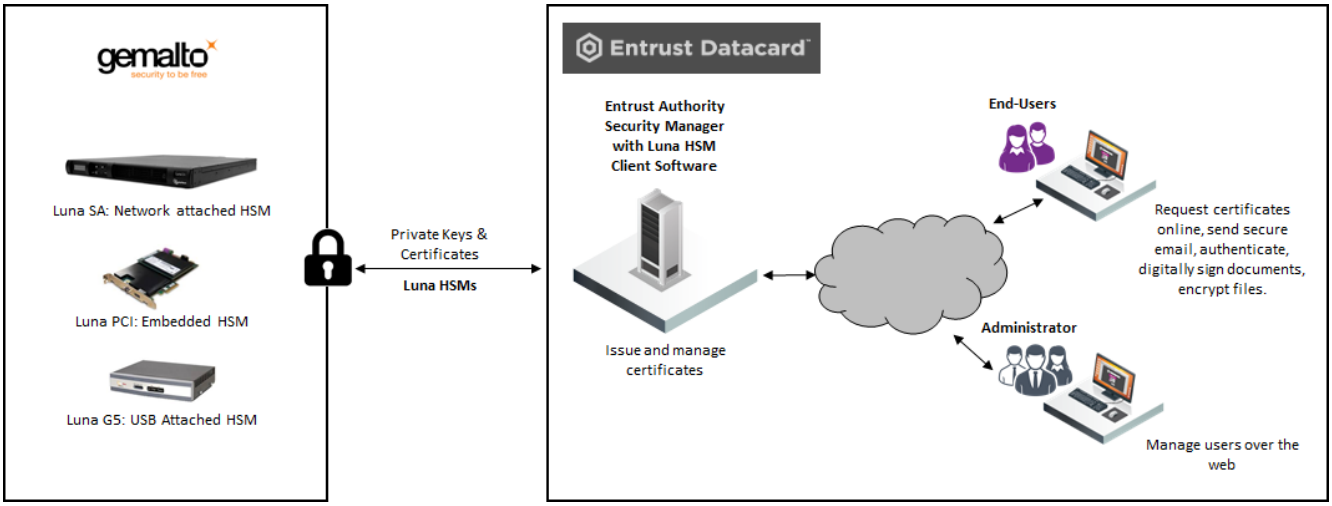


Figure 1: Entrust Authority Security Manager with Luna HSM Client Software

2

Integrating Entrust Authority Security Manager with SafeNet Luna HSM

Prerequisites

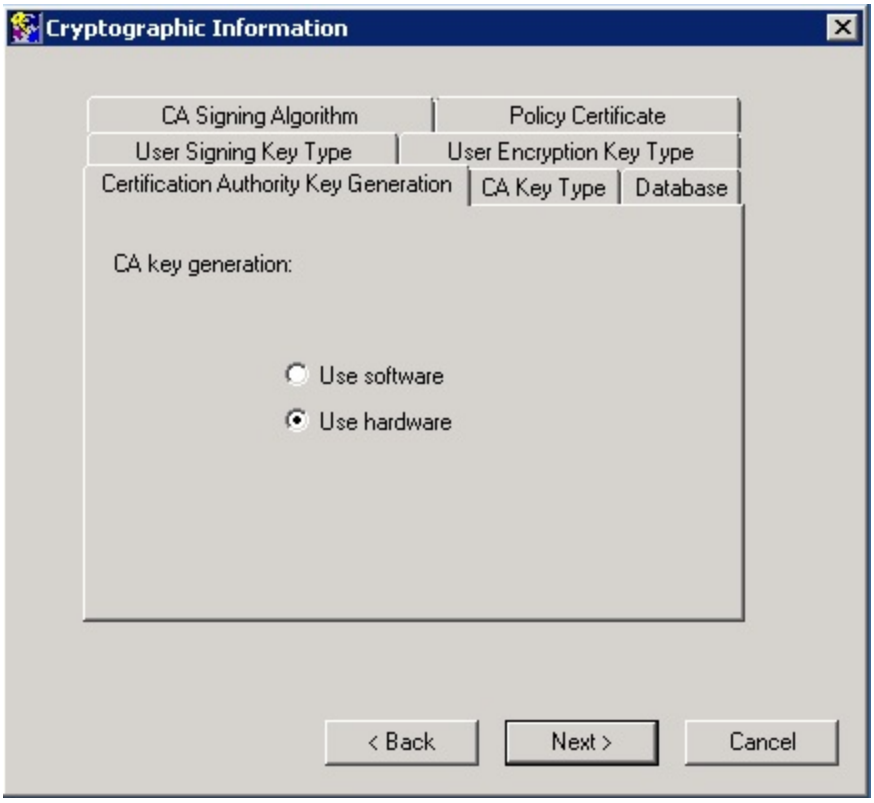
Ensure following third party software are installed before proceeding further.

- Entrust Authority Security Manager PostgreSQL
- Directory Server
- Entrust Authority Security Manager

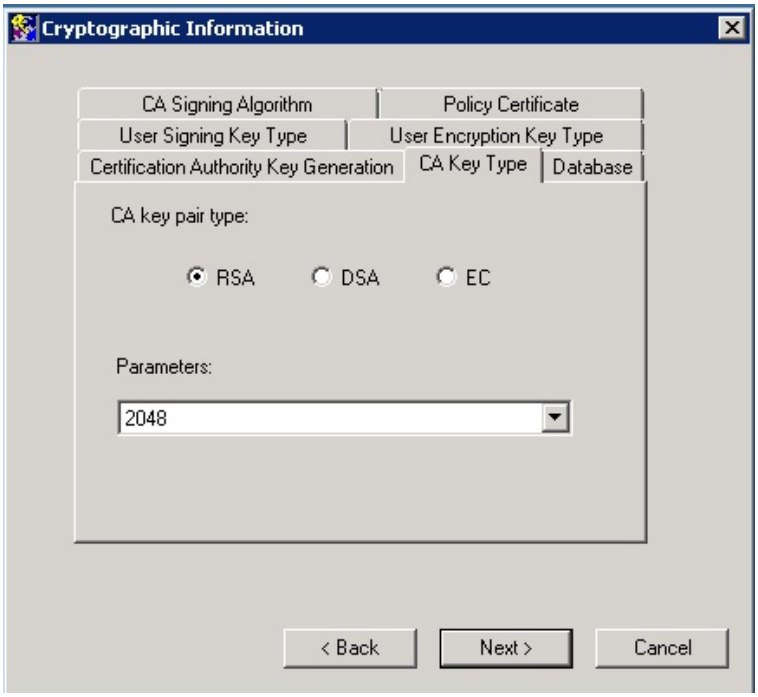
Configuring Entrust Authority Security Manager with SafeNet Luna HSM on Windows

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 Luna HSM library path **C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll** on Windows.

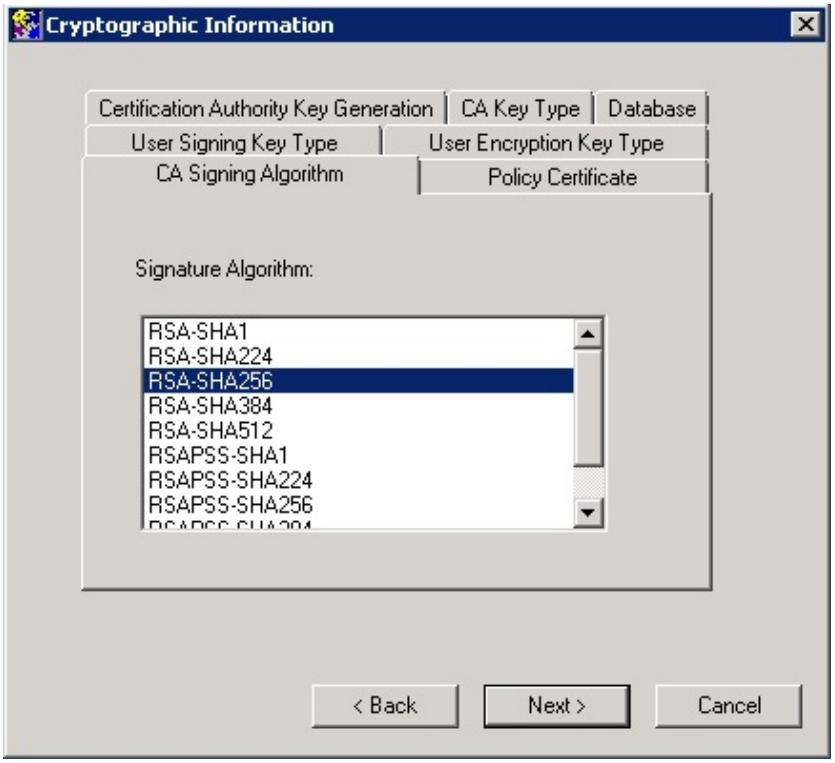
2. For “Cryptographic Information”, select **Use hardware** and click **Next**.



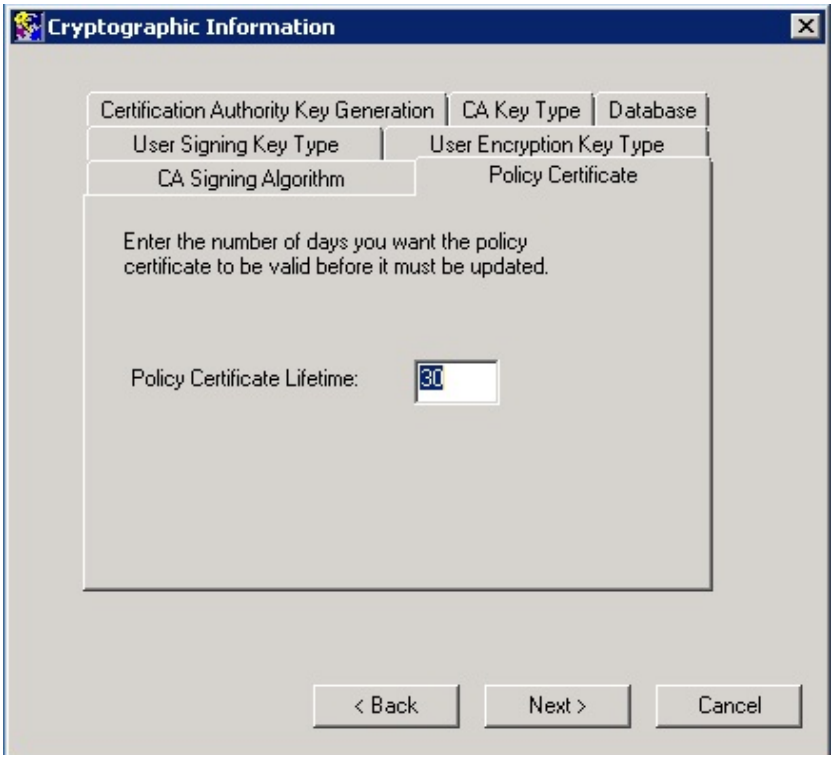
3. Select CA key pair as “RSA 2048” and click **Next**.



4. Select “RSA-SHA256” as CA Signing Algorithm and click **Next**.

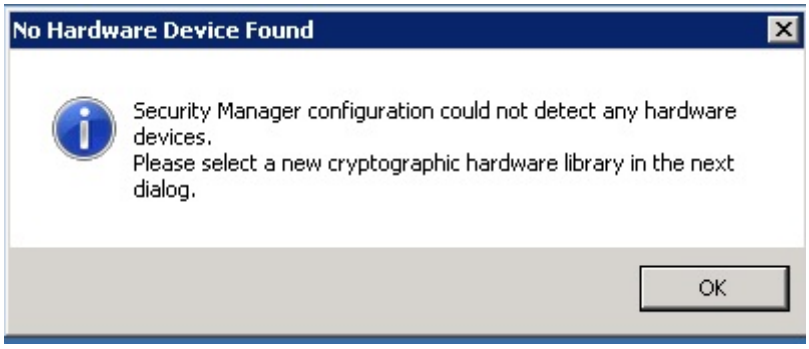


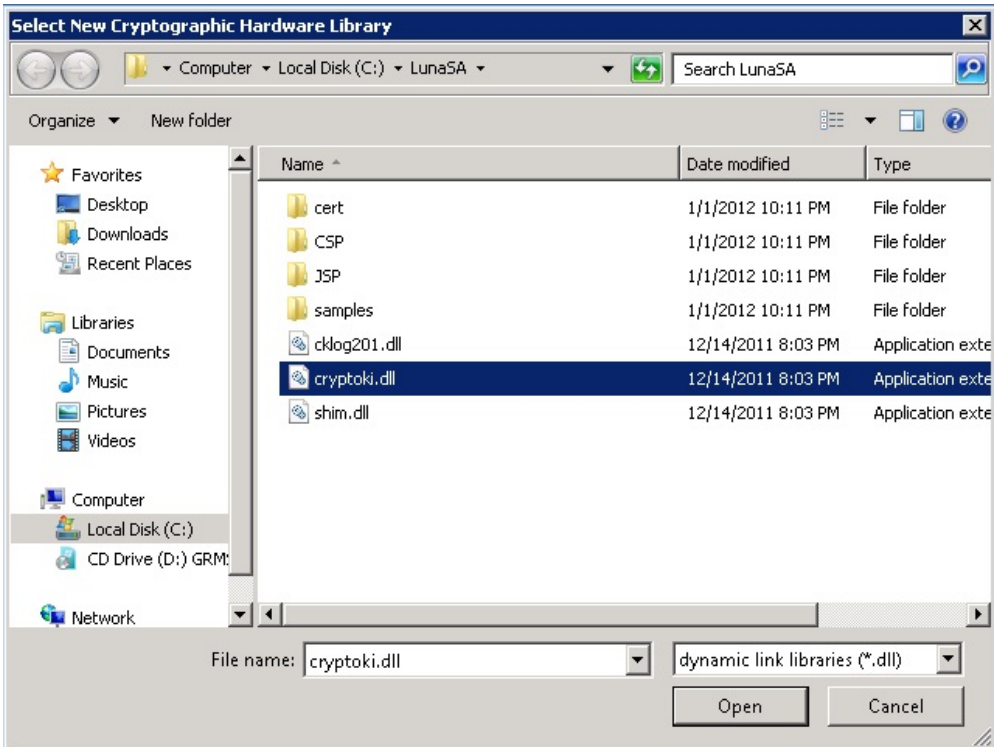
5. Keep default for Policy Certificate Lifetime and click **Next**.



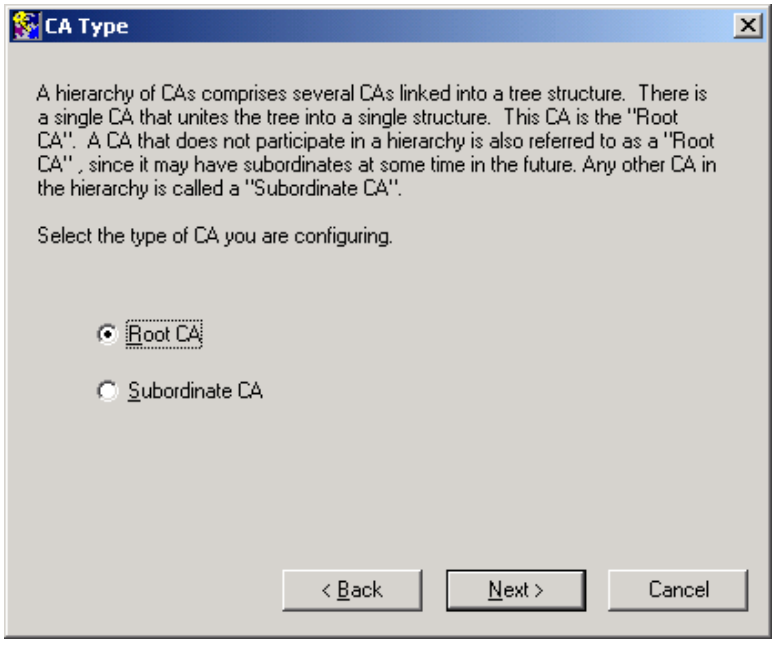
A dialog box displays “**No Hardware Device Found**”. Click **OK.**

Select “Cryptoki.dll” from open dialog box and click **Open**.

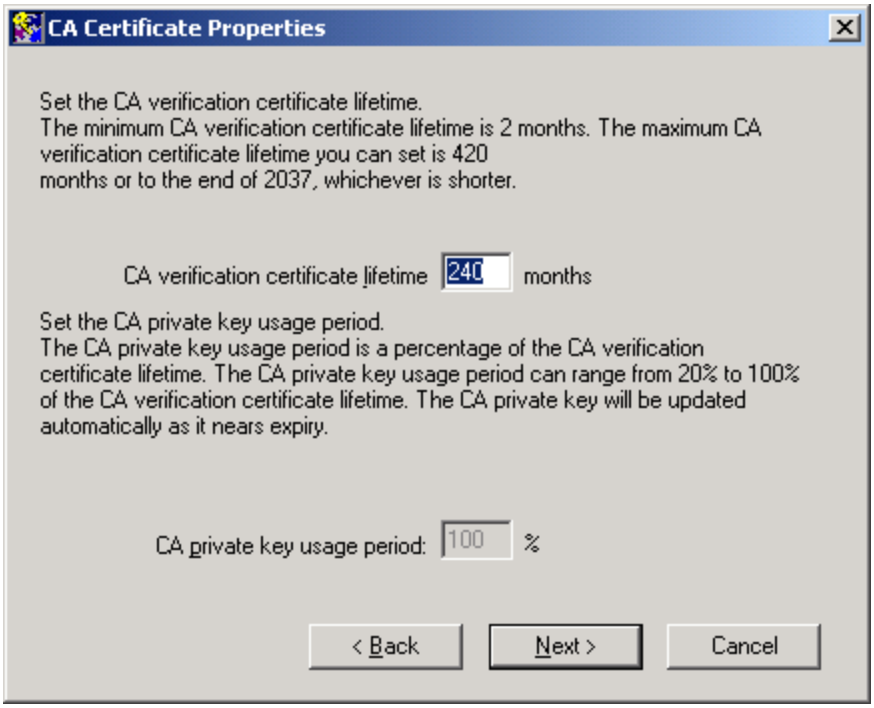




6. Specify “CA Type” as “Root CA” and click **Next**.

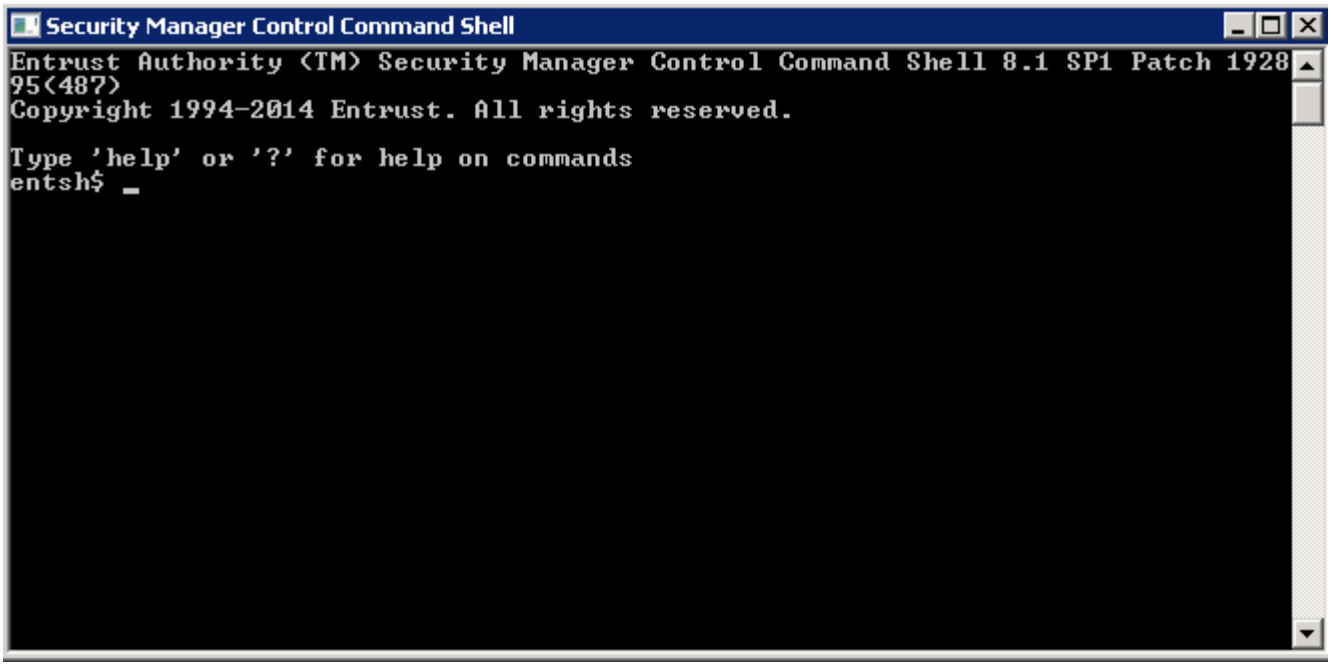


7. Accept “CA Certificate Properties” and click **Next**.



8. The configuration complete message displays. Click **OK** to complete the configuration process.

9. Click Start → Programs → Entrust → Security Manager Control Command Shell.



10. Initialize the HSM via the "Entrust Authority Security Manager Control Command Shell" / Initialize Entrust Authority Security Manager following Entrust Authority Security Manager documentation.
11. Entrust Authority Security Manager detects hardware and requests for the hardware password. Enter the HSM Partition's Partition Password/login secret.
12. Entrust Authority Security Manager generates the CA keys on the Luna HSM.

Configuring Entrust Authority Security Manager with SafeNet Luna HSM on Solaris 10 Sparc/RHEL/HP-UX

1. Create “Entrust Authority Security Manager” user and which will own the Entrust Authority Security Manager installation
2. Install Entrust Authority Security Manager PostgreSQL following the Entrust Authority Security Manager documentation (SM_81_Installation_issue5.pdf).
3. Install Entrust Authority Security Manager 8.1 SP1, following the Entrust Authority Security Manager documentation.
4. Run the Entrust Authority Security Manager Configuration Utility. At the point where you choose whether to store keys in hardware or in software, select hardware. Point to the SafeNet Network HSM library path for libCryptoki2.so */usr/safenet/lunaclient/lib/*libCryptoki2.so
5. Entrust Authority Security Manager Configuration Utility presents the option to use SafeNet Network HSM hardware, with a given serial number. Select the SafeNet Network HSM hardware.
6. Continue with the Configuration until complete.
7. Initialize Entrust Authority Security Manager for the first time with Entrust Authority Security Manager Master Control Command Shell. Add the passwords for Master1, Master2, Master3 and First Officer, following Entrust Authority Security Manager documentation.
8. Entrust Authority Security Manager detects hardware and requests for the hardware password. Enter the HSM Partition’s Partition Password/login secret that was generated at the creation of the HSM Partition. If you are using a SafeNet Network HSM with Secure Authentication & Access Control, ensure that the black PED Key is inserted in the PED.
9. Entrust Authority Security Manager generates the root CA keys on the SafeNet Network HSM in the provided partition.
10. Entrust Authority Security Manager performs a database backup.
11. Entrust Authority Security Manager is now running.

The Integration of SafeNet 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 integration.

Also you can use Partition show Content command on the HSM to display the content of the Partition used for Entrust Authority security Manager.

3
Troubleshooting

Troubleshooting

- While running entsh on RHEL if it gives “segmentation fault” kindly go to directory “/opt/entrust/authdata/CA” and execute following command (Note the space between two full stops):

  # . ./env_settings.sh

- Luna 5.4 does not support **CAST5-CBC-128** for Database Hardware Encryption Protection.

4
Legacy Platform Supported

Legacy Platform Support

This section lists the legacy platforms supported for this integration.

Entrust Authority Security Manager 8.1

FIPS Validated

Platforms Tested	Luna Client Software version	Firmware Version
Solaris 10 SPARC x64	5.x (v5.1)	6.2.1
Windows 2008 R2	5.x (v5.4.7)	6.10.9

Entrust Authority Security Manager 8.1 with SP1 with Patch 192895

Platforms Tested	Luna Client Software version	Firmware Version
Windows 2008 R2 Windows 2012 R2	5.x (v5.4.7)	6.2.4
Windows 2012 R2	5.x (v5.4.2)	6.10.9

Entrust Authority Security Manager 8.1 with Patch 173358

Platforms Tested	Luna Client Software version	Firmware Version
Windows 2008 R2 Solaris 10 SPARC x64 RHEL 6 x64	5.x (v5.2, 5.2.1, 5.3)	6.10.1

Entrust Authority Security Manager 8.1

Platforms Tested	Luna Client Software version	Firmware Version
Windows 2008 R2 Windows 2003 R2	5.x (v5.2, 5.2.1, 5.3)	6.10.1
Solaris 10 SPARC x64	5.x (v5.1)	6.0.8

Entrust Authority Security Manager 8.0

Platforms Tested	Luna Client Software version	Firmware Version
Windows 2008 R2 Windows 2003 R2	5.x (v5.1)	6.0.8
Windows 2008 R2 Windows 2003 Server Solaris 10 SPARC x64 RHEL 5 x64	5.x (v5.0)	6.0.7

Entrust Authority Security Manager 7.1 SP3

Platforms Tested	Luna Client Software version	Firmware Version
Windows 2008 R2 Windows 2003 Server Solaris 10 SPARC x64 RHEL 5 x64	5.x (v5.0)	6.0.7

Entrust Authority Security Manager 7.1

Platforms Tested	Luna Client Software version	Firmware Version
Windows 2003 R2 Windows 2008 R2	5.1	6.0.8

NOTE: Luna G5 v1.3 (f/w 6.2.2) is tested with Windows 2008 R2, Windows 2003 R2.