All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016-2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Number:** 007-013456-001, Rev. L

**Release Date:** May 2018
## Contents

**Preface** .................................................................................................................................. 4  
  Scope........................................................................................................................................ 4  
  Document Conventions .................................................................................................................. 4  
    Command Syntax and Typeface Conventions ............................................................................... 4  
    Support Contacts ....................................................................................................................... 5  

1 **Introduction** ...................................................................................................................... 7  
  Overview ........................................................................................................................................ 7  
  3rd party Application Details ......................................................................................................... 7  
  Supported Platforms .................................................................................................................... 7  
    SafeNet Luna HSM (v7.x) .......................................................................................................... 7  
    SafeNet Luna HSM (v6.x) .......................................................................................................... 8  
  Prerequisites ................................................................................................................................. 11  
    Configuring PED Auth SafeNet Luna HSM (v7.0/v6.1) ................................................................. 11  
    Configuring PED Auth SafeNet Luna HSM (v6.2.x) .................................................................. 12  
    Configuring SafeNet Luna Network HSM 7.x ............................................................................ 12  
    Configuring SafeNet Luna Network HSM (v5.x/6.x) ................................................................. 15  
    Using Luna 6.x/7.x in FIPS Mode ............................................................................................. 16  
  Installation Overview ..................................................................................................................... 17  

2 **Integrating Entrust Authority Security Manager with SafeNet Luna HSM** ................... 18  
  Prerequisites ................................................................................................................................. 18  
  Configuring EASM with SafeNet Luna HSM on Windows ........................................................... 18  
  Configuring EASM with SafeNet Luna HSM on Solaris SPARC/RHEL/HP-UX ...................... 23  

3 **Troubleshooting** .................................................................................................................. 25  
  Troubleshooting ......................................................................................................................... 25  

4 **Legacy Platform Supported** ............................................................................................... 26  
  Legacy Platform Support ............................................................................................................. 26
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 (EASM) with SafeNet Luna HSM.

When using it in “hardware” mode, you can use SafeNet Luna HSM for cryptographic operations and key storage. The operations performed on hardware devices are listed as below:

- 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.

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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**.) |
| *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

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
</table>
| **Address**             | Gemalto  
4690 Millennium Drive  
Belcamp, Maryland  21017, USA                                                  |
| **Phone**               | US 1-800-545-6608  
International 1-410-931-7520                                                   |
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. |
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 (EASM)
- Entrust Authority Security Manager PostgreSQL
- Directory Server (Critical Path Directory server/Open LDAP/OpenDJ/Atos DirX/Microsoft Active Directory LDS).

Supported Platforms

SafeNet Luna HSM (v7.x)

Entrust Authority Security Manager 8.2

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Server 2012R2 RHEL 7</td>
<td>7.2.0</td>
<td>7.2.0</td>
<td>7.2.0</td>
</tr>
<tr>
<td>Window Server 2012R2 RHEL 7</td>
<td>7.1.0</td>
<td>7.1.0</td>
<td>7.1.0</td>
</tr>
</tbody>
</table>
### Entrust Authority Security Manager 8.1 SP1 with Patch 192895

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Server 2012R2</td>
<td>7.0.0</td>
<td>7.0.0</td>
<td>7.0.1</td>
</tr>
<tr>
<td>RHEL 6.5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SafeNet Luna HSM (v6.x)

### Entrust Authority Security Manager 8.2

#### FIPS Validated

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Server 2012R2</td>
<td>Luna SA 6.3.0</td>
<td>Luna SA CS 6.3.0</td>
<td>6.10.9</td>
</tr>
<tr>
<td>RHEL 7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.1 SP1 with Patch 197297

#### FIPS Validated

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 6.8</td>
<td>Luna SA 6.3.0</td>
<td>Luna SA CS 6.3.0</td>
<td>6.10.9</td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.1 with Patch 203960

#### FIPS Validated

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11</td>
<td>Luna SA 6.2.2</td>
<td>Luna SA CS 6.2.1</td>
<td>6.10.9</td>
</tr>
</tbody>
</table>
## Entrust Authority Security Manager 8.1 SP1 with Patch 192895

### FIPS Validated

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Server 2012R2 RHEL 6.5</td>
<td>Luna SA 6.3.0</td>
<td>Luna SA CS 6.3.0</td>
<td>6.10.9</td>
</tr>
<tr>
<td>Windows Server 2012R2 RHEL 6.5</td>
<td>Luna SA 6.2.2</td>
<td>Luna SA CS 6.2.2</td>
<td>6.10.9</td>
</tr>
<tr>
<td>Windows 2012R2 RHEL 6.5</td>
<td>Luna SA 6.2.1</td>
<td>Luna SA CS 6.2.1</td>
<td>6.10.9</td>
</tr>
<tr>
<td>Windows 2012R2</td>
<td>Luna SA 6.2</td>
<td>Luna SA CS 6.2 with 630-010467-001_SW_Patch_SA6_SA5_Compatibility_Shim_CLNT_Luna_6.0_Alpha3</td>
<td>6.10.9</td>
</tr>
<tr>
<td>Windows 2008 R2 Windows 2012 R2 RHEL 6.5</td>
<td>Luna SA 6.1</td>
<td>Luna SA CS 6.1 with 630-010467-001_SW_Patch_SA6_SA5_Compatibility_Shim_CLNT_Luna_6.0_Alpha3</td>
<td>6.10.9</td>
</tr>
<tr>
<td>Windows 2008 R2 Windows 2012 R2</td>
<td>Luna G5</td>
<td>Luna SA CS 6.1 with 630-010467-001_SW_Patch_SA6_SA5_Compatibility_Shim_CLNT_Luna_6.0_Alpha3</td>
<td>6.10.9</td>
</tr>
</tbody>
</table>

## Entrust Authority Security Manager 8.1 with Patch 201641

### FIPS Validated

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11</td>
<td>Luna SA 6.2.2</td>
<td>Luna SA CS 6.2.2</td>
<td>6.10.9</td>
</tr>
<tr>
<td>HP-UX 11</td>
<td>Luna SA 6.2.1</td>
<td>Luna SA CS 6.2.1</td>
<td>6.10.9</td>
</tr>
</tbody>
</table>
### Platforms Tested

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11</td>
<td>Luna SA 6.1</td>
<td>Luna SA CS 6.1 with 630-010467-001_SW_Patch_SA6_SA5_Compatibility_Shim_CLNT_Luna_6.0_Alpha3</td>
<td>6.10.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.2

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Server 2012R2 RHEL 7</td>
<td>Luna SA 6.3.0</td>
<td>Luna SA CS 6.3.0</td>
<td>6.27.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.1 SP1 with Patch 192895

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Server 2012R2 RHEL 6.5</td>
<td>Luna SA 6.3.0</td>
<td>Luna SA CS 6.3.0</td>
<td>6.27.0</td>
</tr>
<tr>
<td>Window Server 2012R2 RHEL 6.5</td>
<td>Luna SA 6.2.2</td>
<td>Luna SA CS 6.2.2</td>
<td>6.24.3</td>
</tr>
<tr>
<td>Windows 2012R2</td>
<td>Luna SA 6.2.1</td>
<td>Luna SA CS 6.2.1</td>
<td>6.24.2</td>
</tr>
<tr>
<td>Windows 2012R2</td>
<td>Luna SA 6.2</td>
<td>Luna SA CS 6.2 with 630-010467-001_SW_Patch_SA6_SA5_Compatibility_Shim_CLNT_Luna_6.0_Alpha3</td>
<td>6.24.0</td>
</tr>
</tbody>
</table>
Entrust Authority Security Manager 8.1 SP1 with Patch 201641

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna HSM Appliance Software version</th>
<th>SafeNet Luna HSM Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11</td>
<td>Luna SA 6.2.2</td>
<td>Luna SA CS 6.2.2</td>
<td>6.24.3</td>
</tr>
<tr>
<td>HP-UX 11</td>
<td>Luna SA 6.2.1</td>
<td>Luna SA CS 6.2.1</td>
<td>6.24.2</td>
</tr>
</tbody>
</table>

Prerequisites

Configuring PED Auth SafeNet Luna HSM (v7.0/v6.1)

You need to obtain the following patch to work with PED based SafeNet Luna HSM when using the version 7.0 and 6.1:

**DOC ID:** DOW4166  
**Part No:** 630-010467-001 Alpha3  
**TITLE:** Luna 5 Compatibility Shim for Luna 6

**NOTE:** The below configuration is only applicable for Version 7.0/6.1 of PED based SafeNet Luna HSM.

**CONFIGURATION:**

1. Copy the libshim.so to <lunaclient installation>/lib directory. It is advised to first rename the previous shim.
2. Point the application to the libshim.so instead of the Cryptoki shared object library. To point it, open the /etc/Chrystoki.conf(Linux) or C:\Program Files\SafeNet\LunaClient\crystoki.ini(Windows) file and make the following changes:
   
   For Linux:
   ```
   Chrystoki2 = {
     LibUNIX = /usr/safenet/lunaclient/lib/libshim.so;
   }
   Shim2 = {
     LibUNIX = /usr/safenet/lunaclient/lib/libCryptoki2.so;
   }
   Misc = {
     ApplicationInstance=SAS_COMPATIBILITY;
     FunctionBindLevel=2;
   }
   ```
For Windows:

[Chrystoki12]
LibNT32 = C:\Program Files\SafeNet\LunaClient\win32\shim.dll

[Shim2]
LibNT32=C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll

[Misc]
  :  
  ApplicationInstance=SAS_COMPATIBILITY  
  FunctionBindLevel=2  
  :

Contact Customer Support if you need assistance for the above configuration.

**Configuring PED Auth SafeNet Luna HSM (v6.2.x)**

For PED based SafeNet Luna HSM make sure ProtectedAuthenticationPathFlagStatus is set to ‘1’ in Misc Section of Chrystoki.conf(Linux) or crystoki.ini(Windows) file.

For Linux:

```
Misc = {
  ProtectedAuthenticationPathFlagStatus = 1;
}
```

For Windows:

```
[Misc]
ProtectedAuthenticationPathFlagStatus = 1
```

**Configuring SafeNet Luna Network HSM 7.x**

SafeNet Luna Network HSM allows to create Per-Partition Security Officer (PPSO) partition. HSM Administrator is not Security Officer (SO) for PPSO partitions. The HSM SO/Administrator elects to create a partition as PPSO-type, which creates an empty structure that is handed to the new owner, who initializes the partition to create the Partition Security Officer (PSO) role or identity for management functions. The PSO in turn creates the partition Crypto Officer (CO) to control client cryptographic operations on the partition.

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX/Windows systems. Before you get started, ensure the following points:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Create a partition on the HSM 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 Luna HSM. The general form of command is "C:\Program Files\SafeNet\LunaClient>vtl verify" for Windows and "/usr/safenet/lunaclient/bin/vtl verify" for Unix.

• Initialize the Partition as mentioned in steps below for Password/PED based respectively.

• Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

**NOTE:** Entrust Authority Security Manager is 32 bit application so update chrystoki.ini file to point to 32 bit SafeNet Luna HSM library. And for UNIX install 32bit SafeNet Luna HSM client.

---

**Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition**

These instructions assume a password-authenticated SafeNet Luna Network HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.

**• Initialize the Partition SO role**

a. Set the active slot to the created, uninitialized, application partition.

b. Type slot set -slot <slot number>

   
   lunacm:> slot set -slot 0
   Current Slot Id: 0   (Luna User Slot 7.0.0 (Password) Signing With Cloning Mode)
   Command Result: No Error

   Initialize the application partition, to create the partition's Security Officer (SO).

c. Type partition init -label <part_label> -password <part_password>

   You are about to initialize the partition.
   All partition objects will be destroyed.
   Are you sure you wish to continue?
   Type 'proceed' to continue, or 'quit' to quit now -> proceed
   Command Result: No Error

**• Initialize the Crypto Officer role**

a. The SO of the application partition can now assign the first operational role within the new partition. Type role login -name Partition SO.

   lunacm:> role login -name Partition SO

b. Type role init -name Crypto Officer.

   lunacm:> role init -name Crypto Officer

c. The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in. Type role logout.

   lunacm:> role logout

---

**Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition**

These instructions assume a PED-authenticated SafeNet Luna Network HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.
Take the following steps to initialize the PSO and CO roles:

- **Initialize the Partition SO role**
  a. Set the active slot to the created, uninitialized, application partition.
  b. Type slot set -slot <slot number>

    ```
    lunacm:> slot set -slot 0
    Current Slot Id:    0      (Luna User Slot 7.0.0 (PED) Signing With Cloning Mode)
    Command Result : No Error
    ```

  Initialize the application partition, to create the partition's Security Officer (SO).

  c. Type partition init -label <part_label>

    ```
    lunacm:> par init -label <part_label>
    You are about to initialize the partition.
    All partition objects will be destroyed.
    Are you sure you wish to continue?
    Type 'proceed' to continue, or 'quit' to quit now -> proceed
    Please attend to the PED.
    Respond to SafeNet PED prompts...
    Command Result : No Error
    ```

- **Initialize the Crypto Officer role**

  The SO of the application partition can now assign the first operational role within the new partition.

  a. Type role login -name Partition SO.
  b. Type role init -name Crypto Officer.

    ```
    lunacm:> role init -name Crypto Officer
    Please attend to the PED.
    Respond to SafeNet PED prompts...
    Command Result : No Error
    ```

  The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.

  c. Type role logout.

  Now, the Crypto Officer or an application using the CO's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto Officer logs in with role login -name Crypto Officer. However, the Crypto Officer can create, modify and delete crypto objects within the partition, in addition to merely using 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.

  **NOTE:** The black Crypto Officer PED key/Crypto Officer Password (in case of PW-Auth) is valid for the initial login only. You must change the initial credential on the key using the command role changepw during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_EXPIRED error while performing role-dependent actions.

**Controlling 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. It thus, allows you to upgrade your client software while retaining your hsmusers group configuration.

**Adding 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. Users you have added to the hsmusers group are able to access the HSM. Users who are not part of the hsmusers group are not able to access the HSM.

- **Adding a user to hsmusers group**
  a. Ensure that you have `sudo` privileges on the client workstation.
  b. Add a user to the hsmusers group.
     ```shell
     sudo gpasswd --add <username> hsmusers
     ```
     where `<username>` is the name of the user you want to add to the hsmusers group.

**Removing users from hsmusers group**

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

- **Removing a user from hsmusers group**
  a. Ensure that you have `sudo` privileges on the client workstation.
  b. Remove a user from the hsmusers group.
     ```shell
     sudo gpasswd -d <username> hsmusers
     ```
     where `<username>` is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

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

**Configuring SafeNet Luna Network HSM (v5.x/6.x)**

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX systems. Before you get started ensure the following:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Create 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 Luna Network HSM. The general form of command is "C:\Program
Files\SafeNet\LunaClient> vtl verify" for Windows and "/usr/safenet/lunaclient/bin/ctl verify" for Unix.

- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

**Using Luna 6.x/7.x 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 SafeNet Luna HSM in FIPS mode, you have to make the following change in configuration file:

For Linux:

```latex
Misc = {
  RSAKeyGenMechRemap = 1;
}
```

For Windows:

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

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

---

**NOTE:** The above configuration is valid for Luna 7.x and Luna 6.x (F/W Version 6.22.0 and above only).
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.
Prerequisites

Ensure following third party software are installed before proceeding further.

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

Configuring EASM 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.

   For "Cryptographic Information", select **Use hardware** and click **Next**.
2. Select CA key pair as “RSA 2048” and click **Next**.

3. Select “RSA-SHA256” as CA Signing Algorithm and click **Next**.
4. Keep default for Policy Certificate Lifetime and click **Next**.

5. A dialog box displays "**No Hardware Device Found**". Click **OK**.
6. Select “Cryptoki.dll” from open dialog box and click Open.

7. Specify “CA Type” as “Root CA” and click Next.
8. Accept “CA Certificate Properties” and click **Next**.

9. The configuration complete message displays. Click **OK** to complete the configuration process.
10. Click Start -> Programs -> Entrust -> Security Manager Control Command Shell.

11. Initialize the HSM via the “Entrust Authority Security Manager Control Command Shell” / Initialize Entrust Authority Security Manager following Entrust Authority Security Manager documentation.

12. Entrust Authority Security Manager detects hardware and requests for the hardware password. Enter the HSM Partition’s Partition Password/login secret.

13. Entrust Authority Security Manager generates the CA keys on the Luna HSM.

Configuring EASM with SafeNet Luna HSM on Solaris 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.
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.
## Legacy Platform Support

This section lists the legacy platforms supported for this integration.

### Entrust Authority Security Manager 8.1

#### FIPS Validated

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris 10 SPARC x64</td>
<td>5.x (v5.1)</td>
<td>6.2.1</td>
</tr>
<tr>
<td>Windows 2008 R2</td>
<td>5.x (v5.4.7)</td>
<td>6.10.9</td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.1 with SP1 with Patch 192895

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 R2</td>
<td>5.x (v5.4.7)</td>
<td>6.2.4</td>
</tr>
<tr>
<td>Windows 2012 R2</td>
<td>5.x (v5.4.7)</td>
<td>6.10.9</td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.1 with Patch 173358

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 R2 Solaris 10 SPARC x64</td>
<td>5.x (v5.2, 5.2.1, 5.3)</td>
<td>6.10.1</td>
</tr>
</tbody>
</table>
### Legacy Platform Supported

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 6 x64</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.1

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 R2</td>
<td>5.x (v5.2, 5.2.1, 5.3)</td>
<td>6.10.1</td>
</tr>
<tr>
<td>Windows 2003 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solaris 10 SPARC x64</td>
<td>5.x (v5.1)</td>
<td>6.0.8</td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 8.0

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 R2</td>
<td>5.x (v5.1)</td>
<td>6.0.8</td>
</tr>
<tr>
<td>Windows 2003 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 2008 R2</td>
<td>5.x (v5.0)</td>
<td>6.0.7</td>
</tr>
<tr>
<td>Windows 2003 Server Solaris 10 SPARC x64 RHEL 5 x64</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Entrust Authority Security Manager 7.1 SP3

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 R2</td>
<td>5.x (v5.0)</td>
<td>6.0.7</td>
</tr>
<tr>
<td>Windows 2003 Server Solaris 10 SPARC x64 RHEL 5 x64</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Entrust Authority Security Manager 7.1

<table>
<thead>
<tr>
<th>Platforms Tested</th>
<th>SafeNet Luna Client Software version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 R2</td>
<td>5.1</td>
<td>6.0.8</td>
</tr>
<tr>
<td>Windows 2008 R2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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