Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust Technical Integration Guide for Entrust Security Manager 8.1 and SafeNet Luna HSM 5.4

July 2015

Table of Contents

Introduction

This technical integration guide provides an overview of how to integrate Entrust Security Manager with Luna HSM 5.4

The Entrust/Authority 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.

Entrust Product Information

Entrust Authority

By managing the full lifecycles of certificate-based digital identities, Entrust Authority enables encryption, digital signature and authentication capabilities to be consistently, transparently applied across a broad range of applications and platforms.

Partner Product Information

Partner Name: SafeNet Inc.
Website: www.safenet-inc.com
Product Name: Luna HSM
Product Version: 5.4
Platform and Service pack: Linux, Windows 2008 R2, Windows 2012 R2

Luna HSM

Product description: Luna HSMs are tamper resistant Hardware Security Modules that securely protect key materials within FIPS certified modules. The Luna HSMs come in several configurations and in 3 form factors:

- Luna SA – a scalable 1u rack mountable appliance
- Luna PCI-E – a high performance PCI-E card
- Luna G5 – a small USB-attached HSM for offline root CAs.

Integration Overview

Entrust Security Manager serves as the Certification Authority in an Entrust infrastructure. 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

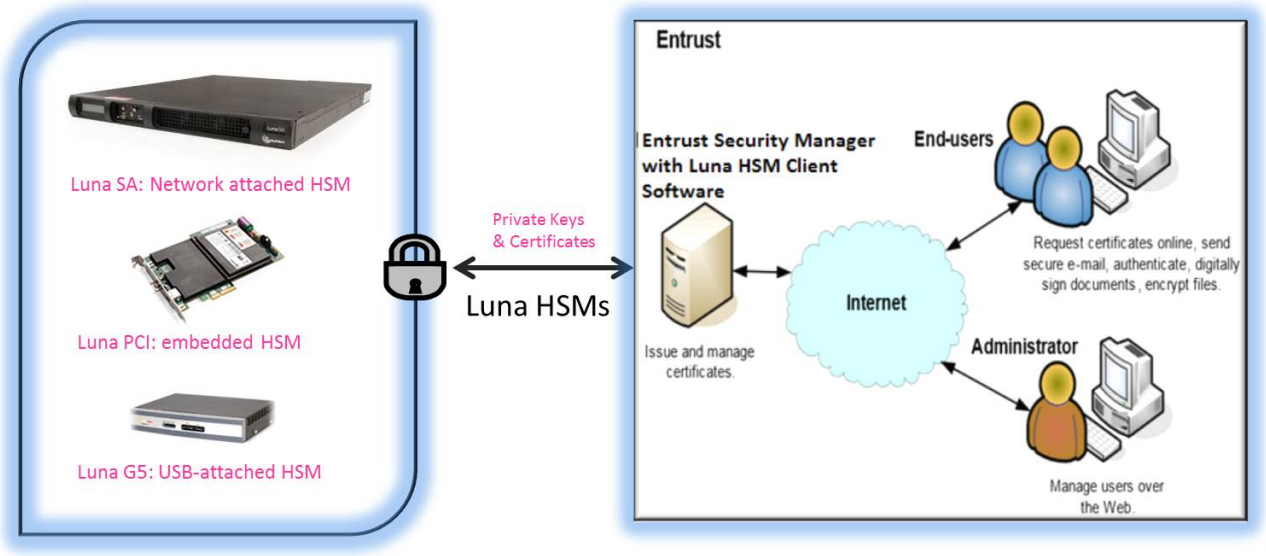
Entrust Authority utilizes the following APIs: PKCS #11.

Integration Details

Luna HSM 5.4 with Entrust Security Manager 8.1

Installation Overview

This section describes how to integrate new installations of Entrust Authority Security Manager 8.1 with Luna HSMs. Note that in the following discussion, there will be Entrust Authority Security Manager Server, and Luna HSM SA/Luna PCI/Luna G5 configured with Entrust Authority Security Manager Server machine. For the purpose of this discussion, the Entrust system assumes the role of Client to the Luna HSM.



Preparing the Luna HSM

i. Install the Luna Client software on the Entrust/PKI server prior to the installation of Entrust software. Refer to the SafeNet Luna HSM documentation.

ii. Ensure that one HSM Partition is created on the Luna HSM and that it has the appropriate policies for your situation. Refer to the SafeNet Luna HSM documentation. The HSM Partition Password/login secret will be used during the Entrust installation. Confirm that the Luna HSM Partition can be accessed with the HSM Partition Password that you can login to the partition. If you are using a PED-Auth HSM, ensure that the partition is activated.

iii. Entrust is 32 bit application so on Windows 2008 R2 & Windows 2012 R2 update chrystoki.ini file to point to 32 bit Luna HSM library. “chrystoki.ini” is located at “C:\Program Files\SafeNet\LunaClient”

For example:

[Chrystoki2]
LibNT= C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll

Installing Entrust Security Manager 8.1 with Luna

i. Install Entrust Security Manager 8.1, following Entrust documentation.

ii. Run the Entrust Security Manager 8.1 Configuration Utility. At the point where you choose whether to store keys in hardware or in software, select hardware. Point to the Luna HSM library path

*/usr/safenet/lunaclient/lib/*libCryptoki2.so on Linux

C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll on Windows

iii. Entrust Configuration Utility presents the option to use SafeNet Luna hardware, and displays the HSM's serial number. Select the correct HSM

iv. Continue with the Configuration until complete.

v. Initialize Entrust Security Manager following Entrust documentation.

vi. Entrust Security Manager detects hardware and requests for the hardware password. Enter the HSM Partition's Partition Password/login secret.

vii. Entrust Security Manager generates the CA keys on the Luna HSM.

System Behavior/Limitations

1. 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

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

Partner Contact Information

Sales Contact: (800) 533-3958
Support Contact: (800) 545-6608

Please check PSIC for the latest supported version information at:
https://www.entrust.com/support/psic/index.cfm

Additional Information

The SafeNet Luna® family of products comprises range of hardware security solutions for digital identity applications. Luna products feature true hardware key management to maintain the integrity of encryption keys. Sensitive keys are created, stored, and used exclusively within the secure confines of the Luna hardware security module (HSM) to prevent compromise.

To learn more about the SafeNet Luna SA product, view the following web site link where additional product information can be found:

http://www.safenet-inc.com/hardware_security_modules/lunasa.aspx