Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012317-001 (Rev B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>March 2015</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimer

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
**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 SafeNet Customer Support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td><a href="mailto:support@safenet-inc.com">support@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

CHAPTER 1 Introduction ...................................................................................................... 5
Understanding the Red Hat Certificate System .................................................................................................... 5
Scope .................................................................................................................................................................... 5
Prerequisites.......................................................................................................................................................... 5

CHAPTER 2 Installing and Configuring Red Hat Certificate System ........................................... 7
Installing and configuring the Red Hat Directory Server 8.2 ................................................................................. 8
Installing and Configuring the Red Hat Certificate System 8.1 ............................................................................. 9
Creating the CA Instance .................................................................................................................................... 11

CHAPTER 3 Integrating Red Hat Certificate System with Luna SA ............................................. 13
Setting up Luna SA with Red Hat Certificate System .......................................................................................... 13
This document covers the necessary information to install, configure and integrate Red Hat Certificate System with SafeNet Luna SA Hardware Security Module (HSM).

The integration between the HSM and Red Hat Certificate System uses the PKCS #11 Cryptographic API.

Understanding the Red Hat Certificate System

Red Hat Certificate System provides a powerful security framework to manage user identities and ensure privacy of communications. Handling all the major functions of the identity life cycle, Red Hat Certificate System simplifies enterprise-wide deployment and adoption of a Public Key Infrastructure (PKI). Support for Global Platform permits direct communication between a registration authority and a smart card for key management tasks such as enrollment and PIN reset.

Red Hat Certificate System works behind the scenes to issue, renew, suspend, revoke, and manage single and dual key X.509v3 certificates needed to handle strong authentication, single sign-on, and secure communications.

Scope

The following combination has been tested:

<table>
<thead>
<tr>
<th>3rd Party Application</th>
<th>Platform</th>
<th>HSM Firmware</th>
<th>Luna Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Certificate System 8.1 with Red Hat Directory Server 8.2</td>
<td>Red Hat Enterprise Linux 5.8 (64 bit)</td>
<td>v6.2.1</td>
<td>v5.x (64 bit)</td>
</tr>
</tbody>
</table>

Prerequisites

Luna SA Setup

Please refer to the Luna SA documentation for installation steps and details regarding configuring and setting up the box on Linux systems. Before you get started ensure the following:

- Luna SA appliance and a secure admin password
- Luna SA, and a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance.
• Created and exchanged certificates between the Luna SA and your Client system.

• Created a partition on the HSM, remember the partition password that will be later used by Red Hat Certificate System. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is <luna client installation directory>/bin/vtl verify for Linux.

• Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).
CHAPTER 2: Installing and Configuring Red Hat Certificate System

Red Hat Certificate System is a highly configurable set of components which create and manage certificates and keys at every point of the certificate lifecycle.

The core of the Certificate System is the Certificate Manager. This is the only required subsystem, and it handles the actual certificate management tasks. The other subsystems can be added for extra functionality.

The Certificate Authority (CA) is a subsystem used to manage certificates, keys, and CRLs through every step of the cycle of a certificate.

Before installing the CA, check the requirements and dependencies for the specific platform, and check which packages are installed. Before proceeding further, see the Red Hat Certificate System Installation Guide, Install_Guide.pdf.

This section describes how to quickly set up and configure Red Hat Certificate System on Red Hat Enterprise Linux x86_64 bit platform:

Check that Java -1.6.0-openjdk is installed:

[root@hostname ~]# yum info java-1.6.0-openjdk
If not, use the following command to install it:

[root@hostname ~]# yum install java-1.6.0-openjdk

Check that pki-selinux is installed:

[root@hostname ~]# yum info pki-selinux
If not, use the following command to install it:

[root@hostname ~]# yum install pki-selinux

Check that httpd is installed:

[root@hostname ~]# yum info httpd
If not, use the following command to install it:

[root@hostname ~]# yum install httpd
CHAPTER 2: Installing and Configuring Red Hat Certificate System

Check the status of SELinux as follows:

[root@hostname ~]# sestatus
Status should be Permissive, if not then change the SELinux status to Permissive in the file /etc/selinux/config
Restart the machine when the file is edited

Installing and configuring the Red Hat Directory Server 8.2

All subsystems require access to Red Hat Directory Server 8.2 on the local machine or a remote machine. This Directory Server instance is used by the subsystems to store their system certificates and user data. The Directory Server used by the Certificate System subsystems can be installed on Red Hat Enterprise Linux 5.8 x86_64-bit. Check that the Red Hat Directory Server is already installed. For example:

[root@hostname bin]# yum info redhat-ds
If the redhat-ds is not installed, download the redhat-ds iso file from the Red Hat Network channel, and then perform the following steps.

- Create a folder called disk in /mnt.
- Create a folder called localrepo in /opt.
- Mount the package rhel-direrv-8.2-x86_64-disc1.iso:
  [root@hostname home]# mount -o loop rhel-dirserv-8.2-x86_64-disc1.iso /mnt/disk
- Copy the folder RPMS into /opt/localrepo/:
  [root@hostname RedHat]# cp -rf RPMS/ /opt/localrepo
- To create the yum local repository, edit the yum.conf in /etc as follows:
  [root@hostname etc]# vi yum.conf
  [main]
  cachedir=/var/cache/yum
  keepcache=0
  debuglevel=2
  logfile=/var/log/yum.log
  distroverpkg=redhat-release
  tolerant=1
  exactarch=1
  obsoletes=1
  gpgcheck=1
  plugins=1
  # Note: yum-RHN-plugin doesn't honor this.
  metadata_expire=1h
  [localrepo]
name=RHEL 5 $releasever - $basearch
baseurl=file:///opt/localrepo/RPMS
enabled=1
# Default.
# installonly_limit = 3
# PUT YOUR REPOS HERE OR IN separate files named file.repo
# in /etc/yum.repos.d

• To create the yum local repository, use the following command:
  [root@hostname RPMS]# createrepo /opt/localrepo/RPMS/
  11/11 - adminutil-1.1.8-2.el5dsrv.x86_64.rpm

• Backup the folder repodata in /opt/localrepo/RPMS as follows:
  [root@hostname RPMS]# cp -rf repodata/ /tmp/

• To install Red Hat Directory Server, use the following command:
  [root@hostname RPMS]# yum install redhat-ds-8.2.0-2.el5dsrv.x86_64.rpm

• To configure the Red Hat Directory Server, use the following commands:
  root@hostname RPMS]# cd /usr/sbin
  [root@hostname sbin]# ./setup-ds-admin.pl

• When prompted:
  o Continue with the setup.
  o Agree to the license terms.
  o Continue with the setup.
  o Select Express as the setup type.
  o Do not register the software with an existing configuration directory server.
  o Enter a password for administrator ID.
  o Enter a password for Directory Manager DN.
  o Continue with setting up your servers.

Installing and Configuring the Red Hat Certificate System 8.1

The individual subsystems for Red Hat Certificate System are installed and then configured individually. The initial installation is done using package management tools such as RPM.

The subsystem setup is done using an HTML-based configuration wizard. Download the Certificate System packages from the Red Hat Network channel. For installing Red Hat Certificate system 8.1, create a folder called localrepo1 in /opt.
• Mount the Red Hat Certificate system 8.1 package RHEL5.8-RHCertSystem-8.1-x86_64-disc1-ftp.iso, and then copy the folder RPMS into /opt/localrepo1:

```
[root@hostname etc]# mount -o loop RHEL5.8-RHCertSystem-8.1-x86_64-disc1-ftp.iso /mnt/disk/
[root@hostname etc]# cd /mnt/disk/RedHat/
[root@hostname RedHat]# cp -rf RPMS/ /opt/localrepo1
```

• To create the yum local repository, edit the yum.conf in /etc as follows:

```
[root@hostname etc]# vi yum.conf
[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
# Note: yum-RHN-plugin doesn't honor this.
metadata_expire=1h
[localrepo]
name=RHEL 5 $releasever - $basearch
baseurl=file:///opt/localrepo1/RPMS
enabled=1
# Default.
# installonly_limit = 3
# PUT YOUR REPOS HERE OR IN separate files named file.repo
# in /etc/yum.repos.d
```

• Back up the repodata in /opt/localrepo1/RPMS as follows:

```
[root@hostname RPMS]# cp -rf repodata/ /tmp/
```

• Use the following command to create the yum local repository:

```
[root@hostname RPMS]# createrepo /opt/localrepo1/RPMS/
38/38 - pki-util-javadoc-8.0.0-16.el5pki.noarch.rpm
```

• To install pki-ca:
[root@hostname RPMS]# yum install pki-ca-8.1.0-10.el5pki.noarch.rpm

Creating the CA Instance

The first step is to create the instance. The command options here are on separate lines to make it clear what options are used; in practice, all options should be on a single line.

    pkicreate -pki_instance_root=/var/lib
    -pki_instance_name=pki-ca
    -subsystem_type=ca
    -agent_secure_port=9443
    -ee_secure_port=9444
    -ee_secure_client_auth_port=9446
    -admin_secure_port=9445
    -unsecure_port=9180
    -tomcat_server_port=9701
    -redirect logs=/var/log/pki-ca

When the pkicreate command completes, it returns a URL to use to access the web-based configuration wizard and a PIN to use to authenticate. This PIN is also contained in the install logs (/var/lib/instance_name/logs-install.log) and in the CS.cfg file for the instance.

    PKI instance creation completed ...
    Starting pki-ca:
    Using Java Security Manager
    Constructing 'pki-ca.policy' Security Policy
    Starting pki-ca:  [ OK ]
    pki-ca (pid 7324) is running ...
    'pki-ca' must still be CONFIGURED!
    (see /var/log/pki-ca-install.log)

Before proceeding with the configuration, make sure the firewall settings of this machine permit proper access to this subsystem.

    Please start the configuration by accessing:
    https://localhost.localdomain:9445/ca/admin/console/config/login?pin=2PjQiVowTIX4LYY0U9v1

    After configuration, the server can be operated by the command:
    /sbin/service pki-ca start | stop | restart

    Check the status:
    # service pki-ca status
Or

```
# service pki-cad status
pki-ca (pid 3967) is running ...
'pki-ca' must still be CONFIGURED!
(see /var/log/pki-ca-install.log)
```

Now make sure Directory server is also started, execute following command to start directory Server:

```
# /usr/lib64/dirsrv/slapd-localhost/start-slapd
```
CHAPTER 3

Integrating Red Hat Certificate System with Luna SA

Setting up Luna SA with Red Hat Certificate System

To set up Luna SA for Red Hat Certificate System, kindly perform the following steps:

- Verify Luna SA entry in /var/lib/pki-ca/conf/CS.cfg file as below:
  ```
  preop.configModules.module2.userFriendlyName=SafeNet's LunaSA Token Hardware Module
  preop.configModules.module2.commonName=lunasa
  ```

To make sure that a Luna HSM works with Certificate System, edit the configuration files for the HSM before configuring the subsystems:

- Check that the LunaSA module has been properly installed:
  ```
  modutil -dbdir /var/lib/pki-ca/alias -list
  ```

  Listing of PKCS #11 Modules
  -----------------------------------------------
  1. NSS Internal PKCS #11 Module
     slots: 2 slots attached
     status: loaded
     slot: NSS Internal Cryptographic Services
     token: NSS Generic Crypto Services

     slot: NSS User Private Key and Certificate Services
     token: NSS Certificate DB

     2. lunasa
        library name: /usr/lunasa/lib/libCryptoki2_64.so
        slots: 4 slots attached
        status: loaded

        slot: LunaNet Slot
CHAPTER 3: Integrating Red Hat Certificate System with Luna SA

token: part1

slot: Luna UHD Slot
token:

slot: Luna UHD Slot
token:

slot: Luna UHD Slot
token:

-----------------------------------------------------------

• If the LunaSA module isn't listed, then install the module manually using below steps:
  Stop the subsystem.
  # service pki-ca stop
  Load the module.
  **For Luna 5.1.1**
  # modutil -dbdir /var/lib/pki-ca/alias -nocertdb -add lunasa -libfile /usr/lunasa/lib/libCryptoki2_64.so
  **For Luna 5.2.1 onwards**
  # modutil -dbdir /var/lib/pki-ca/alias -nocertdb -add lunasa -libfile /usr/safenet/lunaclient/lib/libCryptoki2_64.so

• Verify that the module has been loaded.
  # modutil -dbdir /var/lib/pki-ca/alias --list
Listing of PKCS #11 Modules

  1. NSS Internal PKCS #11 Module
     slots: 2 slots attached
     status: loaded

     slot: NSS Internal Cryptographic Services
     token: NSS Generic Crypto Services

     slot: NSS User Private Key and Certificate Services
     token: NSS Certificate DB

  2. lunasa
library name: /usr/safenet/lunaclient/lib/libCryptoki2_64.so
slots: 4 slots attached
status: loaded

slot: LunaNet Slot
token: arif

slot: Luna UHD Slot
token:

slot: Luna UHD Slot
token:

slot: Luna UHD Slot
token:

-----------------------------------------------------------

• Start the subsystem.
  
  # service pki-ca start

• Open the /etc/Chrystoki.conf configuration file and add this configuration parameter in Misc section:
  
  Misc
  {
    NetscapeCustomize=1023;
  }

• If they are there, remove these two configuration lines for the applet version.
  
  AppIdMajor=2;
  AppIdMinor=4;

• Restart the server.
  
  # service pki-ca restart

• Now open https://noi1-501792.apac.sfnt.local:9445/ca/admin/console/config/login?pin=xU63XMvWokh7sYGFO8dQ to configure the system. This URL can be found in /var/log/pki-ca-install.log
• On Welcome page click Next.
In the Key Store panel, Under SafeNet’s LunaSA Token Hardware Module, Click on Login.
- Provide partition password and click Next.

- Select SafeNet's LunaSA Token Hardware Module as default keystore and click Next.
In the Create a Security Domain panel, enter Red Hat Security as Security Domain Name. Click Next.

<table>
<thead>
<tr>
<th>Security Domain Name:</th>
<th>Red Hat Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Domain HTTP EE URL (unsafe):</td>
<td>http://(no1:901792.apac.sftp.local:9430)</td>
</tr>
<tr>
<td>Security Domain HTTPS Agent URL (clientauth):</td>
<td>https://(no1:901792.apac.sftp.local:9443)</td>
</tr>
<tr>
<td>Security Domain HTTPS EE URL (non-clientauth):</td>
<td>https://(no1:901792.apac.sftp.local:9444)</td>
</tr>
<tr>
<td>Security Domain HTTPS Admin URL (non-clientauth):</td>
<td>https://(no1:901792.apac.sftp.local:9445)</td>
</tr>
</tbody>
</table>

**NOTE:** Since a Security Domain MUST be a CA (although all CAs are not necessarily Security Domains), an appropriate value for this URL may be obtained by logging into the machine which hosts the desired Security Domain CA as 'root' and running the command "/sbin/service <security_domain_instance_name> status" from the command line.
In the Sub System Type panel, select Configure this instance as a New CA Subsystem, and then select Certificate Authority as the Subsystem name. Click Next.
In the PKI Hierarchy panel, select “Make this Selfsigned Root CA within this new PKI hierarchy.” Click Next.
• In the Internal Database panel, fill in the correct LDAP server information. Click Next.

• In the Key Pairs panel, select Use the following custom key Size. Select RSA as the key type, and then enter the key size, for example 1024, 2048, or 4096. Click Next.
• In the Subject Name panel, select Next.
• In the Requests and Certificates panel, select Apply, and then select Next.
• A message will display to import and trust certificate chain from the CA. Click OK and then click Next.
• In the Administrator panel, enter the correct details.
• Click Next through the remaining panels to import the agent certificate into the browser and complete the configuration.
When configuration is complete,

- Run the following command to restart the subsystem:
  
  # service pki-ca restart

  or

  # service pki-cad restart