THALES

gemalto
a Thales company

Red Hat Certificate System

INTEGRATION GUIDE
SAFENET LUNA HSM
SAFENET DATA PROTECTION ON DEMAND

Document Information

Document Part Number	007-012317-001
Release Date	November 2019

Revision History

Revision	Date	Reason
C	November 2019	Update

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. 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 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.

CONTENTS

PREFACE

This document guides security administrators through the steps for securing Red Hat Certificate System Subsystem private encryption keys inside of a SafeNet Luna HSM or SafeNet Data Protection HSM on Demand (HSMoD) service. This guide covers the necessary information to install and configure the Red Hat Certificate System to use the SafeNet HSM.

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. Notes contain 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**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a | b | c] [<a> | <b> | <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a | b | c } { <a> | <b> | <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database 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 Gemalto 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@gemalto.com.

CHAPTER 1: Introduction

The SafeNet Luna HSM or SafeNet Data Protection HSM on Demand (HSMoD) service integrates with the Red Hat Certificate System to secure the Subsystem private signing keys, off-loading cryptographic operations from the host server to the HSM.

The integration with Red Hat Certificate System uses the industry standard PKCS#11 interface. The Red Hat Certificate System users the PKCS#11 interface to generate RSA/ECDSA keys on the SafeNet HSM. The RSA/ECDSA private keys are used by the Red Hat Certificate System CA, KRA, OCSP, TPS or TKS subsystems for encryption and signing. The following key sizes are supported with SafeNet HSMs.

Algorithms	Supported Key Sizes
RSA	> 1024* > 2048 > 3072 > 4096
ECC	> nistp256 > nistp384 > nistp521

* supported only in Non-FIPS mode.

This guide demonstrates how to complete Red Hat Certificate System integration using a signing key generated on a SafeNet Luna HSM or HSM on Demand service.

Using a SafeNet Luna HSM or HSM on Demand service to generate the RSA/ECDSA keys for Red Hat Certificate System provides the following benefits:

> Secure generation, storage and protection of the signing private keys on FIPS 140-2 level 3 validated hardware.

> Full life cycle management of the keys.

> Access to the HSM audit trail**.

> Take advantage of cloud services with confidence.

> Significant performance improvements by off-loading cryptographic operations from signing servers.

**HSMoD services do not have access to the secure audit trail

About the Red Hat Certificate System

Red Hat Certificate System provides five different subsystems, each focusing on different aspects of a PKI deployment:

- **Certificate Authority called Certificate Manager (CA)** – The core operator of the PKI; issues and revokes certificates.
- **Key Recovery Authority (KRA)** – Recovers lost private keys and archival of keys.
- **Online Certificate Status Protocol (OCSP) Responder** – Provide information whether a certificate is valid or revoked.
- **Token Key Service (TKS)** – Manages master key that helps establishing secure channels between smart cards and the Token Management System (TKS/TPS)
- **Token Processing System (TPS)** – Interacts directly with smart cards and manages the keys and certificates on them through client side applications such as Enterprise Security Client (ESC).

The Red Hat Certificate System issues, renews, suspends, revokes, and manages X.509v3 certificates required for strong-authentication, single sign-on, and secure communications.

Third Party Application Details

This integration uses the following third party applications:

- Red Hat Certificate System

Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: SafeNet 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. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic

The following platforms are supported:

Third Party Application	Platform
Red Hat Certificate System 9.5 with Red Hat Directory Server 10.4	Red Hat Enterprise Linux 7.6 (64-bit)
Red Hat Certificate System 8.1 with Red Hat Directory Server 8.2	Red Hat Enterprise Linux 5.8 (64-bit)

NOTE: Red Hat Certificate System is tested with Luna Clients in HA and FIPS Mode.

SafeNet DPoD: SafeNet Data Protection on Demand (DPoD) is a cloud-based platform that provides HSM on Demand services (HSMoD) through a simple graphical user interface. With DPoD, 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 the services you need.

The following platforms are supported:

Third Party Application	Platform
Red Hat Certificate System 9.5 with Red Hat Directory Server 10.4	Red Hat Enterprise Linux 7.6 (64-bit)

Prerequisites

Before beginning the integration, complete the following. Complete the HSM set up for the SafeNet HSM you are using.

Configuring the SafeNet Luna Network HSM

If you are using a SafeNet Luna HSM, ensure the following:

> **NOTE:** Refer to the *SafeNet Luna HSM Product Documentation* for detailed instructions on creating the NTLS connection, initializing the SafeNet Luna HSM partition, and initializing the Security Officer, Crypto Officer, and Crypto User roles.

1. Ensure the HSM is set up, initialized, provisioned and ready for deployment.
2. Create a partition on the SafeNet Luna HSM for use with Red Hat Certificate System.
3. Register a client for the system and assign the client to a partition to create an NTLS connection. Initialize the Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. Connect to LunaCM to verify the registered partitions: `/usr/safenet/lunaclient/bin/lunacm`

```
lunacm (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.

      Available HSMs:

      Slot Id ->              0
      Label ->                rhcs-pki
      Serial Number ->        1280780175938
      Model ->                LunaSA 7.3.0
      Firmware Version ->     7.3.0
      Configuration ->        Luna User Partition With SO (PW) Key Export With
Cloning Mode
      Slot Description ->     Net Token Slot

      Current Slot Id: 0
```

Configuring PED Authenticated SafeNet Luna HSM (v7.x)

If you are using a PED-based SafeNet Luna HSM, ensure the policy `ProtectedAuthenticationPathFlagStatus` is set to "`1`" in the `Misc` section of the `Chrystoki.conf` file.

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

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, allowing you to upgrade your client software while retaining your hsmusers group configuration.

> **NOTE:** Controlling user access to the HSM requires **sudo** privileges.

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 assign to the hsmusers group must exist on the client workstation.

To add users to the hsmusers group

To add a user to the hsmusers group, run the below command:

```
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.

To remove a user from the hsmusers group

To remove a user from the hsmusers group, run the below command:

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

Where <username> is the name of the user you want to remove from the hsmusers group.

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

Provisioning your HSM on Demand Service

Create an HSM on Demand Service for the Red Hat Certificate System to use. Refer to the *SafeNet Data Protection on Demand Platform HELP* for detailed configuration and setup procedures. Please familiarize yourself with the section Constraints on HSMoD Services before proceeding.

Before beginning the integration with an HSMoD service, ensure the following:

1. HSMoD service for Red Hat Certificate System integration exists.
2. HSMoD service client is downloaded and available on the Red Hat Certificate client system.

   NOTE: The HSMoD service client is a zip file that contains system information required to connect the client machine to the HSMoD service.

3. HSMoD service is initialized with the following user roles:
   a. Security Officer (SO)
   b. Crypto Officer (CO)
   c. Crypto User (CU)

Constraints on HSMoD Services

If using an HSMoD service please be aware of the following conditions:

HSM on Demand Service in FIPS mode

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand 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.

Verify HSM on Demand <slot> value

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send the commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use slot list to determine which slot numbers are in use by which HSMoD service.

Using SafeNet 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 SafeNet Luna HSM or an HSMoD service in FIPS mode, you have to make the following change in configuration file:

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

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

Set up Red Hat Certificate System

Before proceeding, we recommend you familiarize yourself with Red Hat Certificate System. Refer to the PLANNING, INSTALLATION, AND DEPLOYMENT GUIDE of Red Hat Certificate System Documentation

for more information on installation and pre-installation requirements. Once familiar, install the Red Hat Certificate System on the target machine to continue the integration process.

All subsystems of the Red Hat Certificate System require access to the Red Hat Directory Server on a local or remote machine. The Red Hat Directory Server instance is used by the subsystems to store the system certificates and user data. The Red Hat Directory Server, used by the Certificate System Subsystems must be installed before installing the Red Hat Certificate System. Refer to the Red Hat Directory Server Installation Documentation for detailed instructions on installing the Red Hat Directory Server.

CHAPTER 2: Integrating SafeNet HSM with Red Hat Certificate System 9.5

To configure Red Hat Certificate System 9.5 to use the SafeNet Luna HSM or HSMoD service, complete the following:

> Configuring the HSM parameters for Red Hat Certificate System

> Installing the Red Hat Certificate System Subsystems

Configuring the HSM parameters for Red Hat Certificate System

The Red Hat Certificate System creates a default configuration file during installation. To use the SafeNet HSM with the Red Hat Certificate System you create a PKI configuration file, **default_luna.txt**, which overrides the default values of the **/etc/pki/default.cfg** file.

Create the **default_luna.txt** file. Copy the following and ensure, you replace all the passwords and HSM parameter values with the appropriate content (the passwords and HSM parameter values that will require replacement are highlighted in **bold**).

```
##############################################################################
##############################################################################
##############################################################################
##                                                                          ##
## EXAMPLE: Configuration File used to override '/etc/pki/default.cfg'    ##

## when using a LunaSA Hardware Security Module (HSM):                      ##
##                                                                          ##
##                                                                          ##
## # modutil -dbdir . -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: rhcs-pki                                                              ##
##                                                                              ##
## slot: Luna UHD Slot                                                          ##
## token:                                                                       ##
##                                                                              ##
## slot: Luna UHD Slot                                                          ##
## token:                                                                       ##
##                                                                              ##
## slot: Luna UHD Slot                                                          ##
## token:                                                                       ##
## ------------------------------------------------------------                 ##
##                                                                              ##
##                                                                              ##
## Based on the example above, substitute all password values,                  ##
## as well as the following values:                                             ##
##                                                                              ##
## <hsm_libfile>=/usr/safenet/lunaclient/lib/libCryptoki2_64.so                 ##
## <hsm_modulename>=lunasa                                                      ##
## <hsm_token_name>=rhcs-pki                                                    ##
##                                                                              ##
## Where hsm_modulename is user-defined value for SafeNet HSM.                  ##
##                                                                              ##
##################################################################################
##################################################################################
##################################################################################

[DEFAULT]
############################
# Provide HSM parameters #
############################
pki_hsm_enable=True
pki_hsm_libfile=<hsm_libfile>
pki_hsm_modulename=<hsm_modulename>
pki_token_name=<hsm_token_name>
pki_token_password=<pki_token_password>

########################################
# Provide PKI-specific HSM token names #
########################################
pki_audit_signing_token=<hsm_token_name>
pki_ssl_server_token=<hsm_token_name>
pki_subsystem_token=<hsm_token_name>

##################################
# Provide PKI-specific passwords #
##################################
pki_admin_password=<pki_admin_password>
pki_client_pkcs12_password=<pki_client_pkcs12_password>
pki_ds_password=<pki_ds_password>

####################################
# Provide non-CA-specific passwords #
####################################
pki_client_database_password=<pki_client_database_password>
```

```
#################################################################
# ONLY required if specifying a non-default PKI instance name #
#################################################################
#pki_instance_name=<pki_instance_name>

#################################################################
# ONLY required if specifying non-default PKI instance ports #
#################################################################
#pki_http_port=<pki_http_port>
#pki_https_port=<pki_https_port>

#################################################################################
# ONLY required if specifying non-default 389 Directory Server ports #
#################################################################################
#pki_ds_ldap_port=<pki_ds_ldap_port>
#pki_ds_ldaps_port=<pki_ds_ldaps_port>

#################################################################################
# ONLY required if PKI is using a Security Domain on a remote system #
#################################################################################
#pki_ca_hostname=<pki_ca_hostname>
#pki_issuing_ca_hostname=<pki_issuing_ca_hostname>
#pki_issuing_ca_https_port=<pki_issuing_ca_https_port>
#pki_security_domain_hostname=<pki_security_domain_hostname>
#pki_security_domain_https_port=<pki_security_domain_https_port>

#################################################################
# ONLY required for PKI using an existing Security Domain #
#################################################################
# NOTE: pki_security_domain_password == pki_admin_password
# of CA Security Domain Instance
pki_security_domain_password=<pki_admin_password>


[Tomcat]
#################################################################
# ONLY required if specifying non-default PKI instance ports #
#################################################################
#pki_ajp_port=<pki_ajp_port>
#pki_tomcat_server_port=<pki_tomcat_server_port>


[CA]
#######################################
# Provide CA-specific HSM token names #
#######################################
pki_ca_signing_token=<hsm_token_name>
pki_ocsp_signing_token=<hsm_token_name>

#################################################################################
# ONLY required if 389 Directory Server for CA resides on a remote system #
#################################################################################
#pki_ds_hostname=<389 hostname>


[KRA]
#######################################
```

```
# Provide KRA-specific HSM token names #
########################################
pki_storage_token=<hsm_token_name>
pki_transport_token=<hsm_token_name>

#############################################################################
# ONLY required if 389 Directory Server for KRA resides on a remote system #
#############################################################################
#pki_ds_hostname=<389 hostname>


[OCSP]
########################################
# Provide OCSP-specific HSM token names #
########################################
pki_ocsp_signing_token=<hsm_token_name>

#############################################################################
# ONLY required if 389 Directory Server for OCSP resides on a remote system #
#############################################################################
#pki_ds_hostname=<389 hostname>
[TKS]

########################################
# Provide TKS-specific HSM token names #
########################################

#############################################################################
# ONLY required if 389 Directory Server for TKS resides on a remote system #
#############################################################################
#pki_ds_hostname=<389 hostname>


[TPS]
###################################
# Provide TPS-specific parameters #
###################################
pki_authdb_basedn=<dnsdomainname where hostname.b.c.d is dc=b,dc=c,dc=d>

########################################
# Provide TPS-specific HSM token names #
########################################

#############################################################################
# ONLY required if 389 Directory Server for TPS resides on a remote system #
#############################################################################
#pki_ds_hostname=<389 hostname>

###########################################################
# ONLY required if TPS requires a CA on a remote machine #
###########################################################
#pki_ca_uri=https://<pki_ca_hostname>:<pki_ca_https_port>

#####################################
# ONLY required if TPS requires a KRA #
#####################################
#pki_enable_server_side_keygen=True
```

```
############################################################
# ONLY required if TPS requires a KRA on a remote machine  #
############################################################
#pki_kra_uri=https://<pki_kra_hostname>:<pki_kra_https_port>

############################################################
# ONLY required if TPS requires a TKS on a remote machine  #
############################################################
#pki_tks_uri=https://<pki_tks_hostname>:<pki_tks_https_port>
```

Installing and Configuring the Required Subsystems

To install and configure the Red Hat Certificate System Subsystems to use the SafeNet HSMs you create an override file, similar to the sample provided in Configuring the HSM parameters for Red Hat Certificate System.

You must install and configure the Certificate Authority Certificate Manager (CA) before installing and configuring any of the dependent subsystems.

To install the Red Hat Certificate System Subsystems

1. To install the **Certificate Authority (CA)** execute:

   ```
   # pkispawn -s CA -f ./default_luna.txt –vvv
   ```

   Ensure that the command completes successfully without any error. The following is the installation summary that is returned when the installation command completes successfully.

   ```
   ==========================================================================
                                INSTALLATION SUMMARY
   ==========================================================================

         Administrator's username:             caadmin
         Administrator's PKCS #12 file:
               /root/.dogtag/pki-tomcat/ca_admin_cert.p12

         To check the status of the subsystem:
               systemctl status pki-tomcatd@pki-tomcat.service

         To restart the subsystem:
               systemctl restart pki-tomcatd@pki-tomcat.service

         The URL for the subsystem is:
               https://HSMNOI1INT-RHCA.noidalab.local:8443/ca

         PKI instances will be enabled upon system boot
   ```

```
==========================================================================
```

2. To install the **Key Recovery Authority (KRA)** execute:

```
# pkispawn -s KRA -f ./default_luna.txt -vvv
```

Ensure that the command completes successfully without any error. The following is the installation summary that is returned when the installation command completes successfully.

```
==========================================================================
                                INSTALLATION SUMMARY
==========================================================================

      Administrator's username:             kraadmin

      To check the status of the subsystem:
            systemctl status pki-tomcatd@pki-tomcat.service

      To restart the subsystem:
            systemctl restart pki-tomcatd@pki-tomcat.service

      The URL for the subsystem is:
            https://HSMNOI1INT-RHCA.noidalab.local:8443/kra

      PKI instances will be enabled upon system boot
==========================================================================
```

3. To install the **Online Certificate Responder Service (OCSP) Responder** execute:

```
# pkispawn -s OCSP -f ./default_luna.txt –vvv
```

Ensure that the command completes successfully without any error. The following is the installation summary that is returned when the installation command completes successfully.

```
==========================================================================
                                INSTALLATION SUMMARY
==========================================================================

      Administrator's username:             ocspadmin

      To check the status of the subsystem:
            systemctl status pki-tomcatd@pki-tomcat.service

      To restart the subsystem:
            systemctl restart pki-tomcatd@pki-tomcat.service
```

```
      The URL for the subsystem is:
            https://HSMNOI1INT-RHCA.noidalab.local:8443/ocsp

      PKI instances will be enabled upon system boot
 ======================================================================
```

4. To install the **Token Key Service (TKS)** execute:

```
# pkispawn -s TKS -f ./default_luna.txt -vvv
```

Ensure that the command completes successfully without any error. The following is the installation summary that is returned when the installation command completes successfully.

```
======================================================================
                                INSTALLATION SUMMARY
======================================================================

      Administrator's username:             tksadmin

      To check the status of the subsystem:
            systemctl status pki-tomcatd@pki-tomcat.service

      To restart the subsystem:
            systemctl restart pki-tomcatd@pki-tomcat.service
      The URL for the subsystem is:
            https://HSMNOI1INT-RHCA.noidalab.local:8443/tks

      PKI instances will be enabled upon system boot
======================================================================
```

5. To install the **Token Processing System (TPS)** execute:

```
# pkispawn -s TPS -f ./default_luna.txt -vvv
```

Ensure that the command completes successfully without any error. The following is the installation summary that is returned when the installation command completes successfully.

```
======================================================================
                                INSTALLATION SUMMARY
======================================================================

      Administrator's username:             tpsadmin

      To check the status of the subsystem:
            systemctl status pki-tomcatd@pki-tomcat.service
```

```
        To restart the subsystem:
              systemctl restart pki-tomcatd@pki-tomcat.service

        The URL for the subsystem is:
              https://HSMNOI1INT-RHCA.noidalab.local:8443/tps

        PKI instances will be enabled upon system boot
======================================================================
```

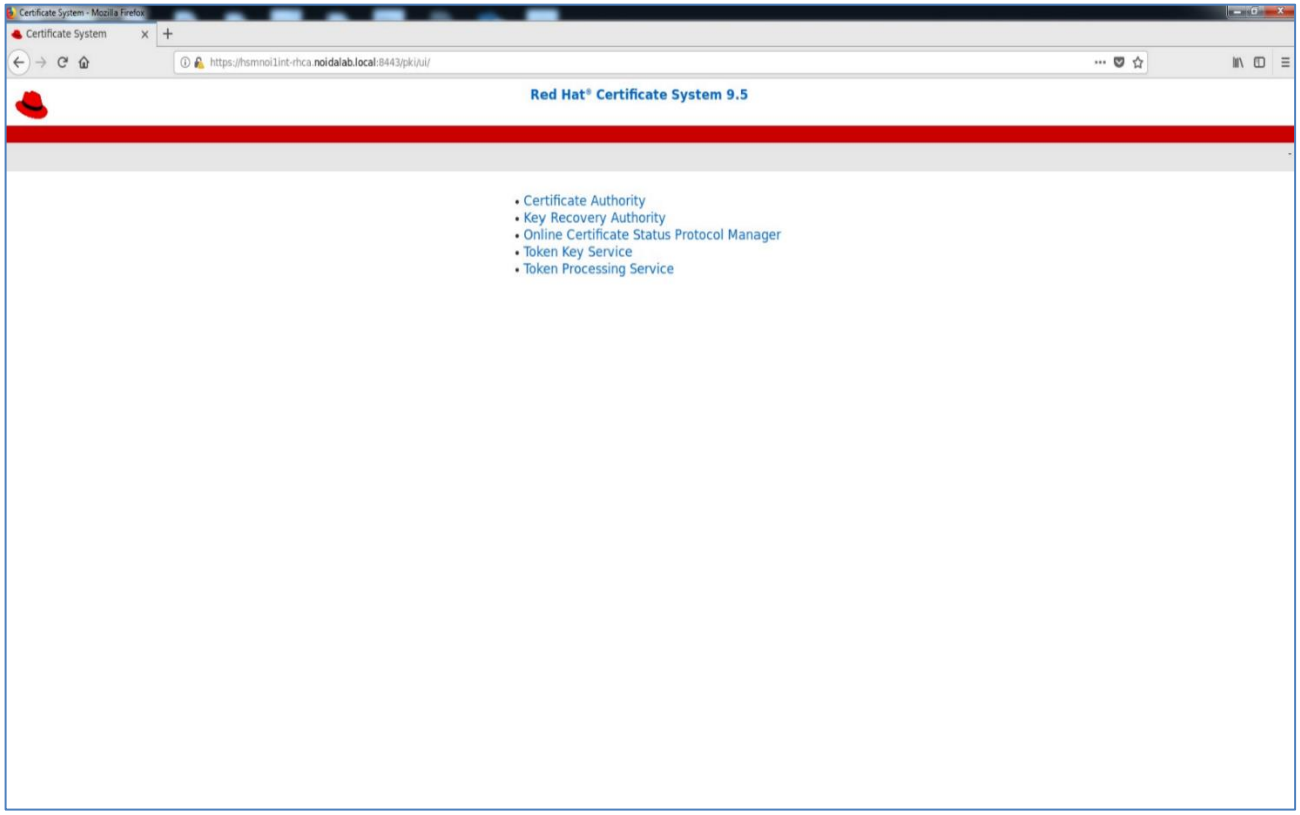
6. You can check the partition contents to ensure that all keys are created on SafeNet HSM using the command below:

```
# /usr/safenet/lunaclient/bin/cmu list
Certificate Management Utility (64-bit) v7.3.0-165. Copyright (c) 2018
SafeNet. All rights reserved.
Please enter password for token in slot 0 : ********

handle=462      label=auditSigningCert cert-pki-tomcat TPS
handle=634      label=auditSigningCert cert-pki-tomcat TPS
handle=641      label=
handle=382      label=auditSigningCert cert-pki-tomcat TKS
handle=572      label=auditSigningCert cert-pki-tomcat TKS
handle=558      label=
handle=385      label=auditSigningCert cert-pki-tomcat OCSP
handle=373      label=ocspSigningCert cert-pki-tomcat OCSP
handle=539      label=auditSigningCert cert-pki-tomcat OCSP
handle=496      label=
handle=686      label=ocspSigningCert cert-pki-tomcat OCSP
handle=534      label=
handle=442      label=auditSigningCert cert-pki-tomcat KRA
handle=419      label=storageCert cert-pki-tomcat KRA
handle=359      label=transportCert cert-pki-tomcat KRA
handle=674      label=auditSigningCert cert-pki-tomcat KRA
handle=362      label=
handle=643      label=storageCert cert-pki-tomcat KRA
handle=523      label=
handle=379      label=transportCert cert-pki-tomcat KRA
handle=644      label=
handle=590      label=Server-Cert cert-pki-tomcat
```

```
handle=370      label=auditSigningCert cert-pki-tomcat CA
handle=416      label=subsystemCert cert-pki-tomcat
handle=584      label=ocspSigningCert cert-pki-tomcat CA
handle=412      label=caSigningCert cert-pki-tomcat CA
handle=639      label=auditSigningCert cert-pki-tomcat CA
handle=638      label=
handle=625      label=subsystemCert cert-pki-tomcat
handle=623      label=
handle=608      label=
handle=599      label=
handle=578      label=ocspSigningCert cert-pki-tomcat CA
handle=577      label=
handle=547      label=caSigningCert cert-pki-tomcat CA
handle=560      label=
```

7. You can browse the Red Hat Certificate Subsystem console using the URL below:
   https://<fully qualified domain name>:8443



This completes the Red Hat Certificate System integration with SafeNet HSM. All subsystems keys are secured on SafeNet HSM partition and available to Red Hat Certificate System when required.

CHAPTER 3: Integrating SafeNet Luna HSM with Red Hat Certificate System 8.1

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.

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 in Red Hat Documentation.

This section describes how to quickly set up and configure Red Hat Certificate System 8.1 on Red Hat Enterprise Linux 5.8 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
```

Check the status of SELinux:

```
[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 and verify that the SELinux status is set to **Permissive**.

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. Verify 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 complete the following procedure:

To install and configure the Red Hat Directory Server

1. Create a folder called disk in **/mnt**.
2. Create a folder called **localrepo** in **/opt**.
3. Mount the package **rhel-dirserv-8.2-x86_64-disc1.iso**:

   ```
   [root@hostname home]# mount -o loop rhel-dirserv-8.2-x86_64-disc1.iso
   /mnt/disk
   ```

4. Copy the folder RPMS into **/opt/localrepo/**:

   ```
   [root@hostname RedHat]# cp -rf RPMS/ /opt/localrepo
   ```

5. Edit the **yum.conf** in **/etc**, using **vi** or a text editor:

   ```
   [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
```

6. Create the yum local repository execute:

```
[root@hostname RPMS]# createrepo /opt/localrepo/RPMS/
11/11 - adminutil-1.1.8-2.el5dsrv.x86_64.rpm
```

7. Backup the folder **repodata** in **/opt/localrepo/RPMS** as follows:

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

8. Install the Red Hat Directory Server:

```
[root@hostname RPMS]#yum install redhat-ds-8.2.0-2.el5dsrv.x86_64.rpm
```

9. Configure the Red Hat Directory Server:

```
[root@hostname RPMS]# cd /usr/sbin
[root@hostname sbin]# ./setup-ds-admin.pl
```

Respond to the prompts as follows:

   a. Continue with the setup.
   b. Agree to the license terms.
   c. Continue with the setup.
   d. Select **Express** as the setup type.
   e. Do **not** register the software with an existing configuration directory server.
   f. Enter a password for administrator ID.
   g. Enter a password for Directory Manager DN.
   h. 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.

To install and configure the Red Hat Certificate System 8.1

1. Create a folder called localrepo1 in **/opt**.
2. 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
```

3. 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
```

4. Back up the **repodata** in **/opt/localrepo1/RPMS** as follows:

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

5. Create the yum local repository:

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

6. Install the **pki-ca**:

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

Creating the CA Instance

Create the Certificate Authority (CA) Certificate Manager on the Red Hat Certificate System. The CA is the core operator of the PKI and responsible for issuing and revoking all certificates.

To create the CA instance

1. The first step is to create the instance. The command options here are on separate lines to clarify 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** that you use 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=2PjQlV
owTIX4LYY0U9v1

After configuration, the server can be operated by the command:

/sbin/service pki-ca start | stop | restart
```

2. 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)
```

3. Start the directory Server:

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

Setting up Luna SA with Red Hat Certificate System 8

With the Red Hat Certificate System installed, you can now configure it to use the SafeNet Luna SA HSM.

To set up Luna SA with Red Hat Certificate System 8

1. Verify the Luna SA entry in **/var/lib/pki-ca/conf/CS.cfg** appears as follows:

```
preop.configModules.module2.userFriendlyName=SafeNet's LunaSA Token
Hardware Module
preop.configModules.module2.commonName=lunasa
```

2. Edit the configuration files for the HSM before configuring the subsystems, to ensure that the Luna HSM works with Certificate System.

   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
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:

a. Stop the subsystem.

```
# service pki-ca stop
```

b. 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
```

3. 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: part1

slot: Luna UHD Slot
token:

slot: Luna UHD Slot
token:

slot: Luna UHD Slot
token:
--------------------------------------------------------------
```

4. Start the subsystem.

   ```
   # service pki-ca start
   ```

5. Open the **/etc/Chrystoki.conf** configuration file and add this configuration parameter in `[Misc]` section:

   ```
   Misc
   {
   NetscapeCustomize=1023;
   }
   ```

6. If the following lines are listed in the **/etc/Chrystoki.conf** configuration file, remove them:

   ```
   AppIdMajor=2;
   AppIdMinor=4;
   ```

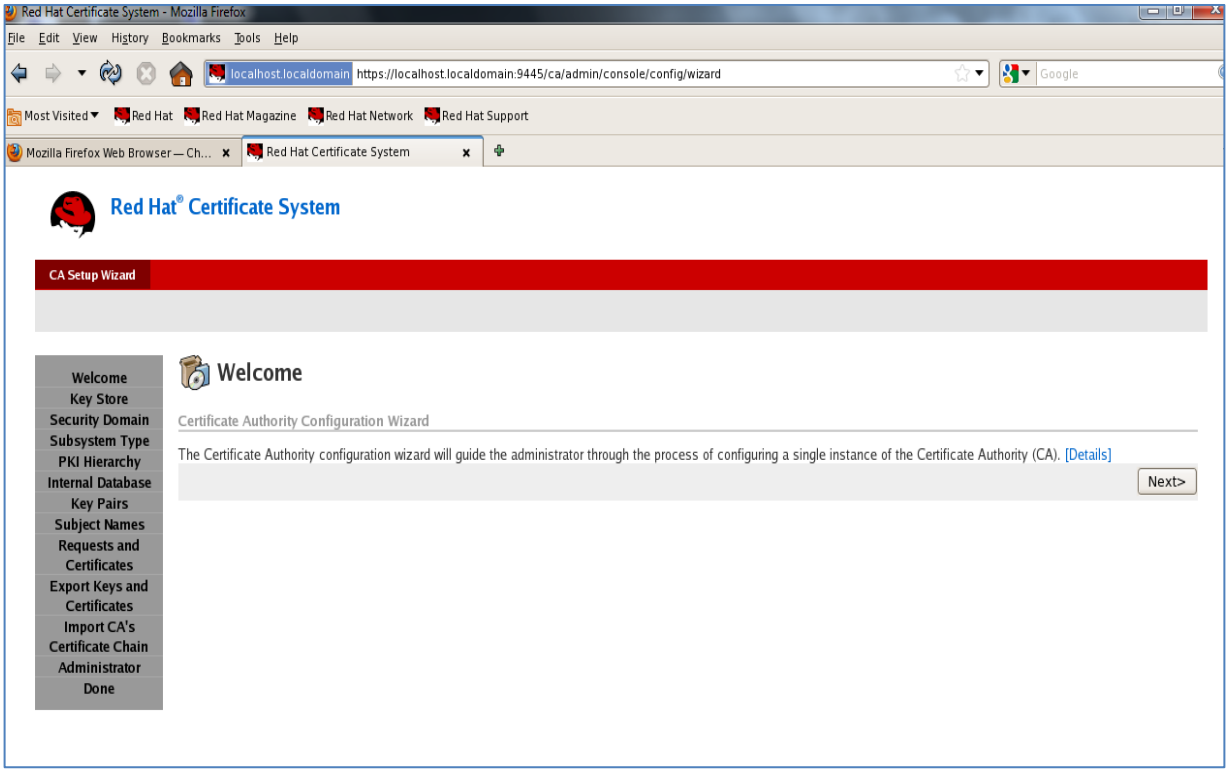
7. Restart the server.

   ```
   # service pki-ca restart
   ```

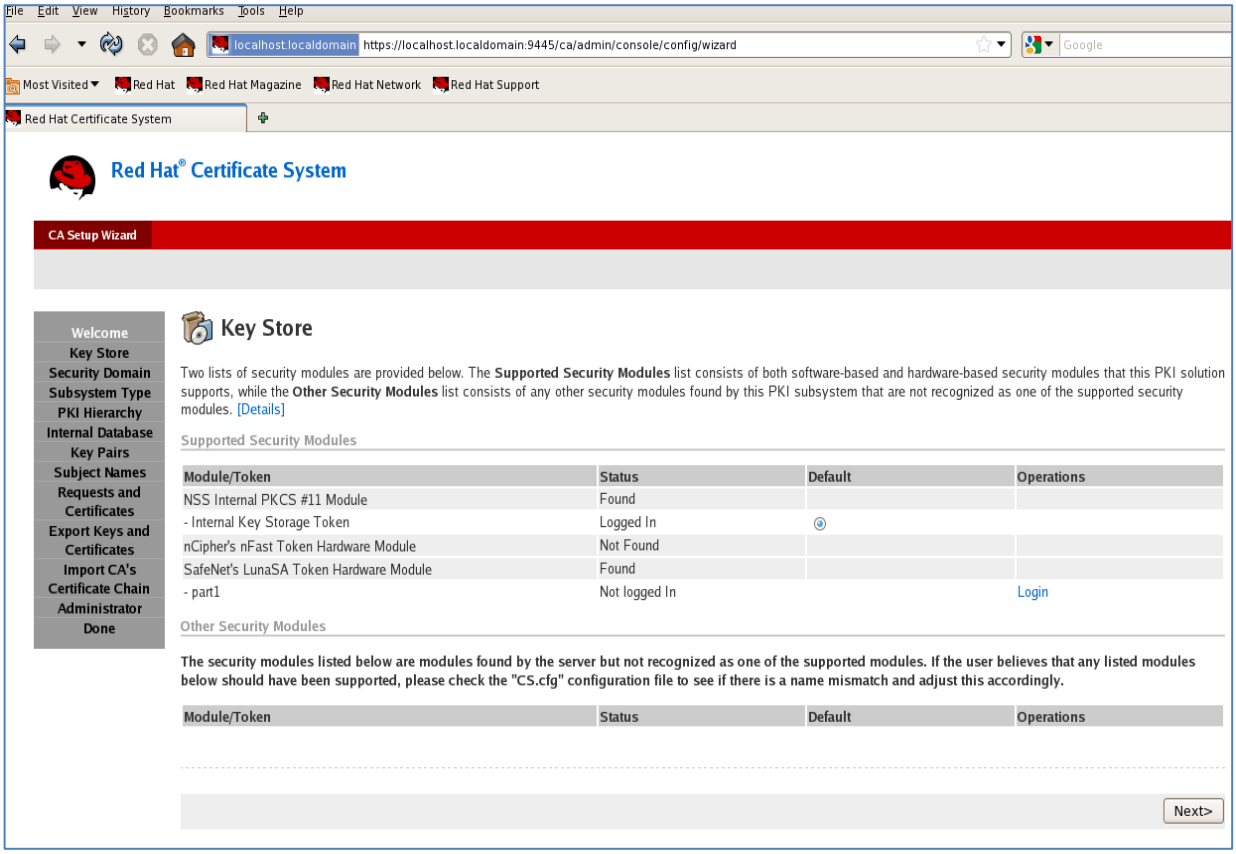
8. Now open the Red Hat Certificate System URL to configure the system. This URL can be found in **/var/log/pki-ca-install.log**

   Example URL: https://noi1-501792.apac.sfnt.local:9445/ca/admin/console/config/login?pin=xU63XMvWokh7sYGFO8dQ

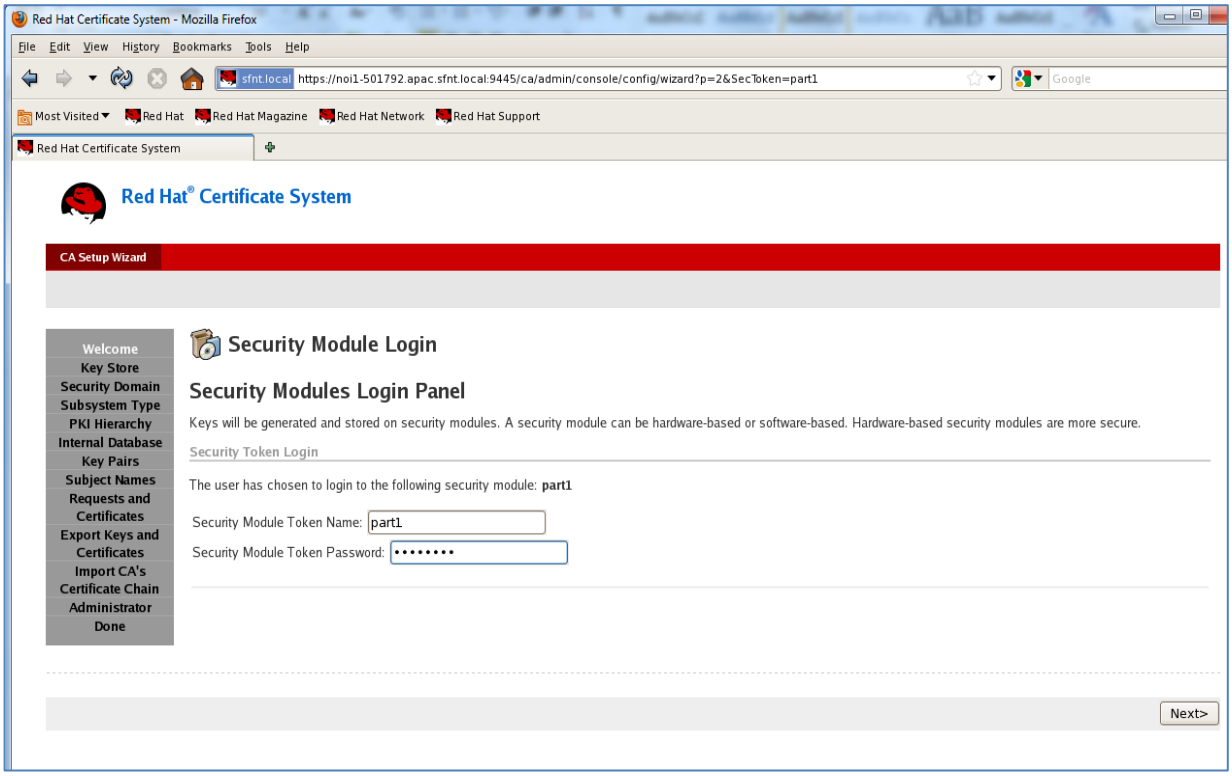
9. On **Welcome** page click **Next>**.



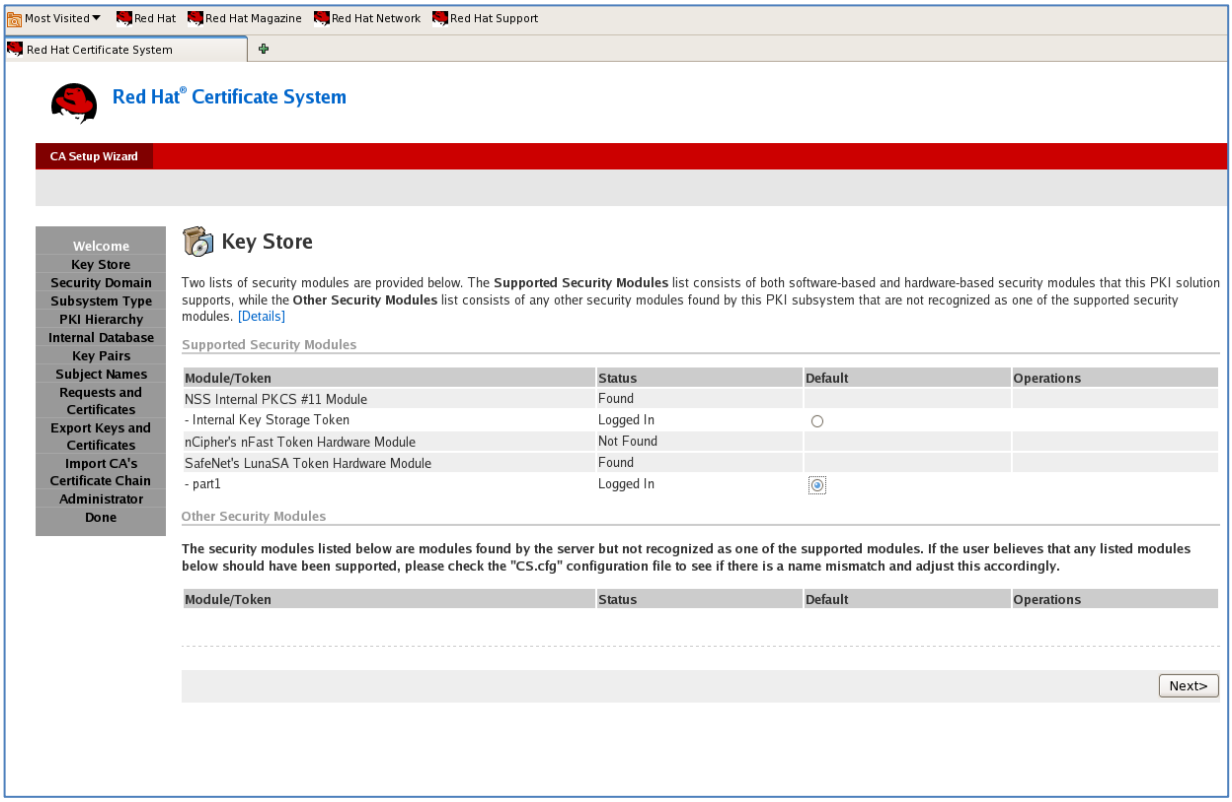
10. In the Key Store panel, Under **SafeNet's LunaSA Token Hardware Module**, click **Login**.



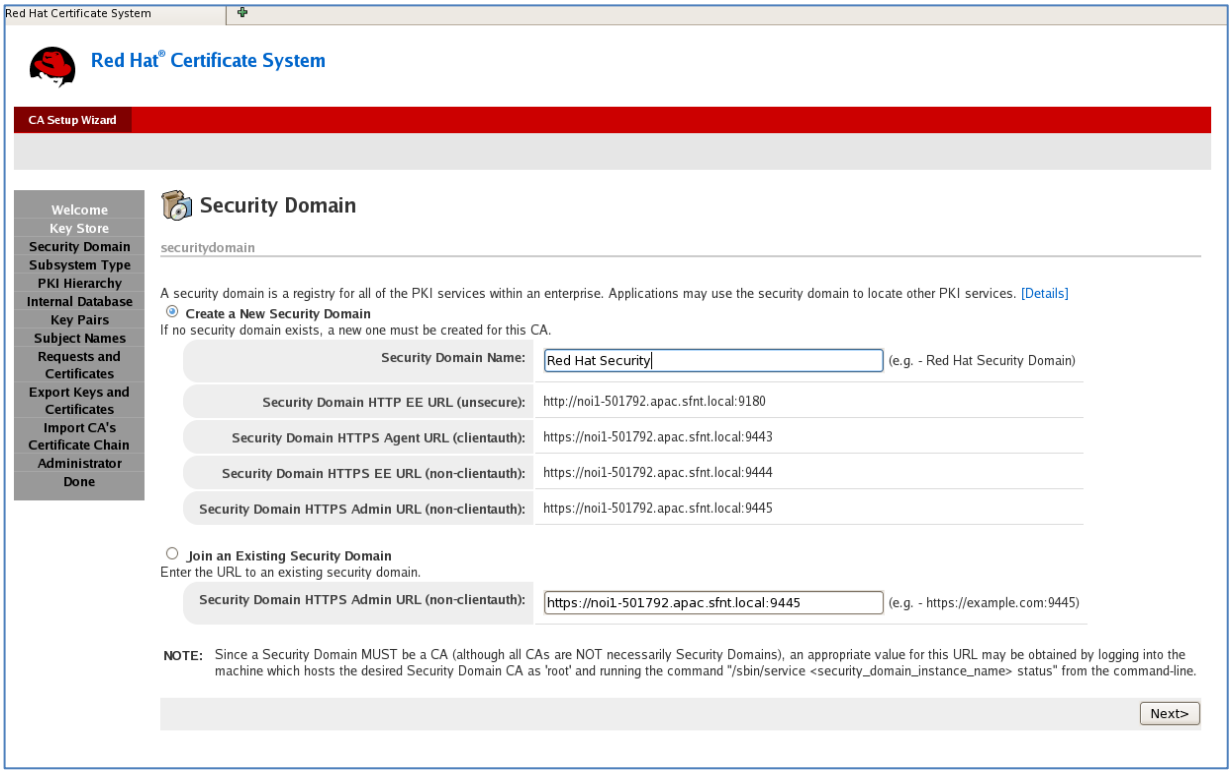
11. Provide partition password and click **Next>**.



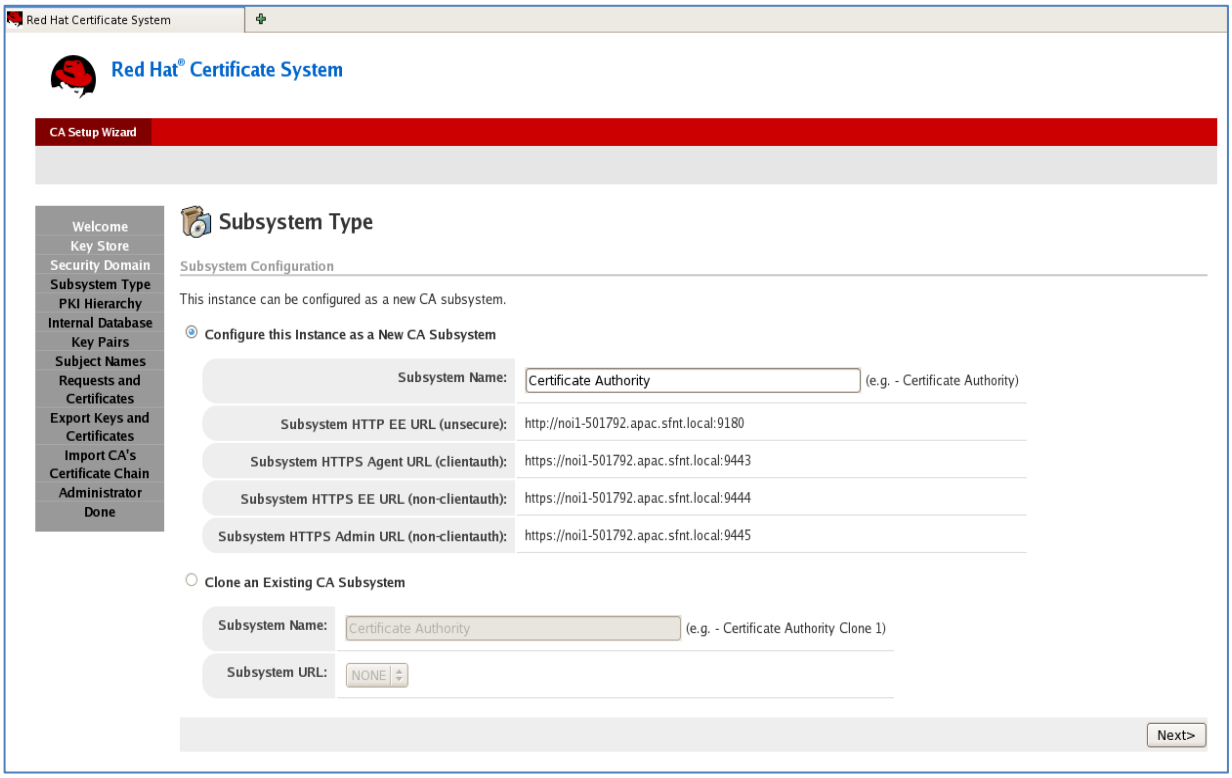
12. Select **SafeNet's LunaSA Token Hardware Module** as default keystore and click **Next>**.



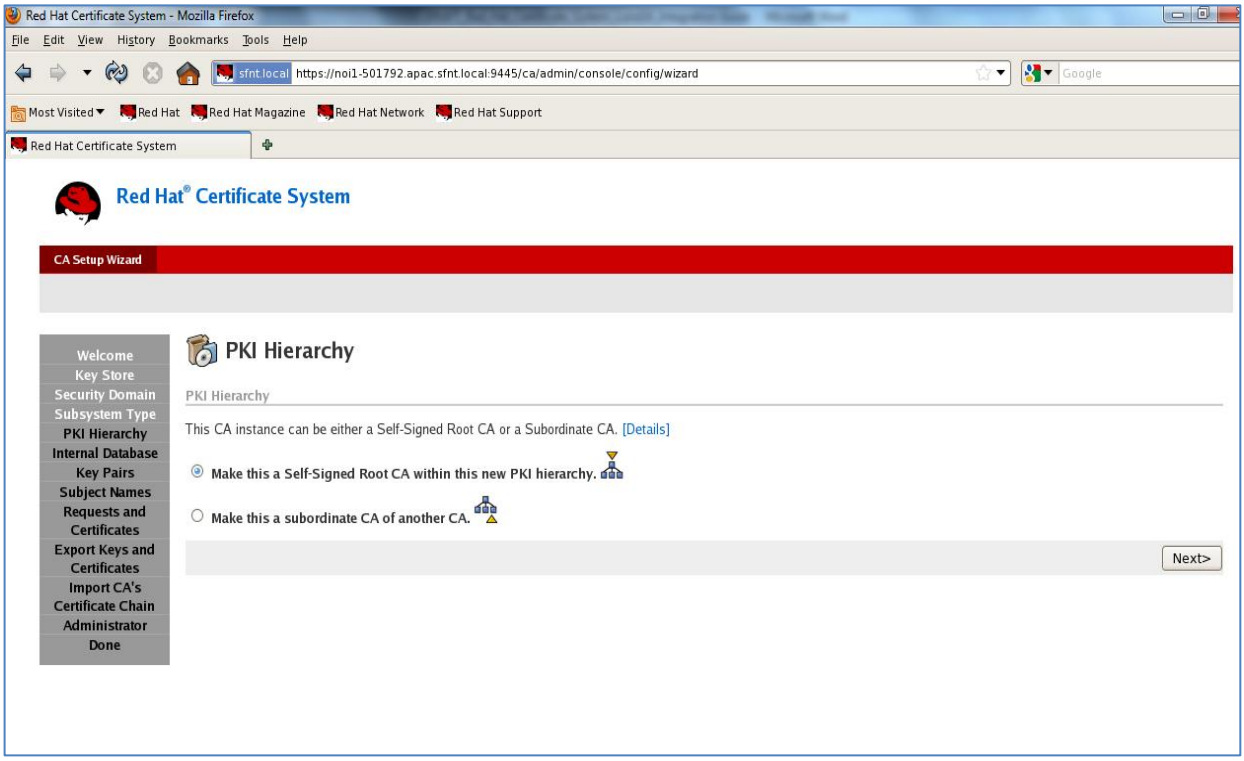
13. In the Create a **Security Domain** panel, enter Red Hat Security as **Security Domain Name**. Click **Next>**.



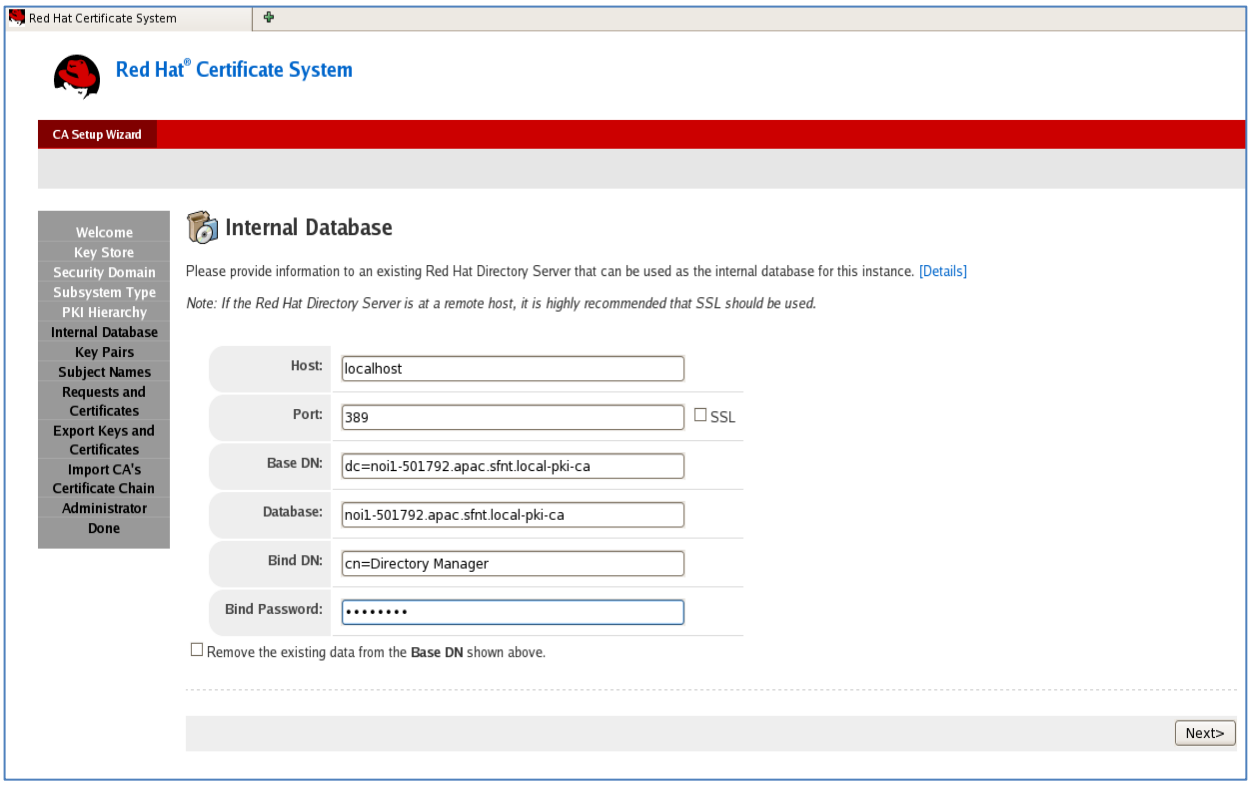
14. In the **Sub System Type** panel, select **Configure this instance as a New CA Subsystem**, and then select Certificate Authority as the **Subsystem Name**. Click **Next>**.



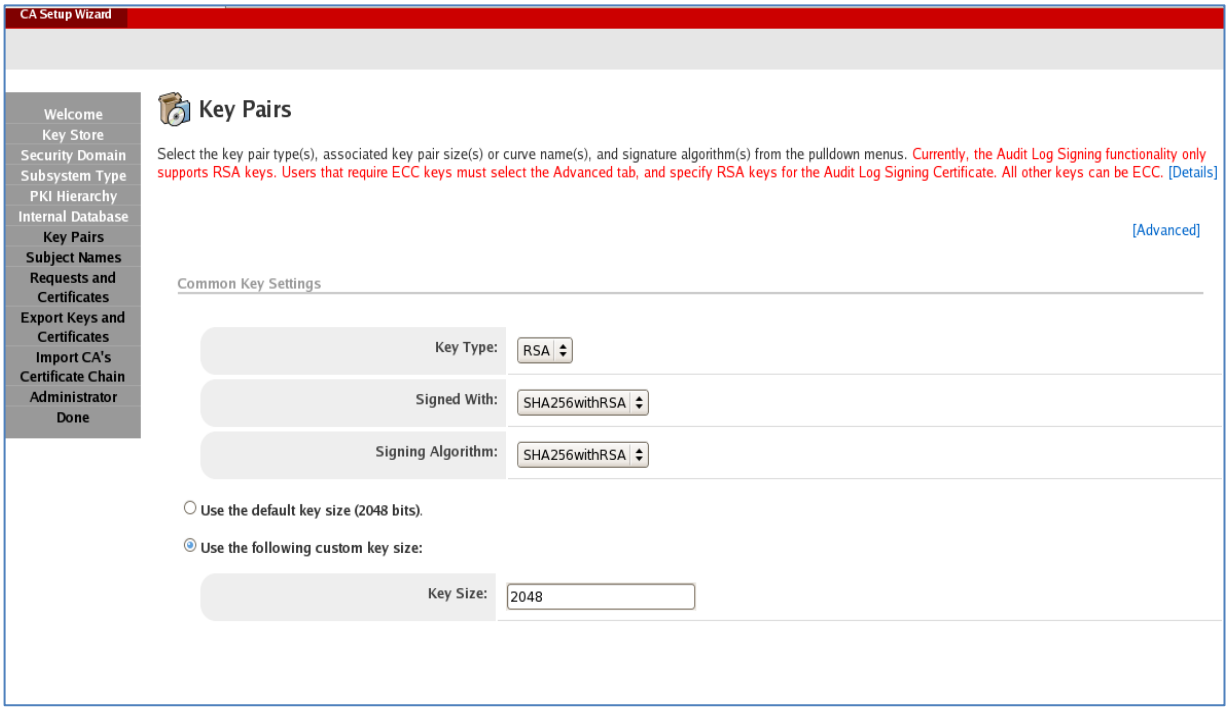
15. In the **PKI Hierarchy** panel, select "**Make this Selfsigned Root CA within this new PKI hierarchy.**" Click **Next>**.



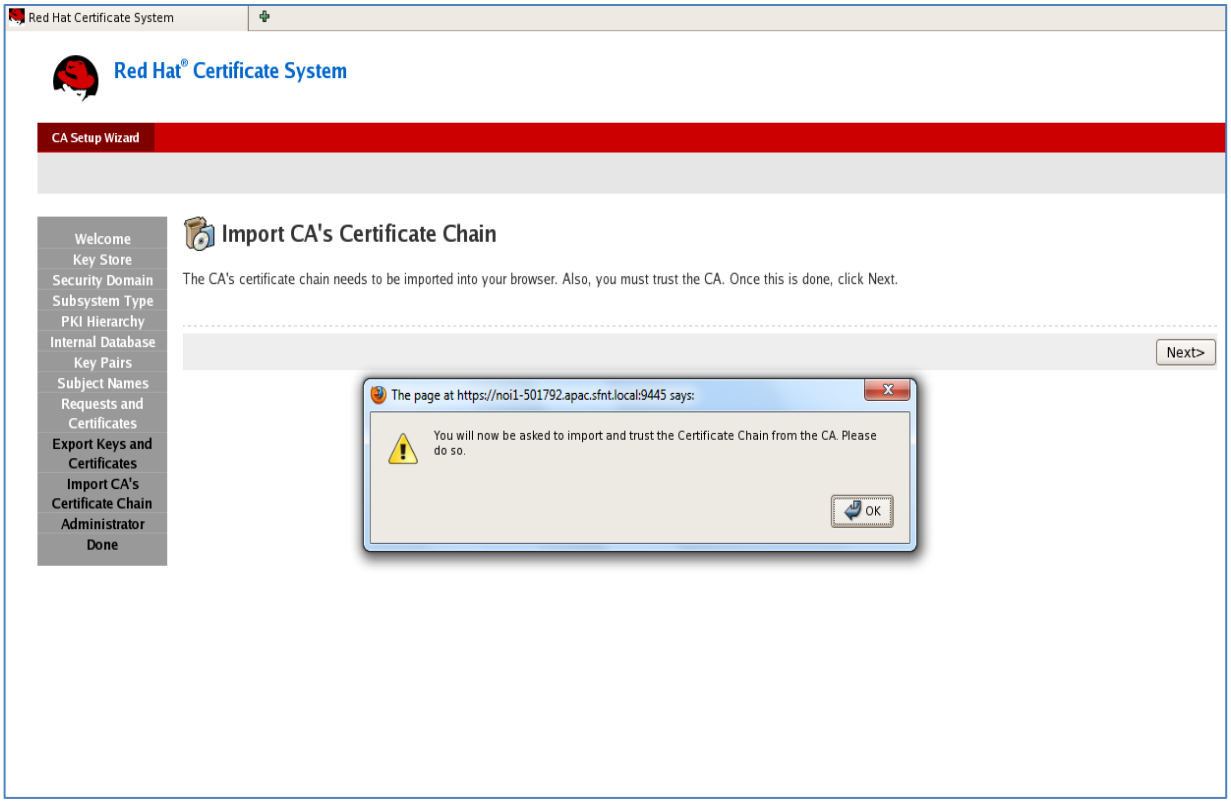
16. In the **Internal Database** panel, fill in the correct LDAP server information. Click **Next>**.

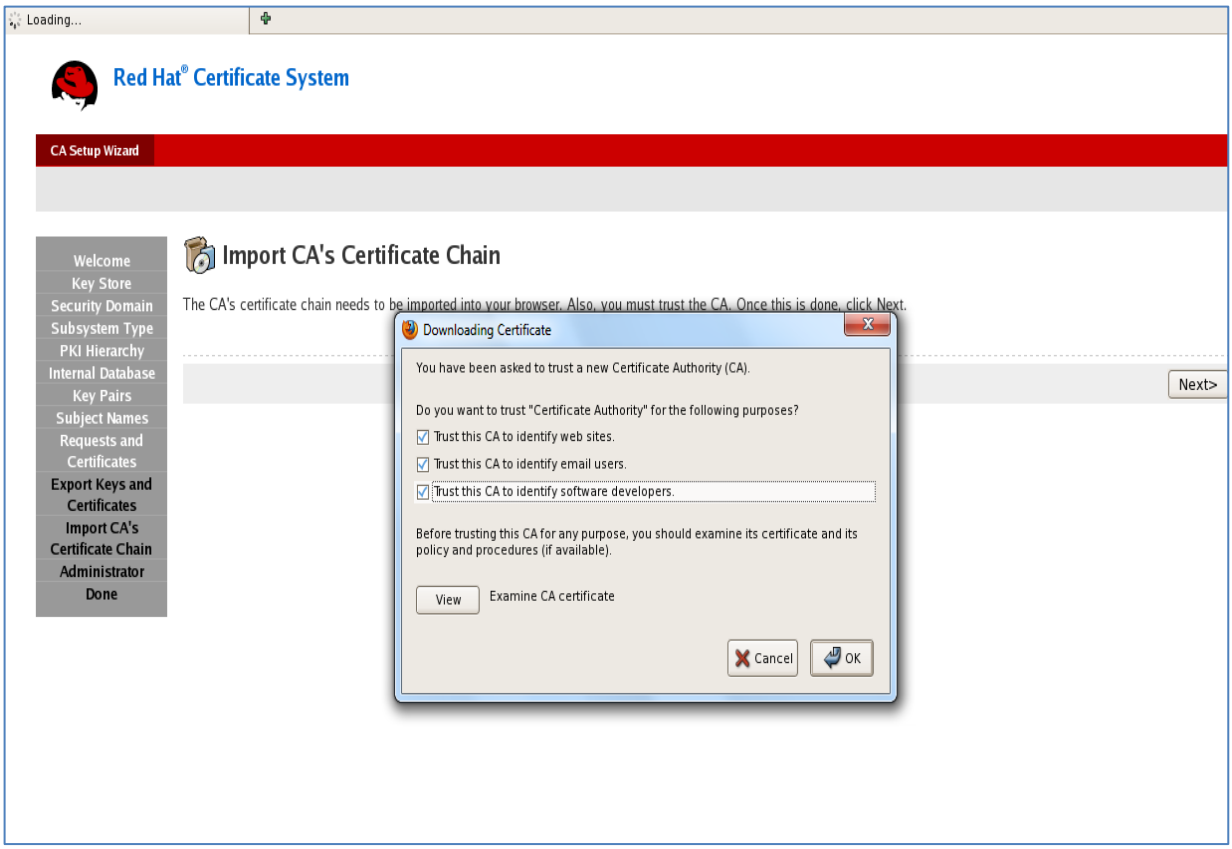


17. In the **Key Pairs** panel, select **Use the following custom key size**. Select **RSA** as the **Key Type**, and then enter the **Key Size**, for example 1024, 2048, or 4096. Click **Next>**.

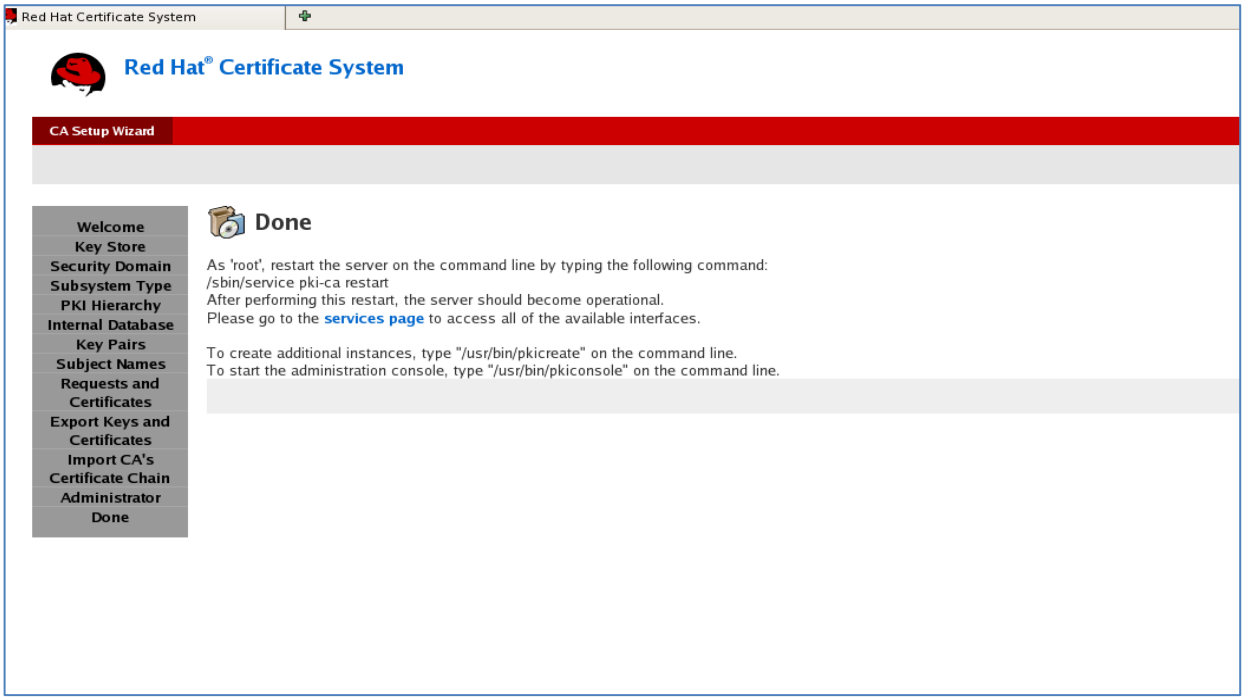


18. In the **Subject Name** panel, click **Next>**.
19. In the **Requests and Certificates** panel, select **Apply**, and then click **Next>**.
20. A message will display to import and trust certificate chain from the CA. Click **OK** and then click **Next>**.
21. In the **Administrator** panel, enter the correct details.
22. Click **Next>** through the remaining panels to import the agent certificate into the browser and complete the configuration.


Red Hat Certificate System
Red Hat® Certificate System
CA Setup Wizard
Welcome
Key Store
Security Domain
Subsystem Type
PKI Hierarchy
Internal Database
Key Pairs
Subject Names
Requests and Certificates
Export Keys and Certificates
Import CA's Certificate Chain
Administrator
Done
Import CA's Certificate Chain
The CA's certificate chain needs to be imported into your browser. Also, you must trust the CA. Once this is done, click Next.
Next>
The page at https://noi1-501792.apac.sfnt.local:9445 says:
You will now be asked to import and trust the Certificate Chain from the CA. Please do so.
OK


Loading...
Red Hat® Certificate System
CA Setup Wizard
Welcome
Key Store
Security Domain
Subsystem Type
PKI Hierarchy
Internal Database
Key Pairs
Subject Names
Requests and Certificates
Export Keys and Certificates
Import CA's Certificate Chain
Administrator
Done
Import CA's Certificate Chain
The CA's certificate chain needs to be imported into your browser. Also, you must trust the CA. Once this is done, click Next.
Next>
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "Certificate Authority" for the following purposes?
Trust this CA to identify web sites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
Cancel
OK

When configuration is complete, the Red Hat Certificate System returns **Done.**



23. Run the following command to restart the subsystem:

```
# service pki-ca restart
```

Or

```
# service pki-cad restart
```

This completes the Red Hat Certificate System Integration with SafeNet Luna HSM. The CA signing keys are now secured by the partition on the SafeNet Luna HSM.