ProtectServer Gold and Red Hat Certificate System v7.3

Integration Guide
Preface

© 2009 SafeNet, Inc. All rights reserved.

Part Number: 009832-001 (Rev A, 07/2009)

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.

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.

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 below.
SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland  21017
USA

Limitations

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

Disclaimers

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.

Technical Support

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, please contact your supplier or SafeNet support.

SafeNet 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.

Technical Support Contact Information:
Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com
# Table of Contents

Preface ............................................................................................................................................................... i

Table of Contents ........................................................................................................................................... iii

Chapter 1: Introduction ...................................................................................................................................... 5
  Audience .......................................................................................................................................................... 5
  Scope ............................................................................................................................................................ 5
  3rd Party Application Details ...................................................................................................................... 5
  Supported Platforms .................................................................................................................................. 5
  HSMs and Firmware Version ...................................................................................................................... 5
  Distributions ................................................................................................................................................ 5
  Prerequisites ............................................................................................................................................... 6
  PSG Setup .................................................................................................................................................. 6

Chapter 2: Integrating PSG in PCI Mode with Red Hat Certificate System 7.3 .......................... 7

Chapter 3: Integrating PSG in Network Mode with Red Hat Certificate System 7.3 ............ 15

References: .................................................................................................................................................... 22
Chapter 1
Introduction

This document is intended to guide security administrators to install, configure and integrate Red Hat Certificate System 7.3 with Safenet PSG Hardware Security Module (HSM) via SafeNet’s PKCS#11 interface.

Audience

This document provides low-level details of how the Hardware Security Modules (HSM) (e.g. SafeNet PSG) can be made to work with RHEL Certificate System. You must have basic knowledge of using RHEL Certificate System and PSG concepts to make full use of the recommendations in this document. This document is intended for:

- Developers and enterprise IT professionals who are planning or implementing a HSM deployment. This includes IT security administrators and IT personnel.

Scope

3rd Party Application Details

- Red Hat Certificate System 7.3
- Red Hat Directory Server 7.1

Supported Platforms

The following platforms are supported for PSG

- Red Hat Enterprise Linux v4.0 32-bit (Kernel 2.6.9-55)

HSMs and Firmware Version

- Fw 2.07
- PSG-220

Distributions

- ProtectToolkit C Release 3.33.00
Prerequisites

PSG Setup

Please refer to the SafeNet PSG documentation for installation steps and details regarding configuring and setting up the box on Linux systems in whatever mode (PCI or Network Mode) you want to use. Brief installation summary is provided here:

- Check the items received to ensure none are missing. A separate page that lists the items included is provided for this purpose.
- Check the battery isolation link is placed for normal operation.
- If an external tamper detector is to be used, modify the printed circuit board accordingly.
- Install the Protect Server Gold in the host computer system.
- Install the PCI HSM Access Provider package that includes the device driver and confirm the correct operation of the adapter and driver installation.
- Run hsmstate command to ensure driver is running correctly or not.
- Install the SafeNet application programming interface (API) or net server software supplied with the product.
Chapter 2
Integrating PSG in PCI Mode with Red Hat Certificate System 7.3

PSG Setup in PCI Mode :

To configure the SafeNet PKCS#11 interface follow the below steps:

The PKCS #11 module is installed using the `modutil` command-line utility.

1. Stop the `rhpki-ca` instance
   
   `/etc/init.d/rhpki-ca stop`

2. Make copy of `/opt/ETpcihsm/lib/linux-i386/libetpcihsm.so` into `/usr/lib` as below:-
   
   `cp /opt/ETpcihsm/lib/linux-i386/libetpcihsm.so /usr/lib/libethsm.so`

3. Enable the No Public Cryptography flag in PSG using `/opt/PTK/bin/ctconf –fc`

4. Permissions of `/dev/e8k0` need to be set so that RedHat CA service users get read/write access to the device driver.

   `chmod 666 /dev/e8k0`

5. Open the alias directory for the subsystem which is being configured with the PKCS #11 module.

   `cd /var/lib/rhpki-ca/alias/`

6. The required security module database file, `secmod db`, should be created by default when the subsystem is created. Use the modutil utility to set the library information.

   `modutil -dbdir . --add PSG -libfile /opt/ETcpsdk/lib/linux-i386/libcthsm.so`

7. Show the information about the installed PKCS #11 modules installed as well as information on the corresponding tokens using the modutil tool.

   `modutil -dbdir . -nocertdb -list`

   Using database directory ....

   Listing of PKCS #11 Modules

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

© SafeNet Inc.
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. PSG
library name: /opt/ETcpsdk/lib/linux-i386/libctshsm.so
slots: 2 slots attached
status: loaded

slot: ProtectServer Gold:34211
token: part1

slot: ProtectServer Gold
token: AdminToken (92404645)

8. In addition, the following parameter is set in the /etc/rhpki-ca/password.conf for login into the particular token:

    hardware-HSM Label=Partition password

Example:-
    hardware-part1=temp123#

9. Start the rhpki-ca server

    /etc/init.d/rhpki-ca start

    PKI service(s) are available at https://localhost.localdomain:9443

    On clicking above URL, you will get the CA configuration wizard.
Open /etc/rhpki-ca/CS.cfg file, search preop.pin parameter and copy the parameter preop.pin value into PIN text Box and Click login button.
Enter the Bind Password whatever you have given at the time of directory server configuration.
Integrating PSG in PCI Mode

Key Store

Two lists of security modules are provided below. The Supported Security Modules list consists of both software-based and hardware-based security modules that this PKI solution supports, while the Other Security Modules list consists of any other security modules found by this PKI subsystem that are not recognized as one of the supported security modules. (Details)

Supported Security Modules

<table>
<thead>
<tr>
<th>Module/Token</th>
<th>Status</th>
<th>Default</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSS Internal PKCS #11 Module</td>
<td>Found</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Internal Key Storage Token</td>
<td>Logged In</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rCipher's nFast Token Hardware Module</td>
<td>Not Found</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SafeNet's LunaSA Token Hardware Module</td>
<td>Not Found</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Other Security Modules

The security modules listed below are modules found by the server but not recognized as one of the supported modules. If the user believes that any listed modules below should have been supported, please check the “CS.cfg” configuration file to see if there is a name mismatch and adjust accordingly.

<table>
<thead>
<tr>
<th>Module/Token</th>
<th>Status</th>
<th>Default</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSG</td>
<td>Found</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- part1</td>
<td>Logged In</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- AdminToken (02804645)</td>
<td>Not logged In</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: After pressing Next, keys will be generated on the server, which will take some time to complete. Please wait for the next panel to appear.

Key Pairs

Select the key pair type(s) and associated key pair size(s) from the pull down menus. [Details] [Advanced]

Common Key Settings

Key Type: RSA

Use the default key size (2048 bits for RSA, 256 bits for ECC).

Use the following custom key size:

Key Size: 2048
Integrating PSG in PCI Mode

Subject Names

Each certificate associated with this instance needs to have a unique name within the PKI hierarchy. The following information will be used to generate these unique names. [Details]

CA Signing Certificate

[Details]

OCSP Signing Certificate

[Details]

SSL Server Certificate

[Details]

Subsystem Certificate

[Details]

A Certificate Authority (CA) is responsible for issuing different kinds of certificates. To obtain the certificates required internally by this subsystem, the user must select a URL to a CA that has been registered in the security domain or to an "External CA".

Note: An "External CA" is defined to be a CA that is not part of the 'Security Domain'. VeriSign®, GeoTrust®, and Netscape® Certificate Management System (CMS) 6.x are examples of "External CAs".

Requests and Certificates

A certificate signing request (CSR) contains a public key and is an unsigned copy of the certificate.

If a given CSR has been successfully signed by a CA, then the certificate will be designated below a certificate icon labeled Certificate Generated Successfully. However, if a given CSR contains an action required label under its certificate icon, then those requests must be manually submitted to a CA for certificate generation.

Press the [Apply] button after certificates and chains are passed in.

Press the [Next] button once all certificates have been generated successfully.

CN=Certificate Authority,O=Domain

Certificate Generated Successfully

View Certificate Request (CSR)

View Certificate in Base64-Encoding

View Certificate Pretty Print

CN=OCSP Signing Certificate,O=Domain

Certificate Generated Successfully

View Certificate Request (CSR)

View Certificate in Base64-Encoding

View Certificate Pretty Print

CN=localhost.localdomain,O=Domain

Certificate Generated Successfully

View Certificate Request (CSR)

View Certificate in Base64-Encoding

View Certificate Pretty Print

CN=CA Subsystem Certificate,O=Domain

Certificate Generated Successfully

View Certificate Request (CSR)
ProtectServer Gold and Red Hat Certificate System v7.3 Integration Guide

Chapter 2
Integrating PSG in PCI Mode

Red Hat Certificate System 7.3.0

Administrator

The administrator is a privileged user who manages this subsystem. Please enter the following relevant information, and a certificate request will be automatically generated and submitted. An administrator's entry will be created in the internal database and an administrator's certificate will be imported into this browser automatically in the next panel.

- **User ID (UID):** Admin
- **Name:** CA Administrator of Instance thpki-ca
- **Email:** sjalan@safenet.com
- **Password:** ********
- **Password (Again):** ********

Copyright © 2002-06 Red Hat, Inc. All rights reserved. http://www.redhat.com

Red Hat Certificate System 7.3.0

CA Setup Wizard

**Done**

Restart the server on the command line by typing "/etc/init.d/thpki-ca restart". After performing this restart, the server should become operational.

Please go to the services page to access all of the available interfaces.

To create additional instances, type "/usr/bin/thpkicreate" on the command line.
To start the administration console, type "/usr/bin/thpkipanel" on the command line.

Copyright © 2002-06 Red Hat, Inc. All rights reserved. http://www.redhat.com

© SafeNet Inc.
10. Verify the Keys and certificates on the token of PSG card:

Start kmu utility /opt/PTK/bin/kmu, Select token and go to token information of selected token.
Chapter 3
Integrating PSG in Network Mode with Red Hat Certificate System 7.3

PSG Setup in Network Mode:-

To configure the SafeNet PKCS#11 interface follow the below steps:

**Server Side:**

1. Permissions of /dev/e8k0 need to be set so that RedHat CA service users get read/write access to the device driver.
   
   ```
   chmod 666 /dev/e8k0
   ```

**Client Side:**

The PKCS #11 module is installed using the `modutil` command-line utility.

1. Stop the rhpki-ca instance
   
   ```
   /etc/init.d/rhpki-ca stop
   ```

2. Make copy of `/opt/ETnethsm/lib/linux-i386/libetnetclient.so` into `/usr/lib/` as below:-
   
   ```
   cp /opt/ETnethsm/lib/linux-i386/libetnetclient.so /usr/lib/libethsm.so
   ```

3. Enable the No Public Cryptography flag in PSG using `/opt/PTK/bin/ctconf –fc`

4. Open the alias directory for the subsystem which is being configured with the PKCS #11 modules. For example:
   
   ```
   cd /var/lib/rhpki-ca/alias/
   ```

5. The required security module database file, secmodule.db, should be created by default when the subsystem is created. Use the modutil utility to set the library information.
   
   ```
   modutil -dbdir . –add PSG –libfile /opt/ETcpsdk/lib/linux-i386/libethsm.so
   ```

6. Show the information about the installed PKCS #11 modules installed as well as information on the corresponding tokens using the modutil tool.
   
   ```
   modutil -dbdir . -nocertdb -list
   ```

Using database directory....

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. PSG
   library name: /opt/ETcpsdk/lib/linux-i386/libcthsm.so
   slots: 2 slots attached
   status: loaded
   slot: ProtectServer Gold:34211
token: part1
   slot: ProtectServer Gold
token: AdminToken (92404645)

7. In addition, the following parameter is set in the /etc/rhpki-ca/password.conf file for login into the particular token:

   hardware-HSM Label=Partition password

   Example:-
   hardware-part1=temp123#

8. Start the rhpki-ca server

   /etc/init.d/rhpki-ca start

   PKI service(s) are available at https://localhost.localdomain:9443

   On clicking above URL, you will get the CA configuration Wizard.
Open /etc/rhpki-ca/CS.cfg file, search preop.pin parameter and copy the parameter preop.pin value into PIN text Box and Click login button.
Chapter 3
Integrating PSG in Network Mode

Subsystem Type

This instance can be configured as a new CA subsystem.

Configure this instance as a new CA Subsystem:

- Subsystem Name: Certificate Authority
- Subsystem URL: https://localhost.localdomain:9443

Clone an existing CA Subsystem:

- Subsystem Name: Certificate Authority
- Subsystem URL: NONE

PKI Hierarchy

This CA instance can be either a Self-Signed Root CA or a Subordinate CA. [Details]

- Make this a Self-Signed Root CA within this new PKI hierarchy.
- Make this a subordinate CA of another CA.
Enter the Bind Password whatever you have given at the time of directory server configuration.
Integrating PSG in Network Mode

Key Pairs

Select the key pair type(s) and associated key pair size(s) from the pull-down menus. [Details]

Common Key Settings

Key Type: RSA

- Use the default key size (2048 bits for RSA, 256 bits for ECC).
- Use the following custom key size:

  Key Size: 2048

Note: After pressing Next, keys will be generated on the server, which will take some time to complete. Please wait for the next panel to appear.

Subject Names

Each certificate associated with this instance needs to have a unique name within the PKI hierarchy. The following information will be used to generate these unique names. [Details]

CA Signing Certificate

DNI: CN=Certificate Authority, O=Domain

OCSP Signing Certificate

DNI: CN=OCSP Signing Certificate, O=Domain

SSL Server Certificate

DNI: CN=localhost,localdomain, O=Domain

Subsystem Certificate

DNI: CN=CA Subsystem Certificate, O=Domain

A Certificate Authority (CA) is responsible for issuing different kinds of certificates. To obtain the certificates required internally by this subsystem, the user must select a URL to a CA that has been registered in the security domain or to an "External CA".

Note: An "External CA" is defined to be a CA that is not part of the "Security Domain": Verisign\textsuperscript{TM}, GeoTrust\textsuperscript{TM}, and Netscape\textsuperscript{TM} Certificate Management System (CMS) 6.0 are examples of "External CAs".

URL: External CA
Red Hat Certificate System 7.3.0

Welcome
Security Domain
Subsystem Type
PKI Hierarchy
Internal Database
Key Stores
Key Pairs
Subject Names
Requests and
Certificates
Export Keys and
Certificates
Administrator
Done

Requests and Certificates

A certificate signing request (CSR) contains a public key and is an unsigned copy of the certificate.

If a given CSR has been successfully signed by a CA, then the certificate will be designated below by a certificate icon labeled Certificate Generated Successfully.

However, if a given CSR contains an action required label under its certificate icon, then those requests must be manually submitted to a CA for certificate generation.

Press the [Apply] button after certificates and chains are passed in.

Press the [Next] button once all certificates have been generated successfully.

Red Hat Certificate System 7.3.0

CA Setup Wizard

Welcome
Security Domain
Subsystem Type
PKI Hierarchy
Internal Database
Key Stores
Key Pairs
Subject Names
Requests and
Certificates
Export Keys and
Certificates
Administrator
Done

Administrator

The administrator is a privileged user who manages this subsystem. Please enter the following relevant information, and a certificate request will be automatically generated and submitted. An administrator's entry will be created in the internal database and an administrator's certificate will be imported into this browser automatically in the next panel.

Name: CA Administrator of Instance rhpki-ca
Email: hjalmaz@safenet-inc.com
Password: Password
Password (Again): Password

Next >
9. Verify the Keys and certificates on token of PSG card

Start kmu utility `/opt/PTK/bin/kmu`, Select token and go to token information of selected token.

References: