Apache HTTP Server

Integration Guide
Preface

© 2013 SafeNet, Inc. All rights reserved.

Part Number: 007-011228-001 (Rev D, 08/2013)

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 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.

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

**Chapter 1 Introduction** ......................................................................................................................................................... 5
  - Luna SA Setup .................................................................................................................................................................... 7
  - Luna PCI Setup ................................................................................................................................................................... 7
  - Apache Toolkit .................................................................................................................................................................. 7

**Chapter 2 Configuring Apache Toolkit for v2.2.x (An Example)** .......................................................................................... 8

**Chapter 3 Integration of Apache Server 2.2.x with Luna** ........................................................................................................ 9
Chapter 1
Introduction

This document covers the necessary information to install, configure and integrate Apache HTTP Server v2.2.x with SafeNet Luna SA Hardware Security Modules (HSM).

The Luna HSMs integrates with the Apache HTTP Server to provide significant performance improvements by off-loading cryptographic operations from the Apache HTTP Server to the Luna HSMs. In addition, the Luna HSMs provides extra security by protecting and managing the server’s high value SSL private key within a FIPS 140-2 certified hardware security module.

Scope

3rd Party Application Details

- Apache HTTP Server v2.2.x for Unix

Supported Platforms

The following platforms are supported for Luna SA 1U v4.4:

- RHEL 5.8 (64-bit) running on VMWare ESXi

The following platforms are supported for Luna SA 1U v5.0:

- RHEL 5 (32/64-bit) running on VMWare ESXi, Microsoft Hyper-V and Citrix XenServer
- Solaris 10 SPARC 32-bit

The following platforms are supported for Luna PCI v5.0:

- RHEL 5 (32 / 64-bit)

The following platforms are supported for Luna Client v5.2.1:

- RHEL 6 (64-bit) running on VMWare ESXi
- RHEL 5.8 (64-bit) running on VMWare ESXi

HSMs and Firmware Version

- K5 HSM f/w 4.8.1 (Luna SA v4.4.3)
- K6 HSM f/w 6.0.8 (Luna SA v5.0)
- K6 HSM f/w 6.1.3 (Luna PCI v5.0)
- K6 HSM f/w 6.10.1 (Luna SA 5.2.1)

Library and Driver Support

- PKCS#11 v2.01 dynamic library
- PKCS#11 v2.20 dynamic library

Distributions

- Luna SA 1U Appliance s/w v4.4.3
- Luna SA 1U Appliance s/w v5.0
- Luna SA 1U Appliance s/w v5.2.1
- Luna SA Client s/w v4.4.1
- Luna SA Client s/w v5.0
- Luna PCI Client s/w v5.0
- Luna Client s/w v5.2.1
- Apache Toolkit
Prerequisites:

Luna SA Setup

Please refer to the Luna SA documentation for installation steps and details regarding to configure and setup the box on UNIX 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
- Initialize the HSM on the Luna SA appliance
- Create a partition on the HSM and remember the partition password that will be later used for APACHE HTTP Server.
- Create and exchange certificates between the Luna SA and your "Client" system (registered the Client with the Partition).
- Run the command, vtl verify to display a partition from Luna SA. The general form of command is /usr/lunasa/bin/ vtl verify.

For Solaris 10 SPARC, you need to export LD_LIBRARY_PATH. export
LD_LIBRARY_PATH=/opt/lunasa/lib:$LD_LIBRARY_PATH

For Solaris 10 SPARC platform in Luna SA v5.0, the general form of the command is /opt/lunasa/bin/vtl verify.

For Luna Client v5.2.1, the general form of the command is /usr/safenet/lunACLient/bin/ vtl verify

- Enable 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).

Luna PCI Setup

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

- Initialize the HSM on the Luna PCI appliance
- Create a partition on the HSM that will be later used by the Apache HTTP Server.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna PCI with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Apache Toolkit

The APACHE toolkit is provided to make the installation quick and easy. The installation CD can be obtained from the SafeNet Customer Connection Center.

APACHE toolkit installs Server version: Apache/2.2.14 (Unix) by default as it is build by using this version. However you can use any version of Apache with our toolkit which is described in Chapter 2. You can skip the Chapter 2 if you need to install Apache 2.2.14 anyway.

Note: If you already have Apache installed, uninstall it before proceeding with the installation.
Chapter 2
Configuring Apache Toolkit for v2.2.x (An Example)

To configure Apache HTTP Server 2.2.x to recognize the Luna SA / Luna PCI cryptographic device:

1. Download the desired version from the following site:

   http://archive.apache.org/dist/httpd/

   Note: We have downloaded Apache v2.2.21 but you can download any v2.2.x available.

2. Traverse to toolkit, e.g. /root/_cdrom_apache.

3. Copy and paste the httpd-2.2.21.tar.gz, downloaded from the above site.

4. Extract the luna-samples-0.9.8 from luna-samples-0.9.8.tar.gz by using the following commands:

   gunzip luna-samples-0.9.8.tar.gz
   tar -xvf luna-samples-0.9.8.tar

5. Now execute the following commands

   cd luna-samples-0.9.8
   cp httpd-luna-2.2.14.conf httpd-luna-2.2.21.conf
   cp mpm-luna-2.2.14.conf mpm-luna-2.2.21.conf
   cp ssl-luna-2.2.14.conf ssl-luna-2.2.21.conf
   tar -cvf luna-samples-0.9.8.tar luna-samples-0.9.8/*
   gzip luna-samples-0.9.8.tar

6. Traverse to toolkit, e.g. /root/_cdrom_apache.

7. Edit the abuild-2.2 script for apache version change the APACHEVER="2.2.14" as APACHEVER="2.2.21"

8. Save the script after changing the version.

Now you have completed all the changes required to integrate Apache v2.2.21 with Luna SA. Follow the steps mentioned in the next Chapter.
Chapter 3
Integration of Apache Server 2.2.x with Luna

To configure Apache HTTP Server 2.2.x to recognize the Luna SA / Luna PCI cryptographic device:

1. Traverse to toolkit, e.g. /root/_cdrom_apache.

2. Run the OptimizeApache.sh to configure the Luna SA configuration file (/etc/Chrystoki.conf) for APACHE:

```
./OptimizeApache.sh fork
```

For further information, refer to the README-OPTIMIZE under the APACHE toolkit.

3. The Luna SA / Luna PCI configuration file (/etc/Chrystoki.conf) is now configured for Apache HTTP Server.

**Luna SA**

```
Misc = {
  Apache = 1;
  PE1746Enabled=1;
}
EngineLunaCA3 = {
  DisableCheckFinalize = 0;
  DisableEcdsa = 1;
  DisableDsa = 1;
  DisableRand = 1;
  EngineInit = 1:10:11;
  LibPath64 = /usr/lunasa/lib/libCryptoki2_64.so;
  LibPath = /usr/lunasa/lib/libCryptoki2.so;
}
```

⚠️ Make sure that the value of LibPath and LibPath64 should be the path of libCryptoki2.so or libCryptoki2_64.so respectively in /etc/Chrystoki.conf after running OptimizeApache.sh script.

**Luna PCI**

```
Misc = {
  Apache = 1;
  PE1746Enabled=1;
}
EngineLunaCA3 = {
  DisableCheckFinalize = 0;
  DisableEcdsa = 1;
  DisableDsa = 1;
  DisableRand = 1;
  EngineInit = 1:10:11;
  LibPath64 = /usr/lunapci/lib/libCryptoki2_64.so;
  LibPath = /usr/lunapci/lib/libCryptoki2.so;
}
```
4. Traverse to the toolkit: /root/_cdrom_apache, run the configuration script (**abuild-2.2**) to install Apache HTTP Server v2.2.x and Openssl 0.9.8n for Luna SA with

For (32-bit):

```
LUNA_CONFIG_BITS=32
LUNA_CONFIG_BITS=32 ./abuild-2.2 --build
```

For (64-bit):

```
LUNA_CONFIG_BITS=64
LUNA_CONFIG_BITS=64 ./abuild-2.2 --build
```

For further information, refer to the README-ABUILD under the APACHE toolkit.

5. Open a session to Luna SA using the sautil utility provided under the /usr/local/sautil/bin:

```
sautil -v -s 1 -i 10:11 -o –q
```

For further information, refer to the README-RSA under the APACHE toolkit.

6. Enter the partition password of the HSM in which you have registered the APACHE server as a client

7. Traverse to the toolkit: /root/_cdrom_apache, run the abuild-2.2 script to generate keys on the Luna SA / Luna PCI.

For (32-bit):

```
LUNA_CONFIG_BITS=32 ./abuild-2.2 --genrsa
```

For (64-bit):

```
LUNA_CONFIG_BITS=64 ./abuild-2.2 --genrsa
```

Enter the relevant information as prompted for the keys to be generated.

8. Traverse to apache installation directory:

```
/usr/local/apache2/conf
```

9. Open the apache configuration file (**httpd.conf**) and edit the **ServerName** field with the hostname or IP address of the server.

10. Traverse to the directory:

```
/usr/local/apache2/conf/extra
```

11. Open the ssl configuration file (**httpd-ssl.conf**) and edit the Virtual Host section as below:

```
<Virtual Host Hostname or IP Address: 443>
```

12. Traverse to the directory:

```
/usr/local/apache2/bin
```

13. Start the Apache HTTP Server with the SSL option:

```
.apachectl --DSSL
```

Make sure you have disabled iptables or allow http/https traffic through iptables.
14. Open any browser (IE/Firefox) and access the HTTP Server:

https://<HostName or IP Address>

15. Accept the certificate.