Apache HTTP Server

Integration Guide

gemalto
security to be free

Document Number: 007-011228-001, Rev. H

Release Date: April 2017

Contents

Preface 4
Scope 4
Gemalto Rebranding 4
Document Conventions 4
Command Syntax and Typeface Conventions 5
Support Contacts 6
1 Introduction 7
Overview 7
Understanding the Apache 7
3rd Party Application Details 8
Supported Platforms 8
Library and Driver Support 9
Prerequisites 10
SafeNet Network HSM Setup 10
SafeNet PCI-E HSM Setup 10
SafeNet Network HSM Configuration Settings 10
Apache Toolkit 11
2 Configuring Apache Toolkit for v2.x.x (An Example) 12
3 Integration of Apache Server with SafeNet Luna HSM 14
Apache Installation and Configuration 14

Preface

This document is intended to guide administrators through the steps for Apache HTTP Server and SafeNet Luna HSM integration. This guide provides the necessary information to install, configure, and integrate Apache HTTP Server with SafeNet Luna Hardware Security Modules (HSM).

Scope

This guide provides instructions for setting up a small test lab with Apache HTTP Server running with SafeNet Luna HSM for securing the SSL keys of server. It explains how to install and configure the software that is required for setting up Apache HTTP Server while storing SSL keys on SafeNet Luna HSM.

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna Client	SafeNet HSM Client

NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

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. Contains 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.)
`Consolas`	Denotes syntax, prompts, and code examples.

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 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.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

This document covers the necessary information to install, configure, and integrate Apache HTTP Server (provided in Apache Toolkit) with SafeNet Luna HSM.

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

The installation is performed in several steps:

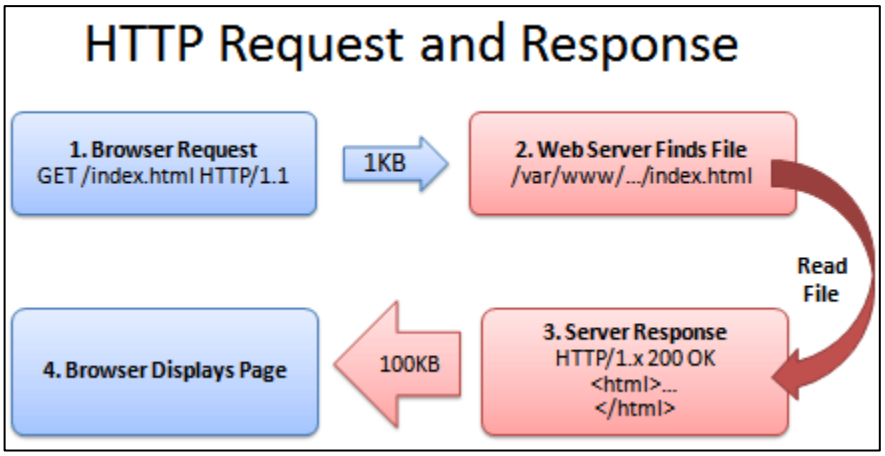
- Install and configure SafeNet Luna HSM.
- Install and configure Apache HTTP Server using SafeNet Luna HSM.

Understanding the Apache

Apache is the most popular web server (after which comes Microsoft's IIS) available. The reasons behind its popularity, to name a few, are:

1. It is free to download and install.
2. It is open source: the source code is visible to anyone and everyone, which basically enables anyone (who can rise up to the challenge) to adjust the code, optimize it, and fix errors and security holes. People can add new features and write new modules.
3. It suits all needs: Apache can be used for small websites of one or two pages, or huge websites of hundreds and thousands of pages, serving millions of regular visitors each month. It can serve both static and dynamic content.

A web server's job is basically to accept requests from clients and send responses to those requests. A web server gets a URL, translates it to a filename (for static requests), and sends that file back over the internet from the local disk, or it translates it to a program name (for dynamic requests), executes it, and then sends the output of that program back over the internet to the requesting party. If for any reason, the web server was not able to process and complete the request, it instead returns an error message. The word, web server, can refer to the machine (computer/hardware) itself, or the software that receives requests and sends out responses.



3rd Party Application Details

- Apache HTTP Server v2.4.x for Unix
- Apache HTTP Server v2.2.x for Unix

Supported Platforms

The following platforms are tested with SafeNet Luna HSM:

Operating Systems	SafeNet HSM	Apache Version
Red Hat Enterprise Linux 6.9 (64 bit)	Luna SA Appliance Software v5.4.7 Firmware 6.10.9 Luna Client 5.4.1	Apache v2.4.25
Red Hat Enterprise Linux 6.9 (64 bit)	Luna SA Appliance Software v5.4.7 Firmware 6.10.9 Luna Client 5.4.2	Apache v2.4.25
Red Hat Enterprise Linux 6.8 (64 bit)	Luna SA Appliance Software v5.4.7 Firmware 6.10.9 Luna Client 5.4.1	Apache v2.4.25
Red Hat Enterprise Linux 6.8 (64 bit)	Luna SA Appliance Software v5.4.7 Firmware 6.10.9 Luna Client 5.4.2	Apache v2.4.25
Red Hat Enterprise Linux 6.5 (64 bit)	Luna SA Appliance Software v5.4.7 Firmware 6.10.9 Luna Client 5.4.1	Apache v2.4.23

Operating Systems	SafeNet HSM	Apache Version
Red Hat Enterprise Linux 6.5 (64 bit)	Luna SA Appliance Software v6.2.1 Firmware 6.10.9 Luna Client 6.2.1	Apache v2.4.3
Red Hat Enterprise Linux 5.11 (64 bit)	Luna SA Appliance Software v6.2.1 Firmware 6.10.9 Luna Client 6.2.1	Apache v2.4.3 Apache v2.2.26
Red Hat Enterprise Linux 6.5 (64 bit)	Luna SA Appliance Software v5.4.7 Firmware 6.21.0 / 6.2.4 Luna Client 5.4.1	Apache v2.4.4
Solaris 10 Sparc	Luna SA Appliance Software v5.0.0 Firmware 6.0.8 Luna Client 5.0	Apache v2.2.21
Red Hat Enterprise Linux 6.0 (64 bit)	Luna SA Appliance Software v5.2.1 Firmware 6.10.1 Luna Client 5.2.1	Apache v2.2.14
Red Hat Enterprise Linux 5.8 (64 bit / 32 bit)	Luna SA Appliance Software v5.0.0 Firmware 6.0.8 Luna Client 5.0	Apache v2.2.14
	Luna PCI 5.0 Firmware 6.1.3	
Red Hat Enterprise Linux 5.8 (64 bit)	Luna SA Appliance Software v5.2.1 Firmware 6.10.1 Luna Client 5.2.1	Apache v2.2.14
	Luna SA Appliance Software v4.4.3 Firmware 4.8.1 Luna Client 4.4	Apache v2.0.59

Library and Driver Support

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

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX systems. Before you get started ensure the following:

- SafeNet Network HSM appliance and a secure admin password.
- SafeNet Network HSM, and a hostname, suitable for your network.
- SafeNet Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and your Client system.
- Create a partition on the HSM, remember the partition password that will be later used by Apache HTTP Server.
- Create and exchange certificate between the SafeNet Network HSM and Client system. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Network HSM. The general form of command is “/usr/safenet/lunaclient/bin/vtl verify” for UNIX.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

NOTE: 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 onwards, the general form of the command is

/usr/safenet/lunaclient/bin/vtl verify

SafeNet PCI-E HSM Setup

Refer to the SafeNet 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 SafeNet 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).

SafeNet Network HSM Configuration Settings

When Luna Client is installed a configuration file is loaded at the following location:

/etc/Chrystoki.conf

This file is automatically configured and do not require any changes to communicate with the HSM.

However for Luna Client 6.x we have to edit this configuration file for slot id because by default it is 0 but LunaCA3 engine configured to use slot id as 1. In Luna 6.x you need to set the slot id to 1 by making the following changes in configuration file:

```
Presentation = {
   OneBaseSlotId =1;
}
```

Another major change in Luna 6.x (firmware 6.21.0 or above) for FIPS mode, Under FIPS 186-3/4, the only 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. So if you are using the HSM in FIPS mode you have to make the following change in configuration file:

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

Above setting “RSAKeyGenMechRemap” will redirect the older calling mechanism to new approved mechanism when HSM is in FIPS mode for firmware 6.21.0 or above.

Apache Toolkit

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

APACHE toolkit installs by default the apache version that was built with the toolkit. 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 version provided with toolkit anyway.

NOTE: If you already have Apache installed, uninstall it before proceeding with the installation.

2

Configuring Apache Toolkit for v2.x.x (An Example)

This is an example of how to use the version of Apache Server that is not build in Apache Toolkit by default. To configure Apache HTTP Server 2.x.x to recognize the SafeNet Network HSM / SafeNet PCI-E HSM cryptographic device:

1. Download the desired version from the following site:

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

   NOTE: We have tested below steps with Apache (v2.2.21, v2.4.3, v2.4.23) but you can use any v2.x.x available.

2. Traverse to toolkit, e.g. /root/_cdrom_apache.
3. Copy and paste the httpd-2.x.x.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. Copy existing configuration files and save the with the name of version you want to build, using the following commands:

   ```
   # cd luna-samples-0.9.8
   ```

   For Apache v2.2.x

   ```
   # cp httpd-luna-2.2.14.conf httpd-luna-2.2.x.conf
   # cp mpm-luna-2.2.14.conf mpm-luna-2.2.x.conf
   # cp ssl-luna-2.2.14.conf ssl-luna-2.2.x.conf
   ```

   For Apache v2.4.x

   ```
   # cp httpd-luna-2.4.4.conf httpd-luna-2.4.x.conf
   # cp mpm-luna-2.4.4.conf mpm-luna-2.4.x.conf
   # cp ssl-luna-2.4.4.conf ssl-luna-2.4.x.conf
   ```

6. Now zip the luna-samples-0.9.8 folder as it was originally using the following commands:

   ```
   # tar -cvf luna-samples-0.9.8.tar luna-samples-0.9.8/*
   # gzip luna-samples-0.9.8.tar
   ```

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

8. Edit the abuild-2.x script for apache version, change the APACHEVER="2.2.14" or APACHEVER="2.4.4" as APACHEVER="2.x.x"
9. Save the abuild-2.x script after changing the version you want to install.

Now you have completed all the changes required to integrate Apache v2.x.x with Luna SA. Follow the steps mentioned in the next Chapter.

3

Integration of Apache Server with SafeNet Luna HSM

Apache Installation and Configuration

To configure Apache HTTP Server to recognize the SafeNet Network HSM / SafeNet PCI-E HSM cryptographic device:

1. Traverse to toolkit, e.g. /root/_cdrom_apache.
2. Run the OptimizeApache.sh to configure the SafeNet Network HSM / SafeNet PCI-E HSM configuration file (/etc/Chrystoki.conf) for APACHE:

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

   For further information, refer to the README-OPTIMIZE under the APACHE toolkit.
3. The SafeNet Network HSM / SafeNet PCI-E HSM configuration file (/etc/Chrystoki.conf) is now configured for Apache HTTP Server.

   SafeNet Network HSM

   ```
   Misc = {
      PE1746Enabled = 0;
      Apache = 0;
   }

   EngineLunaCA3 = {
      LibPath = /usr/safenet/lunaclient/lib/libCryptoki2.so;
      LibPath64 = /usr/safenet/lunaclient/lib/libCryptoki2_64.so;
      EngineInit = 1:10:11;
      DisableRand = 1;
      DisableDsa = 1;
      DisableEcdsa = 1;
      DisableCheckFinalize = 0;
      EnableRsaGenKeyPair = 0;
      EnableDsaGenKeyPair = 0;
   }
   ```

NOTE: 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. Path of Cryptoki library has been changed in Luna 5.2.1 onwards.

SafeNet PCI-E HSM

```
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.x) to install Apache HTTP Server and Open SSL for Luna SA with

   For (32-bit):

   ```
   # LUNA_CONFIG_BITS=32
   # LUNA_CONFIG_BITS=32 ./abuild-2.x --build
   ```

   For (64-bit):

   ```
   # LUNA_CONFIG_BITS=64
   # LUNA_CONFIG_BITS=64 ./abuild-2.x --build
   ```

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

5. Open a session to SafeNet Luna HSM 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.x script to generate keys on the SafeNet Luna HSM.

   For (32-bit):

   ```
   # LUNA_CONFIG_BITS=32 ./abuild-2.x --genrsa
   ```

For (64-bit):

```
# LUNA_CONFIG_BITS=64 ./abuild-2.x --genrsa
```

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

8. Traverse to apache installation directory:

   ```
   # cd /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:

    ```
    # cd /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:

    ```
    # cd /usr/local/apache2/bin
    ```

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

    ```
    # ./apachectl -DSSL
    ```

    or

    ```
    # ./apachectl -k (stop/start/restart)
    ```

    Make sure you have disabled iptables or allow http/https traffic through firewall.

14. Open any browser (IE/Firefox) and access the HTTP Server:

    https://<HostName or IP Address>:443

15. Accept the certificate.