THALES

gemalto
a Thales company

Apache HTTP Server

INTEGRATION GUIDE
SAFENET LUNA HSM

Document Information

Document Part Number	007-011228-001
Release Date	9 April 2020

Revision History

Revision	Date	Reason
K	9 April 2020	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 guide describes the steps involved in integrating Apache HTTP Server with SafeNet Luna HSM. It contains the following chapters:

- Getting Started describes the third party applications, supported platforms, prerequisites, and the setup required for the integration.
- Integrating Apache Server with SafeNet Luna HSM Using GemEngine in Windows explains the steps to configure and integrate Apache Server with SafeNet Luna HSM using GemEngine in Windows. This chapter also includes the steps to migrate existing SSL Keys from local software to SafeNet Luna HSM.
- Integrating Apache Server with SafeNet Luna HSM Using GemEngine in UNIX explains the steps to configure and integrate Apache Server with SafeNet Luna HSM using GemEngine in UNIX.
- Integrating Apache Server with SafeNet Luna HSM Using LunaCA3 Engine in UNIX explains how to integrate Apache Server with SafeNet Luna HSM using LunaCA3 Engine in UNIX.

Audience

This document is intended to guide security administrators through the steps for integrating Apache HTTP Server with SafeNet Luna HSM.

All products manufactured and distributed by Gemalto, Inc. are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Document Conventions

This section provides information on the conventions used in this document.

Notes

Notes are used to alert you to important or helpful information.

> **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.

> **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.

> ****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.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<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>] [a | b | c] [<a> | <b> | <c>]	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. 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: Getting Started

This chapter covers the following topics:

About SafeNet Luna HSMs

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.

The benefits of integrating Apache HTTP Server with SafeNet Luna HSMs include:

- Secure generation, storage, and protection of the SSL keys on FIPS 140-2 level 3 validated hardware.
- Full life cycle management of the keys.
- HSM audit trail.
- Significant performance improvements by off-loading cryptographic operations from servers.

Third Party Applications

This integration uses the following third party application:

- Apache HTTP Server v2.4.x for UNIX
- Apache HTTP Server v2.4.x for Windows
- 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
Windows Server 2016	Luna SA Appliance Software v7.3.0 Firmware 7.3.0 Luna Client 7.3.0	Apache v2.4.41 Apache v2.4.17
Red Hat Enterprise Linux 7.0 (64 bit)	Luna SA Appliance Software v7.0.0 Firmware 7.0.1 Luna Client 7.0.0	Apache v2.4.27
Red Hat Enterprise Linux 7.0 (64 bit)	Luna SA Appliance Software v6.3.0 Firmware 6.27.0 Luna Client 6.3.0	Apache v2.4.27
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
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 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 5.11 (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 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**
Red Hat Enterprise Linux 5.8 (64 bit / 32 bit)	**Luna PCI 5.0** **Firmware 6.1.3**	**Apache v2.2.14**
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**
Red Hat Enterprise Linux 5.8 (64 bit)	**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

Before beginning the integration, ensure you complete the following processes:

> Configuring the SafeNet Luna HSM

> Setting SafeNet Network HSM Configuration

> Downloading Apache Toolkit

> Downloading GemEngine Toolkit

> Setting up Apache HTTP Server on Windows

Configuring the SafeNet Luna HSM

If you are using a SafeNet Luna HSM:

1. Verify the HSM is set up, initialized, provisioned, and ready for deployment. Refer to the *SafeNet Luna HSM Product Documentation* for more information.

2. Create a partition on the HSM that will be used by Apache later on.

3. If you are using a SafeNet Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize the Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that each partition is successfully registered and configured. The command to see the registered partitions is:

   ```
   # /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 ->                apache

   Serial Number ->        1280780175949

   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
   ```

   > **NOTE:** Follow the *SafeNet Luna Network HSM Product Documentation* for steps to create the NTLS connection, initialize the partitions, and initialize the Security Officer, Crypto Officer, and Crypto User roles.

Setting SafeNet Network HSM Configuration

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

/etc/Chrystoki.conf

This file is automatically configured and does not require any changes to communicate with the HSM. However for Luna Client 6.x onwards, we have to edit this configuration file for slot id because the default slot id is 0, but LunaCA3 engine is configured to use slot id as 1. To set the slot id to 1, you need to make the following changes in the configuration file:

```
Presentation = {

   OneBaseSlotId =1;

}
```

Using SafeNet Luna 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 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 is in FIPS mode.

> **NOTE:** For Universal Client above setting is not required. This setting is applicable for Luna Client 6.x and 7.x only.

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.

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. Users you add to the hsmusers group are able to access the HSM. Users who are not part of the hsmusers group are not able to access the HSM.

> **Adding a user to hsmusers group**

For Apache-toolkit to work with Luna7, add daemon user to hsmusers group.

a. Ensure that you have **sudo** privileges on the client workstation.

b. Add a user to the hsmusers group.

```
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.

> **Removing a user from hsmusers group**

a. Ensure that you have sudo privileges on the client workstation.

b. Remove a user from the hsmusers group.

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

Where <username> is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

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

Downloading 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. This toolkit is used for LunaCA3 Engine. However, for GemEngine it is not needed.

Downloading GemEngine Toolkit

The GemEngine toolkit is provided to integrate Apache HTTP Server with SafeNet HSM. The installation CD can be obtained from the SafeNet Customer Support.

> **NOTE:** For GemEngine setup, contact Customer support. Doc ID for GemEngine v1.2 is DOW0002177/KB0016309 and Doc ID for GemEngine v1.3 Alpha 3 is DOW0003059/KB0017806.

Setting up Apache HTTP Server on Windows

Download Apache HTTP Server from https://httpd.apache.org/download.cgi and extract apache zip file to C:\Apache24.

> **NOTE:** Ensure to install latest Visual C++ Redistributable for Visual Studio 2015-2019 before running Apache.
>
> **NOTE:** If you want to integrate Apache HTTP server with HSM in FIPS mode then rebuild Apache HTTP Server and OpenSSL FIPS version.

CHAPTER 2: Integrating Apache Server with SafeNet Luna HSM Using GemEngine in Windows

Integration of Apache HTTP Server with SafeNet Luna HSM using GemEngine in Windows involves the following use cases:

- Integrating SafeNet Luna HSM with Apache HTTP Server by generating new SSL keys
- Integrating SafeNet Luna HSM with Apache HTTP Server by migrating existing SSL keys

Integrating Apache HTTP Server with SafeNet Luna HSM by generating new SSL keys

This integration involves the following steps:

- Configuring GemEngine for OpenSSL
- Generating keys and certificates
- Configuring Apache HTTP Server for SSL

Configuring GemEngine for OpenSSL

To configure GemEngine for OpenSSL:

1. Check the OpenSSL and engine directory of the OpenSSL bundled with Apache:

   ```
   # C:\Apache24\bin\openssl.exe version -d
   ```

   The output will appear like this:

   ```
   OPENSSLDIR: C:\Program Files\Common Files\SSL
   ```

2. Copy C:\Apache24\conf\openssl.cnf file to the folder specified above in OPENSSLDIR.
3. Copy gem.dll from GemEngine toolkit to C:\Apache24\conf\lib\engines-1_1\
4. Check that the OpenSSL is able to load the gem engine:

   ```
   # C:\Apache24\bin\openssl.exe engine gem -v
   ```

5. Add the following text to the C:\Program Files\SafeNet\LunaClient\crystoki.ini file:

   ```
   [GemEngine]
   LibPath = C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll
   LibPath64 = C:\Program Files\SafeNet\LunaClient\cryptoki.dll
   EnableDsaGenKeyPair = 1
   EnableRsaGenKeyPair = 1
   DisablePublicCrypto = 1
   ```

```
EnableRsaSignVerify = 1
EnableLoadPubKey = 1
EnableLoadPrivKey = 1
DisableCheckFinalize = 1
DisableEcdsa = 1
DisableDsa = 0
DisableRand = 0
EngineInit = 0:10:11
```

where 0 is slot id and 10:11 is the application ID in EngineInit.

6. Copy the sautil.exe from GemEngine toolkit to C:\Apache24\bin\.
7. Open the persistent session with the HSM:

   ```
   # C:\Apache24\bin\sautil.exe -v -s 0 -i 10:11 -o -q
   ```

   where 0 is slot id and 10:11 is the application ID.

   Provide the partition password when prompted.

Generating Keys and Certificates

To generate keys and certificates on the HSM:

1. Use the OpenSSL command:

   ```
   # C:\Apache24\bin\openssl.exe genrsa -engine gem 2048
   ```

   This will output the private key reference. Save the private key reference in a file called C:\Apache24\conf\server.key.
2. Create a self-signed certificate using the above private key:

   ```
   # C:\Apache24\bin\openssl.exe req -engine gem -new -x509 -days 365 -key
   server.key -out C:\Apache24\conf\server.crt
   ```

   > **NOTE:** Self-signed certificate is used for test purpose, in production environment facing internet, create the certificate request and signed it by the Trusted Certificate Authority.

Configuring Apache HTTP Server for SSL

To configure Apache HTTP server for SSL:

1. Uncomment the following lines in the C:\Apache24\conf\httpd.conf file:

   ```
   #LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
   #LoadModule ssl_module modules/mod_ssl.so
   #Include conf/extra/httpd-ssl.conf
   ```
2. Add/modify the following lines in C:\Apache24\conf\extras\httpd-ssl.conf file:

   ```
   SSLCryptoDevice gem
   <VirtualHost _default_:443>
   SSLCertificateKeyFile "${SRVROOT}/conf/server.key"
   ```

```
SSLCertificateFile "${SRVROOT}/conf/server.crt"
</VirtualHost>
```

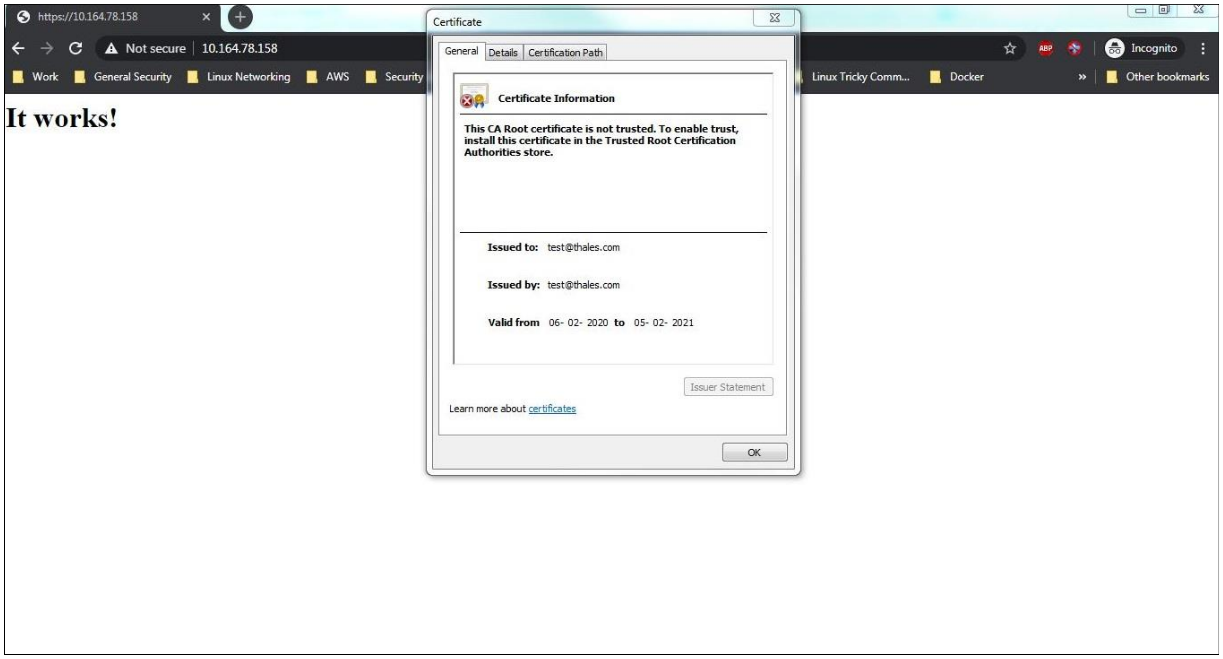
> **NOTE:** If the certicate is signed by root CA then add **SSLCertificateChainFile "${SRVROOT}/conf/server-ca.crt"** where **server-ca.cert** is signing/root CA certificate inside VirtualHost section.

3. Start the Apache HTTP Server:

```
# C:\Apache24\bin\httpd.exe -k start
```

4. Access the HTTP Server over port 443 in web browser and accept the certificate:

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



It works!

Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: test@thales.com

Issued by: test@thales.com

Valid from 06- 02- 2020 to 05- 02- 2021

Learn more about certificates

Integrating Apache HTTP Server with SafeNet Luna HSM by migrating existing SSL keys

It is assumed that Apache HTTP server is already configured and running on SSL where SSL certificate and keys are generated by OpenSSL and saved somewhere in directory.

Migrating Existing SSL Keys

Before proceeding ensure that you have completed the Prerequisites.

To Migrate Existing SSL Keys:

1. Configure OpenSSL to use GemEngine by executing the steps mentioned in the Configuring GemEngine for OpenSSL section.
2. Locate the directory where the SSL private key and certificate are stored.
3. Extract the certificate public key using the command below.

```
# C:\Apache24\bin\openssl.exe rsa -in C:\Apache24\conf\server.key.txt -pubout -
out pubkey.pem
```

4. Extract the private key in PKCS#8 format using the below command.

```
# C:\Apache24\bin\openssl.exe pkcs8 -in  C:\Apache24\conf\server.key.txt -topk8
-nocrypt -out privatekey.pem
```

5. Using CMU utility provided with Luna Client, import the public key and private key to the HSM.

   For Public Key:

```
# "C:\Program Files\SafeNet\LunaClient\Cmu.exe" import -inputFile pubkey.pem -
label apache_pub_key -pubkey=rsa
```

   For Private Key:

```
# "C:\Program Files\SafeNet\LunaClient\Cmu.exe" importkey -PKCS8 -in
privatekey.pem -keyalg RSA
```

6. Verify that the keys are generated on SafeNet Luna HSM partition and note the private key handle which will be used later.

```
# "C:\Program Files\SafeNet\LunaClient\Cmu.exe" 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=83       label=CMU Unwrapped RSA Private Key

handle=76       label=apache_pub_key
```

7. Optionally, you can provide the label to the private key to recognize (in case you have multiple keys) it. Execute the following command.

```
# "C:\Program Files\SafeNet\LunaClient\Cmu.exe" setattribute -handle=83 -
label=apache_priv_key
```

8. Verify that the private key label corresponds to the label of public key.

```
# "C:\Program Files\SafeNet\LunaClient\Cmu.exe" 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=83       label=apache_priv_key

handle=76       label=apache_pub_key
```

9. Run the sautil utility to create Private Key Reference to actual private key imported in SafeNet Luna HSM.

```
# C:\Apache24\bin\sautil.exe -v -s 0 -i 0:0 -a 0:RSA -f
C:\Apache24\conf\HSMKey_ref.pem -o -q -c
```

   Provide the HSM partition CO password and key handle when prompted. After successful completion, HSMKey_ref.pem will be generated which you need to specify in SSL setting in extras/httpd-ssl.conf file.

10. Remove the Private Key generated by OpenSSL which you were using before importing the key in to SafeNet HSM along with the PKCS#8 format key generated in step 4.

11. Add/modify the following lines in C:\Apache24\conf \extras\httpd-ssl.conf file:

```
SSLCryptoDevice gem
<VirtualHost _default_:443>
SSLCertificateKeyFile "${SRVROOT}/conf/HSMKey_ref.pem "
SSLCertificateFile "${SRVROOT}/conf/server.crt"
</VirtualHost>
```

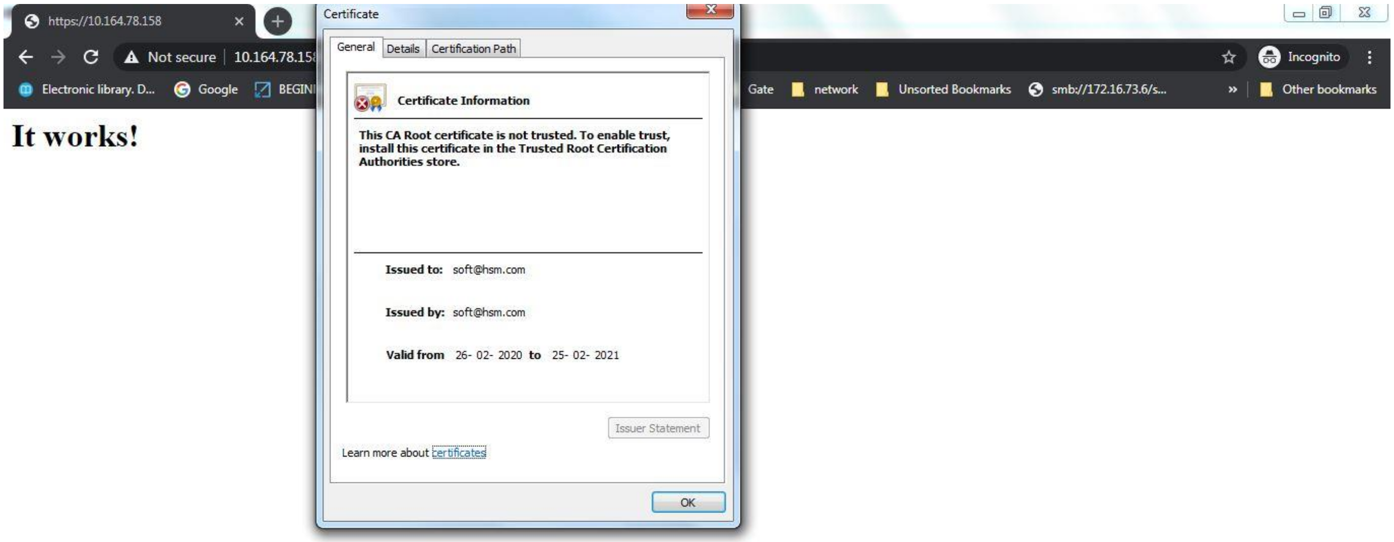
> **NOTE:** If the certificate is signed by root CA, then add SSLCertificateChainFile ${SRVROOT}/conf/server-ca.crt, where server-ca.cert is signing/root CA certificate inside VirtualHost section.

12. Restart the Apache HTTP Server:

```
# C:\Apache24\bin\httpd.exe -k restart
```

13. Access the Apache HTTP Server over port 443 in web browser and accept the certificate:

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



It works!

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: soft@hsm.com

Issued by: soft@hsm.com

Valid from 26- 02- 2020 to 25- 02- 2021

Learn more about certificates

CHAPTER 3: Integrating Apache Server with SafeNet Luna HSM Using GemEngine in UNIX

To integrate SafeNet Luna Network HSM with Apache Web Server using GemEngine in UNIX:

1. Download and extract OpenSSL source tarball. Example:

   Download openssl-1.0.1s.tar.gz from https://www.openssl.org/source/

   ```
   # tar xvfz openssl-1.0.1s.tar.gz
   ```

2. Download and extract **OpenSSL FIPS** module. Ignore this step if the FIPS module is not required. Example:

   Download openssl-fips-2.0.9.tar.gz from https://www.openssl.org/source/

   ```
   # tar xvfz openssl-fips-2.0.9.tar.gz
   ```

3. Download and extract an Apache (httpd) source tarball from https://httpd.apache.org/download.cgi and place the .tar.gz file inside the gemengine directory. Example:

   Download httpd-2.4.27.tar.gz and extract:

   ```
   # tar xzvf httpd-2.4.27.tar.gz
   ```

4. Download and extract an apr source tarball from https://apr.apache.org/download.cgi and place the .tar.gz file inside the gemengine directory. Example:

   Download apr-1.6.2.tar.gz and extract:

   ```
   # tar xzvf apr-1.6.2.tar.gz
   ```

5. Download and extract an apr util source tarball from https://apr.apache.org/download.cgi and place the .tar.gz file inside the gemengine directory. Example:

   Download apr-util-1.6.0.tar.gz and extract:

   ```
   # tar xzvf apr-util-1.6.0.tar.gz
   ```

6. Download and extract an apr iconv source tarball from https://apr.apache.org/download.cgi and place the .tar.gz file inside the gemengine directory. Example:

   Download apr-iconv-1.2.1.tar.gz and extract:

   ```
   # tar xzvf apr-iconv-1.2.1.tar.gz
   ```

7. Run the **gembuild config** command using the -prefix option.

   ```
   # ./gembuild config --openssl-source=<openssl-source path> --apache-
   source=<httpd-src path> --apr-source=<apr-src path> --apr-iconv-
   source=<iconvsrc path> --apr-util-source=<utilsrc path>  --prefix=/usr/local --
   config-bits=64
   ```

   If FIPS module is required, add --openssl-fips-source=<openssl-fips-source path> to the **./gembuild config** command.

8. Compile and install FIPS module. Proceed to Step 9 if FIPS module is not required.

   ```
   # ./gembuild openssl-fips-build
   ```

```
# ./gembuild openssl-fips-install
```

9. Compile and install **OpenSSL**.

```
# ./gembuild openssl-build
# ./gembuild openssl-install
```

10. Compile and install gem dynamic engine and verify engine.

```
# ./gembuild engine-build
# ./gembuild engine-install
# /usr/local/ssl/bin/openssl engine gem –v
(gem) Gem engine support
     enginearg, openSession, closeSession, login, logout, engineinit,
     CONF_PATH, ENGINE_INIT, ENGINE2_INIT,engine2init,DisableCheckFinalize,
     SO_PATH, GET_HA_STATE, SET_FINALIZE_PENDING, SKIP_C_INITIALIZE,
     IntermediateProcesses
```

11. Compile and install **sautil** command.

```
# ./gembuild sautil-build
# ./gembuild sautil-install
```

By default, this installs the **sautil** command to <prefix>/sautil/bin/sautil where <prefix> is the directory specified with --prefix option in the step 7.

If a different location is desired, use the **--sautil-prefix** option to specify the desired directory either by redoing the step 7 with the option or by specifying the option as part of the "./gembuild sautil-install" command.

12. Add **openssl** and **sautil** to PATH. Example:

```
# export PATH=/usr/local/ssl/bin:/usr/local/sautil/bin:$PATH
```

13. Compile and install **Apache**:

```
# ./gembuild apache-build
```

14. Run the **Optimize.sh** command in the gemengine directory to configure the SafeNet Network HSM/SafeNet PCI-E HSM configuration file (/etc/Chrystoki.conf) for Apache:

```
#./ Optimize.sh fork
```

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;
   }
GemEngine = {
```

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

15. Run the **sautil** utility to open the session on the SafeNet Luna HSM slot:

    ```
    # /usr/local/sautil/bin/ sautil -v -s 1 -i 10:11 -o –q
    ```

16. Generate RSA key pair using Apache Toolkit:

    ```
    ./gembuild apache-genrsa
    ```

17. Go to Apache installation directory, update Apache configuration file (httpd.conf) and edit the **ServerName** field with the hostname or IP address of the server with the value specified for the CN in the certificate created in step 16.

18. Go to Apache installation directory for conf/extra for SSL configuration (such as: /usr/local/apache2/conf/extra), update **httpd-ssl.conf** and edit the **Virtual Host** section as below:

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

19. Start the **Apache** server:

    ```
    /usr/local/apache2/bin/apachectl -k start
    ```

20. Open IE or Firefox browser and access the following HTTP server:

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

21. Accept the certificate.

CHAPTER 4: Integrating Apache Server with SafeNet Luna HSM Using LunaCA3 Engine in UNIX

To integrate Apache HTTP Server with SafeNet Luna HSM:

1. Go to the toolkit, such as: /root/_cdrom_apache.
2. Run the **OptimizeApache.sh** command 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.

   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;
}
```

3. Go to toolkit: /root/_cdrom_apache, run the configuration script (abuild-2.x) to install Apache HTTP Server, and Open SSL for Luna SA:

   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.

4. 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.

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

6. Go to toolkit: /root/_cdrom_apache and 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.

7. Go to apache installation directory:

   ```
   # cd /usr/local/apache2/conf
   ```

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

9. Go to the directory:

   ```
   # cd /usr/local/apache2/conf/extra
   ```

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

    <Virtual Host Hostname or IP Address: 443>

11. Go to the directory:

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

12. 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.

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

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

14. Accept the certificate.

APPENDIX A: Configuring Apache Tookit for v2.x.x in UNIX (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. Go to toolkit, such as: /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. Go to the toolkit, such as: /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.