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

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013602-001, Rev. A
Release Date: August 2016
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
  3rd party Application Details .................................................................................................................... 8
  Supported Platforms ................................................................................................................................... 8
    Citrix NetScaler Virtual Appliance Setup .............................................................................................. 8
  Prerequisites ........................................................................................................................................... 9

2 Integrating Citrix NetScaler Virtual Appliance with SafeNet Network HSM ............................ 11
  Configure SafeNet Network HSM with Citrix NetScaler .................................................................. 11
    Generate Key on SafeNet Network HSM .............................................................................................. 11
    Add Key and Certificate on Citrix NetScaler ....................................................................................... 12
    Load Balancing Virtual Server and Service on NetScaler ............................................................... 12
Preface

This document covers the necessary information to install, configure, and integrate Citrix NetScaler Virtual Appliance with SafeNet Luna Hardware Security Module.

Scope

This document provides the necessary steps to install, configure, and integrate Citrix NetScaler Virtual Appliance with SafeNet Luna Hardware Security Module. A SafeNet network HSM is designed to protect critical cryptographic keys and to accelerate sensitive cryptographic operations across a wide range of security applications.

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:

<table>
<thead>
<tr>
<th>Old product name</th>
<th>New product name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Luna SA HSM</td>
<td>SafeNet Network HSM</td>
</tr>
<tr>
<td>Luna PCI-E HSM</td>
<td>SafeNet PCI-E HSM</td>
</tr>
<tr>
<td>Luna G5 HSM</td>
<td>SafeNet USB HSM</td>
</tr>
<tr>
<td>Luna Client</td>
<td>SafeNet HSM Client</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>The bold attribute is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• Command-line commands and options (Type <code>dir /p</code>.)</td>
</tr>
<tr>
<td></td>
<td>• Button names (Click <code>Save As</code>.)</td>
</tr>
<tr>
<td></td>
<td>• Check box and radio button names (Select the <code>Print Duplex</code> check box.)</td>
</tr>
<tr>
<td></td>
<td>• Window titles (On the <code>Protect Document</code> window, click <code>Yes</code>.)</td>
</tr>
<tr>
<td></td>
<td>• Field names (<code>User Name</code>: Enter the name of the user.)</td>
</tr>
<tr>
<td></td>
<td>• Menu names (On the <code>File</code> menu, click <code>Save</code>.) (Click <code>Menu &gt; Go To &gt; Folders</code>.)</td>
</tr>
<tr>
<td></td>
<td>• User input (In the <code>Date</code> box, type <code>April 1</code>.)</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>The italic attribute is used for emphasis or to indicate a related document. (See the <code>Installation Guide</code> for more information.)</td>
</tr>
<tr>
<td>Consolas</td>
<td>Denotes syntax, prompts, and code examples.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland  21017, USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>US</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
1 – Introduction

Introduction

Overview

A non-FIPS NetScaler appliance stores the server’s private key on the hard disk. On a FIPS appliance, the key is stored in a cryptographic module known as a hardware security module (HSM). Storing a key in the HSM protects it from physical and software attacks. In addition, the keys are encrypted with special FIPS approved ciphers.

Only the NetScaler MPX 9700/10500/12500/15500 FIPS appliances support a FIPS card. Support for FIPS is not available on other MPX appliances, or on the SDX and VPX appliances. This limitation is addressed by supporting a SafeNet network HSM on all NetScaler MPX, SDX, and VPX appliances except the MPX 9700/10500/12500/15500 FIPS appliances.

A SafeNet Network HSM is designed to protect critical cryptographic keys and to accelerate sensitive cryptographic operations across a wide range of security applications.

This Integration guide outlines the integration steps for Citrix VPX appliances, but the same integration steps are supported on the MPX and SDX appliances noted previously.
3rd party Application Details

- Citrix NetScaler Virtual Appliance

**NOTE:** You require a VPX Citrix License for Load Balancing feature.

Supported Platforms

<table>
<thead>
<tr>
<th>Third Party Details</th>
<th>SafeNet Appliance version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix NetScaler Virtual Appliance(11.1-47.14_nc)</td>
<td>Appliance Version-5.4.7-1</td>
<td>6.10.9</td>
</tr>
</tbody>
</table>

**NOTE:** SafeNet Luna Client 6.0.0 provided with Citrix build does not work in HA mode with Citrix Virtual Appliance.

**NOTE:** This integration has been also tested using two Citrix NetScaler Virtual appliances in HA mode with SafeNet Luna HSM.

Citrix NetScaler Virtual Appliance Setup

Use the appropriate virtual image file to deploy the virtual appliance on the VMware.

When your virtual appliance is on a VMware, perform the following steps:
• Access the Citrix NetScaler WebGUI through the IP address that was configured during deployment. For example: <http://IP-Address>

![Citrix NetScaler Login Screen](image)

**Prerequisites**

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box. 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 parameters are set to work with your network.
- Initialize the SafeNet Network HSM appliance.
- Copy the corresponding NetScaler build (build-11.1-47.14_nc.tgz) on the NetScaler Virtual Appliance.
- Untar the build and execute the installns script (/var/safenet/safenet/lunaclient/bin/)
  
  This build installs the SafeNet client setup and directory structure. (/var/safenet/safenet/lunaclient/bin/)

- When you load the NetScaler build by using the installns script, the safenet_dirs.tar file is copied into the /var/ directory. If no “/var/safenet/” directory is present, the installns script creates a “safenet” directory in the /var/ directory.

- Configure the NTLS between SafeNet Luna HSM client and HSM. After the “/var/safenet/” directory is created, perform the following tasks:
  
  a. Change directory to /var/safenet/config/ and run the “safenet_config” script. At the shell prompt, type:

     ```
     cd /var/safenet/config
     sh safenet_config
     ```

     This script copies the “Chrystoki.conf” file into the /etc/ directory. It also generates a symbolic link “libCryptoki2_64.so” in the “/usr/lib/” directory.

  b. Create and transfer a certificate and key between the SafeNet Luna HSM Client and the SafeNet HSM. In order to communicate securely, the Client and the HSM must exchange certificates. Create a certificate and key on the SafeNet HSM Client and then transfer it to the HSM. Copy the HSM certificate to the Client.

     a. Change directory to /var/safenet/safenet/lunaclient/bin.

     ```
     ./vtl createCert -n <ip address of NetScaler>
     ```
b. Copy the certificate to the HSM. At the shell prompt, type:

```
scp /var/safenet/safenet/lunaclient/cert/client/<ip address of NS>.pem <SafeNet_HSM account>@<IP address of SafeNet HSM>
```

c. Copy the certificate and key from the HSM to the NetScaler

```
scp <HSM account>@<HSM IP>:server.pem /var/safenet/safenet/lunaclient/server_<HSM_ip>.pem
```

d. Register the NetScaler ADC on the SafeNet HSM.

```
client register -client <client name> -ip <netscaler ip>
```

e. Assign the client a partition from the partition list.

```
client assignPartition -client <Client Name> -par <Partition Name>
```

f. Register the HSM with its certificate on the SafeNet Luna Client.

```
./vtl addserver -n <IP addr of HSM> -c /var/safenet/safenet/lunaclient/server_<HSM_IP>.pem
```

g. Verify the network trust links (NTLS) connectivity between the Client and HSM. At the shell prompt, type:

```
./vtl verify
```

```
root@Citrix# ./vtl v
The following Luna SA Slots/Partitions were found:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Serial #</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>512186018</td>
<td>Mann</td>
</tr>
</tbody>
</table>
```

- Save the configuration.

```
cp /etc/Chrystoki.conf /var/safenet/config/
```

The above steps update the “/etc/Chrystoki.conf” configuration file. This file is deleted when the ADC is started. Copy the configuration to the default configuration file, which is used when an ADC is restarted.

- Configure automatic start of the gateway daemon at boot time.

```
touch /var/safenet/safenet_is_enrolled
```
Integrating Citrix NetScaler Virtual Appliance with SafeNet Network HSM

Configure SafeNet Network HSM with Citrix NetScaler

Perform the following steps to integrate SafeNet Network HSM with Citrix NetScaler:

- Generate a key pair using third party.
- Add Key and Certificate on Citrix NetScaler.
- Create a Load Balancing Virtual Server and Service.

Generate Key on SafeNet Network HSM

Before creating a key on HSM, ensure you have already established the NTLS connection with SafeNet Network HSM.

Traverse to the Luna Client installation directory Path (/var/safenet/safenet/lunaclient/bin/) and execute the following command using Certificate Management utility:

1. Generate the key pair using the below commands.
   ```bash
   ./cmu gen -modulusBits=2048 -publicExponent=65537 -sign=T -verify=T -encrypt=1 -decrypt=1 -wrap=1 -unwrap=1 -label=Citrix_Keys
   ```
2. `cmu list` to list the generated key pair.
   ```bash
   ./cmu list
   Please enter password for token in slot 0 : ********
   handle=31       label=Citrix_Keys
   handle=28       label=Citrix_Keys
   ```
3. Generate a certificate request.
   ```bash
   ./cmu requestcertificate
   Enter the handle id for which request needs to be generated and certificate request details.
   Certificate Request file is by default saved in /var/safenet/safenet/lunaclient/bin/. Get the Signed certificate from the trusted CA and copy the certificate in this directory /var/safenet/safenet/lunaclient/bin/
   ```
4. Import the certificate.
   ```bash
   ./cmu import
   Enter the Certificate input file name.
5. Export the Certificate in .pem format using CMU.
   
   ```
   ./cmu export
   
Enter the output file name (For Example Citrix.pem)
   ```

6. Copy the certificate to the /nsconfig/ssl/ directory on the ADC
   
   ```
   cp <cert.pem> /nsconfig/ssl/
   ```

### Add Key and Certificate on Citrix NetScaler

1. Add an HSM key on the ADC. At the command prompt, type:
   
   ```
   add ssl hsmkey <KeyName> -hsmType SAFENET -serialNum <serial number of partition> -password <Partition_password>
   ```

2. Add a certificate-key pair on the ADC
   
   ```
   add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
   ```

### Load Balancing Virtual Server and Service on NetScaler

We have deployed IBM WebSphere and used the snoop application to test the integration.

Add the details of the Server machine in NetScaler on which IBM WebSphere application server is running and sample application is deployed

1. Traverse to **Traffic Management**->**Load Balancing**->**Servers**
2. Click **Add** to add the Details of the application server.
3. Click **Create** to add the server. The added server displays in the list.
Add Service

Open the NetScaler GUI using the IP Address For example <http://10.164.74.121>

1. Traverse to Traffic Management->Load Balancing->Services

2. Click Add to add the services.
3. Click OK to add the service.

![Load Balancing Service](image1)

We have deployed IBM WebSphere and used the snoop application to test the integration.

In the server field add the IP of the machine where your application is already running. Select the Protocol and port as shown in Screen shot.

4. The Services page displays. The State of the Service should be UP.

![Services](image2)
Virtual Server

Open the NetScaler GUI using the IP Address < http://10.164.74.121>

1. Traverse to Traffic Management->Load Balancing->Virtual Servers

2. Click Add.
3. Enter the details of the Virtual Server. Select the Protocol as SSL and then click **OK**.
4. The Virtual Server should be created in list with State as Down. Click **No Load Balancing Virtual Service Binding**.
5. The Service Binding page displays.
Click **select service** and select the service created above. Click the **Bind** button.

6. After service binding, click **Continue**.

7. Click **No Server Certificate**.
8. Select Server Certificate and click **Bind**.

After Successful Binding of Certificate and service the state of Virtual Server Should be **UP**.
Now access the application over https using the IP of the virtual server on port 443.

For Example: https://10.164.74.140/snoop