Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-000265-001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>March 2019</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>March 2019</td>
<td>Update</td>
</tr>
</tbody>
</table>
Trademarks, Copyrights, and Third-Party Software
© 2019 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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.

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

Scope ................................................................................................................................. 6
Document Conventions .................................................................................................... 6
Command Syntax and Typeface Conventions ................................................................. 7
Support Contacts ............................................................................................................. 8
Customer Support Portal ............................................................................................... 8
Telephone Support .......................................................................................................... 8
Email Support .................................................................................................................. 8

### CHAPTER 1: Introduction

Third Party Application Details ....................................................................................... 9
Supported Platforms ........................................................................................................ 9
Prerequisites .................................................................................................................... 10
Configuring SafeNet Luna HSM ..................................................................................... 10
Provision your HSM on Demand Service ..................................................................... 10
Constraints on HSMoD Services ................................................................................... 10
Using SafeNet HSM in FIPS Mode .............................................................................. 11
Setup F5 BIG-IP ............................................................................................................. 11
Access to Gemalto Customer Support Portal ................................................................. 11

### CHAPTER 2: Integrating F5 BIG-IP with a SafeNet Luna Network HSM

Configuring F5 BIG-IP to use SafeNet Luna Network HSM ........................................ 12
Before you begin ............................................................................................................ 12
Adding the Luna Network Client to the BIG-IP System ............................................. 13
Installing and registering the Luna client ................................................................. 13
Setting up the Luna Client on a newly added or activated blade ......................... 14
Generating a key/certificate using tmsh .................................................................... 15
Creating a self-signed digital certificate .................................................................. 15
Requesting a Certificate from a Certificate Authority ............................................ 16
Configuring a Client SSL Profile to use an External HSM key and certificate ..... 17
Importing a Pre-existing SafeNet Luna HSM key into the BIG-IP ......................... 18
Deleting a Key from the BIG-IP system .................................................................... 19

### CHAPTER 3: Manually setting up the SafeNet Luna HSM with F5 BIG-IP System

Safenet Luna Network HSM 7.2 and Data Protection On Demand (DPoD) can be configured manually with F5 BIG-IP System ......................................................... 20
Configuring F5 BIG-IP to use SafeNet Luna HSM ..................................................... 20
Configuring DPoD with the BIG-IP System .............................................................. 20
Configuring Safenet Luna Network HSM 7.2 with the BIG-IP System ..................... 22
Configure SafeNet as the external-hsm ................................................................. 24
Adding Partition Information to BIG-IP System ...................................................... 24
Generating a Key/Certificate Using Traffic Manager Shell (tmsh) ......................... 25
Creating a self-signed digital certificate ................................................................. 26
Requesting a Certificate from a Certificate Authority ............................................. 27
Configuring a Client SSL Profile to Use an External HSM key and certificate .... 28
Importing a Pre-existing SafeNet Luna HSM key into the BIG-IP ................................................................. 28
Deleting a Key from the BIG-IP system ........................................................................................................... 29
PREFACE

This document guides security administrators through the steps for configuring F5 BIG-IP Systems and integrating them with a SafeNet Luna Hardware Security Module (HSM).

Scope

This document covers the necessary information to configure and integrate F5 BIG-IP Systems with a SafeNet HSM.

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. 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. 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>&gt; Command-line commands and options (Type <code>dir /p.</code>)</td>
</tr>
<tr>
<td></td>
<td>&gt; Button names (Click <code>Save As.</code>)</td>
</tr>
<tr>
<td></td>
<td>&gt; Check box and radio button names (Select the <code>Print Duplex</code> check box.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Window titles (On the <code>Protect Document</code> window, click <code>Yes</code>.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Field names (<strong>User Name:</strong> Enter the name of the user.)</td>
</tr>
<tr>
<td></td>
<td>&gt; 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>&gt; User input (In the <code>Date</code> box, type <code>April 1</code>.)</td>
</tr>
<tr>
<td><strong>italic</strong></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><strong>Double quote marks</strong></td>
<td>Double quote marks enclose references to other sections within the document.</td>
</tr>
<tr>
<td><code>&lt;variable&gt;</code></td>
<td>In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.</td>
</tr>
<tr>
<td><code>[ optional ]</code></td>
<td>Square brackets enclose optional keywords or <code>&lt;variables&gt;</code> in a command line description. Optionally enter the keyword or <code>&lt;variable&gt;</code> that is enclosed in square brackets, if it is necessary or desirable to complete the task.</td>
</tr>
<tr>
<td><code>[ &lt;optional&gt; ]</code></td>
<td>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.</td>
</tr>
<tr>
<td>`{ a</td>
<td>b</td>
</tr>
</tbody>
</table>
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.gemalto.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: Introduction

BIG-IP software products are licensed modules that run on top of F5's Traffic Management Operation System (TMOS). This custom operating system is an event driven operating system designed specifically to inspect network and application traffic and make real-time decisions based on the configurations you provide. The BIG-IP LTM system uses the SafeNet HSM to generate and secure the RSA keys used by the Secure Sockets Layer (SSL).

The SafeNet HSM is an external hardware security module that is available for use with BIG-IP systems. You can use the SafeNet solution with all BIG-IP platforms, including VIPRION Series chassis and appliances and BIG-IP Virtual Edition (VE). With SafeNet Luna Network HSMs, you can also configure multiple HSMs as an HA (high availability) group to use with BIG-IP systems.

NOTE: The BIG-IP system, when in appliance mode, does not support SafeNet Luna Network HSM installation/uninstallation as the user needs root privilege to do the same.

The BIG-IP RSA-based and ECDHE-ECDSA cipher suites use the SafeNet HSM. After installation on the BIG-IP system, the SafeNet HSM is compatible with Access Policy Manager and Application Security Manager, without additional configuration steps.

For information about using the iControl interface to configure the SafeNet HSM with BIG-IP systems, consult the F5 DevCentral site (https://devcentral.f5.com/iccontrol).

Third Party Application Details
This integration guide uses the following third party applications:

> F5 BIG-IP LTM System

Supported Platforms

SafeNet Luna HSM: SafeNet Luna Network 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 Network HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

NOTE: BIG-IP is tested with Luna Clients in HA & FIPS (Federal Information Processing Standard) Mode.

SafeNet Data Protection on Demand (DPoD): SafeNet Data Protection on Demand (DPoD) is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With DPoD, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports and maintain just the services you need.
Prerequisites

Before you proceed with the integration, complete the following:

Configuring SafeNet Luna HSM

Before you get started ensure the following:

1. Ensure the HSM is setup, initialized, provisioned and ready for deployment.
2. Create a partition on the HSM to be used by BIG-IP.

**NOTE:** Follow the SafeNet Luna Network HSM Product Documentation for detailed steps for creating the NTLS connection, initializing the partitions, and various user roles.

Provision your HSM on Demand Service

This service provides your client machine with access to an HSM Application Partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

To use the HSM on Demand service you need to provision your application partition, starting by initializing the following roles:

- **Security Officer (SO)** - responsible for setting the partition policies and for creating the Crypto Officer.
- **Crypto Officer (CO)** - responsible for creating, modifying and deleting crypto objects within the partition. The CO can use the crypto objects and create an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.
- **Crypto User (CU)** - optional role that can use crypto objects while performing cryptographic operations.

**NOTE:** Refer to the SafeNet Data Protection on Demand Application Owner Quick Start Guide for procedural information on configuring the HSM on Demand service and creating a service client.

The HSM on Demand service client package is a zip file that contains system information needed to connect your client machine to an existing HSM on Demand service.

Constraints on HSMoD Services

Please take the following limitations into consideration when provisioning your HSMoD services:

**HSM on Demand Service in FIPS mode**

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the *Mechanism List* in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.
Verify HSM on Demand <slot> value
LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send the commands to. If there is more than one slot, then use the `slot set` command to direct a command to a specified slot. You can use `slot list` to determine which slot numbers are in use by which HSMoD service.

Using SafeNet 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 HSM in FIPS mode, you have to make the following change to the configuration file:

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

This setting redirects the older calling mechanism to a new approved mechanism when SafeNet HSM is in FIPS mode.

**NOTE:** The above configuration is valid for Luna 7.x and Luna 6.x (F/W Version 6.22.0 and above only). Execute `hsm firmware show` in lunash to verify the firmware version.

Setup F5 BIG-IP
Install and configure F5 BIG-IP LTM. Refer to the F5 BIG-IP documentation for further information about installing and configuring F5 BIG-IP. The product documentation for BIG-IP LTM are available at the following link under Product Manuals section:

https://support.f5.com/csp/home

**NOTE:** BIG-IP TMOS with SafeNet HSM only supports IPv4.

Access to Gemalto Customer Support Portal

**NOTE:** Doc IDs for downloading the pkcs1d fix patch from support portal is DOW0003489.
CHAPTER 2: Integrating F5 BIG-IP with a SafeNet Luna Network HSM

Configuring F5 BIG-IP to use SafeNet Luna Network HSM

To configure the BIG-IP system to use the SafeNet Luna Network HSM complete the following:

> Adding the Luna Network Client to the BIG-IP System.
> Installing and registering the Luna client.
> Setting up the Luna Client on a newly added or activated blade.
> Generating a key/certificate using tmsh.
> Creating a self-signed digital certificate.
> Requesting a Certificate from a Certificate Authority.
> Configuring a Client SSL Profile to Use an External HSM key and certificate.
> Importing a Pre-existing SafeNet Luna HSM key into the BIG-IP.
> Deleting a key from the BIG-IP system.

Before you begin

Before you can use SafeNet Luna Network HSM with the BIG-IP system, you must ensure that:

> The SafeNet HSM appliance is installed on your network.
> The SafeNet HSM appliance and the BIG-IP system can communicate with each other.
> The SafeNet HSM appliance has a virtual HSM (HSM Partition) defined before you install the client software on the BIG-IP system.
> The BIG-IP system is licensed for external interface and network HSM. If you do not have an external HSM license, you will not be able to proceed past the section Generating a key/certificate using tmsh in this integration.

NOTE: If you install the Luna Network HSM (external HSM) on a system with a FIPS card (internal HSM) installed, the Luna Network HSM takes precedence.

You cannot use the SafeNet Luna Network HSM on a BIG-IP system that is running another external HSM.
# Adding the Luna Network Client to the BIG-IP System

Before you can set up the SafeNet Luna Client software on a BIG-IP system, you must obtain a valid SafeNet Luna Client license. To use the Network HSM with your BIG-IP system, you need to obtain the software tarball from SafeNet, and install the Luna Client software onto the BIG-IP system.

## To add the Luna Network Client to the BIG-IP system

1. Log in to the Gemalto Support portal.

   [https://supportportal.gemalto.com](https://supportportal.gemalto.com)

   **NOTE:** The supported SafeNet Luna Client for F5 content on the Gemalto Support Portal is password protected. Please contact Gemalto Customer Support for credentials.

2. Download the Luna Network Client for F5 from the support portal.

   **NOTE:** For supported SafeNet Luna client and HSM versions with BIG-IP TMOS versions information, see the Interoperability Matrix for BIG-IP TMOS with SafeNet Clients and HSM supplemental document available in the AskF5 Documentation.

3. Log in to the command-line interface of the BIG-IP system using an account with administrator privileges.

4. Create a directory under `/shared` named `safenet_install`.

   ```
   # mkdir /shared/safenet_install
   ```

5. Copy the SafeNet Luna Client software tarball to `/shared/safenet_install`

## Installing and registering the Luna client

You need to install and register the Luna client so that you can use the Luna Network HSM with the BIG-IP system.

**NOTE:** If you are setting up the Luna client on a VIPRION system, you only need to run the configuration script on the primary blade. The system propagates the configuration to the additional active blades following installation.

## To install and register the Luna client

1. Log in to the command-line interface of the BIG-IP system using an account with administrator privileges.

2. If you are not installing on a VIPRION system, or you are using a self IP address to communicate with the HSM, proceed to step 3. If not, disable the **ip check** on the HSM using Luna Shell (LunaSH).

   ```
   # ntls ipcheck disable
   # service restart ntls
   ```

   This step allows the same certificate to be used from multiple IP addresses, identifying multiple blades.

3. Install and register the Luna client on the BIG-IP system, using the parameters indicated.

   ```
   # nethsm-safenet-install.sh
   ```

   Parameters for a standard installation, or on the standalone or primary blade of a VIPRION system.
The following example sets up the Luna Client v7.1 where the SafeNet Luna Network HSM has an IP address of 10.164.74.111:

```
# nethsm-safenet-install.sh --hsm_ip_addr=10.164.74.111 --image= Luna_7.1_Client_Software.tar
```

The system will prompt for Luna SA admin password and partition password.

From Luna v7.x onwards, you need to initialize the partition and CO/CU user roles using root before entering the password. After initializing the partition and user roles enter the CO password and press Enter.

**NOTE:** The VIPRION system propagates the configuration to additional active blades, but you need to reload the PATH environment variable on any blades with already-open sessions: `source ~/.bash_profile`

Parameters when multiple HSMs are configured as an HA group.

```
--hsm_ip_addr="<SafeNet HSM1_IP_address> <SafeNet HSM2_IP_address>" --hsm_ha_group=<Label name for the SafeNet HSM HA group> --image=<Luna_x.x_Client_Software.tar>
```

The following example sets up the Luna Client v7.1 for an HA group named **F5_Luna_HA** where the SafeNet Luna Network HSMs in the group have IP addresses of 10.10.10.100 and 10.10.10.101:

```
# nethsm-safenet-install.sh --hsm_ip_addr=10.10.10.100 10.10.10.101 --hsm_ha_group= luna_ha_test --image= Luna_7.1_Client_Software.tar
```

Install all components when prompted during the installation. You need to register your client IP address with the SafeNet Luna Network HSM and assign the Luna Client to a previously defined HSM partition.

You need to initialize the partition and CO/CU user roles using root before entering the partition password. Use the same password for all HA members. After initializing the partition and user roles, enter the CO password and press Enter.

**NOTE:** By default, the script sets up the SafeNet Luna client software to use 20 threads. To adjust this number, run this command before you restart the pkcs11d service: `tmsh sys crypto fips external-hsm num-threads <integer>`. Changing the number of threads affects performance.

### Setting up the Luna Client on a newly added or activated blade

After you set up the Luna Client on the primary blade of a VIPRION system, the system propagates the configuration to the additional active blades. If you subsequently add a secondary blade, activate a disabled blade, or power on a powered-off blade, you need to run a script on the new secondary blade.

**To set up the Luna Client on a newly added or activated blade**

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Execute the following on any new or re-activated secondary blade:

   ```bash
   # safenet-sync.sh <HSM partition password> -v
   ```
3. If you make the new blade, a primary blade before running the synchronization script, you need to run the regular client installation and registration procedure on the new primary blade only.

   # nethsm-safenet-install.sh

Generating a key/certificate using tmsh
Use the Traffic Management Shell (tmsh) to generate a key and certificate.

To generate a key/certificate using tmsh

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the TMS Shell (tmsh).
   
   # tmsh
3. Generate the key.

   create sys crypto key <key_name> gen-certificate common-name <cert_name> security-type nethsm

   The following example generates a key on HSM named test_key and a certificate named test_safenet.com with the security type nethsm.

   create sys crypto key test_key gen-certificate common-name test_safenet.com security-type nethsm

4. Verify that the key was created.

   list sys crypto key test_key.key

   Information about the key displays:

   sys crypto key test_key {
   key-id c31fa09a744caa9a558612b303eb0719
   key-size 2048
   key-type rsa-private
   security-type nethsm
   }

   When you generate a key/certificate using tmsh, the system creates a HSM private key. It also creates a local key, which points to the HSM key, residing in the HSM.

Creating a self-signed digital certificate
If you are configuring the BIG-IP system to manage client-side HTTP traffic, you can complete the following procedure to create a self-signed certificate to authenticate and secure the client-side HTTP traffic.

If you are configuring the system to manage server-side HTTP traffic, you must repeat this task to create a second self-signed certificate to authenticate and secure the server-side HTTP traffic.

To create a self-signed digital certificate

   
   The Traffic Certificate Management screen opens.
2. Click **Create**.
   a. In the **Name** field, type a unique name for the SSL certificate.
   b. From the **Issuer** list, select **Self**.
   c. In the **Common Name** field, type a name.
      This is typically the name of a web site, such as www.siterequest.com.
   d. In the **Division** field, type your department name.
   e. In the **Organization** field, type your company name.
   f. In the **Locality** field, type your city name.
   g. In the **State or Province** field, type your state or province name.
   h. From the **Country** list, select the name of your country.
   i. In the **E-mail Address** field, type your email address.
   j. In the **Lifetime** field, type a number of days, or retain the default, **365**.
   k. In the **Subject Alternative Name** field, type a name.
      This name is embedded in the certificate for X509 extension purposes.
      By assigning this name, you can protect multiple host names with a single SSL certificate.
   l. From the **Security Type** list, select **NetHSM**.
   m. From the **Key Type** list, RSA is selected as the default key type.
   n. From the **Size** list, select a size, in bits.
   o. Click **Finished**.

**Requesting a Certificate from a Certificate Authority**

Generate a certificate signing request (CSR) that can then be submitted to a third-party trusted certificate authority (CA).

**NOTE:** Please consult the CA to determine the specific information required for each step in this task.

**To request a certificate from a certificate authority**

1. On the Main tab, click **System > Certificate Management > Traffic Certificate Management**.
   The Traffic Certificate Management screen opens.

2. Click **Create**.
   a. In the **Name** field, type a unique name for the SSL certificate.
   b. From the **Issuer** list, select **Certificate Authority**.
   c. In the **Common Name** field, type a name.
      This is typically the name of a web site, such as www.siterequest.com.
   d. In the **Division** field, type your department name.
   e. In the **Organization** field, type your company name.
   f. In the **Locality** field, type your city name.
g. In the **State or Province** field, type your state or province name.

h. From the **Country** list, select the name of your country.

i. In the **E-mail Address** field, type your email address.

j. In the **Lifetime** field, type a number of days, or retain the default, **365**.

k. In the **Subject Alternative Name** field, type a name.

   This name is embedded in the certificate for X509 extension purposes.

   By assigning this name, you can protect multiple host names with a single SSL certificate.

l. In the **Challenge Password** field, type a password.

m. In the **Confirm Password** field, re-type the password you typed in the **Challenge Password** field.

n. From the **Security Type** list, select **NetHSM**.

o. From the **Key Type** list, **RSA** is selected as the default key type.

p. From the **Size** list, select a size, in bits.

q. Click **Finished**.

   The Certificate Signing Request screen displays.

3. Do one of the following to download the request into a file on your system.

   In the **Request Text** field, copy the certificate.

   For **Request File**, click the button.

4. Follow the instructions on the relevant certificate authority web site for either pasting the copied request or attaching the generated request file.

5. Click **Finished**.

   The Certificate Signing Request screen displays.

6. Submit the generated certificate signing request to a trusted certificate authority for signature.

### Configuring a Client SSL Profile to Use an External HSM key and certificate

After you have added the SafeNet HSM key and certificate to the BIG-IP system configuration, you can use the key and certificate as part of a client SSL profile. This task describes using the browser interface. Alternatively, you can use the Traffic Management Shell (**tmsh**) command-line utility.

**To configure a client SSL profile to use an external HSM key and certificate**

1. On the Main tab, click **Local Traffic > Profiles > SSL > Client**.

   The Client screen opens.

2. Click **Create**.

   The New Client SSL Profile screen opens.

3. In the **Name** field, type a name for the profile.

4. From the **Parent Profile** list, select **clientssl**.

5. From the **Configuration** list, select **Advanced**.

   This selection makes it possible for you to modify additional default settings.
6. For the Configuration area, select the **Custom** check box.
   The settings in the Configuration area become available for modification.

7. Using the **Certificate Key Chain** setting, specify one or more certificate key chains:
   a. From the **Certificate** list, select the name of a certificate that you imported.
   b. From the **Key** list, select the name of the key that you imported.
   c. From the **Chain** list, select the chain that you want to include in the certificate key chain.
   d. Click **Add**.

8. Click **Finished**.

After you have created the client SSL profile, you must assign the profile to a virtual server, so that the virtual server can process SSL traffic according to the specified profile settings.

**Importing a Pre-existing SafeNet Luna HSM key into the BIG-IP**

A pre-existing key on the SafeNet Luna HSM can be imported to use with BIG-IP.

**NOTE:** F5 BIG-IP does not support the ability to import/migrate any existing keys from BIG-IP to HSM.

### To import a pre-existing SafeNet Luna HSM key into the BIG-IP

1. On the Main tab, click **System > Certificate Management > Traffic Certificate Management > SSL Certificate List > Import**.
   The SSL Certificate/Key Source page opens.

2. Within **Import Type**, select **Key**.
   The key name should be the same as the SafeNet Luna HSM key label.

3. Within **Key Name**, select **Overwrite Existing** and from the drop-down menu, select the key you would like to overwrite.

4. Within Key Source, select **From NetHSM**.
   For this option to be available, the system must have External HSM licensed, and SafeNet External HSM is configured.

5. Click **Import**.
   You can also import an existing key by using tmsh commands:

   ```
   # tmsh install sys crypto key nethsm_key_label from-nethsm security-type nethsm
   or
   # tmsh install sys crypto key nethsm_key_label from-nethsm
   ```

   Use the NetHSM key label as the key name. For example:

   ```
   root@(ssl18519)(cfg-sync Standalone)(Active)(/Common)(tmos)# install sys crypto key
   nethsm_key_label (tab)
   Options:
   from-editor from-nethsm
   ```
Properties:
from-local-file from-url

root@(ssl8519)(cfg-sync Standalone)(Active)(/Common)(tmos)# install sys crypto
delete nethsm
key nethsm_key_label from-nethsm security-type nethsm

This completes the F5 BIG-IP integration with SafeNet Luna HSM. The F5 BIG-IP SSL private key is
secured on SafeNet Luna HSM.

Deleting a Key from the BIG-IP system
You perform this task to delete an existing key from the BIG-IP.

To delete a key from the BIG-IP

1. On the Main tab, click **System > Certificate Management > Traffic Certificate Management.**
   The Traffic Certificate Management screen opens.

2. From the **SSL Certificate List**, select the check box next to the key you wish to delete.

3. Click **Delete**.
   The key you selected is deleted from BIG-IP. The key stored in the SafeNet Luna Network HSM is not deleted.
Safenet Luna Network HSM 7.2 and Data Protection On Demand (DPoD) can be configured manually with F5 BIG-IP System.

Configuring F5 BIG-IP to use SafeNet Luna HSM

To configure the BIG-IP system to use SafeNet Luna HSM complete the following:

> Configuring DPoD with the BIG-IP System
> Configuring Safenet Luna Network HSM 7.2 with the BIG-IP System
> Configure SafeNet as the external-hsm
> Adding Partition Information to BIG-IP System
> Generating a Key/Certificate Using Traffic Manager Shell (tmsh)
> Creating a self-signed digital certificate
> Requesting a Certificate from a Certificate Authority
> Configuring a Client SSL Profile to Use an External HSM key and certificate
> Importing a Pre-existing SafeNet Luna HSM key into the BIG-IP
> Deleting a Key from the BIG-IP system

Configuring DPoD with the BIG-IP System

A patch must be installed to integrate F5 BIG-IP with SafeNet Data Protection on Demand.

To apply the patch to the BIG-IP System

1. Before applying the patch, take a backup of the existing pkcs11d configuration file, so that it can be recovered again:
   ```
   # cp /usr/bin/pkcs11d /shared/pkcs11d_bk
   ```
2. Download the pkcs11d fix patch and copy it to /shared directory:
3. Install the patch by running:
   ```
   # rpm -Uvh /shared/pkcs11d-14.1.0-0.0.118.x86_64.rpm -force
   ```
4. Restart pkcs11 service to apply the changes.
   ```
   # bigstart restart pkcs11d
   ```
Follow these steps to set up the DPoD Client so that the pkcs11d service can correctly locate the libraries and engine:

**To Set up the DPoD client on a Newly Added or Activated Blade**

1. Create a toolkit directory `/shared/safenet/toolkit/` and copy the gemengine library to it.
   
   ```
   # mkdir -p /shared/safenet/toolkit
   # cp ./builds/linux/rhel/64/1.0.2/libgem.so /shared/safenet/toolkit/
   ```

   **NOTE:** The GemEngine toolkit is not available in the OpenSSL toolkit. You must acquire the GemEngine toolkit from Gemalto customer support.

2. Create a lunasa directory and copy the DPoD client files into it.
   
   ```
   # mkdir -p /shared/safenet/lunasa
   # cp -rf ~/bigip_client/* /shared/safenet/lunasa/
   ```

   **NOTE:** Where "bigip_client" is the name of downloaded client files for DPoD. You must contact Gemalto customer support for access to download the DPoD client zip file.

3. Set the environment and generate the Chrystoki.conf configuration file.
   
   ```
   # source ./setenv
   ```

   **NOTE:** As the BIG-IP system is Linux-based, you interact with the Linux artifacts in the client package, present in cvclient-min.tar.

4. Create a lib directory and move the crypto libraries into the created directory.
   
   ```
   # mkdir /shared/safenet/lunasa/lib
   # mv /shared/safenet/lunasa/libs/64/libCryptoki2.so /shared/safenet/lunasa/lib
   ```

5. Create a password file to store the partition password. This file is used for the password when gemengine is called. For demonstration, we are using `userpin1` as partition password.
   
   ```
   # echo userpin1 > passfile
   ```

   
   **a.** Modify the Chrystoki2 and Misc sections.

   ```
   Chrystoki2 = {
   LibUNIX64 = /shared/safenet/lunasa/lib/libCryptoki2.so;
   }
   Misc = {
   Apache = 0;
   
   ........
   }
   ```

   **b.** Create a new GemEngine section with the indicated values.

   ```
   GemEngine = {
   ```
CHAPTER 3: Manually setting up the SafeNet Luna HSM with F5 BIG-IP System

EnableDsaGenKeyPair = 1;
EnableRsaGenKeyPair = 1;
DisablePublicCrypto = 1;
EnableRsaSignVerify = 1;
EnableLoadPubKey = 1;
EnableLoadPrivKey = 1;
DisableCheckFinalize = 1;
DisableEcdsa = 1;
DisableDsa = 0;
DisableRand = 0;
EngineInit = "<token_label>:0:0:passfile=/shared/safenet/lunasa/passfile;"
EnableLoginInit = 1;
LibPath64 = /shared/safenet/lunasa/lib/libCryptoki2.so;
LibPath = /shared/safenet/lunasa/lib/libCryptoki2.so;
}

7. Check if the paths are set correctly and the partition is accessible by running LunaCM.
   # /shared/safenet/lunasa/bin/64/lunacm

8. Mount the /usr directory in read-write mode.
   # mount -o remount,rw /usr

9. Create the following soft links:
   # ln -sf /shared/safenet/lunasa /usr/lunasa
   # ln -sf /shared/safenet/lunasa /usr/safenet/lunaclient
   # ln -sf /shared/safenet/lunasa/Chrystoki.conf /etc/Chrystoki.conf
   # ln -sf /shared/safenet/lunasa/lib/Cryptoki2.so /usr/lib/Cryptoki2_64.so
   # ln -sf /shared/safenet/lunasa/lib/Cryptoki2.so /usr/lib/Cryptoki2.so

10. Now install pkcs11d to the BIG-IP system.
    # bigstart add pkcs11d
    # bigstart stop pkcs11d
    # bigstart add --default pkcs11d

11. Remount the /usr directory in read-only mode to prevent further modification.
    # mount -o remount,ro /usr

Configuring SafeNet Luna Network HSM 7.2 with the BIG-IP System

Follow these steps to configure SafeNet Luna Network HSM 7.2 with BIG-IP system.

NOTE: Before configuring ensure that lunaclient is installed in /usr directory and partition is assigned to the client.
To Configure Safenet Luna Network HSM 7.2 with the BIG-IP System

1. Mount the /usr directory in read-write mode.

   ```bash
   # mount -o remount,rw /usr
   ```

2. Copy the gemengine library to /usr/lib64/openssl/engines.

   ```bash
   # cp ./builds/linux/rhel/64/1.0.2/libgem.so /usr/lib64/openssl/engines/
   ```

3. Create a lunasa directory /shared/safenet/lunasa

   ```bash
   # mkdir -p /shared/safenet/lunasa
   ```

4. Create link for lunaclient

   ```bash
   # ln -sf /usr/safenet/lunaclient /shared/safenet/lunasa
   ```

5. Adjust the location and permission of the Chrystoki.conf file

   ```bash
   # mv /etc/Chrystoki.conf /shared/safenet/lunasa/Chrystoki.conf
   # restorecon -R /shared/safenet
   # chmod 644 /shared/safenet/lunasa/Chrystoki.conf
   ```


   a. Modify the Chrystoki2 and Misc sections.

      ```bash
      Misc = {
      Apache = 0;
      PE1746Enabled = 1;
      ........
      }
      ```

   b. Create a new GemEngine section with the indicated values.

      ```bash
      GemEngine = {
      EnableDsaGenKeyPair = 1;
      EnableRsaGenKeyPair = 1;
      DisablePublicCrypto = 1;
      EnableRsaSignVerify = 1;
      EnableLoadPubKey = 1;
      EnableLoadPrivKey = 1;
      DisableCheckFinalize = 1;
      DisableEcdsa = 1;
      DisableDsa = 0;
      DisableRand = 0;
      LogLevel = 6;
      EngineInit = 1:10:11;
      LibPath64 = /shared/safenet/lunasa/lib/libCryptoki2_64.so;
      ```
7. Create following links.
   
   ```bash
   # ln -sf /shared/safenet/lunasa/Chrystoki.conf /etc/Chrystoki.conf
   # ln -sf /shared/safenet/lunasa/lib/libCryptoki2_64.so /usr/lib/libCryptoki2_64.so
   ```

8. Now install pkcs11d to the BIG-IP system.
   
   ```bash
   # bigstart add pkcs11d
   # bigstart stop pkcs11d
   # bigstart add --default pkcs11d
   ```

9. Remount the /usr directory in read-only mode to prevent further modification.
   
   ```bash
   # mount -o remount,ro /usr
   ```

10. Open sautil session.
    
    ```bash
    # ./builds/linux/rhel/64/1.0.2/sautil -o -s <slot_id> -i 10:11 -v -p <partition_password>
    ```

Configure SafeNet as the external-hsm

You must add safenet as external-hsm vendor to BIG-IP System.

To Configure SafeNet as the external-hsm

1. Set the vendor name to SafeNet.
   
   ```bash
   # fipskey.nethsm --hsm=Safenet
   ```

2. Configure the vendor name and partition password in tmsh.
   
   ```bash
   # tmsh create sys crypto fips external-hsm vendor safenet password <partition_password>
   ```

3. Restart the services to apply the changes.
   
   ```bash
   # bigstart start pkcs11d
   # bigstart restart tmm
   ```

Adding Partition Information to BIG-IP System

You must add the partition information so that Traffic Manager Shell (tmsh) automatically uses the partition name and password when generating keys.

NOTE: Before adding partition information using web console you must ensure that the external hsm vendor must be safenet. You can check it by running "tmsh -a list sys crypto fips external-hsm vendor | grep vendor | tr -s ' ' | cut -d ' ' -f 3". If its output is "safenet" go ahead, If not then verify again all the previous steps.
There are two ways to add partition information:

> Add partition information using command line
> Add partition information using the web console

### To add partition information using command line

1. On terminal run:
   ```
   # tmsh -a create sys crypto fips nethsm-partition <partition_name> password <partition_password>
   ```

### To add partition information using the web console

1. Open web console `https://<big-ip_address>`
2. On the Main tab, click `System > Certificate Management > HSM Management > External HSM`
   The External HSM screen opens.
3. Select `Safenet` from `Vendor`.
4. Enter the following to:
   - **Name**: `<partition name>`
   - **Password**: `<partition password>`
5. Click on `Add`. The partition is added.
6. Click on `Update` to save the changes.
7. Restart the services.
   ```
   # bigstart restart pkcs11d
   # bigstart restart tmm
   ```

    **NOTE:** After adding partition info verify that partition is listed using `tmsh -a list sys crypto fips nethsm-partition`.

### Generating a Key/Certificate Using Traffic Manager Shell (tmsh)

Use the Traffic Management Shell (`tmsh`) to generate a key and certificate.

### To generate a key/certificate using tmsh

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the `tmsh`.
   ```
   # tmsh
   ```
3. Generate the key.
   ```
   create sys crypto key <key_name> gen-certificate common-name <cert_name> security-type nethsm
   ```
   The following example generates a key on HSM named `test_key` and a certificate named `test_safenet.com` with the security type `nethsm`. 
create sys crypto key test_key gen-certificate common-name test_safenet.com
security-type nethsm

4. Verify that the key was created.

list sys crypto key test_key.key

Information about the key displays:

sys crypto key test_key {
key-id c31fa09a744ca9a558612b303eb0719
key-size 2048
key-type rsa-private
security-type nethsm
}

When you generate a key/certificate using tmsh, the system creates a HSM private key. It also creates a
local key, which points to the HSM key, residing in the HSM.

Creating a self-signed digital certificate

If you are configuring the BIG-IP system to manage client-side HTTP traffic, you can complete the following
procedure to create a self-signed certificate to authenticate and secure the client-side HTTP traffic.

If you are configuring the system to manage server-side HTTP traffic, you must repeat this task to create a
second self-signed certificate to authenticate and secure the server-side HTTP traffic.

To create a self-signed digital certificate

The Traffic Certificate Management screen opens.

2. Click Create.
   a. In the Name field, type a unique name for the SSL certificate.
   b. From the Issuer list, select Self.
   c. In the Common Name field, type a name.
      This is typically the name of a web site, such as www.siterequest.com.
   d. In the Division field, type your department name.
   e. In the Organization field, type your company name.
   f. In the Locality field, type your city name.
   g. In the State or Province field, type your state or province name.
   h. From the Country list, select the name of your country.
   i. In the E-mail Address field, type your email address.
   j. In the Lifetime field, type a number of days, or retain the default, 365.
   k. In the Subject Alternative Name field, type a name.
      This name is embedded in the certificate for X509 extension purposes.
      By assigning this name, you can protect multiple host names with a single SSL certificate.
CHAPTER 3: Manually setting up the SafeNet Luna HSM with F5 BIG-IP System

I. From the Security Type list, select NetHSM.

m. From the Key Type list, RSA is selected as the default key type.

n. From the Size list, select a size, in bits.

o. Click Finished.

Requesting a Certificate from a Certificate Authority

Generate a certificate signing request (CSR) that can then be submitted to a third-party trusted certificate authority (CA).

NOTE: Please consult the CA to determine the specific information required for each step in this task.

To request a certificate from a certificate authority

   The Traffic Certificate Management screen opens.

2. Click Create.
   a. In the Name field, type a unique name for the SSL certificate.
   b. From the Issuer list, select Certificate Authority.
   c. In the Common Name field, type a name.
      This is typically the name of a web site, such as www.siterequest.com.
   d. In the Division field, type your department name.
   e. In the Organization field, type your company name.
   f. In the Locality field, type your city name.
   g. In the State or Province field, type your state or province name.
   h. From the Country list, select the name of your country.
   i. In the E-mail Address field, type your email address.
   j. In the Lifetime field, type a number of days, or retain the default, 365.
   k. In the Subject Alternative Name field, type a name.
      This name is embedded in the certificate for X509 extension purposes.
      By assigning this name, you can protect multiple host names with a single SSL certificate.
   l. In the Challenge Password field, type a password.
   m. In the Confirm Password field, re-type the password you typed in the Challenge Password field.
   n. From the Security Type list, select NetHSM.
   o. From the Key Type list, RSA is selected as the default key type.
   p. From the Size list, select a size, in bits.
   q. Click Finished.
      The Certificate Signing Request screen displays.
3. Do one of the following to download the request into a file on your system.
   
   In the Request Text field, copy the certificate.
   
   For Request File, click the button.

4. Follow the instructions on the relevant certificate authority web site for either pasting the copied request or attaching the generated request file.

5. Click Finished.
   
   The Certificate Signing Request screen displays.

6. Submit the generated certificate signing request to a trusted certificate authority for signature.

### Configuring a Client SSL Profile to Use an External HSM key and certificate

After you have added the SafeNet HSM key and certificate to the BIG-IP system configuration, you can use the key and certificate as part of a client SSL profile. This task describes using the browser interface. Alternatively, you can use the Traffic Management Shell (`tmsh`) command-line utility.

**To configure a client SSL profile to use an external HSM key and certificate**

1. On the Main tab, click Local Traffic > Profiles > SSL > Client.
   
   The Client screen opens.

2. Click Create.
   
   The New Client SSL Profile screen opens.

3. In the Name field, type a name for the profile.

4. From the Parent Profile list, select clientssl.

5. From the Configuration list, select Advanced.
   
   This selection makes it possible for you to modify additional default settings.

6. For the Configuration area, select the Custom check box.
   
   The settings in the Configuration area become available for modification.

7. Using the Certificate Key Chain setting, specify one or more certificate key chains:
   
   a. From the Certificate list, select the name of a certificate that you imported.
   
   b. From the Key list, select the name of the key that you imported.
   
   c. From the Chain list, select the chain that you want to include in the certificate key chain.
   
   d. Click Add.

8. Click Finished.
   
   After you have created the client SSL profile, you must assign the profile to a virtual server, so that the virtual server can process SSL traffic according to the specified profile settings.

### Importing a Pre-existing SafeNet Luna HSM key into the BIG-IP

A pre-existing key on the SafeNet Luna HSM can be imported to use with BIG-IP.

**NOTE:** F5 BIG-IP does not support the ability to import/migrate any existing keys from BIG-IP to HSM.
CHAPTER 3: Manually setting up the SafeNet Luna HSM with F5 BIG-IP System

To import a pre-existing SafeNet Luna HSM key into the BIG-IP

1. On the Main tab, click **System > Certificate Management > Traffic Certificate Management > SSL Certificate List > Import.**
   The SSL Certificate/Key Source page opens.
2. Within **Import Type**, select **Key**.
   The key name should be the same as the SafeNet Luna HSM key label.
3. Within **Key Name**, select **Overwrite Existing** and from the drop-down menu, select the key you would like to overwrite.
4. Within Key Source, select **From NetHSM**.
   For this option to be available, the system must have External HSM licensed, and SafeNet External HSM is configured.
5. Click **Import**.

You can also import an existing key by using tmsh commands:

```
# tmsh install sys crypto key nethsm_key_label from-nethsm security-type nethsm
```

or

```
# tmsh install sys crypto key nethsm_key_label from-nethsm
```

Use the NetHSM key label as the key name. For example:

```
root@(ssl8519)(cfg-sync Standalone)(Active)(/Common)(tmos)# install sys crypto key
nethsm_key_label (tab)
Options:
from-editor from-nethsm
Properties:
from-local-file from-url
```

```
root@(ssl8519)(cfg-sync Standalone)(Active)(/Common)(tmos)# install sys crypto key nethsm_key_label from-nethsm security-type nethsm
```

This completes the F5 BIG-IP integration with SafeNet Luna HSM. The F5 BIG-IP SSL private key is secured on SafeNet Luna HSM.

Deleting a Key from the BIG-IP system

You perform this task to delete an existing key from the BIG-IP.

To delete a key from the BIG-IP

1. On the Main tab, click **System > Certificate Management > Traffic Certificate Management.**
   The Traffic Certificate Management screen opens.
2. From the **SSL Certificate List**, select the check box next to the key you wish to delete.
3. Click **Delete**.
   The key you selected is deleted from BIG-IP. The key stored in the SafeNet Luna HSM is not deleted.