OpenStack Barbican

INTEGRATION GUIDE

SAFENET LUNA HSM

SAFENET DATA PROTECTION ON DEMAND

Document Information

Document Part Number	007-013570-001
Release Date	April 2019

Revision History

Revision	Date	Reason
B	April 2019	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 document guides administrators through the steps for integrating OpenStack Barbican with a SafeNet HSM.

Scope

This document outlines the steps to integrate OpenStack Barbican with a SafeNet HSM. The SafeNet HSM is used to secure the encryption keys.

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

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>]	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.
[a | b | c] [<a> | <b> | <c>]	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.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

Overview

This document guides security administrators through the steps for integrating OpenStack Barbican with a SafeNet Luna HSM or SafeNet Data Protection on Demand HSM on Demand service.

OpenStack Barbican is a REST API designed for the secure storage, provisioning and management of secrets. You can configure OpenStack Barbican to encrypt sensitive information using a hardware security module (HSM). OpenStack Barbican crypto components allow users to encrypt and decrypt cryptographic information using an HSM.

The benefits of integrating OpenStack Barbican with a SafeNet HSM include:

- Full life cycle management of the keys.
- HSM audit trail.**
- Significant performance improvements by off-loading cryptographic operations from servers.

*HSMoD services do not have access to the secure audit trail.

Third Party Application Details

This integration guide uses the following third party applications:

- OpenStack Barbican

Supported Platforms

SafeNet Luna HSM: 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 Network 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. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

SafeNet Luna HSM works with the following platforms:

- RHEL
- Centos

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.

SafeNet Data Protection on Demand (DPoD) works with the following platforms:

- RHEL
- Centos

Prerequisites

Before you proceed with the integration, complete the following:

> **NOTE:** The OpenStack Barbican integration does not work with a SafeNet Luna HSM or Data Protection on Demand HSM on Demand services operating in FIPS mode. To integrate an HSMoD service with OpenStack barbican you must create a non-FIPS HSMoD service.

Configure the 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 for use by OpenStack Barbican.
3. If 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 initialized partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partition 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 ->                barbican
  Serial Number ->        1280780175865
  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 detailed steps for creating the NTLS connection, initializing the partitions, and initializing the user roles.

5. Add the user barbican to the hsmusers group.

```
# gpasswd --add barbican hsmusers
```

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.

> **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.

To use the HSM on Demand (HSMoD) service you need to provision your application partition, starting by creating an HSMoD service on DPoD as an Application Owner, downloading the HSMoD service client and initializing the service client and 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.

When the HSMoD service is available on the system and the roles are initialized, create a link between the HSMoD configuration file, `Chrystoki.conf`, and `/etc`.

```
# ln -sf  <DPoD client directory>Chrystoki.conf /etc/Chrystoki.conf
```

Constraints on HSMoD Services

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

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.

Setup OpenStack Barbican

We recommend you familiarize yourself with OpenStack barbican before beginning the integration. Refer to the OpenStack Barbican Documentation for more information about installation and pre-installation requirements.

Complete the installation of OpenStack Barbican on the target machine for integration with the SafeNet HSM.

CHAPTER 2: Integrating OpenStack Barbican with a SafeNet HSM

Integrate OpenStack barbican with the SafeNet HSM to secure application encryption keys. Complete the following:

> Configuring the PKCS11 Provider for OpenStack Barbican

Configuring the PKCS11 Provider for OpenStack Barbican

Configure OpenStack Barbican to use the SafeNet PKCS#11 provider for generating encryption keys.

To configure PKCS11 Provider for OpenStack Barbican

1. Open the OpenStack Barbican configuration file `/etc/barbican/barbican.conf` and locate the section `Crypto plugin`. Make the following changes in the configuration file:

```
# ================= Secret Store Plugin =============
[secretstore]
namespace = barbican.secretstore.plugin
enabled_secretstore_plugins = store_crypto
# ================= Crypto plugin ===================
[crypto]
enabled_crypto_plugins = p11_crypto
[p11_crypto_plugin]
library_path = '<path_to_cyptoki_library>'
login = '<partition_password>'
mkek_label = '<mkek_label>'
mkek_length = 32
hmac_label = '<hmac_label>'
slot_id = <partition_slot_id>
```

> **NOTE:** Update the `barbican.conf` file for your SafeNet Luna HSM or HSMoD service implementation.

2. Generate the Master Key Encryption Key (MKEK). The MKEK generates on the registered HSM partition or HSMoD service.

```
# barbican-manage hsm gen_mkek --library-path '<path_to_cyptoki_library>' --
passphrase '<partition_password>' --slot-id <partition_slot_id>
--label '<mkek_label>' --length 32
```

3. Generate the HMAC key using the following command. The HMAC key generates on the registered HSM partition.

```
# barbican-manage hsm gen_hmac --library-path '<path_to_cyptoki_library>' --
passphrase '<partition_password>' --slot-id <partition_slot_id> --label
'<hmac_label>' --length 32
```

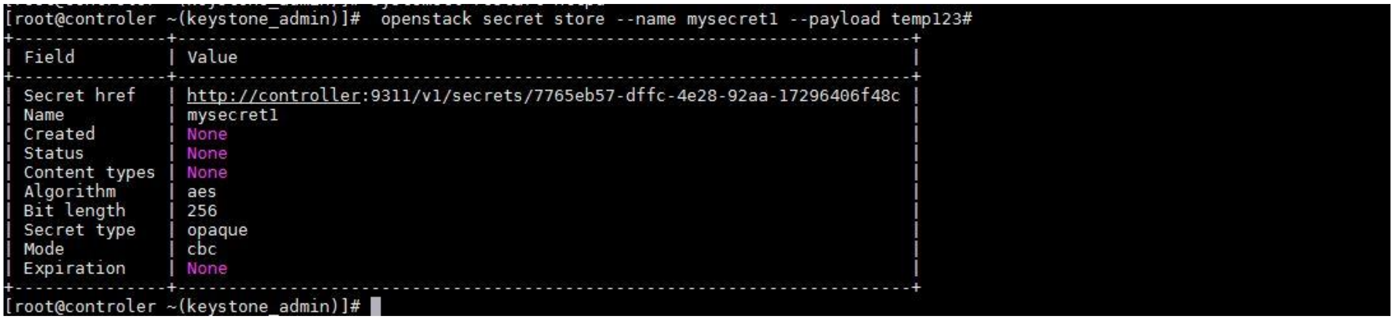
4. Restart the OpenStack Barbican API and the http service.

```
# systemctl restart openstack-barbican-api.service
```

```
# systemctl restart httpd.service
```

5. Use the OpenStack CLI to store a secret.

```
# openstack secret store --name mysecret1 --payload temp123#
```

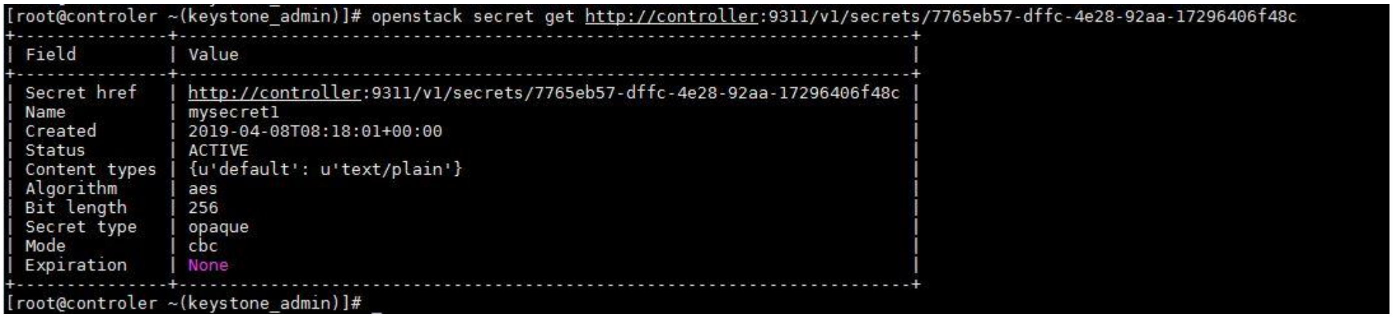


```
[root@controler ~(keystone_admin)]#  openstack secret store --name mysecret1 --payload temp123#
+---------------+-----------------------------------------------------------------------+
| Field         | Value                                                                 |
+---------------+-----------------------------------------------------------------------+
| Secret href   | http://controller:9311/v1/secrets/7765eb57-dffc-4e28-92aa-17296406f48c |
| Name          | mysecret1                                                             |
| Created       | None                                                                  |
| Status        | None                                                                  |
| Content types | None                                                                  |
| Algorithm     | aes                                                                   |
| Bit length    | 256                                                                   |
| Secret type   | opaque                                                                |
| Mode          | cbc                                                                   |
| Expiration    | None                                                                  |
+---------------+-----------------------------------------------------------------------+
[root@controler ~(keystone_admin)]#
```

> **NOTE:** If the command fails with the error `CKR_INVALID_ATTRIBUTE`, open your `pkcs11.py` file at `/usr/lib/python2.7/site-packages/barbican/plugin/crypto/pkcs11.py` and set `CKA_SENSITIVE = True`.

6. Confirm that the secret was stored by retrieving it without using the secret payload.

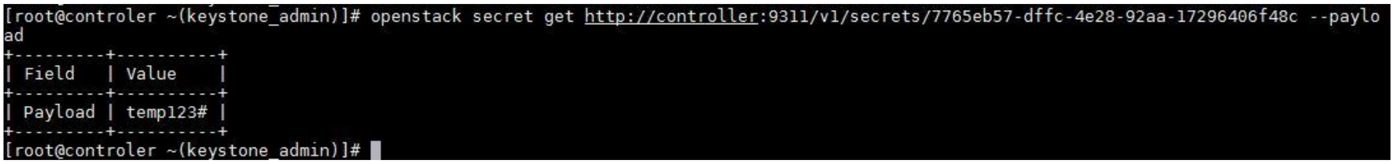
```
# openstack secret get http://controller:9311/v1/secrets/7765eb57-dffc-4e28-
92aa-17296406f48c
```



```
[root@controler ~(keystone_admin)]# openstack secret get http://controller:9311/v1/secrets/7765eb57-dffc-4e28-92aa-17296406f48c
+---------------+-----------------------------------------------------------------------+
| Field         | Value                                                                 |
+---------------+-----------------------------------------------------------------------+
| Secret href   | http://controller:9311/v1/secrets/7765eb57-dffc-4e28-92aa-17296406f48c |
| Name          | mysecret1                                                             |
| Created       | 2019-04-08T08:18:01+00:00                                             |
| Status        | ACTIVE                                                                |
| Content types | {u'default': u'text/plain'}                                           |
| Algorithm     | aes                                                                   |
| Bit length    | 256                                                                   |
| Secret type   | opaque                                                                |
| Mode          | cbc                                                                   |
| Expiration    | None                                                                  |
+---------------+-----------------------------------------------------------------------+
[root@controler ~(keystone_admin)]# _
```

7. Retrieve the secret payload.

```
# openstack secret get http://controller:9311/v1/secrets/7765eb57-dffc-4e28-
92aa-17296406f48c --payload
```



```
[root@controler ~(keystone_admin)]# openstack secret get http://controller:9311/v1/secrets/7765eb57-dffc-4e28-92aa-17296406f48c --paylo
ad
+---------+----------+
| Field   | Value    |
+---------+----------+
| Payload | temp123# |
+---------+----------+
[root@controler ~(keystone_admin)]#
```

You should see the original decrypted secret in the response.

This completes the Integration of OpenStack Barbican with a SafeNet Luna HSM or SafeNet DPoD HSMoD service.