KeyScaler and DPoD

Integration Guide

gemalto
a Thales company

Document Number: xxx-xxx-xxx, Rev. A

Release Date: July 2019

Contents

Preface

This document is intended to guide security administrators through the steps for the KeyScaler Integration with SafeNet Network HSM, and also covers the necessary information to install, configure and integrate KeyScaler with SafeNet Network HSM.

Scope

This document outlines the steps to integrate KeyScaler with SafeNet HSM. SafeNet HSM is used to secure the Master Encryption Key for KeyScaler.

Gemalto Rebranding

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

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

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

Document Conventions

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

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

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

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

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

Contact Method	Contact Information	
Address	Device Authority Level 2, FORA, Thames Tower Station Road, Reading, RG1 1LX, UK	
Phone	US	+1 650-603-0997
	International	+44 1344-535-233
Email	support@deviceauthority.com	
Technical Support Customer Portal	https://deviceauthority.zendesk.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents and access the DeviceAuthority Knowledge Base.	

1
Introduction

Overview

This document is intended to guide security administrators through the steps required for KeyScaler 6.4 Integration with SafeNet Luna HSM, and covers the necessary information to install, configure and integrate.

KeyScaler supports deployment with Hardware Security Modules (HSMs) and is used to generate and protect KeyScaler system keys and private Certificate Authority root keys. The keys protected by the HSM are used for various operations to harden the KeyScaler processes including:

- Encrypting the database
- Encrypting communication with devices
- Signing managed device certificates

KeyScaler is delivered and deployed as a set of services, to allow for flexible system configurations depending on scale requirements. One of the deployed services is the "Key Management Service" (KMS). The Key Management Service is responsible for orchestrating all cryptographic actions within the KeyScaler system, and provides a common service interface backed by interchangeable key stores, "under the hood". The KMS can be deployed and configured with two different types of key store, depending on the level of security that is required for the system root keys.

Integrating KeyScaler with the Gemalto SafeNet Luna hardware security module (HSM) is operationalizing trust and security at IoT scale, providing high-assurance device authentication, managed end-to-end encryption, and certificate provisioning for connected devices. Deploying KeyScaler with a Gemalto SafeNet Luna HSM enables organizations to secure the generation and storage of the KeyScaler master and tenant private keys within a FIPS 140-2 certified Hardware Security Module. Doing so provides the highest level of security and assurance against private key compromise and theft. Fig 1 details the overall system solution for IoT devices in a typical deployment.

KeyScaler Enterprise IoT Solution Blueprint

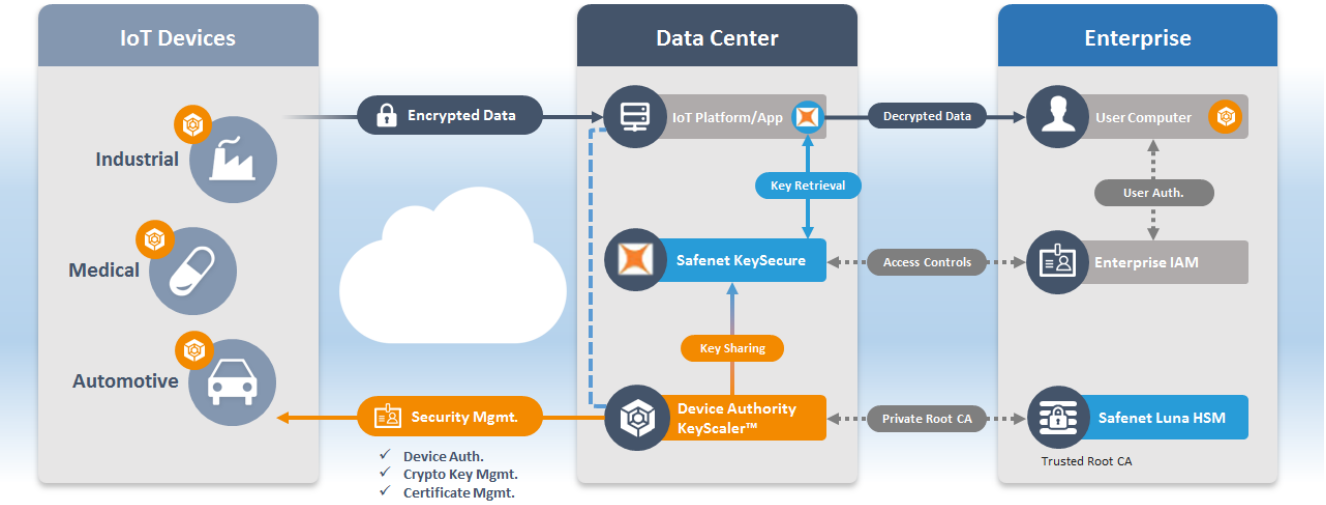

Figure 1 - KeyScaler Enterprise IoT Solution Blueprint

- KeyScaler™ delivers comprehensive IoT security automation at scale. Secure device registration and provisioning, automated password management, policy-driven crypto and credential management, along with the delivery of Public Key Infrastructure (PKI) certificates to devices without human intervention.Security Suite for Microsoft Azure IoT - Enhanced security for Microsoft customers and partners to accelerate, optimize and leverage their investments in IoT deployments with connectors for Azure DPS, Azure IoT Hub, Microsoft Active Directory, Azure Event Hub data privacy and Windows credential manager
- Registration Controls - Automated device registration and authorization policies for headless onboarding of IoT devices
- End-to-End Data Security – Granular, efficient policy-driven crypto that provides secure, end-to-end delivery and storage when using third party networks and cloud services
- Automated Certificate Management – Automated certificate provisioning and management
- Delegated Security Management (DSM) - Providing high assurance device authentication for IoT platforms, network and power efficiency, and simplified integration with KeyScaler
- Always-On Agent - A crypto agent for ThingWorx Always-On protocol provides transparent, policy-based encryption for device applications connected to ThingWorx.
- PKI Signature+ - Designed for low-power devices, where Dynamic Device Key Generation (DDKG) is not suitable. Utilizing asymmetric key signatures with automated authentication key rotation policies to deliver strong device identity
- Amazon Web Services (AWS) IoT PKI Connector - A service connector, utilizing the AWS SDK, supports certificate provisioning, revocation as well as ‘thing’ creation and certificate assignment
- Azure IoT Hub connector - A service connector that provides Shared Access Signature (SAS) tokens. KeyScaler authenticates to devices and delivers SAS tokens. Devices use SAS tokens to authenticate to Azure IoT Hub
- Automated Password Management - Automatically set and manage local account passwords on devices and rotate as per policy, with the ability to restrict access to device passwords for privileged individuals only

- Internal Private PKI - Customers can generate their own internal private root certificate authority and key, to enable provisioning of self-signed certificates to devices and the AWS IoT service
- Security Suite for PTC ThingWorx - Simplified integration between ThingWorx and KeyScaler offering data security, device authentication, management interface and device authorization
- Secure Soft Storage - To prevent theft of certificates and unauthorized usage, the agent stores the certificate and associated key pair in an encrypted state. Decryption is available only to authorized applications as defined in the policy on the KeyScaler server
- Development Tools - Client-side SDK and development libraries provide an easy integration method into new and existing applications. Server-side REST APIs make it simple to consume KeyScaler services
- Docker Support - Support for deploying KeyScaler services inside Docker Containers
- Integration with Gemalto SafeNet Networked HSMs – Providing a proven and auditable way to secure valuable cryptographic material inside a FIPS 140-2 certified protected environment. Giving the highest level of security and assurance against key compromise and theft.

3rd Party Application Details

- KeyScaler v6.4

Supported Platforms

The following platforms are tested with SafeNet Luna HSM:

KeyScaler Version: v6.4

Platforms Tested	SafeNet Luna HSM Client Software Version	SafeNet Network HSM Appliance S/W version	SafeNet Network HSM Appliance F/W version
CentOS 7.6	7.0	7.0.0-956	7.0.1
RHEL 7.6	7.0	7.0.0-956	7.0.1

Table 1 – KeyScaler and HSM compatibility Matrix

Prerequisites

Configuring SafeNet Luna Network HSM 7.x

SafeNet Luna Network HSM allows to create Per-Partition Security Officer (PPSO) partition. HSM Administrator is not Security Officer (SO) for PPSO partitions. The HSM SO/Administrator elects to create a partition as PPSO-type, which creates an empty structure that is handed to the new owner, who initializes the partition to create the Partition Security Officer (PSO) role or identity for management functions. The PSO in turn creates the partition Crypto Officer (CO) to control client cryptographic operations on the partition.

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX/Windows systems. For details on configuration please refer to section Integrating SafeNet Luna HSM with KeyScaler v6.4. Before you get started ensure the following:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Luna HSM. The general form of command is "C:\Program Files\SafeNet\LunaClient> vtl verify" for Windows and "/usr/safenet/lunaclient/bin/vtl verify" for Unix.
- Initialize the Partition as mentioned in steps below for Password/PED based respectively
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

KeyScaler Hardware Prerequisites for Installation

Before installing KeyScaler on Linux CentOS 7.6, ensure that the system chosen meets the necessary operating system, hardware, software, and communications requirements. The following information provides guidelines for picking appropriate hardware to deploy the KeyScaler software to.

Basic Provisioning Deployment

The KeyScaler system can be installed on a single node/system using the minimum hardware requirements depicted below.

Hardware Component	Minimum Requirement
Processor	Intel Xeon E5, 8 cores
RAM	32GB
Storage	1TB

Table 2 – KeyScaler Hardware Requirements

High Availability (HA) Deployment

The KeyScaler system can be installed as a High Availability system using the minimum hardware requirements depicted below.

Node 1 Hardware Component	Minimum Requirement
Processor	Intel Xeon E5, 8 cores
RAM	32GB
Storage	1TB
Node 2 Hardware Component	**Minimum Requirement**
Processor	Intel Xeon E5, 8 cores
RAM	32GB
Storage	1TB

Table 3 - KeyScaler Hardware Requirements for HA

n-Scale Deployment

The Device Authority IoT Security Platform architecture is designed for high-scalability environments and distributed services deployment. Each deployment is comprised of the following service application components:

- Device Authority Engine (DAE)
- Key Management Service
- Control Panel (CP)
- Database
- Service Access Controller

Service	Processor	RAM	Storage
DAE	Intel Xeon, 2 cores	32GB	500GB
KMS	Intel Xeon, 2 cores	4GB	256GB
CP	Intel Xeon, 2 cores	4GB	256GB
DB	Intel Xeon, 2 cores	8GB	1TB
SAC	Intel Xeon, 2 cores	4GB	256GB

Table 4 – KeyScaler n-Scale Deployment Requirements

KeyScaler Software Prerequisites for Installation

This section describes the supported platforms and software requirements when deploying KeyScaler.

Operating System

Linux x86_64 running CentOS 7.x (verified up to v7.6)

Software Support Packages

The following are installed as part of the Installation Prerequisites:

- Java Runtime Version - Oracle JRE 1.8
- Application Server - Apache Tomcat 8.5.x
- Memcached v1.4.15

- Database - MySQL v 5.5.x with the JDBC Connector/J 5.1.x
- Galera Cluster for MySQL (needed for High Availability installations)
- HAProxy (needed for High Availability installations)

Notes:

1. Device Authority only supports deploying on 64-bit derivatives of physical x86 hardware.
2. Device Authority only supports deploying the server components on Linux distributions.

2
Integrating SafeNet Luna HSM with KeyScaler v6.4

There are two options available for integrating KeyScaler:

1. Safenet Luna HSM
2. With Data Protection on Demand (DPoD)

Setup KeyScaler with your SafeNet Luna HSM

This section of the document details the process for setting up and configuration of the SafeNet Luna 7.0 HSM prior to connecting to KeyScaler v6.4.

Installation and Configuration Overview

Installation of the KeyScaler software and configuration to the HSM should be completed at the same time. The process can be summarized as the following steps:

1. Install and connect SafeNet Luna HSM in network
2. Install CentOS operating system on KeyScaler server
3. Install Security World client on KeyScaler server
4. Configure Remote File System (RFS) on KeyScaler server
5. Install and Configure KeyScaler software prerequisites
6. Install and Configure KeyScaler using the Wizard
7. Configure KeyScaler KMS and connection to SafeNet Luna 7 HSM
8. Deploy DDKG packages

Install and Configure KeyScaler Software Prerequisites

Before the KeyScaler software can be configured, you must install the software prerequisites on the KeyScaler instance. Device Authority provides an installer script to simplify this process - the script can be found in the KeyScaler software package available for download from your customer portal account.

It is recommended that you read and adhere to the following step-by-step guide, available in the Device Authority Knowledge Base, for the full details of the prerequisite installation process:

https://deviceauthority.zendesk.com/hc/en-us/articles/226370787-DAE-KMS-and-CP-Installation-Prerequisites

The install script will perform the following tasks for you:

- Synchronizing Time with NTP
- Installing Java with Cryptography Extension (JCE)
- Installing Memcached
- MySQL Installation and Database Creation
- Installing the Tomcat Webserver and necessary KeyScaler software
- Modifying your iptables rules to secure Tomcat

After running the install script you will need to:

- Install an SSL certificate
- Change the MySQL database passwords
- Start up Tomcat and verify the Wizard is running. The Wizard is used to facilitate installation of the KeyScaler software modules.

Install and Configure KeyScaler using the Wizard

Once the KeyScaler prerequisites have been installed and configured, you will be able to access the installation and configuration wizard using a web browser. This Wizard will step you through installation and setup of the main key scaler services.

Figure 2 - KeyScaler Installation Setup Wizard

The steps will cover:

1) Welcome Page (see above image)
2) Database Configuration
3) KMS Deployment
4) Memcached Configuration
5) Account Creation
6) System License
7) Apache Kafka Configuration
8) Device Authority Engine (DAE) Deployment
9) Message Queue Service Deployment
10) Control Panel Deployment

KeyScaler is delivered and deployed as a set of services, to allow for flexible system configurations depending on scale requirements. One of the deployed services as described above is the "Key Management Service" (KMS). The Key Management Service is responsible for orchestrating all cryptographic actions within the KeyScaler system, and provides a common service interface backed by interchangeable key stores, "under the hood".

This guide focusses on the KMS Deployment configuration details of the wizard, to highlight the key steps to connect KeyScaler (in the setup process) to a Gemalto SafeNet Luna HSM. For more information on how to complete the rest of the installation wizard, please see the following article in the Device Authority Knowledge Base:

https://deviceauthority.zendesk.com/hc/en-us/articles/226506108-DAE-KMS-and-CP-Installation

After completing the 2nd step of the installation wizard (Database Configuration), step 3 will prompt you to configure the KMS service, and choose the type of Key Store that you wish to use. The KMS can be deployed and configured with several different types of key store, depending on the level of security that is required for the system root keys. Options include:

1. Gemalto Safenet
2. Software-only NSSKeyStore module

For deployments that require a higher degree of security and assurance, Device Authority recommends using the Gemalto Safenet Luna 7.0 HSM.

To configure the KMS to use the Gemalto SafeNet Luna 7 HSM, simply select "Gemalto SafeNet" from the drop-down menu, under the "Key Store Options" label. Then enter the “Gemalto SafeNet Slot Number” followed by “Gemalto SafeNet Partion Name” and lastly enter the “Gemalto SafeNet KeyStore Password” . Finally, enter the host address (including the protocol) for the location of the KMS service. In a single-node deployment this will be the same address as the Device Authority Engine (DAE). The KMS host name must be resolvable by your DNS or the server's /etc/hosts file.

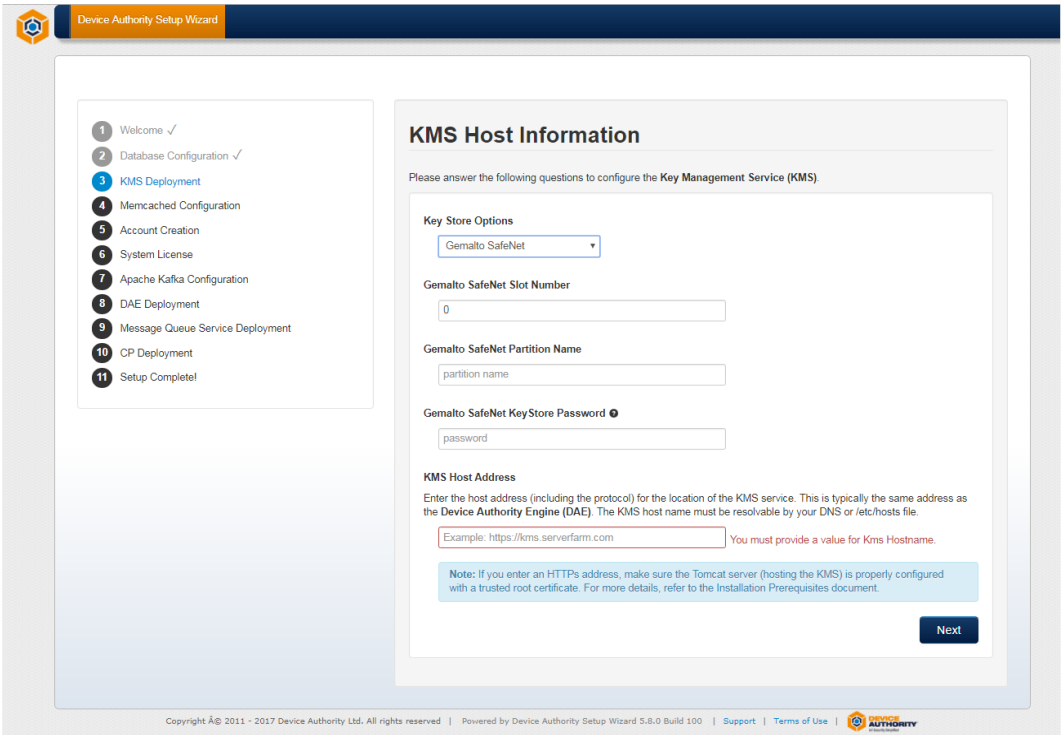

Figure 3 - Configuration page for the KMS and underlying key store

After successfully configuring the KMS, continue with the rest of the installation wizard using the guide available in the Device Authority Knowledge Base:

https://deviceauthority.zendesk.com/hc/en-us/articles/226506108-DAE-KMS-and-CP-Installation

Setup KeyScaler with Luna HSM for DPoD Service

For DPoD, the installation and configuration is very similar to the previously described section except there are a few additional configuration step for DPoD Installation prior to Step 1 Luna HSM Installation and a few configuration changes to Step 7 (Configure KeyScaler KMS) KeyScaler Installation and as described below.

DPOD Installation

Before starting the Luna HSM install, the DPoD Service needs to be set up.

1. Login to Gemalto DPOD web console:
    - *https://company.uaa.system.snakefly.dpsas.io/login*

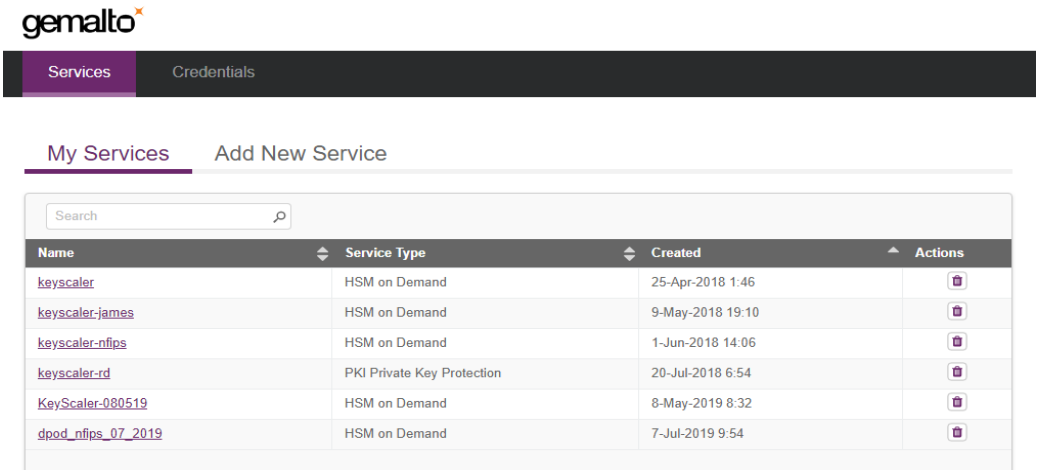

Figure 4 – Gemalto DPoD web console

2. Create a new Partition on DPOD Service console:

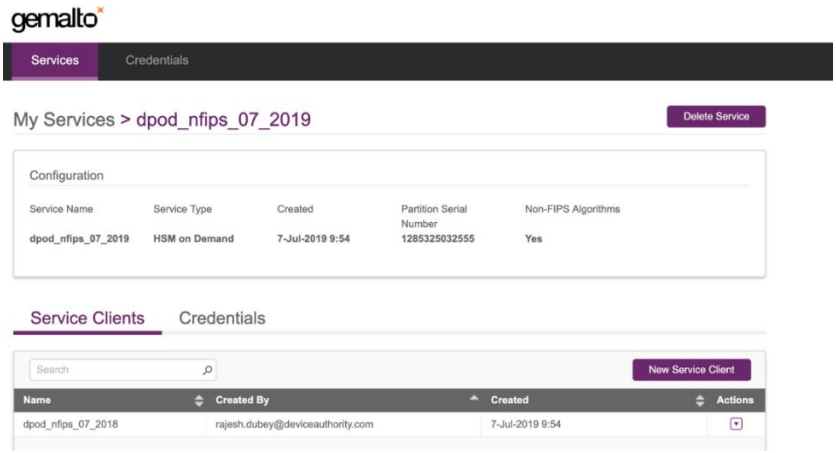

Figure 5 – DPoD Service Console – Create New Partition

3. Download the client *dpod_nfips_07_2019.zip* from the DPoD service console and upload it to the CentOS 7.6 server where KeyScaler system will be deployed
4. Move the file *dpod_nfips_07_2019.zip* to */opt/dpod* folder. Create folders if they don't already exist.

```
[root@ks dpod]# mv dpod_nfips_07_2019.zip /opt/dpod/
```

Item 1 – Move the file to */opt/dpod* folder

5. Unzip the file *dpod_nfips_07_2019.zip*

```
[root@ks dpod]# gunzip dpod_nfips_07_2019.zip
```

Item 2 – gunzip the dpod file

6. Also, expand the file using tar command

```
[root@ks dpod]# tar -xvf cvclient-min.tar
```

Item 3 - tar file Client configuration file

7. Edit the file (e.g. using nano or vi) */etc/profile*. Add following at the end to */etc/profile* and save the changes

```
[root@ks dpod]# nano /etc/profile

# DPOD Client Setup
cd /opt/dpod
source setenv
```

Item 4 – Configuration file: /etc/profile

8. Run the following while in /opt/dpod directory to list the current HSM that is available:

```
[root@ks dpod]#  ./bin/64/lunacm
LunaCM v1.1.0-1044. Copyright (c) 2006-2017 SafeNet.

Available HSMs:

Slot Id ->              3
Label ->
Serial Number ->        1285325032555
Model ->                Cryptovisor7
Firmware Version ->     7.1.3
CV Firmware Version ->  1.1.0
Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->     User Token Slot
Current Slot Id: 3
```

Item 5 – Luna HSM configuration

List the current Role List

```
lunacm:> role list
        Roles             (short)
        ========================
        Partition SO        po
        Crypto Officer      co
        Crypto User         cu
Command Result : No Error
```

Item 6 – Current Role List

Note: These instructions assume a password-authenticated SafeNet Luna Network HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer

9. Initialize the Partition SO role

Set the active slot to the created, uninitialized, application partition.

- Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 3
Current Slot Id: 3 (Luna User Slot 7.0.0 (Password) Signing With Cloning Mode)
Command Result : No Error
```

Item 7 – Activate Slot (3) to be created

Initialize the application partition, to create the partition's Security Officer (SO).

- **Type partition init -label <part_label>**

```
lunacm:>par init -label HSMoDnFIPS

        Enter password for Partition SO: ******** (password)
        Re-enter password for Partition SO: ********
        You are about to initialize the partition.
        All contents of the partition will be destroyed.
        Are you sure you wish to continue?
        Type ‘proceed’ to continue, or ‘quit’ to quit now ->proceed
        Neither option -domain nor -defaultdomain was specified.  One is required.
        Enter the domain name: ********** (entered testme.com)
        Re-enter the domain name: **********

Command Result : No Error
```

Item 8 – Create New Partition

10. Now we login using the new ‘Partition’ to we can Initialize the’ Crypto Officer’ role

```
[root@ks dpod]#  ./bin/64/lunacm
LunaCM v1.1.0-1044. Copyright (c) 2006-2017 SafeNet.

        Available HSMs:

        Slot Id ->              3
        Label ->                HSMoDnFIPS
        Serial Number ->        1285325032555
```

```
Model ->                Cryptovisor7
Firmware Version ->     7.1.3
CV Firmware Version ->  1.1.0
Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->     User Token Slot
Current Slot Id: 3
```

Item 9 – Show the new Partition

The SO of the application partition can now assign the first operational role ‘Crypto Office’ within the new partition:

- **Type role login -name Partition SO**

```
lunacm:>role login -name Partition SO
        enter password: ********
Command Result : No Error
```

Item 10 – Login as SO

- **Type role init -name Crypto Officer**

```
lunacm:>role init -name Crypto Officer
        enter new password: ********
        re-enter new password: ********
Command Result : No Error
```

Item 11 – Add new ‘Crypto Office’ role to new partition

The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.

- Type **role logout**.

```
lunacm:>role logout
Command Result : No Error
```

Item 12 – Logout

Now, the Crypto Officer, or an application using the CO's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto Officer logs in with **role login -name Crypto Officer**. However, the Crypto Officer can create, modify and delete crypto objects within the partition, in addition to merely using existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them.

NOTE: The black Crypto Officer PED key/Crypto Officer Password is valid for the initial login only. You must change the initial credential on the key using the command role changepw during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_EXPIRED error while performing role-dependent actions.

11. Now we will login as “Crypto Officer” to create “Crypto User” role

```
lunacm:>role login -name Crypto Officer
        enter password: ********
Command Result : No Error

lunacm:>role changepw -name Crypto Officer
        enter existing password: ********
        enter new password: ********
        re-enter new password: ********
Command Result : No Error

lunacm:>role init -name Crypto User
        enter new password: ********
        re-enter new password: ********
Command Result : No Error
```

Item 13 – Create ‘Crypto User’ role

12. Check the Partition Details

```
[root@ks dpod]#  ./bin/64/lunacm
LunaCM v1.1.0-1044. Copyright (c) 2006-2017 SafeNet.

        Available HSMs:

        Slot Id ->              3
        Label ->                HSMoDnFIPS
        Serial Number ->        1285325032555
        Model ->                Cryptovisor7
        Firmware Version ->     7.1.3
        CV Firmware Version ->  1.1.0
        Configuration ->        Luna User Partition With SO (PW) Signing With Cloning Mode
        Slot Description ->     User Token Slot
        Current Slot Id: 3
```

Item 14 – Change Partition details

Show the Partition Information:

```
lunacm:> role login -name Partition SO
        enter password: ********
Command Result : No Error

lunacm:> par showinfo

        Partition Label -> HSMoDnFIPS
        Partition Manufacturer -> SafeNet
        Partition Model -> Cryptovisor7
        Partition Serial Number -> 1285325032555
        Partition Status -> L3 Device, Error querying state
        HSM Part Number -> Not Available
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_TOKEN_INITIALIZED
        RPV Initialized -> Not Available
        Slot Id -> 3
```

```
        Session State -> CKS_RW_SO_FUNCTIONS
        Role Status ->   Partition SO logged in
        Token Flags ->
                TOKEN_KCV_CREATED
        Partition OUID: 26f11f00160000016b6c0800

        Partition Storage:
                Total Storage Space:  159744
                Used Storage Space:   0
                Free Storage Space:   159744
                Object Count:         0
                Overhead:             9664

        *** The partition is NOT in FIPS 140-2 approved operation mode. ***

Command Result : No Error
```

Item 15 – Show Partition Information

Note: The above steps are valid for both FIPS and non-FIPS Partition.

13. Continue KeyScaler deployment. Refer to KeyScaler Installer Document. Choose Gemalto SafeNet during KMS deployment during wizard installation of KeyScaler, as shown below:

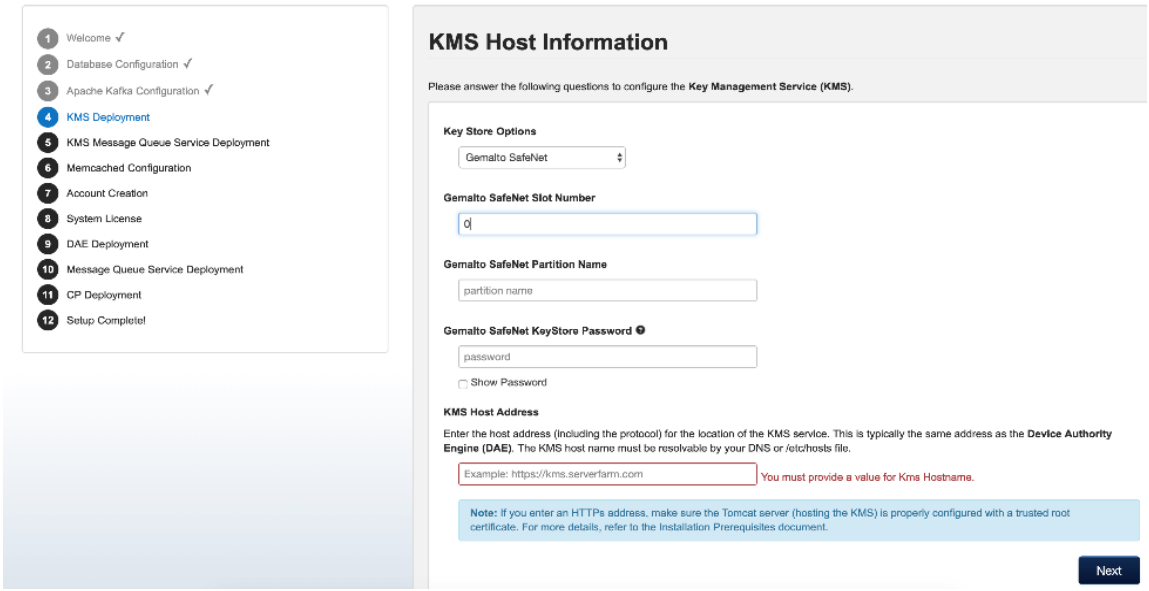

Figure 6 – KeyScaler Installation Wizard - KMS Configuration

On the Wizard pages enter the relevant info for DPOD configuration:

In this case, (refer to Step 11 for details obtained from Item **15** – Show Partition Information, 'par showinfo'
For example:

- Gemalto SafeNet Slot Number: **3**
- Gemalto SafeNet Partition Name: **HSMoDnFIPS**
- Gemalto SafeNet KeyStore Password :**********
    - (this is same password as Crypto Officer, which was configured in Section 9)

Complete, the rest of KeyScaler Installation, wizard using the guide available in the Device Authority Knowledge Base.

Troubleshooting

For assistance troubleshooting your KeyScaler installation, please contact support via the Device Authority support portal available at:

https://deviceauthority.zendesk.com/hc/en-us/requests/new