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**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>Document Conventions</td>
<td>5</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>5</td>
</tr>
<tr>
<td>Customer Support Portal</td>
<td>6</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>6</td>
</tr>
<tr>
<td>Email Support</td>
<td>7</td>
</tr>
</tbody>
</table>

**CHAPTER 1: Getting Started**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About SafeNet Luna HSMs</td>
<td>8</td>
</tr>
<tr>
<td>About AWS KMS Integration with SafeNet Luna HSM</td>
<td>8</td>
</tr>
<tr>
<td>Supported Wrapping Algorithms</td>
<td>8</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>8</td>
</tr>
<tr>
<td>Configure the SafeNet Luna HSM</td>
<td>8</td>
</tr>
<tr>
<td>Access AWS Key Management Services</td>
<td>9</td>
</tr>
</tbody>
</table>

**CHAPTER 2: Integrating AWS Key Management Services with SafeNet Luna HSM**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Wrapping Key and Import Token</td>
<td>10</td>
</tr>
<tr>
<td>Importing Wrapping Key to SafeNet Luna HSM</td>
<td>15</td>
</tr>
<tr>
<td>Generating Encrypted Key Material</td>
<td>16</td>
</tr>
<tr>
<td>Uploading Encrypted Key Material to AWS KMS</td>
<td>20</td>
</tr>
</tbody>
</table>
PREFACE

This guide outlines the steps to integrate an AWS Key Management Services (KMS) with SafeNet Luna HSM and provides the necessary information to install, configure, and integrate AWS Key Management Services with SafeNet Luna HSM. This guide contains the following chapters:

> **Getting Started** describes the third-party applications, supported platforms, prerequisites, and guide to prepare the setup for AWS Key Management Services.

> **Integrating AWS Key Management Services with SafeNet Luna HSM** explains the steps involved in integrating AWS Key Management Services with SafeNet Luna HSM.

Audience

This document is intended to guide security administrators through the steps for integrating AWS Key Management Services with SafeNet Luna HSM.

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

Document Conventions

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

**Notes**

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

**NOTE:** Take note. Notes contain important or helpful information.

**Cautions**

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

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

**Warnings**

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

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

<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 dir /p.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Button names (Click Save As.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Check box and radio button names (Select the Print Duplex check box.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Window titles (On the Protect Document window, click Yes.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Field names (User Name: Enter the name of the user.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Menu names (On the File menu, click Save.) (Click Menu &gt; Go To &gt; Folders.)</td>
</tr>
<tr>
<td></td>
<td>&gt; User input (In the Date box, type April 1.)</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>The italic attribute is used for emphasis or to indicate a related document. (See the Installation Guide for more information.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Double quote marks</th>
<th>Double quote marks enclose references to other sections within the document.</th>
</tr>
</thead>
<tbody>
<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>[ optional ]</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></td>
</tr>
<tr>
<td>[ a</td>
<td>b</td>
</tr>
<tr>
<td>[a&gt;</td>
<td>&lt;b&gt;</td>
</tr>
<tr>
<td>{ a</td>
<td>b</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 Thales Customer Support.

Thales 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 Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at [https://supportportal.thalesgroup.com](https://supportportal.thalesgroup.com) is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems.
and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

### Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales 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.DIS@thalesgroup.com](mailto:technical.support.DIS@thalesgroup.com).
CHAPTER 1: Getting Started

This chapter covers the following topics:

- About SafeNet Luna HSMs
- About AWS KMS Integration with SafeNet Luna HSM
- Supported Wrapping Algorithms
- Prerequisites

About SafeNet Luna HSMs

SafeNet Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs.

About AWS KMS Integration with SafeNet Luna HSM

The AWS BYOK solution enables customers to generate their own AES-256 bit key on SafeNet Luna HSMs and export this key to AWS KMS. As part of the export process, a public key (wrapping key) will be used to wrap off the AES-256 bit key. To export the AES-256 bit key from the HSM, the key must be generated with the exportable attribute set to true. In case an existing AES-256 bit key is to be exported, that key must have either the exportable attribute set to true or the modifiable attribute set to true.

Supported Wrapping Algorithms

- RSAES_PKCS1_V1_5
- RSAES_OAEP_SHA_1
- RSAES_OAEP_SHA_256

Prerequisites

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

Configure the SafeNet Luna HSM

If you are using a SafeNet Luna HSM, complete the following:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to the SafeNet Luna HSM Product Documentation for more information.
2. Create a partition on the HSM that will be later used by AWS KMS.
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 registered partition.

4. Ensure that each partition is successfully registered and configured. The command to see the registered partitions is:

   ```bash
   # /usr/safenet/lunaclient/bin/lunacm
   lunacm (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
   ```

   Available HSMs:

<table>
<thead>
<tr>
<th>Slot Id</th>
<th>Label</th>
<th>Serial Number</th>
<th>Model</th>
<th>Firmware Version</th>
<th>Configuration</th>
<th>Slot Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kms</td>
<td>1280780175949</td>
<td>LunaSA 7.3.0</td>
<td>7.3.0</td>
<td>Luna User Partition With SO (PW) Key Export With Cloning Mode</td>
<td>Net Token Slot</td>
</tr>
</tbody>
</table>

   **NOTE:** Follow the SafeNet Luna Network HSM Product Documentation for detailed steps for creating the NTLS connection, initializing the partitions, and initializing the Security Officer, Crypto Officer, and Crypto User roles.

Access AWS Key Management Services

You need an AWS account to access AWS Key Management Services.
Integrating AWS Key Management Services with SafeNet Luna HSMs involves the following steps:

- Creating Wrapping Key and Import Token
- Importing Wrapping Key to SafeNet Luna HSM
- Generating Encrypted Key Material
- Uploading Encrypted Key Material to AWS KMS

Creating Wrapping Key and Import Token

The process of creating the wrapping key and import token is as follows:

2. Click IAM under Security, Identity & Compliance.
3. Click Users and then Add User. Enter User name and select Programmatic access in Access type. Click Next: Permissions button to continue.
4. Click Attach existing policies directly, select AdministratorAccess in Policy type list and then click Next: Tags to continue. You can add Tags but it is optional.

5. Click Next:Review and then click Create user. It will create an IAM user that will be used later for assigning the permissions on the Master Key.

6. Click Key Management Services and then click Create key to continue.

7. Select the Key type as Symmetric.

8. Click Advanced Options and select External for Key Material Origin. Select the I understand the security, availability and durability implications of using an imported key check box and then click Next.
CHAPTER 2: Integrating AWS Key Management Services with SafeNet Luna HSM

9. Enter the name of the key in **Alias** text box and provide **Description**. On the **Add Tags**, enter the **Tag key** and **Tag Value**. Click **Next**.

10. On the **Define Key Administrative Permissions** page, select **Name** of IAM user whom you want to provide the key access and select **Allow key administrators to delete this key**. After that, click **Next**.
11. On the Define Key Usage Permissions page, select IAM user created by you and click Next.

12. On the Preview Key Policy page, the key policy is displayed. Click Finish.
13. On the **Download wrapping key and import token** page, select the wrapping algorithm you want to use from the **Select wrapping algorithm** drop down, and then click **Download wrapping key and import token**. A zip file named **ImportParameters.zip** will be downloaded.

14. Extract the **ImportParameters.zip** file. It contains the wrapping key and import token. Now import the wrapping key (RSA Public Key) on the HSM.
Importing Wrapping Key to SafeNet Luna HSM

For importing the wrapping key to SafeNet Luna HSM, you need to undertake the following steps:

1. Convert wrapping key to pem format using openssl.
   
   ```bash
   # openssl rsa -in wrappingKey_f046d05f-6944-411b-958a-928e0215a1a2_0426062751 -inform DER -out pub_key.pem -outform PEM -pubin -pubout
   writing RSA key
   ```

   It will save the Public key in the `pub_key.pem` file.

2. Import the `pub_key.pem` on the HSM using the CMU utility provided with Luna Client.
   
   ```bash
   # ./cmu import -inputfile=pub_key.pem -pubkey=pub_key.pem -label "AWS Public Key"
   Please enter password for token in slot 0: ********
   ```

   Provide the HSM partition password when prompted.

3. Run the `cmu list` command to ensure the key is imported successfully.
   
   ```bash
   # ./cmu list
   Please enter password for token in slot 0: ********
   handle=228      label=AWS Public Key
   ```

   Provide the HSM partition password when prompted and note down the handle of the public key.

4. Ensure the Public Key attributes (Encrypt, Verify, Wrap) are set to true using the `cmu` utility below:
   
   ```bash
   # ./cmu getattribute -handle=228
   Please enter password for token in slot 0: ********
   class=publicKey
token=true
private=true
label=AWS Public Key
keytype=RSA
subject=
id=
   encrypt=false
   wrap=false
   verify=true
derive=false
   startdate=
   enddate=
   modulus=b699afb4d7afa2ce540b0cf0d78e78e39da61c872b5cf22f1b65b3de9e5ce75ebb89533ea91b5f07a9c50ba8d1bd69de49285555c3fa1f096a0f9f3c41719e1a059ec4d109c262e98e61059e4be6ec3776c10fcd7926c051c35fa6896bf939dc76dac32c99c93dca90a1c0287a6af6d36572
   ```
Generating Encrypted Key Material

Following are the steps to generate the encrypted key material:

1. Create an AES256 key on the HSM partition that will be used as CMK in AWS KMS. To generate the key, run the ckdemo utility provided with Luna Client.

   ```bash
   # ckdemo
   (1) Open Session
   Enter your choice: 1
   Status: Doing great, no errors (CKR_OK)
   (3) Login
   Enter your choice : 3
   Partition SO      [0]
   Crypto Officer    [1]
   Crypto User       [2]: 1
   Enter PIN            : ********
   Status: Doing great, no errors (CKR_OK)
   (45) Simple Generate Key
   Enter your choice: 45
   Select type of key to generate
   ```
[31] EC Montgomery

> 16
Enter Key Length in bytes (16, 24, 32): 32
Enter Is Token Attribute [0-1]: 1
Enter Is Sensitive Attribute [0-1]: 1
Enter Is Private Attribute [0-1]: 1
Enter Is Modifiable Attribute [0-1]: 1
Enter Encrypt Attribute [0-1]: 1
Enter Decrypt Attribute [0-1]: 1
Enter Sign Attribute [0-1]: 1
Enter Verify Attribute [0-1]: 1
Enter Wrap Attribute [0-1]: 1
Enter Unwrap Attribute [0-1]: 1
Enter Derive Attribute [0-1]: 1
Enter Extractable Attribute [0-1]: 1
Generated AES Key: 231 (0x000000e7)
Status: Doing great, no errors (CKR_OK)

Where 231 is the handle of generated AES Key.

2. Change OAEP hash algorithm to selectable in CKDEMO. Skip this step if you are using wrapping key algorithm as RSAES_PKCS1_V1_5.

Status: Doing great, no errors (CKR_OK)

(98) Options

Enter your choice : 98

Options:
1 - Open Session Type : Always R/W and Serial
2 - Display Help : Always
3 - PIN path : user supplies ASCII password
4 - Echo input : Disabled
5 - Sleep for n seconds after writing special instructions to stderr
6 - KCV Default : user supplies KCV Domain
CHAPTER 2: Integrating AWS Key Management Services with SafeNet Luna HSM

7 - MofN path : user supplies MofN path
8 - Show Response Code : SHOW_RESPONSE_BEFORE_AND_AFTER_MENU
9 - Input data for sign/derive : input from keyboard
10 - Object Usage Counters : disabled
11 - GCM IV Source : external
12 - ECIES Parameters : use default (XOR with HMAC_SHA1)
13 - X9.31 Signatures : allow X9.31 generated keys only
14 - Multipart enc/dec/sig/ver : use single part operations
15 - Use Old Enc/Dec Menu : use old menu
16 - Role Support : enhanced roles
17 - OAEP Hash Params : use default (SHA1 Digest and MGF1)
18 - Array Template Attributes : use array template attributes
19 - Specify Number of Objects Handles to Find per Update call? : No
20 - Specify Number of Objects to Create/Keys to generate? : No
21 - Prompt for CKA_CHECK_VALUE during key unwrap/derive? : No
0 - Finished

Enter option to change: 17

Options:
1 - Open Session Type : Always R/W and Serial
2 - Display Help : Always
3 - PIN path : user supplies ASCII password
4 - Echo input : Disabled
5 - Sleep for n seconds after writing special instructions to stderr
6 - KCV Default : user supplies KCV Domain
7 - MofN path : user supplies MofN path
8 - Show Response Code : SHOW_RESPONSE_BEFORE_AND_AFTER_MENU
9 - Input data for sign/derive : input from keyboard
10 - Object Usage Counters : disabled
11 - GCM IV Source : external
12 - ECIES Parameters : use default (XOR with HMAC_SHA1)
13 - X9.31 Signatures : allow X9.31 generated keys only
14 - Multipart enc/dec/sig/ver : use single part operations
15 - Use Old Enc/Dec Menu : use old menu
16 - Role Support : enhanced roles
17 - OAEP Hash Params : selectable
18 - Array Template Attributes : use array template attributes
19 - Specify Number of Objects Handles to Find per Update call? : No
20 - Specify Number of Objects to Create/Keys to generate? : No
21 - Prompt for CKA_CHECK_VALUE during key unwrap/derive? : No
0 - Finished
Enter option to change: 0

3. Wrap your key using the public key downloaded from AWS KMS console. To wrap the key, use the same CKDEMO session and provide the choices to wrap the AES key.

(60) Wrap key
Enter your choice : 60
Select mechanism for wrapping: 26

NOTE: Select Option 9 if your wrapping key algorithm is RSAES_PKCS1_V1_5.

Mechanism to use:

NOTE: Option 3 is for Wrapping key Algorithm RSAES_OAEP_SHA_256. Select Option 1 if your wrapping key algorithm is RSAES_OAEP_SHA_1.

Enter filename of OAEP Source Data [0 for none]:
Enter handle of wrapping key (0 to list available objects): 228
Enter handle of key to wrap (0 to list available objects): 231

Wrapped key was saved in file wrapped.key
Status: Doing great, no errors (CKR_OK)
Where 228 and 231 is the handle of Public Key and AES256 key respectively.

NOTE: wrapped.key is the encrypted key material that contains the wrapped AES256 key.

4. Exit from ckdemo session now by providing the choice as 0.
Enter your choice: 0
Uploading Encrypted Key Material to AWS KMS

After generating the encrypted key material, you need to complete the following steps to upload it to AWS KMS:

1. Open the AWS KMS console where you left after downloading the wrapping key and import token. Select the **I am ready to upload my exported key material** check box and click **Next**.

2. From the **Specify key material details** section:
   - i. Click **Choose file** for **Encrypted key material** and select the wrapped AES key file.
   - ii. Click **Choose file** for **Import token** and then select the importToken file.

3. From the **Choose an expiration option** section, check the **Key material does not expire** option and then click **Finish**.
4. A message for successfully imported key will appear on the screen and the key will be listed under the Encryption keys panel with status as Enabled.

This completes the integration of AWS Key Management Services with SafeNet Luna HSM.