THALES

Thales Luna PCIe HSM 7

COMPLIANCE GUIDE

Document Information

Last Updated	2024-04-15 13:35:06 GMT-04:00

Disclaimer
All information herein is either public information or is the property of and owned solely by Thales Group 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 Thales Group's information.

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales Group 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, Thales Group reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales Group 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 Thales Group 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.

Thales Group 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 Thales Group be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales Group 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.

Regulatory Compliance

This product complies with the following regulatory regulations. To ensure compliancy, ensure that you install the products as specified in the installation instructions and use only Thales-supplied or approved accessories.

USA, FCC

This equipment has been tested and found to comply with the limits for a “Class B” digital device, pursuant to part 15 of the FCC rules.

Canada

This class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Europe

This product is in conformity with the protection requirements of EC Council Directive 2014/30/EU. This product satisfies the CLASS B limits of EN55032.

CONTENTS

PREFACE: About the Compliance Guide

This guide provides information about Luna HSM's compliance with various international standards, and how you can ensure that the HSM is configured to comply with these standards. This document contains the following chapters:

> "FIPS Compliance" on page 1

> "Common Criteria/eIDAS Compliance" on page 11

The preface includes the following information about this document:

> "Customer Release Notes" below

> "Audience" below

> "Document Conventions" below

> "Support Contacts" on page 8

For information regarding the document status and revision history, see "Document Information" on page 2.

Customer Release Notes

The Customer Release Notes (CRN) provide important information about specific releases. Read the CRN to fully understand the capabilities, limitations, and known issues for each release. You can view the latest version of the CRN at www.thalesdocs.com.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes Luna HSM users and security officers, key manager administrators, and network administrators.

All products manufactured and distributed by Thales 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.

It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This document uses standard conventions for describing the user interface and for alerting you to important information.

Notes

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

> **CAUTION!** Exercise caution. Contains 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. They 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

Format	Convention
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.) > Dialog box titles (On the **Protect Document** dialog box, 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**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<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>]	Represent 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.

Format	Convention
{**a**|**b**|**c**} {<a>|<b>|<c>}	Represent 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.
[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent 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.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. 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 is governed by the support plan negotiated between Thales and your organization. Please consult this plan for details regarding your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems and create and manage support cases. It offers 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.

> **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

The support portal also lists telephone numbers for voice contact (Contact Us).

CHAPTER 3: FIPS Compliance

Luna HSMs are compliant with the Federal Information Processing Standard (FIPS), defined by the National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce. The full capabilities of Luna HSMs, however, extend far beyond the limitations prescribed by FIPS. If your organization requires FIPS compliance, you must configure the HSM to ensure compliance by restricting these extended capabilities. This section provides guidance on setting up and using the Luna HSM to comply with FIPS, and ensuring that compliance is maintained across firmware updates. Luna Network HSM 7 and Luna PCIe HSM 7 are FIPS 140-3 Level 3 certified; Luna USB HSM 7 and Luna Backup HSM 7 are currently FIPS 140-2 certified, with FIPS 140-3 certification pending approval by NIST.

Refer to the following sections for guidance on FIPS compliance:

Install Only FIPS-Validated Firmware

The Luna HSM firmware introduces new functionality with each new version, and to be compliant with FIPS, a new firmware version must be inspected and validated by NIST. Since this validation can take a long time, Thales does not submit every firmware version it releases to NIST as a FIPS candidate. In order to be compliant with the FIPS standard, you must have a FIPS-validated firmware version installed. If your organization requires FIPS validation, *update the HSM firmware only to versions listed below*.

> **NOTE** Luna HSM Client software does not affect FIPS compliance; only the HSM firmware version. Thales recommends keeping your clients updated to the latest version whenever possible, to take advantage of the latest functionality and bug fixes.

While older firmware versions on the list below are still considered validated, each new version contains changes to the HSM functions that ensure continued compliance with the revised standard. Certain mechanisms or specific operations that have fallen below the security standard set by NIST since the last certified version are restricted. Likewise, newer mechanisms that have been validated by NIST may be allowed in FIPS mode, where they were restricted in older versions. Thales recommends that you keep your Luna HSMs requiring FIPS compliance updated to the latest FIPS-validated version, as specified in the list below.

FIPS 140-3 Level 3 Certified Luna HSM Firmware Versions

The following Luna HSM firmware versions are FIPS 140-3 Level 3 certified per certificate #4684:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/4684

> Luna HSM Firmware 7.8.4 (recommended)

FIPS 140-2 Level 3 Certified Luna HSM Firmware Versions

The following Luna HSM firmware versions are FIPS 140-2 Level 3 certified per certificate #4090:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/4090

> Luna HSM Firmware 7.7.1-20 Patch
> Luna HSM Firmware 7.7.0

The following Luna HSM firmware versions are FIPS 140-2 Level 3 certified per certificate #3205:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3205

> Luna HSM Firmware 7.3.3
> Luna HSM Firmware 7.0.3
> Luna HSM Firmware 7.0.2
> Luna HSM Firmware 7.0.1

FIPS 140-2 Level 3 Certified Luna Backup HSM 7 Firmware Versions

The following Luna Backup HSM 7 firmware versions are FIPS 140-2 Level 3 certified per certificate #4195:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4195

> Luna Backup HSM 7 Firmware 7.7.1 (recommended)

Configuring the HSM to Operate in FIPS Mode

Luna HSMs have many capabilities that are not certified by NIST. To be FIPS-compliant, the HSM must be set to **FIPS mode**, where any mechanisms or cryptographic operations that are not FIPS-certified are blocked from use. FIPS mode is set using HSM or partition policies as described below.

Setting FIPS Mode on the HSM

You can set the HSM to FIPS mode using **HSM policy 12:** Allow non-FIPS algorithms. When this policy is set to **0**, algorithms that are not FIPS-validated are blocked from use on every partition on the HSM, and the HSM is operating in FIPS mode. There are two methods of setting this policy:

> The HSM SO can use a policy template to set the policy at initialization (see Setting HSM Policies Using a Template). This method is recommended for auditing purposes -- it ensures that the HSM is in FIPS mode for its entire use cycle.
> The HSM SO can set the policy manually after initializing the HSM (see Setting HSM Policies Manually).

> **NOTE HSM policy 12:** Allow non-FIPS algorithms is destructive; changing it results in the entire HSM being zeroized and all partitions destroyed. This is to prevent keys that were created and used in a non-FIPS approved environment from existing in a FIPS-approved environment, and vice-versa.

To check the current status of FIPS mode on the HSM, log in to LunaSH and use lunash:> hsm show. In FIPS mode, a variation of the following text is displayed:

```
FIPS Operation:
====================
The HSM is in FIPS approved operation mode.
```

Setting FIPS Mode on Individual Application Partitions

Using Luna HSM Firmware 7.7.1 or newer (Luna HSM Firmware 7.7.1-20 Patch recommended), you can now set FIPS mode on individual application partitions, independently of other partitions on the same HSM.

Prerequisite
HSM policy 12: Allow non-FIPS algorithms must be set to **1** on the HSM.

To set FIPS mode on an application partition

You can set the partition to FIPS mode using **partition policy 43:** Allow non-FIPS algorithms. When this policy is set to **0**, algorithms that are not FIPS-validated are blocked from use, and the partition is operating in FIPS mode. There are two methods of setting this policy:

- The Partition SO can use a policy template to set the policy to **0** at initialization (see Setting Partition Policies Using a Template). This method is recommended for auditing purposes -- it ensures that the partition is in FIPS mode for its entire use cycle.
- The Partition SO can set the policy to **0** manually after initializing the partition (see Setting Partition Policies Manually).

> **NOTE** **Partition policy 43:** Allow non-FIPS algorithms is destructive when changing from **0** to **1**; this change results in the partition being zeroized. This is to prevent keys that were created and used in a FIPS-approved environment from existing in a non-FIPS-approved environment.

Setting FIPS Mode on Luna Backup HSM 7

Luna Backup HSM Firmware 7.7.1 and newer uses the same updated cloning protocol as Luna HSM Firmware 7.7.0 and newer. For the Luna Backup HSM 7 to be FIPS-compliant, it must restrict restore operations to application partitions that use the new protocol. This restriction is applied by setting **HSM policy 55: Enable Restricted Restore** to **1** on the backup HSM. The Luna Backup HSM 7 must be initialized and connected to a Luna HSM Client computer to set this policy.

When this policy is enabled on the Luna Backup HSM 7, objects that have been backed up from partitions using firmware older than Luna HSM Firmware 7.7.0 can be restored to Luna HSM Firmware 7.7.0 or newer (V0 or V1) partitions only.

> **CAUTION!** FIPS compliance requires that objects are never cloned or restored to an HSM using less secure firmware, and this includes restoring from Luna Backup HSM 7 firmware.
>
> If you have backups already stored on the Luna Backup HSM 7 that were taken from pre-7.7.0 partitions, turning this policy ON will prevent you from restoring them to the same source partition. You must update the HSM containing the source partition to Luna HSM Firmware 7.7.0 or newer before restoring from backup.

> **NOTE** **HSM policy 12: Allow non-FIPS algorithms**, which is used to set FIPS-compliant mode on other Luna HSMs, does not apply to the Luna Backup HSM 7. Attempts to change this policy will fail with the error `CKR_CANCEL`.

To configure the Luna Backup HSM 7 for FIPS compliance

1. On the Luna HSM Client computer, run LunaCM.
2. Set the active slot to the Luna Backup HSM 7.

   lunacm:> **slot set -slot** <slot_id>
3. Log in as Backup HSM SO.

   lunacm:> **role login -name so**
4. Set **HSM policy 55: Enable Restricted Restore** to **1**.

   lunacm:> **hsm changehsmpolicy -policy 55 -value 1**
5. [Optional] Check that the Luna Backup HSM 7 is now in FIPS approved operation mode.

   lunacm:> **hsm showinfo**

   ```
   *** The HSM is in FIPS 140-2 approved operation mode. ***
   ```

Other FIPS Considerations

Certain Luna features can affect FIPS compliance, or the behavior of the HSM in FIPS mode. Those features and their effects on FIPS are described below.

Functionality Modules and FIPS Mode

FMs change the abilities of the HSM firmware, adding new cryptographic algorithms or other functions. Since the new functionality is not certified by NIST, be sure that your FM does not break FIPS compliance. To be certain that your organization is meeting FIPS requirements, ensure that you are using a FIPS-certified version of the Luna HSM firmware, and that your Luna PCIe HSM 7 has the following HSM policy settings:

- **HSM policy 12: Allow non-FIPS algorithms**: **0**
- **HSM policy 50: Allow Functionality Modules**: **0**

> **NOTE** Using Luna HSM Firmware 7.4.2 and older, this restriction is enforced; it is not possible to set **HSM policy 50: Allow Functionality Modules** to **1** while **HSM policy 12: Allow non-FIPS algorithms** is **0**. Using newer firmware versions, it is possible to enable FMs in FIPS mode, but your FM functionality may not be FIPS-compliant; refer to NIST standards to ensure compliance.

If FIPS compliance is not required, then enabling FMs does not present an issue for you. Enabling Functionality Modules (setting **HSM policy 50: Allow Functionality Modules** to **1**) is not reversible. For more information about HSM policies, see HSM Capabilities and Policies.

Mixed FIPS/non-FIPS High-Availability Groups

Thales does not recommend creating HA groups using a combination of FIPS and non-FIPS partitions, as such groups would not be FIPS compliant for auditing purposes. If you do wish to create such groups, however, you require a minimum client version or the operation will be blocked:

- If you are using Luna HSM Client 10.4.0 or newer, you *can* set up an HA group with a mix of FIPS and non-FIPS partitions as members. However, some limitations must be considered. For more information, refer to Key Replication.
- If you are using Luna HSM Client 10.3.0 or older, you *cannot* set up an HA group with a mix of FIPS and non-FIPS partitions as members.

RSA-186 Mechanism Remapping for FIPS Compliance

Under FIPS 186-3/4, the only RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. RSA PKCS and X9.31 key generation is not approved in a FIPS-compliant HSM. While Luna 6.10.9 firmware allows these older mechanisms, later firmware does not (and keys created using these mechanisms cannot be replicated to Luna 7 HSMs or Luna Cloud HSM services).

If you have older applications that use RSA PKCS and X9.31 key generation, you can remap these calls to use the newer, secure mechanisms. Add a line to the **Chrystoki.conf**/**crystoki.ini** configuration file as follows:

```
[Misc]
RSAKeyGenMechRemap=1
```

> **NOTE** This setting is intended for older applications that call outdated mechanisms, to redirect calls to FIPS-approved mechanisms. The ideal solution is to update your applications to call the approved mechanisms.
>
> Mechanism remapping is automatic, and ignores the configuration file entry if:
>
> - you are using Luna HSM Client 10.1.0 or newer, and
> - HSM firmware is older than Luna HSM Firmware 7.7.1 (which introduced FIPS mode on individual partitions; clients up to and including Luna HSM Client 10.3.0 are unaware of the independent partition setting and do not remap mechanisms).
>
> Luna HSM Client 10.4.0 and newer are aware of the change in Luna HSM Firmware 7.7.1 and perform the mechanism remapping as expected when the current partition is in FIPS mode.

RNG Entropy

Luna HSM 7 Firmware includes a FIPS 140-2 Level 3-certified Random Bit Generator with an SP 800-90B certified entropy source. The entropy source is the bit that generates the raw entropy bits, conditions these to increase entropy per-bit and health-tests the samples. These bits are then fed to a Deterministic Random Bit Generator (DRBG) which independently is NIST CAVP approved.

The Random Bit Generator and entropy source are FIPS 140-2 Level 3 certified per certificate #E98:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/98

Changes to FIPS Mode Mechanisms and Operations by Firmware Version

This section provides details about changes to mechanisms and their functionality when in FIPS mode.

> **NOTE** Thales is continuously updating FIPS criteria with each new firmware version; even if a particular firmware is not submitted for FIPS validation, it may include changes to the way mechanisms work in FIPS mode. It is possible to operate any Luna firmware version in FIPS mode, but only versions validated by NIST are considered compliant with the standard (see "Install Only FIPS-Validated Firmware" on page 1).

FIPS Changes in Luna HSM Firmware 7.8.7 and Newer

New restrictions have been added to some mechanisms when the HSM is in FIPS mode (**HSM policy 12:** Allow non-FIPS algorithms set to OFF), to comply with FIPS 186-5 Digital Signature Standard (NIST SP 800-186).

Mechanisms no longer available in FIPS mode

The following mechanisms are now restricted from use in FIPS mode:

- CKM_AES_MAC
- CKM_AES_MAC_GENERAL
- CKM_DES3_MAC
- CKM_DES3_MAC_GENERAL
- CKM_DSA_KEY_PAIR_GEN
- CKM_DSA_PARAMETER_GEN

Mechanisms not permitted to sign objects in FIPS mode

The following mechanisms are not permitted to sign objects in FIPS mode:

- CKM_DSA
- CKM_DSA_SHA224
- CKM_DSA_SHA256
- CKM_RSA_X9_31
- CKM_SHA3_224_DSA
- CKM_SHA3_256_DSA
- CKM_SHA3_384_DSA
- CKM_SHA3_512_DSA
- CKM_SHA224_RSA_X9_31
- CKM_SHA256_RSA_X9_31
- CKM_SHA384_RSA_X9_31
- CKM_SHA512_RSA_X9_31

FIPS Changes in Luna HSM Firmware 7.8.4 and Newer

New restrictions have been added to some mechanisms when the HSM is in FIPS mode (**HSM policy 12:** Allow non-FIPS algorithms set to OFF), to comply with NIST's planned withdrawal of FIPS SP800-67 Rev2 on January 1, 2024.

Mechanisms not permitted to encrypt objects in FIPS mode

The following mechanisms are not permitted to encrypt objects in FIPS mode:

- CKM_DES_CFB8
- CKM_DES_CFB64
- CKM_DES_OFB64
- CKM_DES3_CBC
- CKM_DES3_CBC_PAD
- CKM_DES3_CTR
- CKM_DES3_ECB

The following encryption mechanisms are no longer available in FIPS mode:

- CKM_DES3_CBC_ENCRYPT_DATA
- CKM_DES3_ECB_ENCRYPT_DATA

DES3 encryption is blocked in ECIES mechanisms.

HMAC mechanisms are blocked from using a DES3 key for signing.

- CKM_SHA3_224_HMAC
- CKM_SHA3_224_HMAC_GENERAL
- CKM_SHA3_256_HMAC
- CKM_SHA3_256_HMAC_GENERAL
- CKM_SHA3_384_HMAC
- CKM_SHA3_384_HMAC_GENERAL
- CKM_SHA3_512_HMAC
- CKM_SHA3_512_HMAC_GENERAL

Mechanisms not permitted to sign objects in FIPS mode

The following mechanisms are not permitted to sign objects in FIPS mode:

- CKM_DES3_CMAC
- CKM_DES3_CMAC_GENERAL

CKM_RSA_PKCS not permitted to decrypt/unwrap objects in FIPS mode

CKM_RSA_PKCS is now restricted from performing decrypt/unwrap operations in FIPS mode.

Firmware 7.8.4 and newer - behavior notes

In addition to the above, if you update your HSM's firmware to version 7.8.4 or newer, be aware of the following.

Cloning protocol versions and interactions

Cloning protocol version 1 (CPv1) has been the standard protocol for many years,

- to clone keys and objects between Luna HSMs (between application partitions on the same or different HSMs) directly, including Luna Cloud HSM
- to clone keys and objects among members of HA groups
- to clone keys and objects when backing up to a Luna backup HSM or when restoring from backup.

CPv1 uses older mechanisms, and is being superseded by CPv4.

Noteworthy between the two is that CPv4 permits a selection of cipher suites to secure the cloning process. Most situations would be perfectly fine with whatever ciphers are negotiated from those available, while some industries or government standards might mandate excluding certain ciphers.

As of firmware 7.8.4, CPv1 is *disallowed* when the HSM is in FIPS mode (HSM Policy 12: *Enable non-FIPS algorithms* set to value 0), which means that only CPv4 is available for cloning. See Cloning Protocols and Cipher Suite Selection. This includes cloning in either direction between Luna Cloud HSM and on-premises Luna HSMs. When that HSM-level policy is 0 (known as FIPS mode) all application partitions in the HSM are forced to FIPS mode.

If the HSM is in non-FIPS mode (HSM Policy 12 set to value 1), then FIPS mode can be set ON or OFF for individual application partitions. This has the effect that CPv1 is still allowed for an individual partition within the HSM if Partition Policy 43 is set to value 0, for that partition.

Firmware update effects on crypto mechanism behaviors always prevail

Partition Policy 33: Allow RSA PKCS mechanism can still be set to value 1 to function as before, if you had been using that setting. However, the mechanism settings enforced by your current firmware version will prevent disallowed operations -- as newer and newer firmware versions are released, older/weaker mechanisms can be further restricted or disallowed, for reasons of security and of compliance with standards. Always check the latest documentation in case a new firmware might disrupt your use-case.

HA Login implication

High Availability Indirect Login is a form of High Availability grouping that some customers implement via the Luna Software Development Kit and Thales' extensions to PKCS#11. See High Availability Indirect Login. Older versions, prior to HSM firmware version 7.7.0 use RSA_PKCS to encrypt the RND value during HA Indirect Login Setup. Versions 1.x cannot be used (we block logging in from latest-FW primary to a secondary FW that uses Version 1.x). Version 2 (FW >= 7.7.0) uses AES-256-KWP instead.

FIPS Changes in Luna HSM Firmware 7.8.0 and Newer

The following mechanism is now restricted from use in FIPS mode:

- CKM_X9_42_DH_PARAMETER_GEN

FIPS Changes in Luna HSM Firmware 7.7.2 and Newer

The following mechanisms have new operation restrictions in FIPS mode:

- CKM_RSA_PKCS: cannot encrypt | Cannot legacy decrypt | Cannot legacy unwrap
- CKM_RSA_PKCS_OAEP: Cannot legacy decrypt | Cannot legacy unwrap

FIPS Changes in Luna HSM Firmware 7.7.0 and Newer

New restrictions have been added to some mechanisms when the HSM is in FIPS mode (**HSM policy 12:** Allow non-FIPS algorithms set to OFF), to comply with FIPS SP800-131a Rev2, published in March 2019.

Mechanisms not permitted to wrap objects in FIPS mode

The following mechanisms are not permitted to wrap objects in FIPS mode (unwrap operations are permitted):

- CKM_AES_CBC
- CKM_AES_CBC_PAD
- CKM_AES_CTR
- CKM_AES_ECB
- CKM_DES3_CBC
- CKM_DES3_CBC_PAD
- CKM_DES3_CTR
- CKM_DES3_ECB
- CKM_RSA_PKCS

Mechanisms not permitted to sign data in FIPS mode

The following mechanisms are not permitted to sign data in FIPS mode (verify operations are permitted):

- CKM_AES_MAC
- CKM_AES_MAC_GENERAL
- CKM_DES3_MAC
- CKM_DES3_MAC_GENERAL
- CKM_DSA_SHA1
- CKM_ECDSA_SHA1
- CKM_SHA1_RSA_PKCS
- CKM_SHA1_RSA_PKCS_PSS
- CKM_SHA1_RSA_X9_31

3DES Usage Counter

Using Luna HSM Firmware 7.7.0 and newer, 3DES keys have a usage counter attribute (CKA_BYTES_REMAINING) that limits each key instance to encrypting a maximum of 2^{16} 8-byte blocks of data when the HSM is in FIPS mode (**HSM policy 12:** Allow non-FIPS algorithms set to **0**). When the counter runs out, that key can *no longer* be used for encryption, wrapping, deriving, or signing, but can still be used for decrypting, unwrapping, and verifying pre-existing objects.

The CKA_BYTES_REMAINING attribute is available when **HSM policy 12:** Allow non-FIPS algorithms is set to **0**, but cannot be viewed if the policy is set to **1**.

The attribute is preserved through backup/restore using a Luna Backup HSM 7; restoring the key restores the counter's setting at the time of backup.

The attribute is not preserved through backup/restore using a Luna Backup HSM G5; restoring the key resets the counter to the maximum.

Mechanisms approved for use in FIPS mode

The following mechanisms are now approved for use in FIPS mode:

- CKM_SHA3_224
- CKM_SHA3_224_DSA
- CKM_SHA3_224_ECDSA
- CKM_SHA3_224_RSA_PKCS
- CKM_SHA3_224_RSA_PKCS_PSS
- CKM_SHA3_256
- CKM_SHA3_256_DSA
- CKM_SHA3_256_ECDSA
- CKM_SHA3_256_RSA_PKCS
- CKM_SHA3_256_RSA_PKCS_PSS
- CKM_SHA3_384
- CKM_SHA3_384_DSA
- CKM_SHA3_384_ECDSA
- CKM_SHA3_384_RSA_PKCS
- CKM_SHA3_384_RSA_PKCS_PSS
- CKM_SHA3_512
- CKM_SHA3_512_DSA
- CKM_SHA3_512_ECDSA
- CKM_SHA3_512_RSA_PKCS
- CKM_SHA3_512_RSA_PKCS_PSS
- CKM_SHAKE_128
- CKM_SHAKE_256

FIPS Changes in Luna HSM Firmware 7.1.0 and Newer

The following mechanisms are now available in FIPS mode:

- CKM_EC_MONTGOMERY_KEY_PAIR_GEN

CHAPTER 4: Common Criteria/eIDAS Compliance

Luna HSMs regularly qualify against relevant standards that are important in the information security, data protection, and transaction protection spaces, and for which a business case supports the resource expenditure. Validation is repeated/updated when product changes warrant doing so, according to the respective standards and the requirements of the qualified testing laboratories.. HSM validations are reacquired when major new versions of applicable standards are released, and are also kept up with minor submissions and adjustments when a standard is tweaked or when interpretations shift on the part of testing/validation laboratories.

Under Common Criteria, Thales has looked to qualify our Luna HSM products against eIDAS standards relevant to general purpose hardware security modules.

Luna HSMs are eIDAS certified as Qualified Signature Creation Devices and Qualified Seal Creation Devices (QSCD), and are used by Qualified Trust Service Providers (QTSP) in the role of their root of trust.

See https://cpl.thalesgroup.com/compliance/eidas and https://cpl.thalesgroup.com/compliance/americas/fips-140-2

CC takes the view that a solution is validated for a purpose, which generally means that a number of moving parts are considered in concert. Thus an HSM is evaluated as an element of an overall solution that also includes software products, procedures, and systems all interacting. The following documents provide expanded detail on the relevant topics.

DOW0006186 (KB0023049) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 1: PREPARATIVE PROCEDURES"

DOW0006187 (KB0023050) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 2: OPERATIONAL GUIDANCE"

DOW0006188 (KB0023051) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 3: EIDAS GUIDANCE"

DOW0006189 (KB0023052) is "Thales Luna K7(+) Cryptographic Module COMMON CRITERIA USER GUIDANCE - PART 4 TOE INTEGRATION FOR USE IN COMPOSITE EVALUATION"

The K7 module referred to, in those document titles,

- is the heart of the Luna Network HSM 7 (Luna Network HSM appliance) and
- is also available in a separate PCIe card format for insertion in a host system (Luna PCIe HSM).

Roles	Principal Duties
HSM Security Officer (HSM SO) [Admin Partition Role]	The HSM SO is responsible for managing the HSM. As such, they are authorized to install and configure the HSM, set and maintain global HSM security policies. They are also able to request the load of new HSM firmware update files (FUF), new Configuration Update Files (CUF) and new Functional Modules (FM). The HSM SO is able to create and delete partitions, but is not authorized to generate, load or use keys stored on the user partitions that have been created. The HSM SO is able to create, manage and use keys created in the Admin Partition alongside is responsible for initializing the 'Administrator role'. The HSM SO can reset the Administrator password (configuration dependent). The HSM can have only one HSM SO.
[Admin Partition Role]	The Administrator is authorized to create, use, transfer and destroy key objects contained in the Admin partition. This role has privileges that are a subset of the HSM SO role.
Partition Security Officer (Partition SO) [User Partition Role]	The Partition SO creates the partition level Partition CO role, activates partition, sets and changes partition-level policies, with an option to reset the Partition CO password (configuration dependent).
Partition Crypto Officer (Partition CO) [User Partition Role]	The Partition CO role is authorized to create, use, destroy and transfer key objects for a given partition. The Partition CO can optionally create the Partition LCO and Partition CU, and perform initial assignment of key authorization data.
Partition Limited Crypto Officer (Partition LCO) [User Partition Role]	The Partition LCO is an optional partition role authorized to create and use key objects, and perform initial assignment of key authorization data. The role is only permitted to delete key objects where per-key authorization is used and the correct authorization data for a given key object can be presented to the cryptographic module.
Partition Crypto User (Partition CU) [User Partition Role]	The Partition CU is the partition role authorized to use the key objects within the partition (e.g. sign, encrypt/decrypt).
Audit User [Admin Partition Role]	The Audit User initializes the secret key used to generate Message Authentication Code (MAC) for secure audit messages alongside configuring logging levels for the HSM.
Key Owner [Admin or User Partition Role]	Implicit role used to authenticate the owner of a key through verification of the related key authorization data.

Roles	Principal Duties
STC User [Admin or User Partition Role]	The STC user is optional role used with a remote Thales Luna client to initiate a secure tunnel with a target partition. Once successfully authenticated based on pre-registered authentication credentials, the STC user is able to submit commands to the target partition over a trusted channel.

Network HSM

This section is an overview of how the Luna Network HSM 7 can fit in, and satisfy the requirements for deployment in an environment complying with the demands of Common Criteria.

Consider a fresh/raw from the factory appliance, or an appliance that has been re-imaged (see Re-Imaging the Appliance to Baseline Software/Firmware Versions). You want to use it in a relevant Common Criteria environment, such as eIDAS compliant.

Planning deployment

In order to provide data security in depth, you must house your HSM appliance in a suitably secure environment, and surround it with proper data-handling procedures to ensure the security of your data, or your clients' data, both before it goes into the HSM and after it comes out.

First, where will your network HSM appliance reside?

The document 007-013968-001_K7_CC_User_Guidance_Part1_AGD_PRE_RevE.pdf or newer (available on the Thales Support Portal) goes into the specifics of site selection and site security in more detail, but at the very least consider a dedicated area (secure server farm or data center) with monitored, audited, and controlled physical access by vetted personnel. Also, consider if you have redundancy requirements, necessitating backup/standby/fail-over HSMs, and whether a suitable disaster-recovery plan would require redundant installation at widely separated sites.

The HSM is a secure, tamper-resistant, tamper-evident, hardware cryptographic module, connected to the PCIe bus, and embedded within its host, a network-accessible, hardened, tamper-resistant, tamper-evident, rack-mountable appliance.

For configuration and management of the cryptographic module, and of the appliance that provides network availability, access is achieved via one of the appliance interfaces:

- local serial connection for initial network configuration and for recovery (see Opening a Serial Connection),
- SSH for configuration and management activity of the appliance, and configuration and management of the cryptographic module inside (see Configuring the Luna Network HSM 7 for Your Network),
- NTLS/STC for crypto operations on the HSM, once it has been configured with the proper partitioning and roles(see Client-Partition Connections),
- REST API for appliance management and management and use of the embedded crypto module, once the appliance has been initially configured to the point of launching the webservice that handles REST interactions (see webserver and REST API References).

1. Connect to the appliance, log into the appliance as "admin" and change the password (see Logging In to LunaSH).

2. Configuring IP and Network Parameters.
3. Enable the built-in appliance Monitor and appliance Operator accounts if your situation will make use of administrative users who require less than the full "admin" access/authority, or alternatively create any named users that have desired levels of access. This can be revisited later.
   - You can make accounts that copy the access of the default accounts, but give them names that are more appropriate in your situation/industry/market.
   - As well, you can go further and create named appliance administrative accounts that have access to only a specific list of commands that you choose for them.

   To access the cryptographic module, within the Luna Network HSM 7, for administrative operations, you log into the outer appliance as users, to which are applied roles that specify the set of appliance-administration commands that role can use, *and* the set of crypto-module commands that role can access (see Appliance Users and Roles)and see also CustomRoleTemplate for a list of all appliance-admin and HSM/crypto-module-admin commands (except Audit user commands) that you can copy or edit for fine control of access by a named user/role.

   Equally as important, you should determine who is permitted access to the appliance via any of the appliance roles. That is, you must have processes and procedures, developed and approved in advance,
   - to track and control who can have possession of appliance-level and crypto-module-level credentials,
   - along with predetermined responses to possible compromise of personnel or credentials, and
   - standing practices with respect to refresh or rollover of credentials (password-change interval).
4. Initialize the HSM and log in (this presupposes successful appliance login, as the HSM or cryptographic module resides within the appliance).
   a. If the HSM is Password authenticated, then all roles and activities within the HSM are protected by text strings, which must be secured by procedures that mandate who is allowed to know them, and that frequently rotate/change passwords. Password security is basically "the honor system"; you must trust your personnel to keep the authentication text strings secure.
   b. If the HSM is multi-factor quorum authenticated then the iKey (PED Key) tokens must be physically and procedurally managed to ensure that only authorized personnel have access. For the most sensitive roles, you can split an authentication secret such that a quorum of trusted personnel must present their portions in order to gain access. Separation of roles is ensured by separating who is able to physically access the relevant physical tokens while also knowing the passcode (PED PIN) associated with an iKey token.
5. Initialize partitions that will be the logically distinct areas within the HSM where your important keys and data objects are handled. The HSM Security Officer (SO) has overall management authority over the HSM (including creation and deletion of partitions), but you can configure such that the HSM SO has no view or access inside partitions. Partition SOs have administrative authority inside their partition and create the roles (Crypto Officer, Limited Crypto Officer, Crypto User that provide application access to perform cryptographic operations.

Options to perform partition management include:

> doing so via ssh session to the appliance, using the lunash commands (Luna Shell is a restricted shell within the hardened Network HSM appliance, that accesses and implements all the features and capabilities, see About the LunaSH Command Reference) - this might be done in situations where the HSM SO is also expected to own other roles

> using a client NTLS

- Network Trust Link Service (see Client-Partition Connections), the default SSL-based protocol secured with self-signed or CA-signed certificates, between the client and the network HSM appliance that then passes commands and results to and from the embedded cryptographic module

or

using an STC connection (see Creating an STC Connection)

- Secure Trusted Channel, provides a tunnel from the remote application directly into the HSM, affording confidentiality, integrity, and anti-replay protection for data submitted from outside the cryptographic module

...in either case, making use of lunacm and other client-side tools - this is the approach when partition and application-related roles are held separately from HSM administration

> using the REST API (see REST API References) to provision and manage the HSM - once the appliance admin has launched the webserver, the REST API provides equivalents to the lunash commands.

6. Exchange certificates and register client hosts with the partitions where your application(s) will create and use crypto keys and objects.

The HSM maintains all contents encrypted, as a matter of course, and decrypts them only in temporary memory for immediate use. In the case where large numbers of keys/objects must be securely maintained, the Scalable Key Storage option (SKS Scalable Key Storage - requires firmware 7.7.0 onward) allows those keys and objects to be exported to your file system or database in the form of *encrypted* blobs. The SKS Master Key (SMK) that encrypts/decrypts those blobs, is itself always protected within an HSM/cryptographic module. Your keys and objects, stored in blob form, are brought back to the HSM when your application needs to use them. This extends the HSM's cryptographic perimeter and complies with any requirement that sensitive data be kept logically separate from other data in the IT environment.

The secure handling and management of (for example) Data To Be Signed (DTBS), coming to the HSM, and the result (such as a signature) coming from the HSM is the responsibility of you and the application(s) you use.

Audit

The HSM logs events within the HSM. You must initialize the Audit role within the HSM, to configure the criteria (such as event severity, whether certain key usage is logged for first use only, or for every use, etc.), to ensure a balance between logging necessary for the regime under which you operate, and the effect on cryptographic performance as logging demands increase. The more events are logged, the faster the HSM memory fills, and the more urgent the need for you to configure *rotation of log entries off the HSM* and into log files in the host file-system. The secure audit function ensures that audit log integrity can be validated. It is then your responsibility to secure the further handling of such logs within your organization.

The appliance also logs system events, which is a separate function from HSM logging.

The HSM (cryptographic module) and the appliance that hosts it provide their logs (as configured), but what you do with them is determined by the security regime under which you operate.

Compliance

Common Criteria validation ensures that a given version of HSM is suitable and can be used in conformity with the stipulated behaviors within the larger framework of operational security for applications and services. Thales Group regularly submits HSM products for Common Criteria evaluation, and provides links and updates as appropriate.